United States Use of Cyberweapons: Theory and Practice

by

Vijai T. Singh

A Dissertation submitted to the

Graduate School-Newark

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Global Affairs

written under the direction of

Dr. Yale Ferguson

and approved by

_____

_____

_____

_____

Newark, New Jersey

January, 2018

Copyright page:

Abstract of the Dissertation

United States Use of Cyberweapons: Theory and Practice

By Vijai T. Singh

Dissertation Director:

Dr. Yale Ferguson

In 2010, the Pentagon defined cyberspace as an area of warfare joining land, sea, air, and space as fair game for military action. At the time, the U.S. was focused on defending itself against cyberattacks from China and Russia; the countries they deem to be the biggest cyber threats. But, it was later revealed that China and Russia were also involved in offensive cyberwarfare, or the use of cyberweapons, to attack other countries. While cyberwarfare is not a new concern, the offensive strategy of cyberwarfare, specifically the deployment of cyberweapons, is a relatively new and important phenomenon.

In this dissertation, I have used a three-prong approach to address the central question: under which conditions is the United States likely to deploy a cyberweapon in a first strike? My hypotheses are that in order for the U.S. to deploy a cyberweapon in a first strike: the target country has to be a perceived adversary that poses a threat; the target has to be in an area that is hard to access by other methods; the cyberweapon may be deployed in order to minimize collateral damage; the cyberweapon may be deployed to prevent or end a war.

First, I empirically tested what I classified as 13 cases where the U.S. used or debated about using an offensive cyberweapon from 2001 – 2016. The cases were Stuxnet, Iraq (2007), Shotgiant (2007), Quantum (2008), Turbine (2010), Nitro Zeus, Libya (2011),

Pakistan (2011), Syria, North Korea (2014), ISIS (2016), Russia (2016), and Iraq (2003). Next, I employed the poliheuristic theory of foreign policy-decision making to reconstruct the decision-making process for each case study. Then, I conducted 22 confidential, semi-structured interviews to gather information about these case studies as well as further insights about the decision-making process behind deploying a cyberweapon. My findings are that some key conditions affecting deployment were indeed threat, access and collateral damage. My research also appeared to reveal that the authorization process for deployment is similar to that for a nuclear strike process, although the decision-making process cannot be generalized.

Acknowledgments

When I defended my dissertation proposal in May 2015, I failed to anticipate the effects of the looming U.S. presidential election. During my proposal defense in 2015, my committee suggested that I allow this topic some time to develop. Two years later, the field of cyberwarfare has developed in ways I could not even begin to imagine. First, U.S. intelligence agencies concluded that Russia played a cyber role in the 2016 U.S. presidential election. Second, Wikileaks released the largest trove of stolen C.I.A. documents in the agency's history, which spoke about their covert cyber tools. Third, Donald Trump was elected the 45th president of the United States. Trump's win allowed important persons who would not have had time for me suddenly to have time for me. Additionally, Trump's win propelled my subject to the forefront and forced U.S. officials to have conversations about cyberweapons that they were previously reluctant to have.

I spent a year and a half researching and writing this dissertation. For the first time in my academic career, I did not work for pay. This was initially liberating but, of course, became increasingly stressful as I approached completion. So first, I must thank God, without whom nothing, especially this dissertation, would have been possible. Thank you for always having my back and for granting me the strength, faith, capability, and knowledge, to pursue a Ph.D. degree.

Next, I cannot say thank you enough to my family, especially my mother, who has helped me in every way possible. This dissertation is dedicated to her because it was always her wish that I pursue a doctorate. Mom, this degree is as much yours as it is mine. Thank

you for always encouraging me to dream big and for clearing the way to help me accomplish those dreams.

I would also like to thank my grandmother who once proudly (and loudly, I might add) declared that her birthday wish was for me to get my Ph.D. No pressure. I am able to stand because these two women are my pillars.

Next, I would like to thank Rutgers and the Division of Global Affairs because they gave me the greatest gift– my dissertation advisor, Dr. Yale Ferguson. I am forever indebted to Dr. Ferguson because he was incredibly patient, diligent, supportive, encouraging, respectful and always pushed my research forward. Dr. Ferguson, thank you from the bottom of my heart for not only guiding me through this process but for also sharing your wisdom about the world and life. You have made this whole process not only possible but worthwhile. I am very thankful for you and I will forever cherish our bond.

I would also like to thank my esteemed committee. Dr. Gregg Van Ryzin was promoted to Interim Dean shortly after I started this project and yet, he sat with me for weeks to discuss the quantitative analysis and interview strategies. His advice and insight were also crucial to this dissertation. I would also like to thank Dr. Leslie Kennedy for his patience as well as Dr. Mark Hagerott, my outside advisor who despite being an academic Chancellor, still found the time to respond to my questions. All of you have contributed mightily and always constructively to achieving our mutual goal-- my doctorate!

I also have to thank my brothers, Sunil and Shammi, my sister-in-law Abon, my aunts especially Auntie Chitra and Auntie Indrani, my uncles especially Mamoo and Chacha Anand, and my cousins including Peggy, Kayla and Gavin, who were always cheering for and praying with me along the way. Thanks also to my dad, who always

encouraged me to pursue school. All of you have exemplified the meaning of family. I also have to thank my grandfather who once accompanied me to Rutgers. He passed away shortly after I defended my dissertation.

I would also like to thank all of my colleagues, especially Laura, Eric, and Phil, who graciously shared their time, thoughts and efforts in helping to arrange interviews for me as well as all of those who took the time out of their busy lives to speak with me for this project.

Throughout this journey, I have also been fortunate to have friends who are my family, especially Rakhee and Barin, who always cleared the many doubts. Thank you to all those who always understood when I could not make an event because I was "working on a chapter." And thanks to all the brilliant professors and peers I met at the Division of Global Affairs who made this process a little less lonely.

Last but certainly not least– Jason, I could not have survived this process without you. Thank you for being with me throughout this entire doctoral journey. I hope we are together forever.

Table of Contents

List of Tables

List of Illustrations

Introduction

"The Birth of D Weapons"[1]

"If America, or U.S. Cyber Command, wanted to wage cyber war, it would do so from inside a glass house."[2]

-Fred Kaplan

In an interview about cybersecurity in 2015, President Barack Obama referenced one of his national security advisers, who told him "This is more like basketball than football, in the sense that there's no clear line between offense and defense. Things are going back and forth all the time."[3] This seems an accurate description of both the state of affairs and my own thinking over the last two years I have spent researching offensive U.S. cyberwarfare.

Ever since 9/11, terrorism has been deemed the number one threat to the U.S.; however, starting in 2013, it was determined that cyber was "the number one strategic threat to the United States."[4] Cyber threats include data theft and the disruption or destruction of critical infrastructure networks that could lead to significant loss of life as

---

[1] Jacob Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle," *Spiegel Online International,* January 17, 2015, accessed May 26, 2016, http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html.

[2] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016a), 216.

[3] Kara Swisher, "White House. Red Chair. Obama Meets Swisher," *Recode,* February 15, 2015, accessed August 12, 2017, https://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher.

[4] Department of Defense, *The DoD Cyber Strategy*, (April 2015), 9, accessed March 27, 2016, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

well as economic paralysis.[5] In an effort to regain the trust of the American public after the fallout caused by the trove of documents leaked by N.S.A. employee Edward Snowden in 2013 that revealed the N.S.A.'s massive accumulation and retention of the public's telephone records, on March 28, 2014, the N.S.A. engaged in its first live-broadcast where U.S. Defense Secretary Chuck Hagel declared, "cyberspace will be a part of all future conflicts. And if we don't adapt to that reality, our national security will be at great risk."[6] This statement signaled the administration's intention to increase U.S. Cyber Command[7] to 6,000 people by 2016, making it one of the largest units of its kind in the world.[8] The increase in personnel underscores the growing importance of cyberspace,[9] which the Pentagon defined in 2010 as an area of warfare joining "land, sea, air, and space," as fair game for military action.[10]

---

[5] *The DoD Cyber Strategy*, 9.

[6] Chuck Hagel, "As Delivered Remarks by Secretary of Defense Chuck Hagel at the Retirement Ceremony for General Keith Alexander," (speech, Fort Meade, M.D., March 28, 2014), accessed May 1, 2016, *Office of the Director of National Intelligence IC on the Record*, https://icontherecord.tumblr.com/post/81297943300/as-delivered-remarks-by-secretary-of-defense-chuck.

[7] U.S. Cyber Command was created in 2009 to focus on warfare in cyberspace. "U.S. Cyber Command," "U.S. Cyber Command," accessed March 17, 2014, http://www.stratcom.mil/factsheets/2/Cyber_Command/.

[8] Ellen Nakashima, "U.S. accelerating cyberweapon research," *The Washington Post,* March 18, 2012, accessed November 29, 2016, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html?utm_term=.a7280c3b0778.

[9] According to the Department of Defense, cyberspace is "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." *DOD Dictionary of Military Terms*, s.v. "cyberspace," accessed April 2, 2014, http://www.dtic.mil/doctrine/dod_dictionary/.

[10] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October, 2010): 101, http://www.jstor.org/stable/20788647.

At first, the U.S. was focused on defending itself against cyberattacks from other countries and trying to prevent a 'cyber-Pearl Harbor.'[11] Speaking to the Business Executives for National Security in New York on October 11, 2012, Secretary of Defense Leon Panetta proclaimed that we are in "a pre-9/11 moment" warning that we could be on the precipice of "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."[12] But, it was later revealed that some of those countries were also involved in offensive cyberwarfare, or the use of cyberweapons, to attack other countries. In the 20th century, there were "ABC weapons – atomic, biological and chemical."[13] Now there are "D" (digital) weapons.[14]

According to a leaked directive, the Obama administration was compiling a list of targets for these weapons.

> The United States Government shall identify potential targets of national importance where OCEO (offensive cyber effects operations) can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive.[15]

---

[11] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times,* October 11, 2012, accessed April 16, 2014, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

[12] Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," (speech, New York City, N.Y., October 11, 2012), accessed April 10, 2016, *U.S. Department of Defense*, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[13] Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle."

[14] Ibid.

[15] "Presidential Policy Directive," 9, in Glenn Greenwald and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian,* June 7, 2013b,

The thinking was that "these new weapons dramatically expanded the president's ability to wage nonstop, low-level conflict, something just short of war, every day of the year."[16] However, some other experts claim this is not "low-level conflict" but cyberwarfare, while critics counter that this is not cyberwarfare because there have been no fatalities. In this dissertation, I argue that because the severity of destruction caused by these attacks could lead to fatalities, this is cyberwarfare. These cyberattacks are being carried out by weapons that could potentially destroy infrastructure including electrical power girds and transportation facilities. We have entered a new age of warfare where wars are being waged online through the use of networks and the U.S. is one of the biggest players in the game.

BACKGROUND OF THE PROBLEM

According to The Commission on America's National Interests, the U.S. has five levels of classifications for their national interests: Vital, Extremely Important, Important and Less Important, respectively.[17] Information falls into the Extremely Important category. Specifically, the mandate says that the U.S. has to "maintain a lead in key military-related and other strategic technologies, particularly information systems."[18]

---

accessed November 1, 2014, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[16] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012a), 244.

[17] Graham Allison, "U.S. National Interests," *Belfer Center for Science and International Affairs*, February 18, 2010, accessed October 15, 2014, https://dnnpro.outer.jhuapl.edu/media/RethinkingSeminars/021810/Allison_ppt.pdf.

[18] Ibid.

According to Gen. Keith B. Alexander, the head of N.S.A. in 2013, cyberweapons have already been used "a handful of times" in the past 8 years.[19] In 2016, Admiral Mike Rogers, the current head of the N.S.A. and U.S. Cyber Command, said "You can tell we are at the tipping point now," in regards to cyberweapons.[20] He added, "The capacity and the capability are starting to come online [and] really starting to pay off in some really tangible capabilities that you will start to see us apply in a broader and broader way."[21] However, neither of these men offered any additional insight as to the circumstances under which these weapons have been used, the types of weapons used and the rationale for using them. The U.S. has pondered whether these weapons should be used for hard-to-reach areas, as a part of 'hybrid' conflicts,[22] or just like other weapons[23] and different agencies with varying opinions complicate matters even more.[24] Right now, these weapons are controlled by the N.S.A., which means they are covert.[25] But in 2016, the Air Force sought

---

[19] David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times,* February 24, 2014b, accessed February 24, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?ref=davidesanger.

[20] Damian Paletta, "NSA Chief Says U.S. at 'Tipping Point' on Cyberweapons," *The Wall Street Journal,* January 21, 2016, accessed June 17, 2016, http://www.wsj.com/articles/nsa-chief-says-u-s-at-tipping-point-on-cyberweapons-1453404976.

[21] Ibid.

[22] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times,* February 16, 2016e, accessed May 10, 2016, http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

[23] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[24] William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: The National Academy of Sciences*,* 2009), 300, accessed November 18, 2014, http://www3.nd.edu/~cpence/eewt/Owens2009.pdf.

$10 million, the Navy asked for $4 million and the Army requested $13 million to develop cyber warriors.[26] Like drones, cyberweapons are a classified subject. But just as the Obama administration began discussing drones, they also started discussing cyberweapons. In fact, General James Cartwright, one of the brains behind the Stuxnet operation (the cyberweapon that was supposedly a game-changer), has urged a discussion on these weapons stating "You can't have something that's a secret be a deterrent. Because if you don't know it's there, it doesn't scare you." [27] In 2013, Cartwright was stripped of his security clearance because the Justice Department suspected he was the one who told *The New York Times* about Stuxnet.[28] President Obama pardoned him in January 2017.[29]

The development of cyberweapons is one of the few areas where U.S. defense spending is increasing. The 2017 budget allocates $6.7 billion for cyberspace[30] some of which supports 133 cyber mission force teams that both defend the U.S. and provide

---

[25] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[26] Franz-Stefan Gady, "The US Military Wants to Train More Cyber Warriors," *The Diplomat,* February 6, 2015, accessed June 1, 2016, http://thediplomat.com/2015/02/the-us-military-wants-to-train-more-cyber-warriors/.

[27] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 156.

[28] Gordon Lubold, "Obama's Favorite General Stripped of His Security Clearance," *Foreign Policy,* September 24, 2013, accessed July 1, 2016, http://foreignpolicy.com/2013/09/24/obamas-favorite-general-stripped-of-his-security-clearance/.

[29] Charlie Savage, "Obama Pardons James Cartwright, General Who Lied to F.B.I. in Leak Case," *The New York Times,* January 17, 2017, accessed August 12, 2017, https://www.nytimes.com/2017/01/17/us/politics/obama-pardons-james-cartwright-general-who-lied-to-fbi-in-leak-case.html.

[30] Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2017 Budget Request*, (February 2016), 5-5, accessed March 1, 2016, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_Budget_Request_Overview_Book.pdf.

operational support.[31] David Sanger of *The New York Times* said the notion behind these teams is to integrate them into the U.S. military.[32]

STATEMENT OF THE PROBLEM

In his 2001 article "Virtual Defense," James Adams said, "Although the United States has developed some effective cyber-weapons that can destroy an enemy's computer network or interrupt a nation's fuel and water supplies, there is disagreement about when and how they can be used."[33] This is still true 16 years later. While cyberwarfare is not a new concern, the offensive strategy of cyberwarfare, specifically the deployment of cyberweapons, is relatively new for the United States. "It is a transformation analogous to what happened when the airplane was first used in combat in World War I, a century ago."[34] As previously mentioned, these weapons have already been used a 'handful' of times but the conditions under which the U.S. would engage in offensive cyberwarfare against another country are unclear.

PURPOSE OF THE STUDY

"'At the end of the day, it's the President who gets to decide if this is war or something else,' said James Lewis, a senior fellow at the Center for Strategic and

---

[31] *Defense Budget Overview: United States Department of Defense Fiscal Year 2017 Budget Request*, 5-5.

[32] Sanger, "*Zero Days* Screening."

[33] James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (May/June, 2001): 111, http://www.libraries.rutgers.edu/rul/index.shtml.

[34] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks".

International Studies. 'The standard is ambiguous. Deciding when something is an act of war is not automatic. It's always a judgment.'"[35] This dissertation will try to understand that judgment. In this project I will systematically explore the conditions under which the United States is likely to engage in cyberwarfare as a first strike by applying cluster analysis and poliheuristic theory to 13 cyberweapons, and interviewing 22 individuals.

OUTLINE OF THE DISSERTATION

Chapter 1 provides a brief background on the progression of offensive cyberwarfare in the U.S. Chapter 2 provides an overview of the major literature about offensive cyberwarfare and U.S. policies and practice. Chapter 3 discusses the theory and methodology used in this dissertation to understand the conditions under which the U.S. is likely to deploy a cyberweapon as a first strike. Chapter 4 discusses alleged U.S. cyberweapons used against other countries which are the case studies in this dissertation. In order to tackle this research question, I used a three-prong approach. In Chapter 5, I empirically tested what I classified as 13 cases where the U.S. used or debated about using an offensive cyberweapon from 2001 – 2016. The cases were Stuxnet, Iraq (2007), Shotgiant (2007), Quantum (2008), Turbine (2010), Nitro Zeus, Libya (2011), Pakistan (2011), Syria, North Korea (2014), ISIS (2016), Russia (2016), and Iraq (2003). In Chapter 6, I employed the poliheuristic theory of foreign policy decision-making to reconstruct the decision-making process for each case study so that I could determine the conditions under which a cyberweapon was or was not previously deployed. In Chapter 7, I conducted 22 confidential, semi-structured interviews to gather information about these case studies as

[35] Singer and Friedman, 126.

well as further thoughts about the decision-making process behind deploying a cyberweapon. Chapter 8 is the Discussion and Conclusion where I argue that this three-pronged approach helped construct a more complete picture of what is a very classified subject, although of course there were some limitations.

SIGNIFICANCE OF THE STUDY

This research is applicable to the developing realm of computer warfare, specifically cyberweapons that is rapidly evolving. There is already a cyber black market where states can purchase these weapons.[36] By October 2018, U.S. Cyber Command, which is currently made up of 6,200 people, will be at "full operational capability."[37] Thus, it is important to understand the U.S.' offense.

Some scholars have shied away from studying cyberweapons because this subject is highly classified.[38] However, several experts and journalists have extracted this subject out of the shadows and incorporated it into the national security lexicon. There have also been other works that called for "a spectrum that categorizes scenarios based on imperative to act from none to conditional to high."[39] This dissertation may be able to create that

---

[36] Andy Greenberg, "Shopping for Zero-Days: A Price List for Hacker's Secret Software Exploits," *Forbes,* March 23, 2013, accessed October 30, 2014, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

[37] *Statement of Admiral Michael S. Rogers: Hearing on Cybersecurity Threats and Defense Strategy Before the Senate Committee on Armed Services*, 115th Cong., 1, (2017), (statement of Admiral Michael S. Rogers, Commander United States Cyber Command), https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

[38] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 403, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

spectrum in addition to adding to the poliheuristic theory research program by applying it to this new form of warfare.

It is very important to understand the conditions under which the U.S. deploys these weapons, even if it is in a "what if" manner. By addressing some facets of desired or actual usage, the U.S. may be able to construct its own guidelines for these weapons instead of allowing another country to influence the terms of engagement. Fred Kaplan echoed a similar thought claiming it is "vital for *political* leaders to take firm control: to ensure that policy shaped the use of technology, not the other way around."[40] By the end of this study, I could decide that there are too many conditions and differing situations to make one conclusion, but I think we will be able to better understand that the U.S. is covertly deploying cyberweapons in order to address a significant threat that cannot be effectively addressed by traditional methods of warfare.

---

[39] Robert Belk and Matthew Noyes, *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*, (Cambridge, MA: Belfer Center for Science and International Affairs, 2012), 137, accessed October 1, 2014, http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf.

[40] Kaplan, *Dark Territory: The Secret History of Cyber War*, 180.

Chapter 1

CLOUDY WITH A CHANCE OF WARFARE

"It's the great irony of our Information Age -- the very technologies that empower us to create and build also empower those who would disrupt and destroy."[1]

-President Barack Obama

In 2010, the cover of *The Economist* portrayed a pixelated cloud of fire engulfing an obscure skyline with the title "Cyberwar: the threat from the Internet."[2] This cloud is reminiscent of the mushroom cloud hovering over Hiroshima after the U.S. dropped a nuclear bomb on Japan in 1945. What *The Economist* did not know at the time was that the U.S. had just unleashed another new weapon into the world; as they did in 1945. This new weapon was called Stuxnet, named after a word found in the code,[3] but it did not look like *The Economist's* pixelated cloud. Stuxnet was a cyberweapon, which is "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[4] Specifically, Stuxnet was a computer worm allegedly developed by the United States and Israel that destroyed

[1] Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," (speech, Washington, D.C., May 29, 2009), accessed February 4, 2016, *The White House*, https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[2] "Cyberwar: The Threat from the Internet," *The Economist,* July 1, 2010, accessed May 4, 2016, http://www.economist.com/node/16481504.

[3] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012a), 205.

[4] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The Rusi Journal* 157, no. 1 (February 29, 2012c): 7, http://www.libraries.rutgers.edu/rul/index.shtml.

1,000 Iranian nuclear centrifuges.[5] All of the apocalyptic warnings about massive warfare waged in the "dark territory"[6] of cyberspace were no longer merely science fiction.

Such perilous warnings are not new though. Eugene Kaspersky, CEO of Kaspersky Labs, a Russian computer security firm, cryptically said it is "the beginning of the end of the [interconnected] world as we know it."[7] However, some scholars argue that the cyber threat is overblown partly because of the defense industries. "A cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War. This complex may serve not only to supply cybersecurity solutions to the federal government, but to drum up demand for those solutions as well."[8] In 2015, the cybersecurity market was $75 billion; by 2020, it is projected to be $170 billion.[9] This is interesting since, at least until recently,

---

[5] David Albright, Paul Brannan and Christina Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, (Institute for Science and Technology, February 15, 2011), 1, accessed May 27, 2016b, http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8.

[6] "'Dark territory' was the industry's term for a stretch of rail track that was uncontrolled by signals. To [Robert] Gates, it was a perfect parallel to cyberspace, except that this new territory was much vaster and the danger was greater, because the engineers were unknown, the trains were invisible, and a crash could cause far more damage." Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016a), 272.

[7] David Shamah, "Latest Viruses could mean 'end of world as we know it,' says man who discovered Flame," *The Times of Israel,* June 6, 2012, accessed March 20, 2016, http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/.

[8] Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard Law School National Security Journal* 3, no. 1 (2011): 40, accessed May 2, 2016, http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Brito-and-Watkins.pdf.

[9] Steven Morgan, "Cybersecurity Market Reaches $75 Billion in 2015; Expected to Reach $170 Billion by 2020," *Forbes,* December 20, 2015, accessed May 12, 2016, http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#4f9c9e421916.

the defense budget has been shrinking. "In a barren global defence market the cyber security domain has provided a rare oasis."[10]

For these reasons, "the fog of cyberwar"[11] is thick and cloudy (pun intended.) Cyberwarfare is often conflated with the concepts of cyber conflict, cybercrime and cyber terrorism.[12] In fact, a search of cyberwarfare and cyber warfare will produce drastically different results. So what exactly is cyberwarfare? How is it different from other types of warfare? How does cyberwarfare work? Why does this matter? Instead of rehashing the evolution of U.S. rational about cyberwarfare, which some books have already done quite well,[13] these are the questions that will be explored in this chapter.

---

[10] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 163.

[11] Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype," *Foreign Affairs,* November 21 2012, accessed April 4, 2016, https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar.

[12] Cyber conflict is "the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions among states." Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015), 3. Cybercrime is "the use of digital tools by criminals to steal or otherwise carry out illegal activities." Singer and Friedman, 85. "The FBI defines cyber terrorism as a 'premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.'" Singer and Friedman, 96.

[13] See Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Harper Collins Publishers, 2010); Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016a); P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014); Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015).

WHAT'S IN A NAME?

Just as "Dr. Strangelove" came to represent nuclear warfare, twenty years later "War Games" was the impetus for cyber discussions in the United States.[14] Fred Kaplan claims that this movie helped frame President Ronald Reagan's thinking about cyberwarfare even though "War Games" was the Hollywood version of what could happen.[15] Today, however, policymakers still are not entirely sure what exactly cyberwarfare looks like (hence *The Economist's* digital cloud of doom), so how can they conclude that something is a problem if they do not know how to describe it?

Some scholars define cyberwarfare as "an escalation of cyber conflict to include physical destruction and death."[16] In their oft-cited book, *Cyber War: The Next Threat to National Security and What To Do About It*, Richard Clarke and Robert Knake define cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.''[17] Jon Lindsay says cyberwarfare "employs computer network attacks as a use of force to disrupt an opponent's physical infrastructure for political gain."[18] Jeffrey Carr says "Cyber Warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their

---

[14] Kaplan, *Dark Territory: The Secret History of Cyber War*, 1- 21.

[15] Ibid.

[16] Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System,* 3.

[17] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins Publishers, 2010), 7.

[18] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (August 2013): 372, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

blood."[19] However, as we will see later on, a lack of blood is one reason why some are skeptical about the threat of cyberwar.

In "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," Adam Liff defines cyberwarfare as

> a state of conflict between two or more political actors characterized by the deliberate hostile and cost-inducing use of computer network attacks against an adversary's critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes.[20]

This definition is interesting because it specifies that civilian infrastructure is fair game. However, since cyberwarfare is neither conventional nor nuclear war, it was debatable whether it must (or even should) adhere to the Law of Armed Conflict. Hence, the "Tallinn Manual" was born. Written by an impartial "International Group of Experts" under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence, the "Tallinn Manual" attempts to apply international law to cyberwarfare although they do not actually offer a technical definition of "cyberwarfare." The Tallinn Manual clarifies that cyberweapons can be used under the confines of international law, the Law of Armed Conflict and Just War Theory (jus ad bellum [right to conduct war] and jus in bello [how to conduct war]).[21] The Tallinn Manual says cyberweapons have to adhere to

---

[19] Jeffrey Carr, *Inside Cyber Warfare* (California: O'Reilly Media, 2010), 2.

[20] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 407-408, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[21] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2009), 159, accessed February 27, 2016, https://ccdcoe.org/tallinn-manual.html.

proportionality and collateral damage.[22] The manual aims to provide guidance about the parameters of cyberwarfare but since it is not law, some U.S. policymakers have called for "a binding set of international rules for cyberwarfare: an *E-Neva Convention*."[23] It is interesting to note that the U.S. is reluctant to explain the parameters of using these weapons and yet, some U.S. policymakers are calling for an E-Neva Convention. The "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" was released in February 2017. The new version re-ordered some of the rules. This dissertation is based on the first Tallinn Manual.

The U.S. Air Force defines "cyberwar as the ability 'to destroy, deny, degrade, disrupt, [and] deceive,' while at the same time 'defending' against the enemy's use of cyberspace for the very same purpose."[24] The U.S. government says Offensive Cyber Effects Operations are

> operations and related programs or activities – other than network defense, cyber collection, or DCEO [Defensive Cyber Effects Operations]- conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks.[25]

These U.S. Air Force definitions will be used in this dissertation.

---

[22] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 159.

[23] "Himes, Westmoreland, Members of Cybersecurity Subcommittee Call for Cyberwarfare Rules," November 5, 2015, accessed May 10, 2016, https://himes.house.gov/press-release/himes-westmoreland-members-cybersecurity-subcommittee-call-cyberwarfare-rules.

[24] Singer and Friedman, 128.

[25] "Presidential Policy Directive," 3, in Glenn Greenwald and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian,* June 7, 2013b, accessed November 1, 2014, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Other scholars use the terms cyberwarfare, information warfare and electronic warfare interchangeably. Fred Kaplan suggests that cyberwar is the new name for information warfare.[26] Martin Libicki, another influential cyber scholar, says cyberwarfare is one of the seven layers of information warfare, which is "the struggle over information systems."[27] The others are 1) command and control warfare 2) intelligence warfare 3) electronic warfare 4) psychological warfare 5) hacker warfare 6) economic information warfare and 7) cyberwarfare.[28] Libicki says there are two types of cyberwar: strategic and operational where strategic is waged in order to influence behavior[29] and operational supports military operations.[30] These ideas will be discussed in more detail in the next chapter.

In the oft-cited 1993 essay "Cyberwar is Coming!" John Arquilla and David Ronfeldt encourage us not to confuse cyberwar with electronic warfare because cyberwar disrupts or destroys the systems whereas[31] electronic warfare conducts surveillance, gathers intelligence and jams signals. But, they also refrain from defining cyberwar

---

[26] Kaplan, *Dark Territory: The Secret History of Cyber War*, 120.

[27] Martin C. Libicki, "What Is Information Warfare?" (Washington, D.C.: Institute for National Strategic Studies, August 1995): ix, accessed June 10, 2014, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662.

[28] Libicki, "What is Information Warfare?," 75.

[29] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND Corporation, 2009): 117, accessed June 10, 2014, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[30] Libicki, *Cyberdeterrence and Cyberwar*, 139.

[31] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy* 12, no. 2 (Spring 1993): 31, accessed March 16, 2014, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf.

claiming, "As an innovation in warfare, we anticipate that cyberwar may be to the 21st century what blitzkrieg was to the 20th century. Yet for now, we also believe that the concept is too speculative for precise definition."[32] This lack of definitional consensus complicates discerning between what constitutes an act of war. The original Tallinn Manual says that in order to understand when a cyberattack constitutes a use of force, one has to assess severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality.[33] The cyberweapons that will be discussed in Chapter 4 of this dissertation will be assessed under many of these conditions.

AN OFFENSIVE STATE OF MIND

Cyberwarfare is very different from other forms of warfare. First of all, since it is a man-made domain, it is operated and controlled by both the public and private sector and changes at the mercy of technology.[34] Also, cyberattacks are not constrained by geography since they can occur anywhere. Likewise, even though the U.S. has been fortunate enough to be protected by the Arctic, Atlantic and Pacific oceans, these oceans will not be able to protect the U.S. from a cyberattack.

Another difference between cyberwar and conventional war is the amount of damage. Some authors argue that cyberattacks do not rise to the same level of force as

---

[32] Arquilla and Ronfeldt, "Cyberwar Is Coming!," 30.

[33] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 48-51.

[34] Nils Melzer, "Cyberwarfare and International Law," *United Nations Institute for Disarmament Research*, (2011), 5, accessed April 12, 2016, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

conventional attacks.[35] Thus, they question whether cyberwar can extract the same political concessions as other methods such as airstrikes.[36] Some cyber pessimists also argue that the damage can be temporary or reversible. "Shutting down power grids, closing airports, or derailing communication could be tremendously costly, but most damage of this type will be fixed quickly and at comparatively modest investment of tangible resources."[37] I disagree with this point though because shutting down a power grid can potentially result in a grave loss of life. Additionally, since cyberweapons have not directly killed anyone yet, this is a benefit of engaging in cyberwarfare because such targeted attacks minimize casualties and collateral damage, thus adhering to jus in bello. However, as we will see later, this lack of violence is why some question the existence of cyberwarfare.

Another difference between cyberwarfare and other forms of warfare is that it is unclear how long it will take to achieve whatever the intended outcome is and the outcomes are not guaranteed. This is not a tit-for-tat scenario. The outcome could differ or there can be "blowback" or "spillover" effects. (Blowback is the idea that U.S. systems could suffer from their own attack. Spillover effects are unintentional consequences such as these weapons spreading to U.S. allies.) Furthermore, instead of not causing enough damage, these weapons could cause more damage than intended. Either way, deploying a cyberweapon first can be seen as an act of war as it can be viewed as an attack upon a

---

[35] Robert Belk and Matthew Noyes, *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*, (Cambridge, MA: Belfer Center for Science and International Affairs, 2012), 116, accessed October 1, 2014, http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf.

[36] Libicki, *Cyberdeterrence and Cyberwar*, xv.

[37] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall, 2013): 57, EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

state.[38] Thus, the ambiguity of a cyberweapon could result in unwarranted and unwanted retaliation.

Some scholars say that if there were a conflict between the U.S. and an adversary, cyberwarfare could place them on equal footing.[39] "The low cost of computing devices means that U.S. adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to U.S. military capabilities."[40] Some scholars call this 'death by a thousand cuts' "to contrast with a catastrophic 'digital Pearl Harbor' or 'digital 9/11.'"[41] However, other scholars argue that weak states cannot strong-arm strong states solely with a cyberweapon because in order to do serious damage, the weak state would have to develop an advanced weapon which is probably beyond their means.[42] However, Chinese cyber operations such as "Titan Rain, Byzantine Haydes, Aurora, and Shady RAT"[43] seem to refute this point.

Another way in which cyberwarfare differs from other types of warfare is that cyberweapons are basically one-time use only.[44] In cyberwarfare, once a state deploys a cyberweapon, that weapon may become worthless, because once the vulnerability is

---

[38] William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: The National Academy of Sciences, 2009), 234, accessed November 18, 2014, http://www3.nd.edu/~cpence/eewt/Owens2009.pdf.

[39] Ibid., 330.

[40] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," 98.

[41] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 370.

[42] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," 411.

[43] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 370.

[44] Gartzke, 60; Belk and Noyes, 35.

revealed; the attacked state will try to correct the flaw. So the attacker has to assess whether deploying this cyberweapon is worth it.

Attribution is another very important difference between conventional warfare and cyberwarfare. "Whereas a missile comes with a return address, a computer virus generally does not."[45] In cyberwarfare, a state does not always know who the attacker is much less if it is an attack. This makes retaliation problematic.[46] On the other hand, countries may engage in cyberwarfare because of "plausible deniability." Plausibility deniability is the idea that an attacker can wage an attack without implicating themselves.[47] The flip side is that the wrong person could be intentionally or mistakenly blamed or framed. This was the other interesting part of Liff's definition but it is rather perplexing, because Liff also argues that if the point of cyberwarfare is to coerce an actor, then by anonymously attacking a state, or in this case, framing another state, the attacker will not be able to obtain their desired political concessions.[48] "The "attribution problem" is thus not only a headache for the defender, but also a liability for an attacker who insists on anonymity or deniability."[49] Attribution is also why some people have compared cyberwarfare to terrorism. "With today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but cyberterrorism."[50]

---

[45] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," 99-100.

[46] Libicki, *Cyberdeterrence and Cyberwar,* 120.

[47] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," 412.

[48] Ibid., 414.

[49] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 399.

[50] Shamah, "Latest viruses could mean 'end of world as we know it,' says man who discovered Flame."

While attribution complicates retaliation, it also complicates deterrence. Deterrence is "the ways in which an actor manipulates threats to harm others in order to coerce them into doing what he desires."[51] States are influenced by each other's behavior, interests and actions.[52] Since states often assume the worst about each other and conflate intentions with capabilities, they rush to obtain weapons in order to prevent an attack.[53] In deterrence, parties are aware of each other's capabilities but the world of cyberwarfare is classified.[54] Thus, inaccurate information can lead to misperceptions about a state's arsenal. About 30 states have created cyberwarfare departments,[55] and more states are arming themselves with cyberweapons in what some call an arms race.[56] (Although, some experts argue that there are no causal links between arms races and war.[57]) When Admiral Mike Rogers became head of the N.S.A. and CYBERCOM in 2014, Sanger said he asked Rogers how he wanted to be remembered at the end of his term and Rogers replied, I want to be remembered as the guy who created a high cost for these attacks on the U.S. because right

---

[51] Robert Jervis, "Deterrence Theory Revisited," *World Politics* 31, no. 2 (January 1979): 292, JSTOR via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[52] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, N.J: Princeton University Press, 1976), 61.

[53] Ibid., 65.

[54] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," 420.

[55] Clarke and Knake, 46.

[56] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 270.

[57] Robert Powell, "Bargaining Theory and International Conflict," *Annual Review of Political Science* 5, no. 1 (2002): 14, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

now there is no cost.[58] Cyberweapons represent a security dilemma since states are creating weapons to deter conflict but by inventing more weapons they are also increasing the chances of conflict.[59] (In 2016, Ben Buchanan released a book called *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*.) Although attribution makes cyber deterrence difficult, it does not make cyberwar difficult because in cyberwar, a state knows who the target is.[60] I will revisit deterrence in the next chapter.

COMMAND

Caught off guard by the Soviet Union's launch of Sputnik 1 in 1957, the U.S. created the Advanced Research Projects Agency, (known today as the Defense Advanced Research Projects Agency [DARPA]) whose purpose was to advance the technology of the military.[61] DARPA was one of the main funders of the Internet, or ARPANET (Advanced Research Projects Agency Network), as it was known back then. Today, one of DARPA's projects is "Plan X" which is a program that helps the Department of Defense execute and evaluate cyberwarfare operations. However, DARPA claims that they do not participate in the creation of offensive cyber operations.[62]

---

[58] Sanger, "*Zero Days* Screening."

[59] Timothy J. Junio, "The Politics and Strategy of Cyber Conflict," (PhD diss., University of Pennsylvania, 2013b), 10.

[60] Libicki, *Cyberdeterrence and Cyberwar*, 120.

[61] "Where the Future Becomes Now," *Defense Advanced Research Projects*, accessed April 23, 2016, http://www.darpa.mil/about-us/timeline/where-the-future-becomes-now.

[62] "Plan X," *Defense Advanced Research Projects*, accessed April 23, 2016, http://www.darpa.mil/program/plan- x.

In 2008, the Department of Defense's classified computer systems were infiltrated after a flash drive containing unknown malware (malicious software) was injected into a U.S. computer at a Middle Eastern base.[63] It was the largest breach of U.S. military networks and the Pentagon responded with Operation Buckshot Yankee.[64] This operation was the impetus for creating U.S. Cyber Command[65] as the Joint Task Force-Global Network Operations (defense) and Joint Functional Component Command-Network Warfare (offense) worked together.[66] In June 2009, Defense Secretary Robert Gates consolidated all of the various agencies involved in cyber operations such as the Army Forces Cyber Command, the U.S. Navy's Tenth Fleet, the 24th Air Force, and the Marine Corps Forces Cyberspace Command into U.S. Cyber Command (CYBERCOM).[67] Some of CYBERCOM's goals are to "build and maintain ready forces and capabilities to conduct cyberspace operations" and "plan to use those options to control conflict escalation."[68]

CYBERCOM was strategically located in Fort Meade, Maryland, right next to the N.S.A. (who conducts "signals and information intelligence protection"),[69] so that the two

---

[63] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," 97.

[64] Ibid.

[65] Ibid., 97 – 98.

[66] "Key Players in Operation Buckshot Yankee," *The Washington Post,* December 8, 2011, accessed August 12, 2017, https://www.washingtonpost.com/world/national-security/key-players-in-operation-buckshot-yankee/2011/12/08/gIQASJaSgO_story.html?utm_term=.5280e6e02a7d.

[67] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," 102.

[68] Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2017 Budget Request*, (February 2016), 5-5, accessed March 1, 2016, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_Budget_Request_Overview_Book.pdf.

organizations could share resources. The head of the N.S.A. is also the head of CYBERCOM. "A single chain of command runs from the U.S. president to the secretary of defense to the commander of Strategic Command to the commander of Cyber Command and on to the individual military units around the world."[70] However, in December 2016, the Obama administration decided to split the dual-hatted structure.[71] The Trump administration is going ahead with the split.[72]

In order to carry out a cyberattack, there are three things that need to happen: "(1) flaws in the design of the Internet; (2) flaws in hardware and software; and (3) the move to put more and more critical systems online."[73] Software is made up of hundreds, even millions of lines of code. "Each line of that code had to be written by a computer programmer, and each additional line of code increased the number of bugs introduced into the software."[74] These bugs or holes are called zero-days meaning there have been zero days since the hole has been discovered.[75] Once a zero-day is found, malware can be

---

[69] Singer and Friedman, 134.

[70] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," 102.

[71] Ellen Nakashima, "Obama Moves to Split Cyberwarfare Command from the NSA," *The Washington Post,* December 23, 2016b, accessed May 25, 2017, https://www.washingtonpost.com/world/national-security/obama-moves-to-split-cyberwarfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html?utm_term=.74a3793bc045.

[72] Lolita C. Baldor, "U.S. to Create the Independent U.S. Cyber Command, Split Off from NSA," *PBS,* July 17, 2017, accessed August 1, 2017, http://www.pbs.org/newshour/rundown/u-s-create-independent-u-s-cyber-command-split-off-nsa/.

[73] Clarke and Knake, 73.

[74] Ibid., 90 – 91.

[75] "What is a Zero-Day Vulnerability?," *Security News*, accessed April 20, 2016, http://www.pctools.com/security-news/zero-day-vulnerability/.

implanted. Once the malware is inside, it can modify system logs to mask itself and carry out its mission.[76]

Zero-days are key because once the hole is discovered, security companies issue patches to fix it.[77] (Imagine routine software updates for your phone or laptop.) Finding a zero-day is like catching the Golden Snitch in Quidditch; it is extremely difficult and malware is just as fleeting as that tiny golden ball with wings. "In 2009, a new type or variant of malware was entering cyberspace every 2.2 seconds."[78] Sophisticated malware is usually developed by the N.S.A. Tailored Access Operations' (T.A.O.) elite unit, Remote Operations Center (R.O.C.)[79] In 2013, the N.S.A. spent $25 million on 'additional covert purchases of software vulnerabilities' from European malware vendors,[80] reflecting the growing cyber black market where states can purchase these weapons.[81]

As one can see, there are a lot of things that need to happen in order to engage in offensive cyberwarfare.

---

[76] Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," *The Washington Post,* August 30, 2013, accessed March 22, 2016, https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[77] "What is a Zero-Day Vulnerability?," *Security News.*

[78] Clarke and Knake, 89.

[79] Gellman and Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show."

[80] Ibid.

[81] Andy Greenberg, "Shopping for Zero-Days: A Price List for Hacker's Secret Software Exploits," *Forbes,* March 23, 2013, accessed October 30, 2014, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

> Cyber planners must gather detailed intelligence on the mechanical and organizational dimensions of their target, gain access to the target's computer network, exploit system vulnerabilities to navigate through the network to the ICS [industrial control systems], and then activate a custom-engineered payload to sabotage it.[82]

This is why CYBERCOM also works with the C.I.A. which has its own unit called Information Operations Center (IOC) that conducts 'field operations' oversees. Sometimes the networks are not connected to the Internet. This is known as an "air gap."[83] In order to get around the air gap, intelligence operatives may be needed to physically access the site and transfer the malware from a USB drive onto the network or the operatives can surreptitiously get the malware onto the computer of someone who has access to the target network so that person could then unknowingly transfer the payload to the target.[84] (This is similar to what happened to the Department of Defense's computer networks in 2008.)

The Snowden documents also revealed a program that could "transmit reprogramming across many miles using low frequency waves" so that the N.S.A. could access a network that is air-gapped.[85]

> What's remarkable about cyberwar is that the hard part of this is getting the implants into a country's network and then sort of keeping them and feeding them and tending to them sort of like bonsai and then you can use it for espionage or you can use it later on for attack. [86]

---

[82] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 378.

[83] Kim Zetter, "Hacker Lexicon: What is an Air Gap?," *Wired,* December 8, 2014b, accessed February 2, 2016, https://www.wired.com/2014/12/hacker-lexicon-air-gap/.

[84] Sanger, "*Zero Days* Screening."

[85] Ibid.

[86] Ibid.

Due to the complex nature of carrying out such complicated operations, there are some scholars who deny that cyberwarfare is the future.

IS THIS FICTION?

Many cyberwarfare skeptics cite Carl von Clausewitz's classic *On War* to deny the existence of cyberwarfare. Thomas Rid is one of the most well-known critics of cyberwarfare. In 2011, Rid wrote a provocative article, (which eventually became a book), called "Cyber War Will Not Take Place." Using Clausewitz's three criteria for war (violent, instrumental and political) to analyze cyberwarfare, Rid concluded that based on these three criteria, cyberwarfare does not, nor will it ever exist.[87] Rid stated, "No cyber offense has ever caused the loss of human life. No cyber offense has ever injured a person. No cyber attack has ever damaged a building."[88] Thus, he claimed that all of this is fiction and that cyberwar proponents such as Richard Clarke are alarmist because cyberattacks are advanced versions of subversion, sabotage and espionage, which are all traditional tactics of warfare.[89] Rid argued that in subversion, "human minds are the targets, not machines"[90]

---

[87] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012a): 6, Journal of Strategic Studies via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[88] Ibid., 11.

[89] Ibid., 4. "Subversion is the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order. The ultimate goal of subversion may be overthrowing a society's established government. But subversive activity may also have more limited causes, such as undermining an organization's or even a person's authority." Rid, "Cyber War Will Not Take Place," 22. "Sabotage, first, is a deliberate attempt to weaken or destroy an economic or military system." Rid, "Cyber War Will Not Take Place," 16. "Espionage is an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information." "Its main purpose is not achieving a goal but to gather the information that may be used to design more concrete instruments or policies." Rid, "Cyber War Will Not Take Place," 20.

so subversion is irrelevant when discussing cyberwarfare. Additionally, Rid explained that sabotage is not an act of war because it could lack violence and attribution.[91] However, since cyberwarfare is classified, we do not definitively know if anyone has been directly killed because of a cyberweapon so we cannot say that this has never happened or even be so bold as to declare that this will never happen. As we will see in Chapter 4, there are cases where offensive cyber operations have led to the killing of militants.

In his emphatic article, "Cyber War Will Take Place!," John Stone refutes many of Rid's points arguing that Rid incorrectly conflates lethality, violence and force. "All war involves force, but force does not necessarily imply violence – particularly if violence implies lethality."[92] Stone argues "Clausewitz's definition of war as an act of force does not require that the act be claimed or attributable."[93] Thus, he proposes, "In the context of war, technology is often described as a 'force multiplier,' although for present purposes it is better termed a 'violence multiplier.'"[94] Many scholars and experts believe that cyber offense is most effective when used in conjunction with other methods.[95]

When Rid wrote his article, he claimed that most of the state-sponsored cyberattacks known to date have been because of espionage.[96] While it is true that many

---

[90] Rid, "Cyber War Will Not Take Place," 22.

[91] Ibid., 16.

[92] John Stone, "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (November 29, 2012): 103, Journal of Strategic Studies via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[93] Ibid., 105.

[94] Stone, 106.

[95] Sanger, "*Zero Days* Screening."

[96] Rid, "Cyber War Will Not Take Place," 20.

adversaries of the U.S. engage in cyberattacks in order to steal information that could provide them with economic or military advantages,[97] the Department of Defense stresses that the theft of intellectual property is the most serious threat. "As military strength ultimately depends on economic vitality, sustained intellectual property losses erode both U.S. military effectiveness and national competitiveness in the global economy."[98] The Chinese believe in using cyberattacks for these purposes[99] but the Department of Defense claims they do "***not*** [emphasis provided by the Department of Defense] engage in economic espionage in any domain, including cyber."[100] However, some experts claim the malware that the U.S. uses is similar to the threats that they ascribe to the Chinese.[101]

Another cyber skeptic is Eric Gartzke who says,

> Unless cyberwar can substitute for a physical surprise attack, there is no reason to believe that it will be used in place of conventional modes of warfare. Nor is it clear why an attacker would choose to strike over the Internet, unless a conventional surprise attack is also planned and when it is expected that the combination of cyber and terrestrial aggression will yield a decisive advantage to the attacker.[102]

I disagree with Gartzke because first of all, Clausewitz says surprise is rarely very successful in war.[103] Additionally, cyberwarfare is not about replacing conventional

---

[97] Owens, Dam and Lin, 226.

[98] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (July 2011), 4, accessed March 1, 2016, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[99] Owens, Dam and Lin, 333.

[100] Gellman and Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show."

[101] Ibid.

[102] Gartzke, 63.

[103] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, New Jersey: Princeton University Press, 1976), 198.

warfare. Cyberwarfare is a new type and possibly the future of warfare. How can a tank or Special Operations Forces (SOF) invade cyberspace? Also, as the leaked intelligence budget demonstrated, one of the advantages of engaging in cyberwarfare is that it can access countries such as North Korea, Russia, Iran and China, all of which are difficult to reach with conventional methods.[104] Thus, I do not think cyberwarfare will be used in place of conventional warfare but rather the opposite- where it is more risky to use conventional warfare. In regards to Gartzke's last point about advantages, this dissertation focused on cyberwarfare waged by the U.S., but Operation Orchard was a 2007 Israeli attack against a Syrian nuclear reactor where Israel's cyberwarfare unit first took out Syria's air defenses, thereby allowing four Israeli jets to enter Syrian airspace undetected and bomb a suspected nuclear site, after which the Israelis escape unscathed.[105] So, Operation Orchard is proof of cyber and conventional methods producing an advantage to the attacker.

Brandon Valeriano and Ryan C. Maness are also skeptical of the term cyberwarfare. In their excellent book, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Valeriano and Maness use the term "cyber conflict" instead of cyberwar because they claim that these attacks do not rise to the level of war. "Cyber conflict is a tactic, not a form of complete warfare. It is not even a separate domain, it is a tool in the arsenal of diplomacy and international interactions just as other forms of threats, and offensive and defensive actions in the toolbox of a state's arsenal of power."[106] Sanger

---

[104] Gellman and Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show."

[105] Kaplan, *Dark Territory: The Secret History of Cyber War*, 161.

[106] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015), 31.

explained that Eisenhower had also declared that nuclear weapons were a new tool in the toolbox although deep down Eisenhower believed differently.[107] So I also disagree with Valeriano and Maness because as we will see in the next few chapters, cyberweapons are more than simply another tool in a state's arsenal.

DECADES OF GLOBAL POLITICS

Although these cyberwar skeptics make some valid points, cyberwarfare has arrived and it is here to stay because it is the one area where U.S. defense spending is increasing (by a lot I might add) so this is not fiction. The catastrophic potential may not be of epic proportions as depicted in the short-lived television series CSI: Cyber but the potential is there. Sanger says that one of the fundamental issues he has tried to elevate is that there needs to be a national discussion the same way there was with nuclear weapons even though nuclear weapons were also classified.[108] Sanger points out that the national debate over nuclear weapons began and ended in a different place with "the country deciding that we are only going to use these in times of national survival" but in cyberwarfare, Sanger says "we have kind of slipped into a decision that we are going to use this as an ordinary weapon of conflict" once we can control the escalation.[109] Just as the "nuclear arms race would shape the next 50 years of global politics,"[110] cyberweapons could shape decades of global politics.

---

[107] Sanger, "*Zero Days* Screening."

[108] Ibid.

[109] Ibid.

[110] Singer and Friedman, 160.

Chapter 2

LITERATURE REVIEW

"The musket of cyberwarfare. What will be its rifle? Its AK-47? Its atomic bomb?"[1]

- P.W. Singer and Allan Friedman

As the U.S. government consistently emphasizes the growing importance of cyberwarfare and there are more news reports about the trove of N.S.A. documents leaked by Edward Snowden, there has been a burgeoning academic interest in the field of cyberweapons. Scholarly articles about cyberweapons can be found in journals such as *Foreign Affairs, Security Studies, Strategic Studies Quarterly, The Journal of Strategic Studies, Contemporary Security Policy, Journal of Peace Research* and the *Journal of Strategic Security.* There are also new journals dedicated entirely to the study of cyberwarfare such as the *Journal of Law & Cyber Warfare,* the *Journal of Cyber Policy* and *The Journal of Cybersecurity* which released "Special Issue: Strategic Dimensions of Offensive Cyber Operations," in March 2017. Some of these articles are cited later on in this dissertation.

Many universities have also formed cyber research centers such as the Cyber Security Project at Harvard University's Belfer Center for Science and International Affairs, Stanford University's Cyber Policy and Security program led by cyber scholar Herbert S. Lin and the Naval War College's Center for Cyber Conflict Studies led by cyber scholar Chris C. Demchak. Think tanks such as the New America Foundation have also

[1] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 118.

jumped into the cybersecurity arena with their own Cybersecurity Initiative and the Atlantic Council has the Cyber Statecraft Initiative.

Only since the discovery of Stuxnet, has advanced malware been labeled as a cyberweapon. Since then "virus hunters" are guilty of over-labeling, incorrectly labeling and perhaps under-labeling malware as cyberweapons. The media is especially guilty of this.[2] Scholars John Arquilla, Lucas Kello, Richard Clarke, Robert Knake and Dorothy Denning think that cyberweapons can be used to great effect. However, other scholars such as Thomas Rid, Adam Liff, Jon Lindsay, Eric Gartzke, Brandon Valeriano, Ryan Maness, James Farwell and Rafal Rohozinski, question the utility and impact of cyberweapons. Those who see both pros and cons are Tim Stevens, Martin Libicki, Herbert Lin, P.W. Singer and Allan Friedman. The objectives of this chapter are to survey the relevant literature about cyberweapons as it applies to this dissertation. This literature can be divided into four categories: norms, government rules of engagement for cyberweapons, academic frameworks for analyzing cyberweapons and actual deployments of cyberweapons.

[2] Stefano Mele says the press also labeled Rocra [Red October], Mahdi and FinFisher as children of Stuxnet but I haven't found such claims. Stefano Mele, "Cyber-Weapons: Legal and Strategic Aspects Version 2.0," *Italian Institute of Strategic Studies Niccolo Machiavelli* (June 2013): XI, accessed June 2, 2016, http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf.

NORMS

Much of the relevant literature about cyberweapons discusses norms. In May 2011, The White House released the "International Strategy For Cyberspace," which attempted to coalesce all stakeholders into adopting "norms of responsible behavior" in cyberspace.[3] In his article "Cyberweapons: Leveling the International Playing Field," Ross Rustici says, "there is currently no international norm against the acquisition or deployment of these weapons."[4] In their piece, "On the Use of Offensive Cyber Capabilities," Robert Belk and Matthew Noyes, argue "the U.S. must establish international norms and understanding on what constitutes an "armed attack" in cyberspace."[5]

Tim Stevens discusses the idea of norms in his article "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." Stevens says that there is an "'acceptable' use" of cyberweapons instead of a "non-use" of cyberweapons which means that unlike the usage of chemical or nuclear weapons which are considered taboo, there is no 'cyber taboo.'[6] Stevens logically argues that the use of Stuxnet means that we are probably past the

---

[3] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, (2011), 8, accessed March 14, 2016, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[4] Ross M. Rustici, "Cyberweapons: Leveling the International Playing Field," *Parameters* 41, no. 3 (Autumn, 2011): 343, ProQuest via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml

[5] Robert Belk and Matthew Noyes, *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*, (Cambridge, MA: Belfer Center for Science and International Affairs, 2012), 89, accessed October 1, 2014, http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf.

[6] Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (April 13, 2012): 343. http://www.libraries.rutgers.edu/rul/index.shtml.

discussion of not using these weapons.[7] In their book, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, one of the conclusions Brandon Valeriano and Ryan Maness proposed was that "The potential initiator is restrained by logic, norms, and fear of retaliation."[8] But, Stuxnet falsifies this argument.

In the oft-cited piece *Cyberdeterrence and Cyberwar*, prominent cyber scholar Martin Libicki discusses operational and strategic cyberwar. Libicki says "strategic cyberwar" is "cyberattacks to affect state policy."[9] In 2016, Libicki published a newer book called *Cyberspace in Peace and War* that featured many of these ideas. He said,

> *Strategic cyberwar,* like strategic war in general, targets a country, notably its critical systems; it is largely undertaken to influence the target or to weakens its ability to resource combat. *Operational cyberwar,* like military operations in general, targets military systems; it is largely undertaken in conjunction with war or a kinetic (that is, force-employing) military operation to enhance the latter's' success.[10]

These two ideas are key as some cyber operations are blurred. Libicki said, "cyberwar is neither a good adjunct to nor an adequate substitute for more conventional forms of strategic coercion."[11] His list of notable "intrusions" consisted of Stuxnet and Libya (2011).[12] Stuxnet will be discussed a little later, and Libya will be discussed in the next chapter.

---

[7] Stevens, 343.

[8] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015), 106.

[9] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND Corporation, 2009): 6, accessed June 10, 2014, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[10] Martin C. Libicki, *Cyberspace in Peace and War* (Maryland: Naval Institute Press, 2016), 343.

[11] Ibid., 195.

I. Nuclear

There are several nuclear threads interwoven throughout the literature about cyberweapons. Nuclear warfare has observable actions such as the fueling of ballistic missiles, but cyberwarfare does not.[13] In cyberwarfare, a cyberweapon could be installed and remotely activated later.[14] Another difference is that it is unclear when a cyberwar starts and ends but it is clear when nuclear warfare starts and ends.

According to the Russian computer security firm, Kaspersky Lab, unsurprisingly, the U.S. has had a 'cyber Manhattan Project' since at least 2001 that focuses on offense. Those behind this cyber Manhattan Project are known as the 'Equation Group' which some suspect is really the N.S.A.'s T.A.O.[15] This alleged rise in the development of cyberweapons has caused scholars to worry because as they point out, there is no '*On Thermonuclear War* for cyber conflict' yet.[16] James Mulvenon, a founding member of the Cyber Conflict Studies Association, says

> 'Here's the problem—it's 1946 in cyber. So we have these potent new weapons, but we don't have all the conceptual and doctrinal thinking that supports those weapons or any kind of deterrence. Worse, it's not just the United States and Soviets that have the weapons—it's millions and millions of people around the

---

[12] Libicki, *Cyberspace in Peace and War*, 6.

[13] Libicki, *Cyberdeterrence and Cyberwar*, xv.

[14] Ibid.

[15] Kevin Poulsen, "Surprise! America Already has a Manhattan Project for Developing Cyber Attacks," *Wired,* February 18, 2015, accessed June 1, 2016, https://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/.

[16] Patrick Cirenza, "Cyberweapons Aren't Like Nuclear Weapons," *Slate,* March 15, 2016, accessed May 28, 2016, http://www.slate.com/articles/technology/future_tense/2016/03/cyberweapons_are_not_like_nuclear_weapons.html.

world that have these weapons.'[17]

Joseph Nye references nuclear strategy in his article "Nuclear Lessons for Cyber Security," where he concluded "that cyber technology gives much more power to nonstate actors than does nuclear technology, and the threats such actors pose are likely to increase."[18] Rustici also frames his article using these nuclear threads.[19] He points out that a state cannot demonstrate its cyberpower the way that it can demonstrate its nuclear power.[20] But, Rustici declared, "Cyberweapons have the latent ability to usher in a new international order founded upon a byte-based MAD [mutually assured destruction]."[21]

However, in his article "The misunderstood acronym: Why cyber weapons aren't WMD," Jeffrey Carr discusses the 1982 Soviet - C.I.A. incident and Stuxnet as proof that since these cyberattacks were not weapons of mass destruction, cyberweapons are not weapons of mass destruction.[22] (These operations will be addressed later.) The most

---

[17] James Mulvenon quoted by Singer and Friedman, 161.

[18] Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 36. ProQuest via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml. For additional information, see Joseph S. Nye Jr., "From bombs to bytes: Can our nuclear history inform our cyber future?," *Bulletin of the Atomic Scientists* 69, no. 5 (2013): 8-14, EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[19] Rustici, 32.

[20] Ibid., 38.

[21] Ibid., 41.

[22] Jeffrey Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," *Bulletin of the Atomic Scientists* 69, no. 5 (September 1, 2013): 33, EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

insightful contribution of Carr's article to this dissertation, though, was his "private discussion" with "a member of the Special Operations Forces."[23]

Since some scholars like to discuss cyberweapons with nuclear weapons, some scholars also like to compare cyberwar to The Cold War, replacing Russia with China.[24] "'What we have to get used to is that even countries like China, with which we are certainly not at war, are in intensive cyber conflict with us.'"[25] However, some scholars caution against this comparison because the Cold War was about the competing ideologies of two superpowers that sought to control certain parts of the world whereas the Internet encompasses various ideologies and stakeholders.[26] Thus, some have suggested that perhaps cyberwarfare is "the cool war," the Cold War's successor, because there are no deaths (yet) but there are an increasing number of offensive strikes.[27]

As discussed earlier, deterrence is also a recurring theme throughout the literature.[28] However, the distinguishing factor between nuclear and cyber deterrence is in the first case, you do not survive.[29] In the case of nuclear weapons, a first-strike and a subsequent response would result in the mutually assured destruction of both states. Thus, rational

---

[23] Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," 35.

[24] Singer and Friedman, 138.

[25] Ibid., 121.

[26] David Rothkopf, "The Cool War," *Foreign Policy,* February 20, 2013, accessed April 18, 2016, http://foreignpolicy.com/2013/02/20/the-cool-war/.

[27] Ibid.

[28] For a great chapter about deterrence and norms, see Panayotis A. Yannakogeorgos and Adam B. Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (Florida: Taylor & Francis, 2014), 49-81.

[29] Libicki, *Cyberdeterrence and Cyberwar*, 72.

states are deterred from using these weapons.[30] On the other hand, a cyberweapon can destroy a state's critical infrastructure and prevent that state from retaliating, so there is an incentive to strike first.[31] This is what Libicki calls "moral hazard."[32] Thus, he wonders if we are sending "the right message" in engaging in such operations and if we do engage, then he says, the "moral burden has already been accepted."[33]

In their article, "The New Reality of Cyber War," James Farwell and Rafal Rohozinski argue that since Stuxnet attacked precise targets, "cyber weapons are in a different category from nuclear devices, which have little practical use except as a deterrent."[34] However, Libicki warns against conflating nuclear deterrence and cyberdeterrence.[35] In *Cyberspace in Peace and War*, Libicki says the damaging effects of nuclear weapons are clear however, in the cyber realm, where attacks are on the lower spectrum of escalation, determining retaliation, threshold and attribution are unclear thus, deterrence may not be as reliable as it is in the nuclear realm.[36]

---

[30] Graham Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Canada: Little, Brown & Company, 1971), 12.

[31] Timothy J. Junio, "The Politics and Strategy of Cyber Conflict," (PhD diss., University of Pennsylvania, 2013b), 105.

[32] Libicki, *Cyberdeterrence and Cyberwar*, 120.

[33] Ibid.

[34] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54, no. 4 (August 2012): 108, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[35] Libicki, *Cyberdeterrence and Cyberwar*, 178.

[36] Libicki, *Cyberspace in Peace and War*, 237.

II. Legality

There is an abundance of scholarship about legality and cyberweapons that focuses on what constitutes a use of force and when such an attack is justified.[37] In their book *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (one of the early books about cyberwarfare), P.W. Singer and Allan Friedman argue one must look at the effects of a cyberweapon in order to understand if it qualifies as a use of force.[38] Singer and Friedman's book is a good primer on how cyberwarfare developed and how it works. They provide helpful examples of cyberwarfare and also make recommendations about how to improve cybersecurity.

According to Clay Wilson, the author of many government reports about cyberwarfare, "Attacks against information systems using computer viruses could be considered an act of war within the scope of the laws of armed conflict."[39] However, in his article "Offensive Cyber Options and the Use of Force," Herbert Lin argues that "offensive cyber operations" are complicated for the Law of Armed Conflict due to the intent of the cyber operation (exploitation, espionage, attack) and the ambiguous effects.[40] But, Lin

---

[37] For more information, see William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: The National Academy of Sciences, 2009), 239-272, accessed November 18, 2014, http://www3.nd.edu/~cpence/eewt/Owens2009.pdf. There is also a whole section dedicated to legality in Jeffrey Carr, *Inside Cyber Warfare* (California: O'Reilly Media, 2010), 45-76.

[38] Singer and Friedman, 124.

[39] Library of Congress, Congressional Research Service, *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, by Clay Wilson, RL31787 (September 14, 2006), 9, accessed April 2, 2014, http://fas.org/irp/crs/RL31787.pdf.

[40] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4, no. 1 (2010): 82-83. Hein Online via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

claims "it is inevitable that some future conflict will have a cyber component to it," thus, "it behooves policy makers to understand the legal landscape before such a conflict occurs."[41] However, in their article "Easier Said Than Done: Legal Reviews of Cyber Weapons," Gary Brown and Andrew Metcalf argue that it is difficult to transform "these broad topics of academic discussion into practical legal advice for those few practitioners advising commanders on the impact of cyber law on operations."[42]

III. Ethics[43]

In his article "The Ethics of Cyberwarfare," Randall Dipert divides the morality of cyberwarfare into five questions, the most pertinent of which is, "Is a cyberattack ever morally justified in cases where the enemy has launched neither a cyber- nor a conventional attack?"[44] Dipert said he answered this "hard case" in a previous paper "on game-theoretic grounds, that a preemptive attack can be morally justified if the evidence exceeds a certain threshold of objective likelihood (roughly 90 percent) and if there will be a high level of expected damage to us if we do not preemptively attack." [45] Thus, he does not fully explicate when a preemptive attack would be ethically justified.

---

[41] Lin, "Offensive Cyber Operations and the Use of Force," 84.

[42] Gary D. Brown and Andrew O. Metcalf, "Easier Said Than Done: Legal Reviews of Cyber Weapons," *Journal of National Security Law & Policy* 7, no. 115 (2014): 116. http://www.libraries.rutgers.edu/rul/index.shtml. Brown was a "Senior Legal Advisor at U.S. Cyber Command" from 2010 – 2012.

[43] For more great articles about ethics, see Panayotis A. Yannakogeorgos and Adam B. Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (Florida: Taylor & Francis, 2014), 195-265.

[44] Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (2010): 392. EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[44] Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," 36.

Valeriano and Maness argue that cyberweapons are not ethical because they are unpredictable[46] whereas cyber scholar Dorothy Denning and Bradley Strawser maintain in their article "Moral Cyber Weapons," that cyberweapons are precise and controlled especially in comparison to kinetic weapons.[47] For these reasons, Denning and Strawser write: "For any just action taken by a given military, if it is possible for the military to deploy remote cyber-attacks in place of manned kinetic attacks without a significant loss of capability, then that military has an ethical obligation to do so."[48] Other scholars also state that "cyber also offers great potential for striking at enemies with less risk than using traditional military means."[49] However, in their article Denning and Strawser do not focus on cyberweapons that stand alone, such as Stuxnet.[50] Thus, their argument is not fully applicable to the bulk of the cyberweapons that will be analyzed in this dissertation.

---

[45] Dipert, 393.

[46] Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 200.

[47] Dorothy E. Denning and Bradley J. Strawser, "Moral Cyber Weapons," *Naval Postgraduate School*, 12, accessed June 5, 2016, http://faculty.nps.edu/dedennin/publications/Moral%20Cyber%20Weapons%20-%20Part-II-CH-6%20-%2024Oct2013%20(3).pdf

[48] Denning and Strawser, 7.

[49] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February - March 2011): 35, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[50] Denning and Strawser, 17.

GOVERNMENT RULES OF ENGAGEMENT FOR CYBERWEAPONS

In July 2011, the Department of Defense released what they claimed was the first "Department of Defense Strategy for Operating in Cyberspace."[51] However, some disputed that this was not the first strategy since in 2006, that there was the "National Military Strategy for Cyberspace Operations" released by the Joint Chiefs of Staff.[52] Even though the 2011 "Department of Defense Strategy for Operating in Cyberspace" did not discuss offense, before its release, the Pentagon stated that they had developed a classified list of cyberweapons and a framework outlining the authorization of a cyberweapon.[53] "The framework breaks the use of weapons into three tiers: global, regional and area of hostility. The threshold for action is highest in the global arena, where the collateral effects are the least predictable."[54] The president has to authorize a virus that is planted in another state's networks and activated at a later point.[55] The framework also specifies that the President has to authorize 'direct action,' which is the use of a cyberweapon in a state that the U.S. is not at war with.[56] But the President does not need to authorize "beacons to mark spots

---

[51] Sean Lawson, "DOD's 'First' Cyber Strategy is Neither First, Nor a Strategy," *Forbes,* August 1, 2011, accessed April 15, 2016, http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/#5ebcfbd133a8.

[52] Ibid.

[53] Ellen Nakashima, "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare," *The Washington Post,* May 31, 2011, accessed May 15, 2014, http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html.

[54] Ibid.

[55] Ibid.

[56] Ibid.

for later targeting by viruses."[57] If it is a war zone, presidential approval can be sought ahead of time so that the military has the approval if quickly needed.[58] Also, cyberweapons have to avoid collateral damage and be proportional to the threat.[59]

The "Department of Defense Strategy for Operating in Cyberspace," focused on "active cyber defense." "Active cyber defense is DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities."[60] "It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems."[61] The strategy also stated that the U.S. reserved "the right to defend these vital national assets as necessary and appropriate" in the wake of a cyberattack.[62]

In the oft-cited report *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, William Owens, Kenneth Dam and Herbert Lin state: "The U.S. Strategic Command has authority to conduct such attacks for active defense under a limited set of circumstances. But it is not known how far down the chain of command such authority has been delegated."[63] Farwell and Rohozinski argue that

---

[57] Nakashima, "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare."

[58] Ibid.

[59] Ibid.

[60] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (July 2011), 7, accessed March 1, 2016, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[61] Ibid.

[62] Ibid, 10.

[63] Owens, Dam and Lin, 112-113.

the military definition of active defense is different from the public and private sector's concept of the term. "As a result, the military's notion of active defence remains unformed: no one is certain what it means or how to apply it."[64] Thus, some scholars argue that there is no clear demarcation between offense and active defense.[65]

Since the "Department of Defense Strategy for Operating in Cyberspace," the White House released the 2011 "International Strategy For Cyberspace," which attempted to coalesce all stakeholders into adopting "norms of responsible behavior" in cyberspace.[66] And in 2015, the Department of Defense updated their 2011 strategy with the 2015 "DoD Cyber Strategy."[67] This document discussed offense and stated that if defensive and legal options fail, the Secretary of Defense or the President may order the military to engage in offensive operations "to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities,"[68] "to support military operations and contingency plans,"[69] or "to counter an imminent or on-going attack against the U.S.

---

[64] Farwell and Rohozinski, "The New Reality of Cyber War," 110.

[65] Farwell and Rohozinski, "The New Reality of Cyber War," 109; Nye, "Nuclear Lessons for Cyber Security?," 27.

[66] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, (2011), 8, accessed March 14, 2016, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[67] Department of Defense, *The DoD Cyber Strategy*, (April 2015), 3, accessed March 27, 2016, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[68] Ibid., 14.

[69] Ibid., 5.

homeland or U.S. interests in cyberspace. The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life." [70]

However, the most significant literature about offensive U.S. cyberwarfare has been among the trove of leaked documents from Edward Snowden, in particular, Presidential Policy Directive PPD-20 (PPD-20) with the subject line "U.S. Cyber Operations Policy." PPD-20 was authored in October 2012,[71] and supersedes a 2004 PPD.[72]

PPD-20 offers unvarnished details about U.S. strategy on offensive cyber operations. The memo, addressed to the Vice President and the Cabinet, defines cyberspace as "the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded processors and controllers."[73] PPD-20 also defines "U.S. National Interests" as "matters of vital interest to the United States to include national security, public safety, national economic security, the safe and reliable functioning of 'critical infrastructure,' and the availability of 'key resources.'"[74] Critical infrastructure includes the defense industries, transportation, banking, communication and energy

---

[70] *The DoD Cyber Strategy*, 5.

[71] Glenn Greenwald and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian,* June 7, 2013b, accessed November 1, 2014, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[72] "Presidential Policy Directive," 1, in Glenn Greenwald and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian,* June 7, 2013b, accessed November 1, 2014, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[73] Ibid., 2.

[74] Ibid., 3.

sectors.[75] One of the growing concerns among policymakers is that malware can disrupt these networks and their industrial control systems (ICS).[76]

PPD-20 states that the President has to approve any cyber operation that could result in 'significant consequences'[77] which is defined as "loss of life, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[78] Furthermore, the policy criteria that the president weighs for both offensive cyber effects operations (OCEO) and defensive cyber effects operations (DCEO) are Impact, Risks, Methods, Geography and Identity, Transparency, and Authorities and Civil Liberties.[79] Impact assesses the threat that the U.S. is facing, and the benefits and scope of a cyber operation in comparison to other approaches.[80] Risks assess retaliation against the U.S. for engaging in such operations, intelligence gained/lost as a result of a cyber operation, the subsequent effects on the Internet and political relationships and setting an unfavorable norm of international conduct.[81] (This confirms that norms are a consideration.) Methods assess the timeliness, effectiveness, capacity, intrusiveness and efficiency of a cyber

---

[75] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (July 2011), 7, accessed March 1, 2016, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[76] Hagel, **"**As Delivered Remarks by Secretary of Defense Chuck Hagel at the Retirement Ceremony for General Keith Alexander."

[77] "Presidential Policy Directive," 9.

[78] Ibid., 3.

[79] Ibid., 13.

[80] Ibid.

[81] Ibid.

operation.[82] Geography and Identity assess the effects of a cyber operation on a location, the users and U.S. adversaries.[83] Transparency assesses the extent to which host countries or network owners need to approve or be notified of a cyber operation, the impact on Americans and U.S. institutions and communications pre- and post-attack.[84] Authorities and Civil Liberties assess the process of cyberattacks within the U.S. [85] PPD-20 also called for

> a plan that identifies potential systems, processes, and infrastructure against which the United States should establish and maintain OCEO capabilities; proposes circumstances under which OCEO might be used; and proposes necessary resources and steps that would be needed for implementation, review, and updates as U.S. national security needs change.[86]

This is the most we know about U.S. decision-making in regards to the deployment of cyberweapons, but the American public barely has a vague idea about the potential and range of cyberweapons at the U.S.' disposal, much less the conditions or scenarios under which the U.S. would engage in offensive cyberwarfare.

In his book, *Dark Territory: The Secret History of Cyber War*, Fred Kaplan pointed out that PPD-20 "established an interagency Cyber Operations Policy Working Group to ensure that such side effects, along with other broad policy issues, were weighed before an attack was launched."[87] Additionally, he noted that "unlike nuclear options, the plans for

---

[82] "Presidential Policy Directive," 13.

[83] Ibid.

[84] Ibid.

[85] Ibid.

[86] Presidential Policy Directive, 15.

[87] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016a), 217.

cyber operations were not intended to lie dormant until the *ultimate* conflict; they were meant to be executed, and fairly frequently" since the directive stated officials, "'shall report annually on the use and effectiveness of operations of the previous year to the President, through the National Security Adviser.'"[88] This is fascinating. Kaplan also pointed out that at this time, the N.S.A. declassified a 1997 issue of their internal journal, *Cryptolog*. This issue declared the N.S.A. had 'the authority to develop Computer Network Attack (CNA) Techniques,' which the Department of Defense defined at the time as 'operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.'[89] Kaplan said this was labeled as a 'cyber effect' in PPD-20.[90] "According to the Joint Chiefs of Staff's official guidance on targeting, much of the decision-making about who and what to attack is up to the head of U.S. Cyber Command."[91]

Furthermore, the U.S. military has 6 categories of Joint Publications that form their military doctrine. These are Personnel Series, Intelligence Series, Operation Series, Logistic Series, Planning Series, and Communications System Series.[92] "Joint Publication 3-12 (R) Cyberspace Operations 5 February 2013" specifies how the military should

---

[88] Kaplan, *Dark Territory: The Secret History of Cyber*, 218.

[89] Ibid., 219.

[90] Ibid.

[91] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing Company, 2014), 58-59.

[92] Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014," *Cyber Defense Review*, August 27, 2015, accessed August 12, 2017, http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/.

conduct cyberspace operations. According to "Joint Publication 3-12 (R) Cyberspace Operations," collateral effects, targeting, intent, political/military assessment and deconfliction are some of the considerations that factor into planning.[93] Selection is based on desire rather than methods.[94] Additionally, military attacks are only allowed against "military targets."[95]

ACADEMIC FRAMEWORKS FOR ANALYZING CYBERWEAPONS

Many scholars urge academic rigor when discussing cyberweapons.[96] In his article, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," Timothy Junio claims that Thomas Rid and Adam Liff "do not commit to a theoretical framework regarding the causes of war."[97] Thus, Junio argues "The principal-agent approach demonstrates how variation in incentives and preferences may make militaries

---

[93] *Joint Publication 3-12 (R) Cyberspace Operations*, (Department of Defense, February 5, 2013), x, accessed March 15, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. Deconfliction is means coordination amongst all those involved. Ibid., II-9.

[94] Ibid., II-9.

[95] Ibid., III- 10.

[96] Timothy J. Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (February 6, 2013a): 125, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 402-404, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," 38, no. 2 (Fall, 2013): 8, Project Muse via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[97] Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," 125. Junio is talking about Rid's work "Cyber War Will Not Take Place." Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012a): 6, Journal of Strategic Studies via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

more likely to favor cyber attack than other kinds of bureaucracies."[98] However, Liff counters that Junio conflated his argument with Rid and that he did have a theoretical framework in his article, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," which Junio himself pointed out was based on James Fearon's 'Rationalist Explanations for War.'[99]

A couple of other excellent academic works include Jason Healey's 2013 book *A Fierce Doman: Conflict in Cyberspace, 1986-2012* that discusses the history of cyber conflict.[100] Ben Buchanan's *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* published in 2016, discusses Nitro Zeus and other operations. The main thrust of his argument is "the core of the cybersecurity dilemma is about fear and escalation" and that shapes decision-making.[101] Adam Segal calls his view *The Hacked World Order*. "The new international order, the hacked world order, is emerging from the interactions of these powers."[102] Segal argues that China and the U.S. are the biggest cyber

---

[98] Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," 125-126.

[99] Adam P. Liff, "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio," *Journal of Strategic Studies* 36, no. 1 (February 12, 2013): 136, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," 125-126.

[100] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (Virginia: Cyber Conflict Studies Association, 2013a).

[101] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (New York: Oxford University Press, 2016), 193.

[102] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016c), 41.

powers.[103] He argues that cyberattacks have accompanied regional conflicts[104] but great powers have mostly been restrained.[105] Segal says "unless strategic gains clearly outweigh the costs to diplomatic and economic interests as well as the potential threat to the stability of the global Internet, cyber operations should not be conducted."[106] Segal also talks about hybrid war,[107] and supported the split of the N.S.A.'s dual-hatted structure.[108]

Thus, there are a few frameworks discussed in the literature that attempt to explain the rationale for using cyberweapons.[109] In their work "On the Use of Offensive Cyber Capabilities," Robert Belk and Matthew Noyes, propose a framework which consists of (in

---

[103] Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, 40.

[104] Ibid., 77.

[105] Ibid., 231.

[106] Ibid., 244.

[107] Ibid., 45.

[108] Ibid., 239.

[109] Over the years, NATO's annual Conference on Cyber Conflict (Tallinn, Estonia) has produced some excellent articles including: Peeter Lorentz and Rain Ottis, "Knowledge Based Framework for Cyber Weapons and Conflict," in Czosseck, C. and Podins, K. (Eds.), *Conference on Cyber Conflict* (2010), 129-142, accessed February 27, 2016, Tallinn: CCD COE Publications, https://ccdcoe.org/sites/default/files/multimedia/pdf/Lorents%20et%20al%20-%20Knowledge%20Based%20Framework%20for%20Cyber%20Weapons%20and%20Conflict.pdf; Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," in C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), *2012 4th International Conference on Cyber Conflict* (2012), 319-331, accessed February 27, 2016, NATO CCD COE Publications, https://ccdcoe.org/cycon/2012/proceedings/d1r3s2_fanelli.pdf; David Raymond et al., "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons," in K. Podins, J. Stinissen, M. Maybaum (Eds.), *2013 5th International Conference on Cyber Conflict,* (2013), accessed February 27, 2016, 1-16, Tallinn: NATO CCD COE Publications, https://ccdcoe.org/cycon/2013/proceedings/d1r2s6_raymond.pdf; Maren Leed, *Offensive Cyber Capabilities at the Operational Level: The Way Ahead*, (Center for Strategic & International Studies, September 2013), 1-10, accessed October 1, 2014, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.

order of importance), Normative (Ethical, Domestic Law, and International Law), Operational (Strategic, Executional and Temporal), and Consequential (Domestic, International, Soft Power and Systemic.)[110] They then apply this framework to 12 types of cyberattacks, the most severe of which is "cyber force."[111] (A lot of the relevant literature discusses different categories of cyberweapons.[112]) Belk and Noyes propose that such attacks have to be focused, used with conventional force and coordinated with allies.[113] (Coordination with allies was also discussed in PPD-20.)

The 2009 National Research Council report also lays out a framework for analyzing cyberattacks.[114] The report states that cyberattacks "can also support covert action, which is generally designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the U.S. government."[115] They propose the following rules of engagement:

> "-When to execute a cyberattack—what are the circumstances under which a cyberattack might be authorized?
> -Scope of a cyberattack—what are the entities that may be targeted?
> -Duration of the cyberattack—how long should a cyberattack last?
> -Notifications—who must be informed if a cyberattack is conducted?
> -Authority for exceptions—what level of authority is needed to grant an exception for standing ROEs [Rules of Engagement]?"[116]

---

[110] Belk and Noyes, 28.

[111] Ibid., 24.

[112] Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 34-37.

[113] Belk and Noyes, 138.

[114] Owens, Dam, and Lin, x.

[115] Ibid., 2.

[116] Ibid., 169.

This report was a guide for Lucas Kello's conceptual framework in "The Meaning of the Cyber Revolution." Lucas Kello, a former associate of the Belfer Center is now the Director of the Cyber Studies Programme at the University of Oxford. Kello argues that the cyber revolution is real and important and thus, deserves strong academic rigor to explain the usage of cyberweapons instead of merely technical reports such as Martin Libicki's book *Conquest in Cyberspace: National Security and Information Warfare*[117] or being attached to the Clausewitz framework unless, he claims, we overlook the international security consequences of using this "virtual weapon."[118] Thus, Kello proposes to "organize and codify data collected after a cyber event becomes known, search for causal chains linking determining factors to the event, and establish conceptual benchmarks for evaluating competing explanations of it."[119]

I. Critiques

Jon Lindsay derides Kello's article in a letter written to the editors in "Correspondence: A Cyber Disagreement." Lindsay disparages Kello for his literature review claiming that Kello should have cited Valeriano and Maness's article "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype" since it is the kind of academic rigor that Kello was arguing for. (Valeriano and Maness' book is discussed throughout this chapter.) Additionally, Lindsay defends Libicki claiming that "Libicki uses strategic and

---

[117] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," 38, no. 2 (Fall 2013): 16, Project Muse via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml. Of course, computer security firms Symantec and Kaspersky Lab have also issued detailed technical reports about known cyberweapons.

[118] Ibid., 22.

[119] Ibid., 17.

political considerations to debunk technological fears and to advocate for an alternative focus on international standards policy."[120]

Kello replied:

> these works barely (or not at all) integrate the virtual weapon into the theoretical matter of international relations. Therein lies the gap: very little of the prevailing scholarship systematically addresses how cyber activity affects foundational notions such as "anarchy," "system," "regimes," "identity," and "the balance of power," which are the prime units of intellectual currency in international relations.[121]

Lindsay also says that Kello should have referenced Derek S. Reveron's *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* and Gregory J. Rattray's *Strategic Warfare in Cyberspace*, since these books support Kello's belief of a cyber revolution.[122] Reveron's book is about "the various operational considerations associated with 'weaponizing' the basic technology available in *cyberspace."*[123] However, Rattray's book is about power, a theme that also appears in much of the literature.

II. Power

In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, John Sheldon points out in "Toward a Theory of Cyber Power," that Rattray's book "tends to overemphasize the technological and organizational dimensions

---

[120] Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (Fall 2014): 186, Project Muse via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[121] Kello, "Correspondence: A Cyber Disagreement," 191.

[122] Lindsay, "Correspondence: A Cyber Disagreement," 185.

[123] Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington: Georgetown University Press, 2012), 225.

at the expense of other pertinent elements and relies exclusively on the analogy of strategic air power."[124] Since Kello is not a fan of technical reports, it makes sense he did not include Rattray's work. Sheldon says "the strategic purpose of cyber power is the ability in peace and war to manipulate the strategic environment to one's advantage while simultaneously degrading the ability of the enemy to comprehend that same environment."[125]

In his article "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," Eric Gartzke argues that cyberweapons and cyberwarfare cannot produce a power shift.[126] Joseph Nye somewhat agrees in "Cyber Power," but he also states "the cyber domain is likely to increase the diffusion of power to non-state actors, and illustrates the importance of networks as a key dimension of power in the 21st century."[127]

Other proposed frameworks include Charles Debeck's "Correlates of Cyber Warfare" database similar to J. David Singer's "Correlates of War" dataset.[128] Debeck's

---

[124] Sheldon also points out that Rattray's work is stronger than Franklin Kramer, Stuart Starr and Larry Wentz's book *Cyberpower and National Security*. John B. Sheldon, "Toward a Theory of Cyber Power," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, D.C.: Georgetown University Press, 2012): 218. Another oft-cited work about cyberpower is David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (Abingdon: Routledge, 2011).

[125] Sheldon, 208.

[126] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall, 2013): 63-64, http://www.libraries.rutgers.edu/rul/index.shtml.

[127] Joseph S. Nye Jr., "Cyber Power," *Belfer Center for Science and International Affairs*, (May 2010), 19, accessed May 1, 2016, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

[128] Charles Debeck, "The Correlates of Cyber Warfare: A Database for the Modern Era," (master's thesis, Iowa State University, 2011), 1-60, accessed November 8, 2014, http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3066&context=etd. (Valeriano and Maness referenced the Correlates of War in order to code what they call territorial militarized disputes. Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 100.)

proposals and Kello's proposals can be found in Brandon Valeriano and Ryan C. Maness' 2015 book, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, one of the few quantitative studies about cyberweapons. The most significant contribution of their work was the "Dyadic Cyber Incident and Dispute Dataset" which is an extensive database compiled from news reports of every cyber skirmish from 2001-2011.[129] From this dataset, Valeriano and Maness concluded, "Few states actually fight cyber battles." Twenty out of 126 rivals engaged in 111 cyber incidents and 45 disputes (they do not use the term "attack")[130] because of regional dominance and rivalries,[131] and most of these have been low-level actions because of restraint.[132] The U.S. is the exception to the regional argument since they are the most targeted even though they are not directly involved in territorial disputes.[133] Valeriano and Maness also found that the U.S. does not usually enter into cyber conflict even though it has advanced capabilities.[134] Their work falsifies Brown and Metcalf's claims that a) it is impossible to differentiate between states and criminal usage of cyberspace by focusing on the technical specifics of cyber operations and b) that it is difficult to apply academic discourse on cyberweapons to practitioners.[135] This dissertation will use Valeriano and Maness' dataset as a guideline in how to carry out

---

[129] Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 82.

[130] Ibid., 89.

[131] Ibid., 96.

[132] Ibid.

[133] Ibid., 100.

[134] Ibid., 93.

[135] Brown and Metcalf, 116.

quantitative analysis of cyberweapons; however, the dissertation will code this information differently since we have different hypotheses and this dissertation focuses only on U.S. cyberweapons used against other states.

Thomas Rid (notable cyberwarfare skeptic) and Ben Buchanan also propose a framework in "Attributing Cyber Attacks," where they use the Q model to help attribute cyberattacks.[136] The Q model can be used by both novice and experts to understand cyberattacks in as general or specific terms. As one moves from the inner part to the outer part of the model, the questions get more detailed. Some of these questions were a useful guideline for both the quantitative and qualitative analyses for this dissertation.

ACTUAL DEPLOYMENTS OF CYBERWEAPONS

In their article, "Cyber-weapons," Thomas Rid and Peter McBurney, discuss three levels of cyberweapons: "low-potential," "unauthorized intrusions" and "high-potential."[137] (Valeriano and Maness differentiate between infiltration and intrusion.) Those on the lower spectrum include a distributed denial of service (DDoS) attack.[138] Higher end cyberweapons are the viruses, worms and Trojan horses — the "fire-and-forget missile" which gets inside a protected high-value target, potentially causes destruction and

[136] For an excellent article about attribution, see David D. Clark and Susan Landau, "Untangling Attribution," *Harvard National Security Journal* 2, no. 2 (2011): 323-352, Hein Online via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[137] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The Rusi Journal* 157, no. 1 (February 29, 2012c): 6, http://www.libraries.rutgers.edu/rul/index.shtml.

[138] Ibid., 5.

negatively alters the system.[139] This dissertation focuses on the higher end cyberweapons. Many scholars cite a 1982 Soviet-C.I.A. incident,[140] Israel's Operation Orchard[141] and Stuxnet[142] as high-potential cyberweapons. Adam Segal said, "cyber weapons are like improvised explosive devices, paintball guns, or antiradiation missiles."[143]

I. Force Multiplier

Many scholars (even skeptics) and officials propose that cyberweapons are best used as a 'force multiplier' or in conjunction with conventional methods.[144] The Tallinn Manual states:

> cyber operations may be an integral part of a wider operation that constitutes an attack. As an example, a cyber operation may be used to disable defences at a target that is subsequently kinetically attacked. In such a case, much as laser designation makes possible attacks using laser-guided bombs. The law of armed conflict on attacks applies fully to such cyber operations.[145]

---

[139] Rid and McBurney, "Cyber-Weapons," 9. Valeriano and Maness call these infiltrations. (Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 35.)

[140] Rid & McBurney, "Cyber-Weapons," 9; Dorothy E. Denning, "Stuxnet: What Has Changed?," *Future Internet* 4 (2012): 676, accessed March 12, 2016, http://www.mdpi.com/1999-5903/4/3/672.

[141] Denning, "Stuxnet What Has Changed?," 676; Singer and Friedman, 126.

[142] Rid and McBurney, "Cyber-Weapons," 9.

[143] Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, 42.

[144] Rustici, 37; John Stone, "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (November 29, 2012): 106, Journal of Strategic Studies via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 110; Denning and Strawser, 17; Emilio Iasiello, "Are Cyber Weapons Effective Military Tools?," *Military and Strategic Affairs* 7, no. 1 (March, 2015): 35-36, accessed June 18, 2016, http://www.inss.org.il/uploadImages/systemFiles/2_Iasiello.pdf; David E. Sanger, "*Zero Days* Screening," (discussion, Harvard University, Cambridge, Massachusetts, April 29, 2016a); Gartzke, 59; Belk and Noyes, 128.

[145] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 110.

Liff says Operation Orchard is an example of a force multiplier.[146] However, many scholars cite the Russian-Georgian war of 2008 as an example of a cyber operation combined with conventional capabilities.[147] Upon the almost 20th anniversary of his foundational piece "Cyberwar is Coming!," John Arquilla offered some new insights in "Cyberwar Is Already Upon Us," where he says the Russian-Georgian war of 2008 was the "virtual 'blitzkrieg'" that he and co-author Ronfeldt imagined when they wrote their seminal article "Cyberwar is Coming!" twenty years ago.[148]

However, in his article "Are Cyber Weapons Effective Military Tools," Emilio Iasiello says the reason we do not see more cyberattacks is not because of targets but "because no strategic advantage would be gained, thereby calling into question the efficacy of cyber-attacks as viable weapons to achieve similar results as conventional weapons."[149] Rustici's article counters this point stating that cyberweapons will be deployed preemptively.[150] An example of such preemption is Stuxnet.

II. Stuxnet

The most discussed cyberweapon in the academic literature is Stuxnet, because Stuxnet allegedly marked the first time that the U.S. had used a cyberweapon against

---

[146] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," 405.

[147] Stevens, 151; Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," 24; Gartzke, 65.

[148] John Arquilla, "Cyberwar Is Already Upon Us," *Foreign Policy,* February 27, 2012, accessed May 25, 2016, http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/.

[149] Iasiello, 33.

[150] Rustici, 32.

another state to inflict damage (though the U.S. has never admitted this).[151] Thus, many experts point to Stuxnet as the first real case of cyberwar.[152] A lot of this information is culled from David Sanger's reporting and his book *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. (David Sanger is also affiliated with the Belfer Center.) I will discuss the mechanics of Stuxnet in-depth in the next chapter.

Paulo Shakarian argues that Stuxnet is a revolution in military affairs because of the exploits it used and the fact that it was able to access unconnected networks.[153] Chris Demchak argues that "Stuxnet marks the official beginning of a new cyber Westphalian world of virtual borders and national cyber commands as normal elements of modern cybered governments."[154] Kello says "the fact that the direct effects of Stuxnet were not comparable to the scale of destruction possible in an air attack was the new weapon's

---

[151] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* June 1, 2012b, accessed March 17, 2014, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

[152] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran,"; Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair,* March 2, 2011, accessed May 20, 2014, http://www.vanityfair.com/news/2011/03/stuxnet-201104; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown Publishers, 2014a); Ralph Langner, "Stuxnet logbook, Sep 16 2010, 1200 hours MESZ," *Langner* (blog), September 16, 2010, accessed June 12, 2016, http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/#more-217; Farwell and Rohozinski, "The New Reality of Cyber War," 108; Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 25. Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[153] Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, (April 15, 2011): 1, accessed May 2, 2016, http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s_eng.pdf.

[154] Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring, 2011): 35, ProQuest via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

principal appeal."[155] Industrial control systems expert Ralph Langner (an instrumental player in the discovery of Stuxnet) argued that Stuxnet "could be considered a textbook example of a 'just war' approach. It didn't kill anyone. That's a good thing. But I am afraid this is only a short-term view. In the long run it has opened Pandora's box."[156] Singer and Friedman claim Stuxnet was ""one of the most notable weapons in history; and not just cyber history, but history overall."[157]

However, many scholars question the effectiveness, implications and whether Stuxnet was in fact a use of force.[158] In her article "Are Cyberweapons Effective?," Ivanka Barzashka argues that while the world was patting itself on the back over the "success" of Stuxnet, the Iranians were quietly producing better highly enriched uranium and updating their centrifuges.[159] Thus, many academics such as Lindsay, Valeriano, Maness, Farwell and Rohozinski dispute the notion that Stuxnet was revolutionary.[160] In their article "Stuxnet and the Future of Cyber War," Farwell and Rohozinski point to that fact that

---

[155] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," 26.

[156] Mark Clayton, "From the man who discovered Stuxnet, dire warnings one year later," *The Christian Science Monitor,* September 20, 2011, accessed July 28, 2016, http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later.

[157] Singer and Friedman, 115.

[158] David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, (Institute for Science and Technology, December 22, 2010), 5, accessed May 27, 2016a, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

[159] Ivanka Barzashka, "Are Cyber-Weapons Effective?," *The Rusi Journal* 158, no. 2 (April 28, 2013): 54, http://www.libraries.rutgers.edu/rul/index.shtml.

[160] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (July 2013): 372, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 209.

Stuxnet's ability to surpass the air-gap had been previously used to steal information from CENTCOM and the usage of numerous zero-days is not remarkable but "a Frankenstein patchwork."[161] However, in their other article "The New Reality of Cyber War," Farwell and Rohozinski claim that an implication of Stuxnet is that "cyber weapons may offer non-kinetic ways to disrupt an operational capability of an adversary." [162]

Farwell and Rohozinski also questioned whether Stuxnet was a use of force stating while the government may have viewed Stuxnet as a use of force, according to Lin, Stuxnet is not a use of force because of the lack of damage.[163] Thomas Rid makes similar arguments in "Think Again: Cyberwar."[164]

John Arquilla's "Cyberwar Is Already Upon Us," was also a rebuttal against Thomas Rid. Arquilla argues against this notion of strategic cyberwar being ineffective using the 2007 incident in Estonia and Stuxnet as proof. (Many scholars claim the 2007 Russian cyberattack against Estonia is an example of what cyberwar looks like.[165] However, Libicki claims NATO was not so sure.[166]) Arquilla claims that eventually these attacks will "scale up."[167] Thus, Arquilla said the focus should be on whether cyberwarfare

---

[161] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 25.

[162] Farwell and Rohozinski, "The New Reality of Cyber War," 115.

[163] Ibid., 111.

[164] Thomas Rid and John Arquilla, "Think Again: Cyberwar," *Foreign Policy* (March/April, 2012b): 82. http://www.jstor.org/stable/23237859.

[165] Rid and McBurney, "Cyber-Weapons," 5; Rid and Arquilla, "Think Again: Cyberwar," 84-85.

[166] Libicki, *Cyberdeterrence and Cyberwar*, 179.

[167] Rid and Arquilla, "Think Again: Cyberwar," 85.

can be controlled. This is why he and other authors are in favor of treaties[168] whereas critics like Rid are not.[169]

When discerning whether Stuxnet was strategic or operational cyberwar Libicki said, "Stuxnet, designed to cripple Iran's nuclear facilities, was not launched to coerce Iran. It was not a good example of strategic cyberwar so defined. But its purpose was not to facilitate kinetic operations, so it is not a good example of operational cyberwar so defined."[170]

Singer and Friedman, proponents of Stuxnet's revolutionary capabilities, argue that an implication of Stuxnet was that although it took a lot of people to code the worm, "once it was used, it was like the Americans didn't just drop this new kind of bomb on Hiroshima, but also kindly dropped leaflets with the design plan so anyone else could also build it, with no nuclear reactor required."[171] Zetter says experts claim these leaflets or breadcrumbs[172] can be reverse-engineered. "A cyberweapon was the 'type of weapon that

---

[168] Rid and Arquilla, "Think Again: Cyberwar," 85; Wilson, *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, 9; Owens, Dam, and Lin, 327-328; Kenneth Geers, "Cyber Weapons Convention," *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 5 (2010): 547-551, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; Ronald Deibert, "Tracking the Emerging Arms Race in Cyberspace," *Bulletin of the Atomic Scientists* 67, no. 1 (January 1, 2011): 7, EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; In *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital* Weapon, Zetter talks about how the Wassenaar Arrangement attempted to regulate cyberweapons in 2013 and the Senate Armed Services Committee asked the President to create a similar policy. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital* Weapon, 114-115.

[169] Rid and Arquilla, "Think Again: Cyberwar," 83; Stevens, 165; Rustici, 39; Farwell and Rohozinski, "The New Reality of Cyber War," 116; Singer and Friedman, 193; Libicki, *Cyberdeterrence and Cyberwar*, 200- 201; Joseph Nye, "Cyber Power," 18.

[170] Libicki, *Cyberspace in Peace and War*, 360.

[171] Singer and Friedman, 159; Rothkopf, "The Cool War."

[172] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First*

you fire and it doesn't die. Somebody can pick it up and fire it right back at you.'"[173] Gary McGraw argues that "creating a Stuxnet-like attack is easier than many non-technical people may believe, which is a prime reason why cyber war is inevitable."[174] However, Liff argues that "although gradual proliferation of cyberwarfare capabilities may be inevitable, the widespread *use* of CNA [Computer Network Attack] is probably not."[175] Jon Lindsay echoes this point in his article "Stuxnet and the Limits of Cyber Warfare," arguing that the amount of technical skill and organizational resources that it takes to develop a cyberweapon "is generally beyond the capacity of a lone hacker, a small group of amateurs, or even organized criminals, some of the favorite bogeymen of cyberwar discourse."[176] So, the notion that cyberweapons are now easier to create[177] because of Stuxnet is a point of conflict in the literature.

III. Leaked N.S.A. Documents About Cyberweapons

Another key document exposed by the Snowden trove was the intelligence community's "Black Budget," which revealed that the U.S. conducted "231 offensive cyber operations in 2011" against "adversaries such as Iran, Russia, China and North Korea

---

Digital Weapon, 97; Liam O'Murchu, "Countdown to Zero Day—Did Stuxnet escape from Natanz?," *Symantec* (blog), November 11, 2014, accessed, July 5, 2016, http://www.symantec.com/connect/blogs/countdown-zero-day-did-stuxnet-escape-natanz.

[173] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 210.

[174] Gary McGraw, "Cyber War is Inevitable (Unless We Build Security In)," *Journal of Strategic Studies* 36, no. 1 (2013): 114, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[175] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," 426.

[176] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 389.

[177] Rid and Arquilla, "Think Again: Cyberwar," 82.

and activities such as nuclear proliferation."[178] The budget labeled these operations as 'active defense' claiming they were an important part of cyber defense.[179] This is interesting because the intelligence community was trying to paint these activities as defensive measures when in fact they are offensive attacks.

The Snowden documents also shed light on a massive toolbox of N.S.A. gadgets called 'QUANTUMTHEORY' that can access all sorts of computers.[180] The Snowden documents also revealed the WARRIORPRIDE program which is "a kind of universal Esperanto software used by all the Five Eyes partner agencies that at times was even able to break into iPhones, among other capabilities."[181] This clued us into the fact that the Five Eyes were creating cyberweapons. (I will discuss the Five Eyes later.) The Snowden documents also revealed a cyberweapon named SHOTGIANT.[182] Hence, Snowden's leaks are of tremendous value. Timothy Junio did not discuss the Snowden documents in his dissertation, citing "practical and moral reasons."[183] Cyber specialist Bruce Schneier

---

[178] Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," *The Washington Post,* August 30, 2013, accessed March 22, 2016, https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[179] Ibid.

[180] "2010 SIGINT Development Conference," *Spiegel Online International,* December 29, 2013, accessed November 2, 2016, http://www.spiegel.de/media/media-35667.pdf.

[181] Jacob Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle," *Spiegel Online International,* January 17, 2015, accessed May 26, 2016. http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html.

[182] Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle."

[183] Junio, "The Politics and Strategy of Cyber Conflict," 185.

stated, "Today's NSA secrets become tomorrow's PhD theses and the next day's hacker tools."[184] This is certainly the case in regards to this dissertation.

IV. News Articles About Cyberweapons

Several news organizations have also provided excellent analysis of the Snowden documents. In fact, in 2014, the journalists who first reported about Edward Snowden's trove founded *The Intercept*. *Der Spiegel* has also published many articles based on the Snowden documents, some which have not been published by American media organizations. One example is a 50-page catalog of devices (with prices) that the N.S.A. can purchase in order to break into almost any computer network.[185]

News organizations such as *Wired, The New York Times, The Washington Post, The Guardian* and *Politico* have all devoted special sections to cyberweapons. Journalists David Sanger, Kim Zetter, and Fred Kaplan authored books from their reporting on the subject. As mentioned earlier, David Sanger's 2012 book *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, is one of the seminal books about Stuxnet, which was also critiqued by others. Sanger's work was also a major part of the 2016 documentary *Zero Day*s which uncovered another cyber plot called Nitro Zeus.[186] An interesting aspect of the film was the National Security Agency (N.S.A.) spokesperson. In

---

[184] Bruce Schneier, "Cyberweapons Have No Allegiance," *Motherboard,* January 25, 2015, accessed June 27, 2016, http://motherboard.vice.com/read/cyberweapons-have-no-allegiance.

[185] Jacob Appelbaum, Judith Horchert and Christian Stöcker, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox," *Spiegel Online International,* December 29, 2013, accessed May 26, 2016, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

[186] Sanger, "*Zero Days* Screening."

order to hide her identity, her face was slightly pixelated perhaps to mimic the ones and zeros that make up computer code. Spoiler alert! At the end of the film, she was revealed to be an actor who was reading a prepared statement written by several N.S.A. employees. It was a surprising twist because the N.S.A., who works in the shadows, emerged from the shadows in order to set the record straight since they were the ones who developed Stuxnet.[187]

Sanger has also written about the U.S.' pivot to using cyberweapons to tackle non-state actors such as ISIS.[188] Kim Zetter offers an "updated" account of Sanger's work based on her reporting for *Wired* in her 2014 book *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*.[189] When I interviewed her for this dissertation, she said *Zero Days* was based on a lot of her reporting.

Another excellent book about cyberwarfare written by a journalist is Shane Harris' *@War: The Rise of the Military-Internet Complex*. This is one of the few works that talks about the Iraq (2007) operation in depth. Harris raised an interesting counterpoint to those who claim that cyberattacks are relatively casualty-free. He said cyberwar can be deadly since some of the N.S.A. employees who were deployed to combat zones died.[190] This

---

[187] *Zero Days*, Screening Harvard University, Cambridge, Massachusetts, April 29, 2016 (2016; Magnolia Pictures, 2016).

[188] David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times,* April 24, 2016c, accessed August 20, 2017, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[189] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 351.

[190] Harris, *@War: The Rise of the Military-Internet Complex*, 79.

dissertation did not distinguish between direct and indirect effects of cyberweapons but this is interesting.

Many of the details about the Iraq (2007) operation coincide with Fred Kaplan's book. Kaplan is also a journalist. Since Kaplan's book was published in 2016, it includes North Korea's hacking of Sony. Kaplan's book gives a nice overview of the formation of the N.S.A.'s Tailored Access Operations unit and the Remote Operations Centers in Georgia, Hawaii, Texas and Colorado.[191] However, cyber scholar P.W. Singer claimed Kaplan did not really bring us out of the darkness.[192]

Foreign Policy, Slate, The Diplomat, and *Vanity Fair* have also done excellent pieces about cyberwarfare including pointing out discrepancies within the reportage.[193] In a great piece for *The New Yorker,* Seymour Hersh tamed the press (and others) by highlighting several things. First, although one of the major targets of cyberweapons is a power grid,[194] the U.S. has no national electric grid.[195] Second, Hersh points out that Carr's book is called *Inside Cyber Warfare* even though Carr admitted he did not like the term

---

[191] Kaplan, *Dark Territory: The Secret History of Cyber*, 135.

[192] P.W. Singer, "'Dark Territory: The Secret History of Cyber War,' by Fred Kaplan," *The New York Times Book Review,* March 1, 2016, accessed August 12, 2017, https://www.nytimes.com/2016/03/06/books/review/dark-territory-the-secret-history-of-cyber-war-by-fred-kaplan.html.

[193] In "A Declaration of Cyber-War," Michael Joseph Gross refutes *The New York Times'* reporting that Stuxnet was tested in Israel. Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair,* March 2, 2011, accessed May 20, 2014, http://www.vanityfair.com/news/2011/03/stuxnet-201104.

[194] For more information on how to build a cyberweapon to destroy a SCADA system, see Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies* 36, no. 1 (February 7, 2013): 120-124, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[195] Seymour M. Hersh, "The Online Threat," *The New Yorker,* November 1, 2010, accessed May 15, 2014, http://www.newyorker.com/magazine/2010/11/01/the-online-threat.

'cyber war' but used it because 'hype sells.'[196] While journalistic accounts may not be considered the best academic material, these accounts were the first to sound the alarm about cyberweapons (albeit, sometimes prematurely) and have continued to provide strong analysis about the leaked N.S.A. documents.

V. Critiques

Despite the examples above, some scholars are not entirely sure what cyber war looks like[197] and thus, many cyber enthusiasts, cyber skeptics and even the media often cite Richard Clarke and Robert Knake's extreme hypothetical example in their book *Cyber War: The Next Threat to National Security and What To Do About It*.

> Within a quarter of an hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed in New York, Oakland, Washington, and Los Angeles. . . . Aircraft are literally falling out of the sky as a result of midair collisions across the country. . . . The financial system has also frozen solid because of terabytes of information at data centers being wiped out. . . . Several thousand Americans have already died, multiples of that number are injured and trying to get to hospitals. . . . In all the wars America has fought, no nation has ever done this kind of damage to our cities. A sophisticated cyber war attack by one of several nation-states could do that today, in fifteen minutes, without a single terrorist or soldier appearing in this country.[198]

In "Loving the Cyber Bomb," Jerry Brito and Tate Watkins point out that the only evidence that Clarke and Knake provide is distributed denial of service (DDOS) attacks, which they admit, cannot cause the kind of catastrophe they describe above.[199] Brito and

---

[196] Hersh, "The Online Threat."

[197] Stevens, 165.

[198] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins Publishers, 2010), 67.

[199] Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard Law School National Security Journal* 3, no. 1

Watkins also point out that Clarke and Knake incorrectly attributed blackouts in the North East and Brazil to cyberattacks.[200] 60 Minutes aired an episode on the Brazil blackout and cyberwar.[201] Additionally, Brito and Watkins point out that Clarke and Knake claimed that the Chinese left logic bombs in the U.S. power grid, information they got from an unnamed source which, *The Wall Street Journal* reported.[202] Brito and Watkins accurately point out that Clarke and Knake's book has no footnotes, bibliography or index.[203] Thus, Brito and Watkins urge caution when talking about cyberwar comparing it to the threat inflation partly drummed up by *The New York Times* in the run-up to the 2003 Iraq War.[204]

HOW THIS DISSERTATION FITS WITHIN THE EXISTING LITERATURE

Although the amount of scholarship about offensive U.S. cyberwarfare is increasing, much of the existing scholarship stresses that there needs to be some rules of engagement to assist in the decision-making process.[205] Thus, this dissertation will analyze the decision-making process behind the deployment of U.S. cyberweapons from 2001 – 2016. The next chapter will introduce the theory and methodology that will be used in this

---

(2011): 53, accessed May 2, 2016, http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Brito-and-Watkins.pdf.

[200] Brito and Watkins, 54; Hersh, "The Online Threat."

[201] Brito and Watkins, 58.

[202] Ibid., 54.

[203] Ibid., 51.

[204] Ibid., 58.

[205] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," 39; Owens, Dam, and Lin, 7.

dissertation in order to discern whether the conditions reviewed here are the actual conditions considered during deliberations about deployments.

Chapter 3

THEORETICAL FRAMEWORK AND METHODOLOGY

This dissertation focuses upon the key question of the conditions under which the United States would be likely to use a cyberweapon as a first strike. In order to extract the conditions, I analyzed previous U.S. decisions about deploying or not deploying a cyberweapon by using the poliheuristic theory of decision-making. As Richard Snyder, H.W. Bruck, and Burton Sapin asserted over a half-century ago: "If one wishes to probe the 'why' questions underlining the events, conditions, and interaction patterns which rest upon state action, then decision-making analysis is certainly necessary."[1]

Other scholars have applied decision-making analysis to cyberwarfare. In his book, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* Aaron Franklin Brantly applied Bruce Bueno de Mesquita's expected utility theory to cyber decision-making[2] and concluded that states engage in offensive cyber operations rationally.[3] In *Cyber Conflict After Stuxnet*, Adam Segal discussed the imagined decision-making process of Stuxnet.[4] In his dissertation "Decision-making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers," Daryl L. Caudle uses

---

[1] Richard C. Snyder, H. W. Bruck and Burton Sapin, *Foreign Policy Decision-Making: An Approach to the Study of International Politics* (New York: The Free Press of Glencoe, 1962), 33.

[2] Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (Athens, GA: University of Georgia Press, 2016), 1.

[3] Ibid., 167.

[4] Adam Segal, "The Stuxnet Story," in *Cyber Conflict After Stuxnet: Essays from the Other Bank of the Rubicon,* eds. Hannah Pitts and Karl Grindal (Vienna, VA: Cyber Conflict Studies Association, 2016b): 6-11.

decision-making theory, complexity theory, cyberpower theory and deterrence theory as his theoretical framework, but after interviewing senior military officers about how to respond to a cyberattack, he found that poliheuristic theory was the best explanation of their decision-making process.[5] This study differs from Caudle's because it is looking at first-strike cases, not retaliation.

None of these explanations are mutually exclusive in explaining the conditions under which the U.S. deploys a cyberweapon. Thus, the particular theoretical "frame" utilized in this study is the poliheuristic theory of decision-making, which is a combination of both the rational and cognitive theories of decision-making.[6] Hence poliheuristic theory literally looks at "the why and how of decision-making, thus addressing both the contents and the processes of decisions."[7]

---

[5] Daryl L. Caudle, "Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers," (PhD diss., University of Phoenix, 2010), 270, ProQuest via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[6] Alex Mintz, "How Do Leaders Make Decisions?: A Poliheuristic Perspective," *The Journal of Conflict Resolution* 48, no. 1 (February 2004): 4, JSTOR via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[7] Alex Mintz and Nehemia Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," in *Decisionmaking on War and Peace: The Cognitive-Rational Debate*, eds. Nehemia Geva and Alex Mintz (Boulder, Colorado: Lynne Rienner Publishers, Inc., 1997a): 82.

POLIHEURISTIC THEORY

Proposed by Alex Mintz and Nehemia Geva in the early 1990s, poliheuristic theory assumes that leaders "employ 'poly' (many) heuristics [shortcuts] in a two-stage decision process"[8] in order to "simplify complex foreign policy decisions."[9] Mintz and Geva argue that other decision-making theories focus on "*what* accounts for the behavior of nations" and less on "*how* policymakers actually make decisions." Thus, they argue "research in foreign policy decision-making has often sacrificed process validity in the quest for outcome validity."[10] A benefit of using this model is that it accounts for both. "Poliheuristic theory promises precision in its predictions (outcome validity) as well as greater accuracy in reflecting the manner in which decisions are made (process validity.)"[11] Therefore, this theory "may help shed light on *why* a certain alternative was chosen. Moreover, knowledge of the process may give us insight into political manipulative and framing effects that may have led to a particular decision."[12]

---

[8] Mintz and Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 82; Alex Mintz, "Applied Decision Analysis: Utilizing Poliheuristic Theory to Explain and Predict Foreign Policy and National Security Decisions," *International Studies Perspectives* 6 (February 2005): 94-95, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[9] Alex Mintz et al., "The Effect of Dynamic and Static Choice Sets on Political Decision Making: An Analysis Using the Decision Board Platform," *The American Political Science Review* 91, no. 3 (September 1997b): 554, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/2952074.

[10] Mintz and Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 81.

[11] David J. Brulé, "The Poliheuristic Research Program: An Assessment and Suggestions for further Progress," *International Studies Review* 10, no. 2 (June 2008): 273, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/25481960.

[12] Mintz and Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 82.

According to Alex Mintz,

> at the core of this theory is the assumption that policy makers are confronted with a set of feasible alternatives and a set of contextual dimensions that enter into their calculus of decision-making. Associated with each policy alternative, there are consequences that follow from the pursuit of the alternative.[13]

Poliheuristic theory highlights specific "dimensions" that decisionmakers are presumed to consider in analyzing the nature of the foreign policy situation at hand and their potential options in responding (or not responding). "Dimensions typically [involve] *groups* of similar criteria."[14] The dimensions commonly used in studies about the use of force are political, economic, diplomatic and military.[15] The political dimension concerns domestic politics.[16] Some variables that are used to evaluate this dimension are "public opinion polls, the leader's popularity, the state of the economy, [and] domestic opposition."[17] Domestic politics is seen by poliheuristic theory as frequently the most influential dimension.[18] The economic dimension weighs the cost of carrying out a decision, not only the cost of implementation but also its likely financial and economic impact.[19] The diplomatic dimension highlights the distribution of power and interactions among "major actors on

---

[13] Alex Mintz, "The Decision to Attack Iraq: A Noncompensatory Theory of Decision Making," *The Journal of Conflict Resolution* 37, no. 4 (December, 1993): 595. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/174541.

[14] Ibid., 600.

[15] Mintz and Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 91.

[16] Ibid., 83.

[17] Mintz, "The Decision to Attack Iraq: A Noncompensatory Theory of Decision Making," 600.

[18] Mintz and Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 83.

[19] Kanishkan Sathasivam, "'No Other Choice': Pakistan's Decision to Test the Bomb," in *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making* (New York: Palgrave Macmillan, 2002): 68.

the world stage."[20] The military dimension considers "capabilities, logistics, and the likelihood of success."[21] The order in which the decisionmaker engages the dimensions matters.[22]

During the first stage of the decision-making process, decisionmakers use heuristics or shortcuts in order to quickly and easily eliminate options.[23] Thus, this first stage draws on the cognitive theories of decision-making.[24] "Decision-making models can be broken down according to search patterns."[25] Many theories of decision-making are rooted in economics but poliheuristic theory "is a theory of political decision-making because it specifically postulates that leaders avoid major political loss and that such a loss is noncompensatory for political decisionmakers."[26] Therefore,

> in a choice situation, if a certain alternative is unacceptable on a given dimension (e.g., it is unacceptable politically), then a high score on a given dimension (e.g., the military) *cannot* compensate/counteract for it, and hence the alternative is eliminated.[27]

---

[20] Sathasivam, "'No Other Choice': Pakistan's Decision to Test the Bomb," 65.

[21] Brulé, "The Poliheuristic Research Program: An Assessment and Suggestions for Further Progress," 271.

[22] Mintz and Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 87.

[23] Ibid., 84.

[24] Ibid.

[25] Karl DeRouen Jr., "The Decision Not to Use Force at Dien Bien Phu: A Poliheuristic Perspective," in *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making*, ed. Alex Mintz (New York: Palgrave Macmillan, 2002): 14.

[26] Mintz, "How Do Leaders Make Decisions?: A Poliheuristic Perspective," 7.

[27] Mintz, "The Decision to Attack Iraq: A Noncompensatory Theory of Decision Making," 598.

This is a key difference from rational theories of decision-making which are usually compensatory.[28] Only if alternatives survive the noncompensatory strategy test in the first stage, decisionmakers move to the second stage which draws from rational theories of decision-making.[29]

During the second stage, decisionmakers move from a dimension-based process to an alternative-based process.[30] During the alternative-based process, decisionmakers weigh the remaining options and pick the alternative that results in the least amount of risk and highest gain.[31] Decisionmakers look for "'acceptable' rather than maximizing alternatives because it allows the possibility that not all dimensions will be considered before a decision is made."[32] This is another difference from other foreign policy decision-making theories because a decision is made without considering all of the options.[33] In other words, another characteristic of poliheuristic theory is that it is nonholistic.[34]

Some decisionmakers use a different decision rule to evaluate options.[35] Leaders may create a decision rule "specific to the crisis at hand, which is typically consistent with

---

[28] DeRouen, Jr., "The Decision Not to Use Force at Dien Bien Phu: A Poliheuristic Perspective," 13.

[29] Mintz, "How Do Leaders Make Decisions?: A Poliheuristic Perspective," 4.

[30] Brulé, "The Poliheuristic Research Program: An Assessment and Suggestions for Further Progress," 269.

[31] Mintz and Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 82.

[32] Ibid., 86.

[33] Ibid., 85.

[34] Ibid., 84.

[35] Ibid., 83.

their desire to maintain political power."[36] Unlike other decision-making theories that use one decision rule, in poliheuristic theory, decisionmakers "use a mixture of decision strategies en route to a single choice."[37] This includes strategies that are not always ideal.[38] The alternatives that fail to meet this decision rule are rejected.[39] In summary, during the first stage of the decision-making process of poliheuristic theory, an alternative is rejected and in the second stage an alternative is accepted.[40] Poliheuristic theory can be falsified if the order of the dimensions change or a compensatory strategy is used.[41]

Poliheuristic theory has been applied to several U.S. presidential foreign policy decisions. In "The Influence of Advisers and Decision Strategies on Foreign Policy Choices: President Clinton's Decision to Use Force in Kosovo," Steven B. Redd looks at 'how' President Clinton reached the decision to launch airstrikes and 'why' this was his chosen decision.[42] Redd has authored several pieces about poliheuristic theory. In this article, he uses poliheuristic theory to explain that President Clinton had five options: do

---

[36] David J. Brulé, "Explaining and Forecasting Leaders' Decisions: A Poliheuristic Analysis of the Iran Hostage Rescue Decision," *International Studies Perspectives* 6, no. 1 (February 2005): 110, EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[37] Mintz & Geva, "The Poliheuristic Theory of Foreign Policy Decisionmaking," 83.

[38] Mintz et al., "The Effect of Dynamic and Static Choice Sets on Political Decision Making: An Analysis using the Decision Board Platform," 554.

[39] Brulé, "Explaining and Forecasting Leaders' Decision: A Poliheuristic Analysis of the Iran Hostage Rescue Decision," 105.

[40] Mintz, "Applied Decision Analysis: Utilizing Poliheuristic Theory to Explain and Predict Foreign Policy and National Security Decisions," 96.

[41] Mintz, "How Do Leaders Make Decisions?: A Poliheuristic Perspective," 8.

[42] Steven B. Redd, "The Influence of Advisers and Decision Strategies on Foreign Policy Choices: President Clinton's Decision to Use Force in Kosovo," International Studies Perspectives 6, no. 1 (Feb 2005): 131, http://www.libraries.rutgers.edu/rul/index.shtml.

nothing, wait for the sanctions to play out, allow the U.N. to take the lead, launch airstrikes or send in ground troops.[43] During the first stage of the decision-making process, Redd argues that President Clinton rejected the first three options because of "political costs"[44] and the advice of Secretary Madeline Albright. Redd claims Secretary Albright helped narrow the choice set and was the "primary architect" behind the airstrikes plan.[45] Therefore, Redd said in the second stage, President Clinton went with airstrikes even though they "may not have been the best option for accomplishing the administration's stated goals," because they were politically safer.[46] 65% of the U.S. public was against using ground troops.[47] Thus, this case study illustrated the role of advisers in poliheuristic theory and that sometimes an alternative is chosen even though it may not accomplish the intended goal.

In "Explaining and Forecasting Leaders' Decisions: A Poliheuristic Analysis of the Iran Hostage Rescue Decision," David J. Brulé utilizes poliheuristic theory to propose 8 alternatives that the Carter administration had for dealing with the Iran hostage crisis.[48] Brulé suggests that the decision rule used by the Carter administration was "Is the alternative expected to result in the immediate and safe release of the hostages?"[49] Brulé

---

[43] Redd, "The Influence of Advisers and Decision Strategies on Foreign Policy Choices: President Clinton's Decision to Use Force in Kosovo," 139.

[44] Ibid.,

[45] Ibid., 140.

[46] Ibid.

[47] Ibid.

[48] Brulé, "Explaining and Forecasting Leaders' Decision: A Poliheuristic Analysis of the Iran Hostage Rescue Decision," 103-104.

uses a decision matrix to score these alternatives on a scale from 1 to 8 within each dimension. Brulé argues that although there were some options that worked in favor of U.S. strategic interests, they were rejected during the first stage of the decision-making process because they failed to cater to the political dimension.[50] "Polls suggested that in order to win re-election, Carter had to take action that would result in the safe return of the hostages."[51] During the second stage of the decision-making process, the Carter administration decided to go with the small hostage rescue mission since it had the highest score on the strategic and military dimensions.[52] This case study demonstrated how to use a decision matrix with poliheuristic theory.

In "Framing and the Poliheuristic Theory of Decision: The United Fruit Company and the 1954 U.S.-Led Coup in Guatemala," Michelle M. Taylor-Robinson and Steven B. Redd, use poliheuristic theory to explain President Eisenhower's decision to support a coup in Guatemala in 1954.[53] Taylor-Robinson and Redd argue that President Eisenhower could not afford to do nothing since Eisenhower had campaigned assertively about fighting communism.[54] Furthermore, the United Fruit company aggressively framed the situation

---

[49] Brulé, "Explaining and Forecasting Leaders' Decision: A Poliheuristic Analysis of the Iran Hostage Rescue Decision," 105.

[50] Ibid., 109.

[51] Ibid., 111.

[52] Ibid., 112.

[53] Michelle M. Taylor-Robinson and Steven B. Redd, "Framing and the Poliheuristic Theory of Decision: The United Fruit Company and the 1954 U.S.-Led Coup in Guatemala," in *Cognitive and Rational Theories of Foreign Policy Decision Making* (New York: Palgrave Macmillan, 2002): 78.

[54] Ibid., 94.

in Guatemala as a communist threat to U.S. interests and the U.S. media, U.S. public and government officials believed them.[55]

President Eisenhower had four other options: economic sanctions, diplomacy, or direct or covert intervention.[56] Taylor-Robinson and Redd argue that during the second stage of the decision-making process, the economic and diplomacy choices were eliminated.[57] The U.S. chose covert intervention because it was the preference of Eisenhower's advisers and because covert intervention was cheaper than direct intervention.[58] Thus, this case study illustrated that framing plays an important role in poliheuristic theory.

In "The Decision Not to Use Force at Dien Bien Phu: A Poliheuristic Perspective," Karl DeRouen Jr., another scholar of poliheuristic theory, argues that non-events are rarely discussed in foreign policy decision-making scholarship but they should be discussed because they could broaden decision-making theory.[59] Hence, DeRouen, Jr. used poliheuristic theory to explain that President Eisenhower had three options to help the French in Vietnam: a) invade, b) air strikes or c) the status quo.[60] DeRouen, Jr. argues that since the U.S. public was averse to boots-on-the-ground because of the Korean War, President Eisenhower ruled out invasion during the first stage of the decision-making

---

[55] Taylor-Robinson and Redd, 95.

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] DeRouen Jr., "The Decision Not To Use Force At Dien Bien Phu: A Poliheuristic Perspective," 11.

[60] Ibid., 17.

process.[61] During the second stage of the decision-making process, President Eisenhower ruled out an airstrike because it did not rank high enough on the political dimension even though it ranked high on the military dimension.[62] If a compensatory strategy was used, the airstrike option could have been chosen.[63] Thus, DeRouen, Jr. argues the noncompensatory strategy "provides a viable alternative to the standard realist/rational actor models that tend to explain uses of force purely in terms of international/systemic factors."[64] Furthermore, this case study illustrated that poliheuristic theory "captures *how* domestic politics enter the decision to use force in terms of constraints."[65]

Poliheuristic theory is a suitable theory for analyzing the proposed conditions and deliberations behind the usage of cyberweapons since it reconstructs the decision-making process thereby helping us understand the menu of options and how and why the U.S. chose an alternative. This theory helped uncover noncompensatory considerations when deploying cyberweapons as well as possible decision rules for choosing between the alternatives. Furthermore, these are complex case studies and poliheuristic theory accounted for that with its "multiple players, multiple alternatives, and multiple dimensions."[66] Another advantage of poliheuristic theory is that it accounts for non-events and there were many instances where the U.S. chose not to deploy a cyberweapon.

---

[61] DeRouen Jr., "The Decision Not To Use Force At Dien Bien Phu: A Poliheuristic Perspective," 20.

[62] Ibid., 21.

[63] Ibid., 22.

[64] Ibid., 24.

[65] Ibid.

[66] Mintz, "How Do Leaders Make Decisions?: A Poliheuristic Perspective," 8.

HYPOTHESES

I propose that in order for the U.S. to deploy a cyberweapon in a first strike, there has to be a combination of conditions.

Hypothesis 1: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary.*[67]

Hypothesis 2: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.*[68]

Hypothesis 3: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they believe they can destroy the intended target(s).*

Hypothesis 4: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they cannot use troops, drones*[69] *or airstrikes.*

Hypothesis 5: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.*

---

[67] According to the U.S. Department of Defense, an adversary is "A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged." *Dictionary of Military and Associated Terms*, s.v. "adversary," February 15, 2016, 3, accessed September 19, 2016, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[68] A viable threat is intending to cause major political, military or economic damage to the U.S. or its interests.

[69] A drone is an "unmanned, remote-controlled airplane." The advantage of using a drone was that you could target individuals without boots on the ground. The downside was that it was now easier to wage warfare. Fred Kaplan, "The First Drone Strike," *Slate,* September 14, 2016b, accessed August 12, 2017, http://www.slate.com/articles/news_and_politics/the_next_20/2016/09/a_history_of_the_armed_drone.html.

Hypothesis 6: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."*[70]

METHODOLOGY

The methodology used in prior applications of poliheuristic theory include single case studies which *explained* previous presidential foreign policy decisions and experiments which *predicted* foreign policy decisions. Some of these single cases studies utilized a decision matrix as their research instrument. This dissertation used mixed-methods of comparative case studies, statistical methods, decision matrixes and interviews in order to offer a more robust appraisal of the conditions under which the U.S. will likely deploy an offensive cyberweapon in a first strike. The comparative case studies were helpful in quantitatively analyzing the dimensions delineated by poliheuristic theory as well as crafting decision matrixes that could qualitatively explain the President's past decisions to deploy or not deploy a cyberweapon as a first strike. Additionally, the several decision-making dimensions outlined by poliheuristic theory were helpful in suggesting interview questions to probe the relative importance of different concerns likely to be considered during the decision-making process. This theory also led us to explore the likelihood of a noncompensatory mindset prevailing in the first stage, and in the second stage, the use of a decision rule that subordinated everything else to maintaining decisionmakers' domestic political power.

[70] Barry M. Blechman and Stephen S. Kaplan, *Force without War: U.S. Armed Forces as a Political Instrument* (Washington, D.C.: The Brookings Institution, 1978), 12.

COMPARATIVE CASE STUDIES

All of the 13 case studies analyzed were cases when the U.S. used or debated about using an offensive cyberweapon. The cases were Stuxnet, Iraq (2007), Shotgiant (2007), Quantum (2008), Turbine (2010), Nitro Zeus, Libya (2011), Pakistan (2011), Syria, North Korea (2014), ISIS (2016), Russia (2016), and Iraq (2003). This dissertation is interested mainly in cyberwarfare between the U.S. and other states, not the U.S. and non-state actors, but ISIS is included. This study is also primarily concerned with first-strike deployments by the U.S., not retaliation for an attack, although North Korea's attack on Sony and Russia's hacking of the D.N.C. are included. The time period was from 2001 – 2016. The unit of analysis was the foreign policy decision whether to deploy or not deploy a cyberweapon as a first strike. First, I performed a quantitative analysis of these 13 case studies according to some of the recommendations from Thomas Rid and Ben Buchanan's Q model.[71] Additionally, Brandon Valeriano and Ryan Maness' dataset[72] was used as a guideline for creating this dataset.

QUANTITATIVE VARIABLES

The dummy variables in this study were *Perceived Adversary (Yes or No), Military Sector (Yes or No), Other Alternatives (Yes or No), Conventional Enabler (Yes or No), Collateral Damage (Yes or No), Covert (Yes or No),* and *Deployed (Yes or No.)* The quantitative analysis statistically tested the military and political dimensions delineated by

---

[71] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (December 23, 2014): 34, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[72] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015), 82.

poliheuristic theory. The *Perceived Adversary* and *Collateral Damage* variables applied to the political dimension. The *Military Sector* and *Conventional Enabler* variables applied to the military dimension. The *Other Alternatives* variable applied to both the political and military dimensions.

QUANTITATIVE PROCEDURES

All of the information was culled from public sources such as news articles and technical reports issued by Symantec and Kaspersky Lab. The STATA program was used to perform cluster analysis on these 13 cyberweapons in order to uncover patterns and develop an empirical typology of cyberweapon attacks. Then, I examined the correlates associated with the different types of attacks. These results were then assessed against some of the hypotheses stated above.

DECISION MATRIXES

Next, I created a decision board for each case study in order to assess and compare the alternatives, dimensions and decision rules when the U.S. thought about pre-emptively using a cyberweapon. This information was culled from the government rules of engagement, academic frameworks, leaked N.S.A. documents and news articles discussed in the Literature Review chapter and forthcoming Cyberweapons chapter. These results were then assessed against some of the hypotheses stated above. Finally, I conducted 22 confidential, semi-structured interviews in order to learn more about these cases as well as other thoughts about the decision-making process.

PARTICIPANTS

Using purposive sampling and then snowball sampling, 22 confidential, semi-structured mostly 30-60 minute interviews from four categories of experts and non-experts were conducted to inquire about the conditions for using these weapons. These interviewees were journalists, ex-government officials, cybersecurity specialists and academics. The identities of these interviewees are confidential and in order to address any potential ethical issues concerning the revelation of sensitive information, broad questions with probes were asked. If they were unable to discuss some of the case studies, then they were asked to speak in a speculative manner.

QUALITATIVE VARIABLES

The independent variable in this study is the deployment of cyberweapons and the explanatory dependent variables were: *THREAT, ACCESS, COLLATERAL DAMAGE* and *VIOLENCE.*

INTERVIEW QUESTIONS

These are the basic questions that I asked almost every interviewee.

1. What do you think is the best definition of a *cyberweapon*?

2. Can you think of a situation in which the U.S. might use a cyberweapon as a first strike?

3. Can you think of any other conditions under which the U.S. might use a cyberweapon as a first strike?

4. Can you think of one or more countries (or perceived adversaries) that the U.S. might use a cyberweapon against as a first strike? And why?

5. Against what sort of target or targets might the U.S. use a cyberweapon as a first strike?

6. What are the advantages of using a cyberweapon rather than U.S. troops, special forces, drones or airstrikes? Disadvantages?

7. Do you think other countries in the Five Eyes Alliance would be likely to be informed before the U.S. were to use a cyberweapon in a first strike?

8. Do you think a cyberweapon might be particularly useful as a tool for initiating, sustaining or ending a proxy war?

9. Do you think public opinion polls might factor into the U.S.' decision to use a cyberweapon as a first strike? The current state of the U.S. economy?

10. Is it possible in any meaningful sense to estimate "the cost" of developing a cyberweapon?

11. What role do you think cyberweapons might play in concurrent military operations?

12. Do you think the U.S. has actually used cyberweapons? If so, against whom? In a first strike?

13. What do you think might have been especially noteworthy about the conditions or decision-making involved in these important cases?

a. Stuxnet

b. Libya

c. Syria

d. ISIS

e. Russia's role in the 2016 U.S. presidential election

f. North Korea's attack on Sony

g. Nitro Zeus

h. Quantum

i. Shotgiant

j. Iraq (2003)

k. Turbine

l. Iraq (2007)

m. 2011 raid on Osama bin Laden

14. Whom else do you think it might be useful for me to interview? Would you be so kind as to help me make contact?

QUALITATIVE PROCEDURES

After coding this data and performing a content analysis using the Nvivo software, I compared these findings to the hypotheses stated above, the quantitative findings and the proposed decision matrixes. One of the benefits of doing mixed-methods research is to reinforce or see if there are discrepancies in the results. Next, I updated the proposed decision boards based on these results and assessed accordingly.

LIMITATIONS OF THIS STUDY

There are some limitations to using poliheuristic theory. For instance, poliheuristic theory focuses on the type of decision (whether it is a group or individual) and the decision unit. This dissertation tends to conflate the decision type since the authority to deploy a

cyberweapon rests with the President, but there are almost always others such as USCYBERCOM that are involved. As Redd argues, many foreign policy decisions are made with advice from advisors and bureaucratic actors,[73] yet many studies focus solely on the President. This study also oversimplifies in that fashion. Also, this study does not account for the decision-making process of other countries that conduct joint offensive cyber operations with the U.S.

Another limitation is that since domestic politics is seen by poliheuristic theory as frequently the most influential consideration in the first stage of decision-making, it would appear that other (first-stage) dimensions are thereby often rendered effectively irrelevant. Furthermore, it is not entirely clear when the decisionmaker moves from the first to the second stage of the decision-making process. However, despite these limitations, I think the benefits of using poliheuristic theory outweigh the negatives.

SIGNIFICANCE OF THIS STUDY

Poliheuristic theory is a practical paradigm to analyze the decision-making process behind using a cyberweapon because it addresses both the use and non-use of weapons and both single and group decisions. Additionally, by focusing on a small number of cases and a restricted set of options, we can better understand the conditions behind using a cyberweapon.

As discussed earlier, although this study will focus on deployments, there are many non-events in regards to cyberwarfare, so having a theory that speaks to both events and

[73] Steven B. Redd, "The Influence of Advisers on Foreign Policy Decision Making: An Experimental Study," *The Journal of Conflict Resolution* 46, no. 3 (June 2002): 343, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

non-events is instrumental in understanding the parameters of using these weapons. Another advantage of using poliheuristic theory is that it can be used to analyze all types of decisions.[74] This is useful because some of the cyberweapons are joint operations whereas others are single decisions, or at least, they were not a joint operation with another country. Hence, it is helpful to have a theory that applies to all of these scenarios.

As mentioned earlier, an additional benefit of using this model is that "poliheuristic theory promises precision in its predictions (outcome validity) as well as greater accuracy in reflecting the manner in which decisions are made (process validity.)"[75] Thus, we will be able to better understand why the U.S. is more inclined to deploy a cyberweapon in some situations and refrain in others. "An understanding of why events turned out as they did contributes to better decision-making."[76] This dissertation will apply poliheuristic theory to 13 cases where the U.S. deployed or did not deploy a cyberweapon. These 13 cyberweapons account for operations that have not yet been widely explored in the academic literature such as Shotgiant (2007), Quantum (2008), Turbine (2010), Syria, North Korea (2014), ISIS (2016) and Russia (2016). These cases as well as other U.S. cyberweapons are the subject of the next chapter.

---

[74] Mintz, "How Do Leaders Make Decisions?: A Poliheuristic Perspective," 4.

[75] Brulé, "The Poliheuristic Research Program: An Assessment and Suggestions for further Progress," 273.

[76] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, N.J: Princeton University Press, 1976), 227.

Chapter 4

MISSION: ZERO DAY

"The most dramatic field test in history of a new weapon in America's arsenal." [1]

-David Sanger

In 1999, the U.S. pondered about destroying Yugoslavia's financial systems and Slobodan Milosevic's bank account however, they refrained out of concern for the legal parameters of such an attack.[2] Thus, after NATO launched airstrikes against Yugoslavia, the U.S. infiltrated Yugoslavia's air defense systems with false images.[3] "The military has never before penetrated an enemy computer system and manipulated it to protect an attacking force, in this case NATO aircraft."[4] However, the impact of these attacks were hard to decipher since NATO was simultaneously conducting airstrikes against Yugoslavia.[5] Nevertheless, Yugoslavia was labeled by some as "the first Internet war."[6]

---

[1] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012a), 190.

[2] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (Virginia: Cyber Conflict Studies Association, 2013a), 141.

[3] David A. Fulghum, "Kosovo Conflict Spurred New Airborne Technology Use," *Aviation Week & Technology* 151, no. 9 (1999): 31, http://www.libraries.rutgers.edu/rul/index.shtml.

[3] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The Rusi Journal* 157, no. 1 (February 29, 2012c): 6, http://www.libraries.rutgers.edu/rul/index.shtml.

[4] Fulghum, 31.

[5] William M. Arkin, "The Cyber Bomb in Yugoslavia," *The Washington Post,* October 25, 1999, accessed November 18, 2016, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

[6] Ashley Dunn, "Battle Spilling Over Onto the Internet," *Los Angeles Times,* April 3, 1999, accessed November 29, 2016, http://articles.latimes.com/1999/apr/03/news/mn-23851.

Another article proclaimed "Offensive computer warfare," "was first used as a precision weapon during the Kosovo conflict."[7] (There were some patriotic hackers targeting the U.S. and NATO.[8]) U.S. Air Force General John Jumper said the offensive cyber operation against Yugoslavia 'points our way toward a future that has to do with both ground-and space-based assets.'[9] However, if Yugoslavia was the first cyberwar[10] this declaration contradicts those scholars who proclaimed the 2007 conflict between Estonia and Russia as the first cyberwar.[11] Furthermore, suggestions that "Yugoslavia merely stands as another demonstration that computer network attack will eventually become an integral part of the way warfare is waged"[12] are misleading because this statement indicates that there are prior (unknown) examples of using computer network attacks in this manner.

Well, in 1994, President Clinton sanctioned the exploitation of Haitian computers as a part of Operation Uphold Democracy.[13] Fred Kaplan said the Serbia plan was similar to the Haiti plan developed by the Air Force Information Warfare Center in 1994 where the U.S. wanted to jam Haiti's phones before launching an (aborted) air campaign.[14] "The

---

[7] Fulghum, 31.

[8] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, 138.

[9] Fulghum, 31.

[10] Healey says the media labeled Yugoslavia a cyberwar referring to propaganda. Healey, *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, 139.

[11] Rid and McBurney, "Cyber-Weapons," 5; Thomas Rid and John Arquilla, "Think Again: Cyberwar," *Foreign Policy* (March/April, 2012b): 84-85, http://www.jstor.org/stable/23237859.

[12] Arkin, "The Cyber Bomb in Yugoslavia."

[13] Ibid.

[14] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016a), 161.

Serbian and Haitian campaigns were classic cases of information warfare in the pre-digital age, when the armed forces of many nations ran communications through commercial phone lines."[15] A 1999 article said ever since the Haiti operation "a number of 'relatively low key' computer exploitations have accompanied other peacekeeping operations. Many of these have been little more than high-tech intelligence collection missions."[16] It is interesting that this was described as exploitation. "The Joint Staff office of 'special technical operations' prepared 'approval packages' for the Secretary of Defense and the President, but the 'process took so long the operations were overtaken by events and we didn't engage in them.'"[17] As we will see in Chapter 7, this may still be true today.

Kaplan claimed "Haiti and the Balkans were experiments in *proto*-cyber warfare; Operation Orchard and the roundup of jihadists in Iraq marked the start of the real thing."[18] Operation Orchard was discussed in the previous chapter and the Iraq (2007) operation will be discussed below. I did not include Yugoslavia or Haiti as case studies in this dissertation because I decided to look at U.S. cyberweapons from 2001 – 2016. My reasons for choosing this timeframe are explained below.

In 2013, Der Spiegel published a 50-page catalogue, leaked by Edward Snowden, of N.S.A. tools that could be purchased by T.A.O. in order to infiltrate equipment and computers and alter data.[19] Those who created these 'implants' were called ANT,

---

[15] Kaplan, *Dark Territory: The Secret History of Cyber War*, 161.

[16] Arkin, "The Cyber Bomb in Yugoslavia."

[17] Ibid.

[18] Kaplan, *Dark Territory: The Secret History of Cyber War*, 161.

[19] Jacob Appelbaum, Judith Horchert and Christian Stöcker, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox," *Spiegel Online International,* December 29, 2013, accessed

(Advanced or Access Network Technology) and were compared to Q, James Bond's inventor.[20] Kaspersky Lab analyzed the catalogue and discovered that there were six families of 'implants' (N.S.A. language) that date back to 2001.[21] Many of these tools were for exploitation purposes but Stuxnet was the first test of this hardware.[22] This indicates that perhaps there are different levels of cyberweapons.

This dissertation adopted Thomas Rid and Peter McBurney's definition of a cyberweapon as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[23] These codes "may quietly 'listen' for a special command sent through the Internet from a remote source, instructing it to begin activation of malicious program instructions."[24] These types of malicious code are worms, viruses, Trojan horses and botnets. Worms find and "automatically install themselves" on all of the computers that

---

May 26, 2016, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html; "The NSA's Spy Catalog," *Der Spiegel,* December 30, 2013, accessed November 2, 2016, http://www.spiegel.de/international/world/a-941262.html.

[20] Spiegel Staff, "Inside T.A.O: Documents Reveal Top NSA Hacking Unit," *Spiegel Online International,* December 29, 2013, accessed November 2, 2016, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html.

[21] Kevin Poulsen, "Surprise! America Already has a Manhattan Project for Developing Cyber Attacks," *Wired,* February 18, 2015, accessed June 1, 2016, https://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/.

[22] David E. Sanger and Thom Shanker, "N.S.A. Devises Radio Pathway Into Computers," *The New York Times,* January 14, 2014f, accessed January 28, 2015, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html.

[23] Rid and McBurney, "Cyber-Weapons," 7.

[24] Library of Congress, Congressional Research Service, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, by Clay Wilson, RL32114 (October 17, 2003), 29, accessed April 2, 2014, fas.org/irp/crs/RL32114.pdf.

have a specific flaw.[25] A virus "corrupts data or causes a malfunction."[26] A Trojan horse "secretly displaces the functions of an existing trusted program on the computer."[27] Botnets are a large amount of infected computers that "can be remotely-controlled through commands sent via the Internet."[28]

Unlike the Iranians and Stuxnet, the Russians impugned the 1982 Soviet-C.I.A. incident.[29] 'The Farewell dossier' was a collection of clandestine Soviet documents that showed the Russians were secretly purchasing equipment to keep their military on par with that of the United States.[30] A K.G.B. officer gave these documents to the French who passed them on to the Americans.[31] At the top of the list was software for the new trans-Siberian pipeline.[32] Since the Soviets were unable to purchase this technology, they decided to steal it from the Canadians.[33] Little did they know that the C.I.A. implanted a

---

[25] Library of Congress, Congressional Research Service, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, by Clay Wilson, 28.

[26] Ibid.

[27] Ibid.

[28] Library of Congress, Congressional Research Service, *Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, by Clay Wilson, RL32114, (January 29, 2008), 4, accessed April 2, 2014, fas.org/sgp/crs/terror/RL32114.pdf.

[29] Anatoly Medetsky, "KGB Veteran Denies CIA Caused '82 Blast," *The Moscow Times,* March 18, 2004, accessed November 28, 2016, World Sources Online via Rutgers Universities Libraries, http://infoweb.newsbank.com/resources/doc/nb/news/1016B69A2902F371?p=AWNB.

[30] William Safire, "The Farewell Dossier," *The New York Times,* February 2, 2004, accessed June 4, 2016, http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html.

[31] Ibid

[32] Ibid.

[33] Ibid.

'Trojan horse' into the software in order to adjust the valve settings and pump speeds.[34] "The result was the most monumental non-nuclear explosion and fire ever seen from space."[35] Not much is known about this June 1982 explosion since it happened in the middle of nowhere in Siberia and the Soviets have not admitted that the software they stole literally blew up in their faces.[36] Thus, this event was not included as a case study in this dissertation.

In 2013, the U.S. Air Force proclaimed that they had six new cyberweapons, though few details were provided.[37] An anonymous U.S. official was quoted as saying "The United States is moving toward the use of tools short of traditional weapons that are unattributable — that cannot be easily tied to the attacker — to convince an adversary to change their behavior at a strategic level."[38] This chapter will discuss 13 cases that adhered to Rid & McBurney's definition of a cyberweapon. The cases were Iraq (2003), Stuxnet, Iraq (2007), Shotgiant (2007), Quantum (2008), Turbine (2010), Nitro Zeus, Libya (2011), Pakistan (2011), Syria, North Korea (2014), ISIS (2016), and Russia (2016). This chapter will also briefly discuss other cyberattacks that were mislabeled as cyberweapons.

---

[34] Safire, "The Farewell Dossier."

[35] Ibid.

[36] Ibid.

[37] Andrea Shalal-Esa, "Six US Air Force Cyber Capabilities Designated "Weapons"" *Reuters,* April 8, 2013, accessed November 16, 2016, http://www.reuters.com/article/net-us-cyber-airforce-weapons-idUSBRE93801B20130409.

[38] Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," *The Washington Post,* August 30, 2013, accessed March 22, 2016, https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

IRAQ (2003)

Before invading Iraq on March 19, 2003 to oust Saddam Hussein for his alleged weapons of mass destruction[39] and alleged connections to 9/11,[40] the U.S. thought about using an offensive cyberattack to obliterate Saddam Hussein's finances and Iraq's financial system.[41] "It would have been the most far-reaching case of computer sabotage in history."[42] But the Bush administration refrained out of concern for the potential financial repercussions which could also affect the U.S.[43] In this case, spillover and blowback mattered[44] even though the U.S. ended up using kinetic force against Iraq's infrastructure.[45] (This is similar to the concerns raised over the Yugoslavia operation in 1999.) So the U.S. destroyed communications systems and used cyberattacks to jam telephones.[46] The U.S. also notified international companies that delivered communications services to Iraq that the U.S. could be disrupting their service and asked these companies to suspend service.[47]

---

[39] David E. Sanger and with John F. Burns, "Bush Orders Start of War on Iraq; Missiles Said to Be Aimed at Hussein," *The New York Times,* March 19, 2003, accessed December 11, 2016, http://www.nytimes.com/2003/03/19/international/bush-orders-start-of-war-on-iraq-missiles-said-to-be-aimed-at.html.

[40] Linda Feldmann, "The Impact of Bush Linking 9/11 and Iraq," *The Christian Science Monitor,* March 14, 2003, accessed December 11, 2016, http://www.csmonitor.com/2003/0314/p02s01-woiq.html.

[41] John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New York Times,* August 1, 2009, accessed July 5, 2016, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

So these cyberattacks disrupted service and "that limited damage was deemed acceptable by the Bush administration."[48] It is unclear if the cyberattacks blew up communication systems or were an indirect effect. According to the Tallinn Manual, "a particular type of cyber operation designed to interfere with the enemy's capability to communicate may not qualify as an attack."[49] However, I decided to list the operation to obliterate Saddam Hussein's finances as a possible cyberweapon. This classification goes against prevailing wisdom since other scholars do not think this is a cyberweapon. According to the 2009 *New York Times* article that discussed this operation as well as others that were considered and some implemented, the U.S. remains 'deeply concerned about the second-and third-order effects of certain types of computer network operations, as well as about laws of war that require attacks be proportional to the threat.'[50] This dissertation does not distinguish between direct and indirect effects. Additionally, cyber scholar John Arquilla was quoted as saying that cyberwarriors were restrained by stringent rules of engagement because "'Policy makers are tremendously sensitive to collateral damage by virtual weapons, but not nearly sensitive enough to damage by kinetic' — conventional — 'weapons.'"[51] I think this was definitely the case when it came to Bush's decision not to use a cyberattack against Iraq's financial system in 2003.

---

[47] Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk."

[48] Ibid.

[49] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2009), 142, accessed February 27, 2016, https://ccdcoe.org/tallinn-manual.html.

[50] Ibid.

[51] Ibid.

STUXNET

On June 17, 2010, VirusBlokAda, a computer security firm in Belarus, unearthed a computer worm[52] that would later be named Stuxnet (based on words found in the code),[53] after the Iranians reached out to them for help in identifying why their machines kept rebooting.[54] Stuxnet entered via a USB drive that when plugged into a PC, a Windows file (.LNK) populated the icons that depicted the data stored on that drive.[55] However, this USB drive had an exploit embedded onto it so when the .LNK file tried to populate the icons, Stuxnet sneakily downloaded itself onto the computer.[56] Stuxnet's creators had used a zero-day.[57] (This zero-day was not used in all versions of Stuxnet.)[58]

The researchers discovered that Stuxnet also used a stolen digital certificate from Realtek to install a rootkit.[59] Digital certificates are the little windows that pop up informing

---

[52] Kupreev Oleg and Ulasen Sergey, *Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.gen.2 Review*, (VirusBlokAda, June 17, 2010), accessed March 20, 2014, ftp://antivirus.by/pub/docs/english/Rootkit.TmpHider_en.pdf.

[53] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American* Power, 205.

[54] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown Publishers, 2014a), 7.

[55] Ibid., 9.

[56] Ibid., 10.

[57] Ibid.

[58] Nicolas Falliere, Liam O'Murchu and Eric Chien, *W32.Stuxnet Dossier*, (Symantec, February 2011), 31, accessed March 3, 2016, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[59] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (August 2013): 382, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

you that what you are about to install may not have been approved by the company who made your computer.[60] A rootkit is software that obtains and sustains access to a machine without being detected.[61] Thus, there was no pop-up warning that a rootkit was about to be installed. While people have used fake certificates in the past, this was the first time a certificate was stolen, which made it a very big deal.[62] Realtek revoked the certificate on July 16, 2010, but the next day, Stuxnet had a new stolen digital certificate; this time from JMicron, which was also subsequently revoked on July 22, 2010.[63] Upon digging further, the researchers at VirusBlokAda noticed that Stuxnet had a self-imposed deadline of June 24, 2012 and after that, the worm would terminate itself.[64]

But it was unclear what Stuxnet was doing and who the target was so VirusBlokAda published their findings and Frank Boldewin, a security specialist, concluded that Stuxnet was targeting Siemens supervisory control and data acquisition systems (SCADA) for espionage purposes.[65] SCADA computers are a type of industrial control system (ICS) that

> monitor and regulate the operations of most critical infrastructure industries (such as the companies that manage the power grid.) These SCADA computers automatically monitor and adjust switching, manufacturing, and other process control activities, based on digitized feedback data gathered by sensors. These

---

[60] "Symantec Code Signing Certificates," *Symantec,* accessed May 28, 2016, https://www.symantec.com/code-signing/.

[61] *Rootkits*, (Symantec Security Response), 2, accessed May 28, 2016, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/rootkits.pdf.

[62] Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair,* March 2, 2011, accessed May 20, 2014, http://www.vanityfair.com/news/2011/03/stuxnet-201104.

[63] *W32.Stuxnet Dossier*, 4.

[64] Ibid., 18.

[65] Frank Boldewin, "Rootkit.TmpHider," *Wilders Security Forums* (blog)*,* July 14, 2010, accessed June 18, 2016, http://www.wilderssecurity.com/threads/rootkit-tmphider.276994/#post-1712134.

> control systems are often placed in remote locations, are frequently unmanned, and are accessed only periodically by engineers or technical staff via telecommunications links.[66]

Stuxnet was a part of a top-secret program called Olympic Games conceived by General James E. Cartwright and a few other intelligence officials[67] that began in 2006 during the Bush administration with the purpose of destroying Iranian centrifuges and deterring the Israelis from launching an airstrike in Iran.[68] Stuxnet was Bush's 'third option' as the Israelis were growing impatient that Iran was about to join the nuclear club thereby threatening their existence as well as regional stability.[69] Upon learning about Iran's secret nuclear facility near Qom in September 2009, Prime Minister Gordon Brown said, "the international community has no choice today but to draw a line in the sand."[70] The U.S. decided 'to throw a little sand in the gears,'[71] or rather, a worm.

---

[66] Library of Congress, Congressional Research Service, *Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, by Clay Wilson, RL32114, (January 29, 2008), 18, accessed April 2, 2014, fas.org/sgp/crs/terror/RL32114.pdf.

[67] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* June 1, 2012b, accessed March 17, 2014, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all. President Bush approved $300 million for covert operations targeting Iran. Stuxnet was the priority. Ewen MacAskill, "Stuxnet Cyberworm Heads Off US Strike on Iran," *The Guardian,* January 16, 2011, accessed August 12, 2017, https://www.theguardian.com/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran.

[68] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American* Power, 188-191.

[69] Ibid., 190-191.

[70] Gordon Brown, "Statements By President Obama French President Sarkozy And British Prime Minister Brown On Iranian Nuclear Facility," September 25, 2009, accessed June 25, 2016, *The White House,* https://www.whitehouse.gov/the-press-office/2009/09/25/statements-president-obama-french-president-sarkozy-and-british-prime-mi.

[71] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American* Power, 192.

The U.S. government spent 8 months developing the plan. They also conversed with lawyers in order to guarantee that they were adhering to the Law of Armed Conflict. "The cyberattack had to be as accurate as the best guided missile- it couldn't take out hospitals or schools; it had to be focused on Iran's centrifuge plants. It had to be stealthy, leaving no 'fingerprints.' And somehow, it had to get inside the heavily guarded Natanz facility."[72] Natanz was Iran's large enrichment facility that was discovered in 2003.[73] The concern was that the 4,000-5,000 centrifuges at Natanz that were producing low-grade enriched uranium, could also produce highly enriched uranium for nuclear weapons.[74] In order to enrich uranium at these levels, the centrifuges are grouped into 164 machines, also called a cascade.[75] The U.S. and Israel were concerned that the Iranians had secret centrifuges thus; Stuxnet was skillfully designed to target all centrifuges.[76] The U.S. developed a 'beacon' that once inserted, would 'phone home' information about the configuration and operations of Natanz[77] through command-and-control servers in

---

[72] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American* Power, 193.

[73] Ibid., 154. "In 2009, Iran developed the capability to obtain high-enriched uranium (HEU) through the gas centrifuge enrichment process at the Natanz facility. HEU is considered a weapons-grade uranium, which is enriched to a point where it consists of 80 percent of the U-235 isotope. Commercial nuclear power reactors only require LEU, which is enriched to only 20 percent of U-235." Healey, *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, 215.

[74] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February - March 2011): 25, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[75] Ivanka Barzashka, "Are Cyber-Weapons Effective?," *The Rusi Journal* 158, no. 2 (April 28, 2013): 52, http://www.libraries.rutgers.edu/rul/index.shtml.

[76] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 25.

[77] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 215.

Malaysia and Denmark.[78] Once the beacon started phoning home with the information, the N.S.A. began coding the 'bug' as they called it. [79] About 30 people wrote the script.[80] Unit 8200 (Israel's N.S.A.) worked on later versions.[81] Due to the technical skills and knowledge required, as well as clues found in the code, many experts attributed the attack to the U.S. and Israel.

Next, the U.S. gathered old P1 centrifuges from the Oak Ridge National Laboratory in Tennessee who was holding the centrifuges for the I.A.E.A. who had recovered them from Muhammad Qaddafi after he abandoned his nuclear weapons program.[82] The U.S. used these centrifuges to test Stuxnet at Oak Ridge National Laboratory.[83] "Only when Bush saw the remnants of a destroyed centrifuge was he convinced the program could work."[84] Stuxnet was also tested at Dimona in Israel, the home of Israel's alleged nuclear

---

[78] Gross, "A Declaration of Cyber-War."

[79] Ibid.

[80] Alexis C. Madrigal, "The Stuxnet Worm? More Than 30 People Built It," *The Atlantic,* November 4, 2010, accessed June 11, 2016, http://www.theatlantic.com/technology/archive/2010/11/the-stuxnet-worm-more-than-30-people-built-it/66156/.

[81] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 195.

[82] Ibid., 197.

[83] Ibid., 198. In 2008, the National Laboratory worked with Siemens to detect vulnerabilities in their SCADA systems. William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times,* January 15, 2011, accessed April 18, 2016, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. Ironically, this is what Stuxnet took advantage of.

[84] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 197.

program.[85] However, in his excellent article, "A Declaration of Cyber War," *Vanity Fair* reporter Michael Joseph Gross refutes this piece of reporting claiming that when he questioned the Israeli official who allegedly provided this information to *The New York Times*, the official claimed, "that information was secondhand."[86] Thus, it is unclear if Stuxnet was tested at Dimona.

When Barack Obama came into office in 2009, he continued the program (after it went through a thorough presidential finding) but President Obama was more concerned about collateral damage and that the program remained covert.[87]

> The architects of Olympic Games would meet him in the Situation Room, often with what they called the 'horse blanket,' a giant foldout schematic diagram of Iran's nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously. [88]

Since Stuxnet was phoning home information about its path, experts were able to "reverse-engineer" the digital trail that it left behind. Reverse-engineering is when you translate computer language (ones and zeros) back to programming language.[89] Many security companies examined Stuxnet but Symantec is the one who issued an in-depth report based on the March 2010 version of Stuxnet.[90]

---

[85] Broad, Markoff and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[86] Gross, "A Declaration of Cyber-War."

[87] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American* Power, 202- 203.

[88] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[89] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 119.

[90] *W32.Stuxnet Dossier*, 53.

Symantec discovered three variants of Stuxnet compiled on June 22, 2009, March 1, 2010 and April 14, 2010.[91] Gross said these dates coincided with events in Iran at that time. Thus, Gross argues that Stuxnet "was deliberately paced and may have been coordinated with diplomatic and economic pressures to slow the progress of Iran's nuclear program."[92] For instance, the June 2009 attack appeared during the Green Revolution in Iran when Iranians protested what they viewed as the rigged election of Mahmoud Ahmadinejad.[93] For all the resources that go into developing these weapons, "only about twelve hours had passed between the time the worm was compiled and when it struck its first victim" on June 22, 2009.[94]

The second version of Stuxnet was created on March 1, 2010 but struck on March 23, 2010.[95] This version followed the I.A.E.A.'s February 2010 claim that Iran was in fact seeking a nuclear weapon[96] thereby confirming the U.S. and Israel's long-held suspicions. Stuxnet was updated to spread via a USB drive.[97] In order to get inside, the U.S. worked

---

[91] *W32.Stuxnet Dossier*, 53. The Iranians reported 5 versions of Stuxnet. Laurent Maillard, "Iran's Nuclear Agency Hit by Computer Worm," *The Sydney Morning Herald,* September 27, 2010, accessed July 2, 2016, http://www.smh.com.au/technology/iran-denies-nuclear-plant-computers-hit-by-worm-20100926-15sam.html. If strategies evolve from their original plans, that can provide some insight as to shifting conditions. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (December 23, 2014): 23, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[92] Gross, "A Declaration of Cyber-War."

[93] Ibid.

[94] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 350.

[95] Ibid.

[96] Gross, "A Declaration of Cyber-War."

[97] Ibid.

with Mossad (Israeli intelligence) who had informants throughout Iran.[98] Jordan was also mentioned as possibly providing a conduit to the contacts who could have walked in the USB drive.[99] Symantec's updated report claimed that Stuxnet infiltrated five industrial facilities that do business with Natanz in the hopes that the workers at these industries would unknowingly sneak the worm into Natanz.[100] Some have dubbed these third parties "unwitting data mules" referring to drug mules.[101]

A third version appeared on April 14, 2010. Infections appeared 12 days after it was compiled.[102] This version surfaced after Iran proclaimed that they were building another uranium enrichment facility.[103] However, Symantec said there were no significant differences between the second and third versions of Stuxnet.[104]

Symantec also discovered three more zero-days ("a Windows keyboard file to gain escalated privileges on the machine"), "a vulnerability in the Windows print-spooler function to spread between machines that shared a printer" and then another affecting the WinCC/Step 7 program that hijacks the login information of the host computer that

---

[98] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 195.

[99] Gross, "A Declaration of Cyber-War."

[100] John Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says," *The New York Times,* February 11, 2011, accessed May 21, 2016, http://www.nytimes.com/2011/02/13/science/13stuxnet.html; Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 351- 352.

[101] Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle."

[102] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 350.

[103] Gross, "A Declaration of Cyber-War."

[104] *W32.Stuxnet Dossier*, 53.

contains this program.[105] Since this is a shared program, anyone who accesses the Step 7 software, would also access Stuxnet.[106] Symantec announced their findings on August 6, 2010.[107] Once Stuxnet was inside, it sought out Programmable Logic Controllers (PLC),[108] which "is an industrial computer control system that continuously monitors the state of input devices and makes decisions based upon a custom program to control the state of output devices."[109] Since these PLCs are air-gapped, Stuxnet used a zero-day vulnerability in the Step 7 software.[110] When Stuxnet found its target, it would alter the code on the PLC.[111] Symantec was still unsure of what exactly was happening to the PLC when industrial control systems expert, Ralph Langner, read Symantec's report, conducted his own tests and concluded that Stuxnet was sabotaging the nuclear facility at Bushehr.[112] "Welcome to cyberwar," Ralph Langner declared.[113] (Gross points out that Langner was

---

[105] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 90-91.

[106] Ibid., 91.

[107] *W32.Stuxnet Dossier*, 4.

[108] Ibid., 3.

[109] "What is a PLC?," *Advanced Micro Controls Inc.,* accessed May 28, 2016, https://www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/.

[110] *W32.Stuxnet Dossier*, 3.

[111] Ibid.

[112] Ralph Langner, "Stuxnet logbook, Sep 16 2010, 1200 hours MESZ," *Langner* (blog), September 16, 2010, accessed June 12, 2016, http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/#more-217.

[113] Ibid.

the only technical source cited in The New York Times' article[114] even though centrifuges are not Langner's area of expertise.)[115] Langner was partially right. Another security specialist, Frank Reiger concluded it was actually the Natanz facility.[116]

Symantec still did not have the proof they needed to connect the dots so they kept at it and with the help of a Dutch programmer, in November 2010 they got the last piece of the puzzle to finally crack the payload. The Dutch programmer pointed out that each component has a manufacturer ID number.[117] That number matched the mysterious numbers Symantec found in Stuxnet's code.[118] Symantec deduced that Stuxnet was targeting both Iranian and Finnish frequency converters.[119] Stuxnet targeted the Finnish converter in order to adjust the speed of the centrifuges.[120] Stuxnet sought centrifuges that were spinning between 807Hz – 1210Hz.[121] Once it found its target, Stuxnet unleashed its payload, waited about 13 days and then increased the speed to 1410Hz for 15 minutes.[122] Then after 27 days, Stuxnet decreased the speed to 2Hz for 50 minutes and then back to

---

[114] Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[115] Gross, "A Declaration of Cyber-War."

[116] Frank Reiger, "Stuxnet: targeting the Iranian enrichment centrifuges in Natanz?," *Knowledge Brings Fear* (blog), September 22, 2010, accessed June 18, 2016, http://frank.geekheim.de/?p=1189.

[117] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 232.

[118] Ibid., 233.

[119] Ibid.

[120] Ibid., 234.

[121] *W32.Stuxnet Dossier*, 41.

[122] Ibid., 42- 44.

1064Hz.[123] After 27 days, it repeated this sequence.[124] By adjusting the speeds, the machines would blow up or malfunction[125] and decrease enrichment production by half.[126] "In uranium enrichment, centrifuges need to spin consistently at high speed to separate the U-235 and U-238 isotopes in the gas."[127] U-235 is needed to make nuclear fuel. Symantec did not know what was happening to the second converter besides something being turned on and off.[128] So Symantec published their findings on November 23, 2011.

David Albright at the Institute for Science and International Security read Symantec's report and eventually concluded that the Iranian converters were responsible for regulating valves.[129] The valves regulated the amount of gas that goes in and out of a centrifuge so if there was a problem, the glitch would be isolated instead of spreading to nearby centrifuges.[130] Stuxnet was trying to alter these valves in order to destroy centrifuges.[131]

---

[123] *W32.Stuxnet Dossier*, 42-44.

[124] Ibid.

[125] Ibid., 43.

[126] Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, 343.

[127] Ibid.

[128] Ibid., 246.

[129] Ibid.

[130] David Albright, Paul Brannan and Christina Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, (Institute for Science and Technology, February 15, 2011), 1, accessed May 27, 2016b, http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8.

[131] Not a lot is known about this second attack because some of the code is still missing. *W32.Stuxnet Dossier*, 45.

Sanger compares what happened next to the scene in *Ocean's Eleven* where the team switches out the security footage monitoring the safe so it seemed like everything was okay when it reality, the thieves were emptying the safe.[132] Stuxnet was telling the operators that everything was fine but in reality, centrifuges were blowing up.[133] This is called a 'man-in-the-middle.'[134] A man-in-the-middle tactic is when "an attacker is able to read, insert, and modify messages between two users or systems."[135] 'This may have been the most brilliant part of the code' because the Iranians had no idea what was going on and started to lose confidence in their abilities, which was another point of the operation.[136] Thus, Langner says Stuxnet had a 'dual warhead.'[137]

In June 2010, when an Iranian scientist hooked up his laptop to the machines at Natanz and then plugged it back into the Internet, Stuxnet failed to realize that it was in a different environment so the worm inadvertently leaked out to the world.[138] The U.S. and Israelis were planning on taking out a huge amount of centrifuges.[139] According to *Zero*

---

[132] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 199.

[133] Ibid.

[134] Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[135] "Man-in-the-middle attack," *Symantec Glossary,* accessed November 29, 2016, https://www.symantec.com/security_response/glossary/define.jsp?letter=m&word=man-in-the-middle-attack.

[136] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 199.

[137] Ibid., 206.

[138] Ibid., 204.

[139] Ibid.

Days the N.S.A. believed Stuxnet remained hidden until the Israelis grew impatient that there was not enough damage and thus, altered the worm without the N.S.A. knowing.[140] However, Kim Zetter offers a different account in her book *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Zetter says Stuxnet originated in Iranian companies that were working with Natanz as opposed to originating from inside Natanz.[141] Symantec concluded "that Stuxnet did not escape from Natanz to infect outside companies but instead spread into Natanz."[142] Gross quotes a former C.I.A. official who claims Stuxnet may have been "dropped" since it was not as successful as some had hoped.[143] This official said the Iranians could have used Stuxnet as psychological warfare to appease the West and claim that Stuxnet worked when in fact, it did not but instead, the Iranians denied any damages.[144] These are all conflicting accounts but the fact of the matter is, Stuxnet spread to 100,000 computers worldwide.[145] Regardless if Stuxnet was intentionally or accidentally leaked, or destroyed 984 or 1,000 centrifuges, Stuxnet is a cyberweapon since it resulted in physical damage.

---

[140] *Zero Days*, Screening Harvard University, Cambridge, Massachusetts, April 29, 2016 (2016; Magnolia Pictures, 2016).

[141] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 351.

[142] Liam O'Murchu, "Countdown to Zero Day—Did Stuxnet escape from Natanz?," *Symantec* (blog), November 11, 2014, accessed, July 5, 2016, http://www.symantec.com/connect/blogs/countdown-zero-day-did-stuxnet-escape-natanz.

[143] Gross, "A Declaration of Cyber-War."

[144] Ibid.

[145] *W32.Stuxnet Dossier*, 6.

Obama decided to speed up Stuxnet anyway even after it was revealed.[146] "It is increasingly accepted that, in late 2009 or early 2010, Stuxnet destroyed about 1,000 IR-1 centrifuges out of about 9,000 deployed at the site."[147] Or more specifically, 984 centrifuges, or 6 cascades.[148] Many claimed that "Stuxnet set back the Iranian nuclear program by two years; a simultaneous catastrophic destruction of all operating centrifuges wouldn't have caused nearly as big a delay."[149] However, many scholars compare Stuxnet to the notion of a 'Pyrrhic victory' where what can seem like a success can "ultimately sow the seeds of defeat" because although Stuxnet caused significant damage, it could also start an arms race.[150] As we will see later, many other "weapons" were discovered soon after.

According to Sanger, this was "the most dramatic field test in history of a new weapon in America's arsenal."[151] "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction," said Michael D. Hayden, ex- C.I.A. chief.[152] 'Somebody has crossed the Rubicon,' he added, 'in one sense at least, it's August

---

[146] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[147] Albright, Brannan, and Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, 1.

[148] Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[149] Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy,* November 19, 2013, accessed June 18, 2016, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

[150] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 156 – 157; Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 270.

[151] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 190.

[152] Ibid., 200.

1945.'[153] While industrial control systems have been attacked in the past, Stuxnet executed the payload on its own "without someone's fingers on a keyboard somewhere, pulling the virtual trigger."[154] Thus, Stuxnet was not a force multiplier. In fact, Langner argues that Stuxnet has "made analog warfare look low-tech, brutal, and *so 20th century*."[155] Langner also touts American might. "If another country — maybe even an adversary — had been first in demonstrating proficiency in the digital domain, it would have been nothing short of another Sputnik moment in U.S. history."[156] Many declared Stuxnet the world's first cyberweapon.

There is a lot of discrepancy however, about the process, effects and implications of Stuxnet. Singer and Friedman claimed Stuxnet was an ideal demonstration of "how ethics can be applied to cyberwar"[157] since Stuxnet adhered to proportionality by limiting its targets and Stuxnet did not kill anyone however; Stuxnet was "indiscriminant" since it spread beyond Iran.[158]

Albright et al. point out that we do not know for sure if Natanz was using these two types of converters since the I.A.E.A. has never been allowed to see Natanz's control

---

[153] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 200.

[154] Gross, "A Declaration of Cyber-War."

[155] Langner, "Stuxnet's Secret Twin."

[156] Ibid.

[157] Singer and Friedman, 118.

[158] Ibid., 119.

equipment.[159] Second, Albright et al. also disputed the speed, which is key to destruction.[160] Third, it is unclear if these damaged centrifuges were a routine swap due to regular failure and if not, then why did Stuxnet not destroy more centrifuges?[161] Fourth, Gross claims it is odd that VirusAdBloka, an unknown computer security company was able to find Stuxnet and that no other country complained about rebooting.[162] However, it is not strange that VirusAdBloka found Stuxnet because the Iranians did not trust anyone, especially the West and many of the big security companies, such as Symantec, are Western corporations. Fifth, "Stuxnet did not lower the production of LEU [low enriched uranium] during 2010."[163] While the world was patting itself on the back over the "success" of Stuxnet, the Iranians were quietly producing better highly enriched uranium and updating their centrifuges.[164]

As previously noted, the revelation of Stuxnet demonstrated how to build a cyberweapon. This point coincides with the asymmetry argument discussed in Chapter 1 that says these weapons place weaker states on an equal footing with more powerful

---

[159] David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, (Institute for Science and Technology, December 22, 2010), 5, accessed May 27, 2016a, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

[160] Ibid.

[161] Barzashka, 53.

[162] Gross, "A Declaration of Cyber-War."

[163] Albright, Brannan, and Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, 10. The I.A.E.A. has not confirmed nor denied that Stuxnet destroyed 984 centrifuges but Iran's parts of Natanz were idle for a bit. Albright, Brannan, and Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, 4.

[164] Barzashka, 54.

states.[165] However, if these weapons can be reverse-engineered, this point conflicts with the discussion in Chapter 1 about these weapons being one-time use only. Perhaps this is why some experts claimed that Stuxnet bore children named Flame, Duqu and Gauss.[166]

On October 14, 2011, the Laboratory of Cryptography and System Security at Budapest University of Technology and Economics discovered another malware, which they called Duqu because it created files with the prefix '~DQ.'[167] They shared their findings with Symantec who then analyzed the malware themselves and concluded, "Duqu

---

[165] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 409, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml; William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October, 2010): 98, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/20788647; William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: The National Academy of Sciences, 2009), 112-113, accessed March 7, 2017, http://www3.nd.edu/~cpence/eewt/Owens2009.pdf; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 370.

[166] Stefano Mele, "Cyber-Weapons: Legal and Strategic Aspects Version 2.0," *Italian Institute of Strategic Studies Niccolo Machiavelli* (June 2013): XI, accessed June 2, 2016, http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf. Mele says the press also labeled Rocra [Red October], Mahdi and FinFisher as children of Stuxnet but I have not found such claims. Red October was an espionage tool dating back to 2007 used to steal data from diplomatic and research groups mainly in Eastern Europe. It is unclear if it was carried out by a state thus, it will not be discussed here. "The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies," *Kaspersky Lab* (blog), January 14, 2013, accessed June 10, 2016, https://securelist.com/blog/incidents/57647/the-red-october-campaign/. Mahdi is an unsophisticated spying operation that infected 800 computers in the Middle East, mainly in Iran and Israel. It is not directly attributed to a state so it will not be discussed here. Kim Zetter, "Mahdi, The Messiah, Found Infecting Systems in Iran, Israel," *Wired*, July 17, 2012, accessed June 10, 2016, https://www.wired.com/2012/07/mahdi/. FinFisher is spying software that states can purchase so it's more of a defensive tool, than an offensive tool. Bill Marczak et al., "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," *Citizen Lab,* October 15, 2015, accessed June 10, 2016, https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/.

[167] *W32.Duqu The precursor to the next Stuxnet*, (Symantec, November 23, 2011), 1, accessed May 20, 2014, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf.

is essentially the precursor to a future Stuxnet-like attack."[168] Duqu was a "remote access Trojan," that gathered intelligence from industrial control systems but did not have any payloads that could attack industrial control systems.[169] "A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer."[170] Some experts suggested that Duqu was part of Olympic Games and "used to copy blueprints of Iran's nuclear program."[171] Since Duqu only stole information, I did not classify Duqu as a cyberweapon.

Flame was a virus that stole sensitive data from 600 institutions across Iran, Lebanon, Egypt, Saudi Arabia and Israel.[172] Flame was 20 times bigger than Stuxnet, which is why it is remarkable that it stayed hidden for five years.[173] Flame uses the 'Tilded Platform' which is what both Duqu and Stuxnet used where the filename contains a tilde, '~d' therefore, 'Tilde-d.'[174] Kaspersky Lab discovered that Flame was used as a plugin in

---

[168] *W32.Duqu The precursor to the next Stuxnet*, 1.

[169] Ibid.

[170] Margaret Rouse, "RAT (Remote Access Trojan)," *Search Security*, accessed November 19, 2016, http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan. "A back door is a means of access to a computer program that bypasses security mechanisms." Margaret Rouse, "Back Door," *Search Security*, accessed November 19, 2016, http://searchsecurity.techtarget.com/definition/back-door.

[171] Nicole Perlroth, "Researchers Find Clues in Malware," *The New York Times,* May 30, 2012, accessed November 12, 2016, http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

[172] David Lee, "Flame: Massive cyber-attack discovered, researchers say," *BBC,* May 28, 2012, accessed April 8, 2014, www.bbc.com/news/technology-18238326.

[173] Perlroth, "Researchers Find Clues in Malware."

[174] *Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected*, (Kaspersky Lab, June 11, 2012), accessed November 29, 2016,

the June 2009 version of Stuxnet and was removed in the 2010 versions of Stuxnet.[175] Thus, Flame is not the "son of Stuxnet."[176] Since Flame's purpose was also data theft, I did not classify Flame as a cyberweapon.

Gauss was a Trojan horse related to Flame that infected 25 countries,[177] particularly banking institutions in Lebanon, Israel and Palestine.[178] Since Gauss did not intend or cause any physical destruction, I do not consider Gauss a cyberweapon.

IRAQ (2007)

By 2007, the U.S. was four years into what would become almost a decade long war with Iraq and rising sectarian violence (some say civil war) [179] was ripping the country apart and taking a toll on American forces. On January 10, 2007, President Bush declared, "America will change our strategy to help the Iraqis carry out their campaign to put down sectarian violence and bring security to the people of Baghdad."[180] Bush proposed to quell

---

http://www.kaspersky.com/au/about/news/virus/2012/resource_207_kaspersky_lab_research_proves_that_stuxnet_and_flame_developers_are_connected.

[175] *Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected*.

[176] Mele, XI.

[177] *Gauss: Abnormal Distribution*, (Kaspersky Lab, August 9, 2012), 6, accessed June 11, 2016, https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf.

[178] Alexander Gostev, "Kaspersky Security Bulletin 2012. Cyber Weapons," *Securelist*, December 18, 2012, accessed January 28, 2015, http://securelist.com/analysis/kaspersky-security-bulletin/36762/kaspersky-security-bulletin-2012-cyber-weapons/.

[179] James D. Fearon, "Iraq's Civil War," *Foreign Affairs* 86, no. 2 (March - April 2007): 2, JSTOR via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

the intensifying sectarian violence and related rising U.S. death toll with a "surge" of an additional 20,000 U.S. troops to Iraq.[181] In his speech Bush admitted, "This new strategy will not yield an immediate end to suicide bombings, assassinations or IED attacks."[182] Kaplan says "The effect was not decisive, nor was it meant to be: the idea was to provide some breathing space, a zone of security, for Iraq's political factions to settle their quarrels and form a unified state without having to worry about bombs blowing up every day."[183]

In *@War: The Rise of the Military-Internet Complex*, Shane Harris provides an intricate account of the cyber operations in Iraq at that time. This cyber operation was different from run-of-the-mill espionage operations because cyber capabilities do not necessarily remain in the systems they entered.[184] This cyber operation's "purpose was to kill people, not stymie mechanical processes. Stuxnet was an act of sabotage. This was an act of war."[185]

In May 2007, Mike McConnell, the director of national intelligence presented a new alternative to President Bush, Stephen Hadley (National Security Adviser), Dick Cheney (Vice President), Henry Paulson (Treasury Secretary), and Robert Gates (Defense Secretary).[186] This option was to infiltrate the phones and computers of Iraqi insurgents in

---

[180] George W. Bush, "President Bush Addresses Nation on Iraq War," (speech, Washington, D.C., January 10, 2007), accessed August 12, 2017, *CQ Transcripts Wire*, http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011002208.html.

[181] Bush, "President Bush Addresses Nation on Iraq War."

[182] Ibid.

[183] Kaplan, *Dark Territory: The Secret History of Cyber War*, 160.

[184] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing Company, 2014), 8.

[185] Ibid., 12.

order to pilfer intelligence about their identities, locations and operations and then use that information to prevent attacks and ensnare these bombers into areas where they could be killed or captured.[187] In *Dark Territory: The Secret History of Cyber War*, Fred Kaplan says it was General John Abizaid, the head of U.S. Central Command in 2003, who originally proposed this operation years prior.[188] According to Kaplan, in January 2004, General Abizaid met with President Bush about using cyberweapons against Iraqi insurgents but the intelligence deputies said no because they did not want to tip off the insurgents about the hack and lose their intelligence pipeline.[189] Now, three years later, here was McConnell with the same ask. Kaplan said the result was a program called Real Time Regional Getaway, focused solely on Iraq.[190] This program was modeled after a previous program called Turbulence which consisted of smaller components called "Turbine, Turmoil, QuantumTheory, QuantumInsert, and XKeyscore" (all of these will be discussed below.)[191] Previously, it would take 16 hours for troops to have the intelligence, now they would have it in one minute.[192] "Over the next few years, six thousand NSA officers were deployed to Iraq, and later, Afghanistan; twenty-two of them were killed, many of them by roadside bombs while they were out with the troops."[193]

---

[186] Harris, 7.

[187] Ibid., 8.

[188] Kaplan, *Dark Territory: The Secret History of Cyber War*, 147.

[189] Ibid., 150.

[190] Ibid., 158. Harris devoted Chapter 2 of *@War: The Rise of the Military-Internet Complex* to RTRG, specifically pages 33- 38.

[191] Kaplan, *Dark Territory: The Secret History of Cyber War*, 158.

[192] Ibid., 159.

This intelligence was also useful in identifying those behind the manufacturing of the horrific beheading videos that were not only scare tactics but unfortunately effective recruiting tools.[194] In addition to penetrating enemy infrastructure, there was the possibility of spillover to Iraqi civilians and blowback to U.S. forces.[195] Furthermore, Harris pointed out that this was a 'politically sensitive" operation because in December 2005, the N.S.A. came under fire for surveilling American citizens without a warrant and now the N.S.A. was going to infiltrate private companies as well as Iraqi civilians.[196] So, Harris explained, this was the N.S.A.'s opportunity to demonstrate that cyberwarfare not only entailed surveillance but could cause fatalities.[197]

After listening to McConnell for 15 minutes, (Kaplan said 10)[198] Bush approved this operation.[199] Harris said now, there was a "hybrid" of U.S. intelligence and military in Iraq using both strategic and tactical information where N.S.A. hackers siphoned information from devices, shared it with analysts who then plotted these locations and then troops or drones captured or killed the enemies.[200] The N.S.A. also issued false texts instructing insurgents to "'Meet at this street corner to plan the next attack,' or 'Go to this

---

[193] Kaplan, *Dark Territory: The Secret History of Cyber War*, 159.

[194] Harris, 8.

[195] Ibid., 9.

[196] Ibid.

[197] Ibid., 10- 12.

[198] Kaplan, *Dark Territory: The Secret History of Cyber War*, 174.

[199] Harris, 12.

[200] Ibid., 17.

point on a road and plant your device.'"[201] Upon arrival, the insurgent would be killed by a drone or captured or killed by U.S. forces.[202] A team of 35 people captured 450 insurgents (2 were killed) over 15 months and roadside bombings declined by 90%.[203] The N.S.A. also hacked al-Qaeda's command-and-control servers and used that information to create counterpropaganda and target propagandists.[204] In one instance, T.A.O. assisted U.S. troops in removing at least 10 senior al-Qaeda leaders.[205] (In 2009, the R.O.C. in Hawaii targeted al-Qaeda again in this same manner.[206])

By 2008, the N.S.A. hacked, tracked and duped over 4,000 Iraqi insurgents.[207] Kaplan said about 4,000 insurgents were killed.[208] So this is another conflicting point. General David Petraeus said these cyber operations were "a prime reason for the significant progress made by US troops."[209] As the additional U.S. troops stabilized violent areas, more Iraqis were won over and committed to helping Americans.[210] Kaplan said this was "Petraeus's counterinsurgency strategy."[211] Petraeus "envisioned a two-prong plan of

---

[201] Harris, 18-19.

[202] Ibid., 19.

[203] Ibid., 15-16.

[204] Ibid., 19.

[205] Ibid., 22.

[206] Ibid., 74.

[207] Ibid., 24.

[208] Kaplan, *Dark Territory: The Secret History of Cyber War*, 160.

[209] Harris, 23.

[210] Ibid.

[211] Kaplan, *Dark Territory: The Secret History of Cyber War*, 160.

attack: forge alliances with those fighters who could be persuaded to help the Americans, or at least lay down their arms, and capture or kill the rest. Petraeus called that latter group "the irreconcilables."[212] The U.S. Army's *Counterinsurgency Field Manual* that was developed in 2006, defines 'hearts' as persuading the population that COIN [counterinsurgency] is in their best interest and minds as convincing the population "that the force can protect them and that resisting it is pointless."[213] The U.S. won over some other insurgents by paying for their allegiance while others were increasingly dismayed by al-Qaeda's ruthlessness which resulted in the "Sunni Awakening."[214] "Nearly 80,000-strong, paid by the Pentagon, and independent of the Iraqi government, these Sunni "awakening councils" are largely made up of former insurgents who have turned their guns on al Qaeda."[215]

However, it was supposedly the cyber capabilities that were considered the game-changer in Iraq since they helped stem the violence and IED threats thereby saving lives. Harris said, "The 2007 surge marked the first time US military and intelligence agencies tested the theories of cyber war on the battlefield."[216] As a result of these successes, these cyber capabilities were transferred to Afghanistan.[217]

---

[212] Harris, 13.

[213] Paul Dixon, "'Hearts and Minds'? British Counter-Insurgency from Malaya to Iraq," *Journal of Strategic Studies* 32, no. 3 (2009): 353-381, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[214] Harris, 23.

[215] John Hendren, "'Sunni Awakening': Insurgents Are Now Allies," *ABCNews*, December 23, 2007, accessed August 12, 2017, http://abcnews.go.com/International/story?id=4045471.

[216] Kaplan, *Dark Territory: The Secret History of Cyber War*, 25.

[217] Harris, 24.

In his article "The misunderstood acronym: Why cyber weapons aren't WMD," Jeffrey Carr had a "private discussion" with "a member of the Special Operations Forces" who informed him that the U.S. government was deploying cyberweapons[218] "in combat in Iraq and Afghanistan when they can be employed as part of the US rules of engagement."[219] The Iraq (2007) case may be what this Special Operations Forces member was referring to. I decided to include Iraq (2007) as a case study because it fits the parameters of a cyberweapon as defined in this dissertation. This case was also the foundation for the cyber operations against ISIS in 2016. However, as with several of the cases in this dissertation, there is debate about whether the Iraq (2007) case is really a cyberweapon. This debate will be discussed further later on in this dissertation but according to Kaplan, the Iraq (2007) operation (which he attributed to General Keith Alexander) was a Computer Network Attack.

> When Alexander penetrated and probed the email and cell phone networks of Iraqi insurgents, that was CNE; when President Bush authorized him to disable and disrupt those networks– to intercept and send false messages that wound up getting insurgents killed– that was CNA, Computer Network Attack. Except for the final step, the decision to attack, CNE and CNA were identical.[220]

As for Afghanistan, Kaplan said a few years earlier, General Abizaid wanted to "get intelligence from al-Qaeda's computers" to troops in Afghanistan.[221] According to Harris, the N.S.A. used these cyber tools against the Taliban.[222] "At the TechNet Land

---

[218] Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," 36.

[219] Ibid.," 35.

[220] Kaplan, *Dark Territory: The Secret History of Cyber War*, 180.

[221] Ibid., 147.

[222] Harris, 78.

Forces East conference in Baltimore" in August 2012, "Marine Lt. Gen. Richard P. Mills, commanding general of Marine Corps Forces Cyberspace Command and former leader of international forces in southwestern Afghanistan, stated," 'I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact.'[223] He said, 'I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations.'[224] Harris discussed "a program called Shifting Shadow" that gathered cellphone information in Afghanistan and added other data in order to assess links between violence and public sentiment.[225] There were differing opinions about whether Shifting Shadow was successful.[226] One U.S. official claimed Shifting Shadow was 60 – 70% accurate in identifying Taliban attacks but others said Shifting Shadow was futile.[227] I have not included Afghanistan as a case study because while I do not have that much information for many of the cases discussed in this dissertation, I have even less information about the cyber operations in Afghanistan to document the case.

[223] Sterling C. Beard, "Marine officer says US using cyberwarfare in Afghanistan," *The Hill,* August 24, 2012, accessed August 12, 2017, http://thehill.com/policy/defense/245421-marine-officer-says-us-using-cyberwarfare-in-afghanistan.

[224] Ibid.

[225] Harris, 78.

[226] Ibid., 78-79.

[227] Ibid., 79.

SHOTGIANT (2007)

Ever since 2007, the N.S.A. enacted a plan called 'Shotgiant' to get into the Chinese telecommunications company Huawei.[228] According to a 2010 record found in the Snowden trove, the N.S.A. penetrated Huawei creating backdoors to discern whether the company was linked to the Chinese army, conduct surveillance on anyone who had Huawei products including 'high priority targets — Iran, Afghanistan, Pakistan, Kenya, Cuba,' and upon presidential orders, could implement offensive cyber operations.[229] The U.S. does not do business with Huawei for this very same reason- they are fearful that Huawei would install "backdoors" into their equipment allowing the Chinese access to conduct intellectual espionage and theft.[230] Since the president could order offensive cyber operations against those who had Huawei products, Shotgiant has the potential to be a cyberweapon.

QUANTUM (2008)

In *Dark Territory: The Secret History of Cyber War*, Fred Kaplan discusses a $1.2 billion antiquated N.S.A. signals intelligence collection program called Trailblazer[231] that was later replaced by Turbulence in 2005.

> Turbulence drew on the same massive databases as Trailblazer; what differed was the processing and sifting of the data, which were far more precise, more tailored to the search for specific information, and more closely shaped to the actual pathways– the packets and streams– of modern digital communications. And

---

[228] David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *The New York Times,* March 22, 2014c, accessed January 28, 2015, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

[229] Sanger and Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat."

[230] Ibid.

[231] Kaplan, *Dark Territory: The Secret History of Cyber War*, 157.

> because the intercepts took place within the network, the target could be tracked on the spot, in real time.[232]

As mentioned in the Iraq (2007) section, Turbulence was made up of nine different programs some of which were called Quantum, QuantumTheory, Turbine, XKeyscore and Turmoil that did different things.[233] XKeyscore is the N.S.A.'s self-proclaimed 'widest-reaching' program that "allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden."[234] Turmoil will be explained in the next section. This is interesting because if these programs were around since 2005, they could predate Stuxnet. What we do know is that ever since 2008, the N.S.A. has implanted software across the globe to conduct Computer Network Exploitation.[235] This program called Quantum, has infected over 100,000 computers specifically targeting the Chinese army, Russian military, Mexican drug cartels, as well as others like Saudi Arabia, the European Union, Pakistan and India in order to carry out "surveillance for national security."[236] The N.S.A. said this was for "active defense" purposes so the U.S. could incapacitate cyberattacks headed its way.[237]

---

[232] Kaplan, *Dark Territory: The Secret History of Cyber War*, 158.

[233] Ibid., 157- 158.

[234] Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *The Guardian,* July 31, 2013a, accessed August 12, 2017, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[235] David E. Sanger and Thom Shanker, "N.S.A. Devises Radio Pathway Into Computers," *The New York Times,* January 14, 2014f, accessed January 28, 2015, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html.

[236] Ibid.

[237] Ibid.

Since many of these computers were air-gapped, the N.S.A. used the old-school tactic of radio frequency technology to implant the malware.[238] This consisted of placing small circuit boards onto USB devices that were secretly injected into the computer to furtively transfer radio waves a few miles away to a relay station the size of a briefcase.[239] This is not the only traditional method that the N.S.A. uses to implant their technology. One of their successful conventional methods is intercepting shipments and installing malware or hardware onto it.[240] The N.S.A. calls this 'interdiction.'[241] The U.S. uses front companies in China to assist with interdiction.[242] Some scholars suggest that the N.S.A.'s implants are exactly the same as those the Chinese are using on American industries but President Obama argues that the N.S.A.'s operations are different because the U.S. does not engage in these operations for intellectual property theft or "nonmilitary purposes" whereas the Chinese use surveillance for intellectual property theft.[243]

Before Quantum, the N.S.A. used spear-phishing emails and faulty websites, techniques utilized by hackers and criminals to install implants onto networks.[244] Now the N.S.A. is getting savvier in reaching air-gapped networks without depending on physical

---

[238] Sanger and Shanker, "N.S.A. Devises Radio Pathway Into Computers."

[239] Ibid.

[240] Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit."

[241] Ibid.

[242] Sanger and Shanker, "N.S.A. Devises Radio Pathway Into Computers."

[243] David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times,* February 18, 2013, accessed June 19, 2016, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

[244] Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit."

access.[245] According to some of the leaked Snowden documents, the N.S.A. now has a massive toolbox of gadgets called "QUANTUMTHEORY" for covert espionage and exploitation in hard-to-reach areas.[246] "Certain Quantum missions have a success rate of as high as 80%, where spam is less than 1%."[247] QUANTUMTHEORY is a man-on-the-side method, which means it intercepts the communication but it cannot alter the communication the way a man-in-the-middle operation does.[248] Quantum also emerged in Iran in 2012 when the Iranian military repositioned a rock outside of the Fordo nuclear plant and the rock detonated revealing circuit boards.[249] While Quantum's stated purpose was Computer Network Exploitation, the exploding rock demonstrates that there are other gadgets that are potentially destructive. Thus, I decided to label Quantum a cyberweapon.

TURBINE (2010)

The "Black Budget" mentioned a project called GENIE where the U.S. spent $652 million on 'covert implants' that they installed onto foreign firewalls, computers and routers.[250] These implants can survive upgrades, duplicate information, serve as a

---

[245] Sanger and Shanker, "N.S.A. Devises Radio Pathway Into Computers."

[246] "The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics," *The Intercept,* March 12, 2014, accessed May 13, 2016, https://theintercept.com/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/.

[247] "NSA Phishing Tactics and Man in the Middle Attacks," *The Intercept,* March 12, 2014, accessed May 13, 2016, https://theintercept.com/document/2014/03/12/nsa-phishing-tactics-man-middle-attacks/.

[248] Ryan Gallagher and Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers With Malware," *The Intercept,* March 12, 2014, accessed May 13, 2016, https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.

[249] Sanger and Shanker, "N.S.A. Devises Radio Pathway Into Computers."

backdoor, "'harvest' communications and tunnel into other connected networks."[251] GENIE had a staff of nearly 2,000 but "made full use of only 8,448 of the 68,975 machines with active implants in 2011."[252]

In order to manage these implants, the N.S.A. created an automated system called TURBINE, which has been active since July 2010.[253] TURBINE automatically configures groups of implants and handles surveillance collection.[254] Previously, these individual implants were manually executed.[255] Now, the "cyberwarrior" was relieved "from needing to know/care about the details."[256] Additionally, by automating the process, the N.S.A. could increase the number of implants.[257] TURBINE "is capable of managing 'potentially millions of implants' for intelligence gathering 'and active attack.'"[258] Turmoil is the codename for the sensors that capture the data from TURBINE and send it to the NSA for

---

[250] Gellman and Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show."

[251] Ibid.

[252] Ibid.

[253] Gallagher and Greenwald, "How the NSA Plans to Infect 'Millions' of Computers With Malware."

[254] Ibid.

[255] Ibid.

[256] "NSA Technology Directorate Analysis of Converged Data," *The Intercept,* March 12, 2014b, accessed May 13, 2016, https://theintercept.com/document/2014/03/12/nsa-technology-directorate-analysis-converged-data/.

[257] Gallagher and Greenwald, "How the NSA Plans to Infect 'Millions' of Computers With Malware."

[258] Gellman and Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show."

exploration.[259] "The TURMOIL system can be used to send alerts or "tips" to TURBINE, enabling the initiation of a malware attack."[260] Since TURBINE has the ability to attack, I labeled it a cyberweapon.

NITRO ZEUS

On April 29, 2016, I attended a screening about Stuxnet at Harvard University's Belfer Center for Science and International Affairs. *Zero Days* is a documentary that effectively portrayed all of the complexities surrounding cyberwarfare: definitions, scope, attribution, responsibility, parameters and response. During a discussion after the screening, *New York Times* journalist David Sanger, who appeared in and was a consultant on the documentary, said that one of the breakthroughs of the film was the discovery of Nitro Zeus.[261] Nitro Zeus was a multimillion dollar plan developed by the U.S. to insert electronic implants into Iranian computers to deactivate their communication systems, power grid and air defenses in case the pending nuclear deal with Iran fell through and conflict erupted.[262] Simultaneously, U.S. intelligence agencies were also developing a

[259] Gallagher and Greenwald, "How the NSA Plans to Infect 'Millions' of Computers With Malware."

[260] Ibid.

[261] David E. Sanger, "*Zero Days* Screening," (discussion, Harvard University, Cambridge, Massachusetts, April 29, 2016a).

[262] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times,* February 16, 2016e, accessed May 10, 2016, http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

worm to immobilize the computers at the inaccessible Fordo nuclear site.[263] The date of creation is unclear.

Nitro Zeus was envisioned to work in conjunction with a conventional attack. "Cyberwarfare has become a standard element of the arsenal for what are now called 'hybrid' conflicts."[264] "Before it was developed, the U.S. had never assembled a combined cyber and kinetic attack plan on this scale."[265] While this may be true, the first paragraph of this chapter pointed out that in 1999, U.S. officials also saw computer network attacks against Yugoslavia as a blueprint for the future. Thus, Nitro Zeus may not be entirely novel but I think Nitro Zeus is a cyberweapon because deactivating and immobilizing systems could also result in destroying systems.

Some administration officials thought President Obama "did not have a credible military contingency plan" in case diplomacy was unsuccessful and conflict erupted.[266] Hence, "Nitro Zeus was part of an effort to assure President Obama that he had alternatives, short of a full-scale war."[267] However, we do not know what those other alternatives were. "While cyberoperations have long been contemplated in other war scenarios, Nitro Zeus

---

[263] Sanger and Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict."

[264] Ibid. Hybrid warfare is the combination of Special Operations Forces (SOF), conventional forces and "new weapons." David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times,* October 25, 2015e, accessed May 10, 2016, http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

[265] Sanger and Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict."

[266] Ibid.

[267] Ibid.

'took it to a new level.'"[268] Nitro Zeus was a sequel to Stuxnet – "a straightforward strike that would destroy the circuitry that powered the centrifuges and their controllers."[269] But the U.S. was worried about collateral damage. "There could be significant effects on civilians, particularly if the United States had to cut vast swaths of the country's electrical grid and communications networks."[270] Nitro Zeus remained lurking in Iranian networks but it was not set into motion since the U.S. along with 5 other nations agreed to a historic deal with Iran in July 2015 to lift sanctions provided Iran abides by the requirements set out in the deal which include verification and limitations on nuclear fuel and research for specific time periods.[271]

LIBYA (2011)

As Libyan leader Colonel Muammar el-Qaddafi pummeled his own citizens in early March 2011, the U.S. considered the following options, a 'no-flight' zone, send in Special Operations, or strikes against military or government infrastructure.[272] The echoes of Rwanda and Bosnia– where the international community failed to prevent the genocides–

---

[268] Sanger and Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict."

[269] Ibid.

[270] Ibid.

[271] Michael R. Gordon and David E. Sanger, "Deal Reached on Iran Nuclear Program; Limits on Fuel Would Lessen with Time," *The New York Times,* July 14, 2015, accessed August 12, 2017, https://www.nytimes.com/2015/07/15/world/middleeast/iran-nuclear-deal-is-reached-after-long-negotiations.html.

[272] Thom Shanker, "U.S. Weighs Options, on Air and Sea," *The New York Times,* March 6, 2011, accessed December 9, 2016, http://www.nytimes.com/2011/03/07/world/middleeast/07military.html.

were sparring with the severe trepidation over U.S. entanglement with another Muslim country.[273] By March 17, 2011 Qaddafi declared that he would show 'no mercy' to anti-government protesters in Benghazi,[274] the second-largest city in Libya. The United Nations quickly authorized a no-fly zone[275] and on March 18th, President Obama declared, "The United States is not going to deploy ground troops into Libya. And we are not going to use force to go beyond a well-defined goal -- specifically, the protection of civilians in Libya."[276] On March 19, 2011, President Obama explained that the U.S. joined the airstrikes "to prevent a humanitarian catastrophe and address the threat posed to international peace and security by the crisis in Libya."[277]

A few days into the conflict, there was still hope for a diplomatic resolution as many assumed that bombs would force the rebels and the government to the bargaining table.[278]

---

[273] Shanker, "U.S. Weighs Options, on Air and Sea."

[274] David D. Kirkpatrick and Kareem Fahim, "Qaddafi Warns of Assault on Benghazi as U.N. Vote Nears," *The New York Times,* March 17, 2011b, accessed December 5, 2016, http://www.nytimes.com/2011/03/18/world/africa/18libya.html?pagewanted=all.

[275] Security Council, "Security Council Approves 'No-Fly Zone' Over Libya, Authorizing 'All Necessary Measures' to Protect Civilians, by Vote of 10 in Favour with 5 Abstentions," *The United Nations,* March 17, 2011, accessed December 5, 2016, http://www.un.org/press/en/2011/sc10200.doc.htm.

[276] "Remarks by the President on the Situation in Libya," *The New York Times,* March 18, 2011, accessed December 5, 2016, https://www.whitehouse.gov/the-press-office/2011/03/18/remarks-president-situation-libya.

[277] Barack Obama, "Letter from the President regarding the commencement of operations in Libya," March 21, 2011, accessed December 5, 2016, *The White House*, https://www.whitehouse.gov/the-press-office/2011/03/21/letter-president-regarding-commencement-operations-libya.

[278] Steven Lee Myers and David D. Kirkpatrick, "Allies Are Split on Goal and Exit Strategy in Libya," *The New York Times,* March 24, 2011a, accessed December 5, 2016, http://www.nytimes.com/2011/03/25/world/africa/25policy.html?pagewanted=all.

Depending on their political affiliation, Americans were split between the preferred goals of the campaign even though President Obama stated that his political, not military, goal was the removal of Qaddafi from power.[279] Of those polled, some preferred the goal of enforcing a no-fly zone but others wanted Qaddafi to be removed from power.[280] Looking back five years later, Benjamin Rhodes, the deputy national security adviser said the limited goal was achieved quickly. 'We basically destroyed Qaddafi's air defenses and stopped the advance of his forces within three days.'[281]

After some back and forth, the U.S. handed over the air campaign to NATO[282] in what became perhaps unfortunately described as "leading from behind."[283] "The U.S. Navy fired 221 Tomahawks in operations against Libyan leader Muammar Gaddafi in 2011, nearly half of them - 110 - in an opening salvo against 22 Libyan military targets, including air defenses, communications and command structures."[284] A Tomahawk missile costs

---

[279] Jo Becker and Scott Shane, "The Libya Game | Part 1 Hillary Clinton, 'Smart Power' and a Dictator's Fall," *The New York Times,* February 27, 2016, accessed December 6, 2016, http://www.nytimes.com/2016/02/28/us/politics/hillary-clinton-libya.html.

[280] Lydia Saad, *Americans Resist a Major U.S. Role in Libya*, (Gallup, March 29, 2011a), accessed December 10, 2016, http://www.gallup.com/poll/146840/americans-resist-major-role-libya.aspx.

[281] Becker and Shane, "The Libya Game | Part 1 Hillary Clinton, 'Smart Power' and a Dictator's Fall."

[282] Elisabeth Bumiller and David D. Kirkpatrick, "NATO Agrees to Take Command of No-Fly Zone in Libya," *The New York Times,* March 24, 2011, accessed December 5, 2016, http://www.nytimes.com/2011/03/25/world/africa/25libya.html?pagewanted=all.

[283] Becker and Shane, "The Libya Game | Part 1 Hillary Clinton, 'Smart Power' and a Dictator's Fall."

[284] David Alexander, "Cost of a U.S. strike against Syria could top Hagel's estimate," *Reuters,* September 5, 2013a, accessed December 13, 2016, http://www.reuters.com/article/us-syria-crisis-usa-costs-idUSBRE98415K20130905.

over one million dollars each.[285] The Pentagon said, "U.S. operations there cost $896 million through the end of July."[286]

Months later we also learned that at the beginning of Operation Odyssey Dawn[287] in 2011, the Obama administration debated about using a cyberweapon to penetrate Libyan military computers and disarm Libya's missile radar systems.[288] (This has a whiff of Operation Orchard, and the Yugoslavia operation, right?) *The New York Times* reported that the Obama administration was worried that they would set a new norm for adversaries such as Russia and China and they were also unsure if the President needed Congressional approval; therefore, this option was not presented to the White House.[289] However, reporting in 2014 claimed "Mr. Obama's advisers warned him that there was no assurance they [cyberweapons] would work against Col. Muammar el-Qaddafi's antiquated, pre-Internet air defenses."[290] There were also conflicting reports about the impact of a

---

[285] Alexander, "Cost of a U.S. strike against Syria could top Hagel's estimate."

[286] John Barry, "America's Secret Libya War," *The Daily Beast,* August 30, 2011, accessed December 13, 2016, http://www.thedailybeast.com/articles/2011/08/30/america-s-secret-libya-war-u-s-spent-1-billion-on-covert-ops-helping-nato.html.

[287] Lt. Cmdr. Kallie D. Fink, U.S. Navy, Maj. John D. Jordan, U.S. Marine Corps, and Maj. James E. Wells, U.S. Air Force, "Considerations for Offensive Cyberspace Operations," *Military Review* (May-June 2014): 8, accessed November 29, 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20140630_art005.pdf.

[288] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times,* October 17, 2011, accessed July 5, 2016, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

[289] Ibid.

[290] David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times,* February 24, 2014b, accessed December 10, 2016, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?ref=davidesanger.

cyberweapon. *The Washington Post* claimed that a cyberweapon would not have destroyed Libya's air defenses and if there was any damage, it would be fleeting.[291] On the other hand, *The New York Times* said a cyberweapon would have been very potent which is why some officials thought we would be wasting a huge capability on "a relatively minor security threat to the United States."[292] *The Washington Post* also pointed out the concern about collateral damage,[293] but that was not mentioned in *The New York Times'* reporting.

These are all fascinating points because despite the Pentagon's announcement in 2011 that they had a list of cyberweapons and despite the fact that the June 2009 version of Stuxnet was compiled and deployed in less than 12 hours, the U.S. was unsure whether this attack could have been launched quickly. Second, despite the Pentagon's announcement in 2011 that the President had the power to authorize such operations, here the U.S. was unsure whether the President did in fact have this power and they refrained from deploying. Since the purpose of this attack was to destroy radar systems, this operation is a cyberweapon. In his book, journalist Shane Harris discussed an operation stating

> the NSA worked with the navy's cyber warriors to track targets in Libya and help create 'strike packages.' The hackers found targets on the ground via their electronic devices and radio signals, then passed along the coordinates to an aircraft carrier strike group, led by the USS *Enterprise.* Those cyber operations were conducted in the navy's Information Operations Command, which is based at Fort Meade along with the NSA.[294]

---

[291] Nakashima, "U.S. cyberweapons had been considered to disrupt Gaddafi's air defenses."

[292] Schmitt and Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya."

[293] Nakashima, "U.S. cyberweapons had been considered to disrupt Gaddafi's air defenses."

This specific operation was not discussed in this dissertation because just as with the cyber operations in Afghanistan, I did not find much information about this operation elsewhere. So using a cyberweapon before Operation Odyssey Dawn was the cyber incident focused upon in this dissertation.

PAKISTAN (2011)

In August 2010, U.S. intelligence officials informed President Obama that they followed an al-Qaeda courier to an obscure residence in Abbottabad, Pakistan.[295] According to Shane Harris, T.A.O. "remotely implanted spyware on the mobile phones of al-Qaeda operatives and other 'persons of interest'" and "The CIA helped find the geographic location of one of those phones, which pointed investigators to the compound."[296] This compound stuck out like a sore thumb because of its size and resources.[297] After watching the compound for several weeks and noticing a man whom U.S. intelligence officials labeled The Pacer, (because he paced around outside but never left the premises), U.S. intelligence officials concluded that this could be the residence of "a 'high-value target,'" possibly Osama bin Laden.[298] President Obama directed C.I.A. Director Leon Panetta to get answers as well as draft options.[299]

---

[294] Harris, 80.

[295] Mark Bowden, "The Hunt for 'Geronimo,'" *Vanity Fair,* October 12, 2012, accessed April 22, 2017, http://www.vanityfair.com/news/politics/2012/11/inside-osama-bin-laden-assassination-plot.

[296] Harris, 38.

[297] Bowden, "The Hunt for 'Geronimo.'"

[298] Ibid.

[299] Ibid.

In "The Hunt for 'Geronimo,'" Mark Bowden presents a riveting account of the operation to catch Osama bin Laden. Four months after discovering The Pacer, U.S. intelligence officials said they could either bomb the compound or conduct a C.I.A. raid.[300] The C.I.A. raid had the advantage of plausible deniability and secrecy, but it consisted of more personnel and scheming.[301] The C.I.A. approached Admiral William McRaven, leader of the Joint Special Operations Command for his advice.[302] Admiral McRaven eliminated the bombing option because even though he thought it would reduce American casualties, he estimated that it could take about 50,000 pounds of artillery to guarantee that this target was killed since it was very likely that there were underground tunnels or bunkers.[303] Thus, McRaven thought a raid presented fewer complications and recommended his SEAL Team Six commander for the operation.[304] The major concern with the raid though was that Abbottabad was in Pakistan, a 'denied' space, so Pakistan could fire back.[305] Panetta decided that if there was a raid, McRaven and the SEALs, not the C.I.A. would handle it.[306]

In March, the C.I.A. informed President Obama there was a 95% chance that Osama bin Laden resided at this compound but other officials at the meeting were not as

---

[300] Bowden, "The Hunt for 'Geronimo.'"

[301] Ibid.

[302] Ibid.

[303] Ibid.

[304] Ibid.

[305] Ibid.

[306] Ibid.

convinced, recalling the flawed weapons of mass destruction intel previously provided by the C.I.A. during the buildup to the U.S. invasion of Iraq in 2003.[307]

> 'Mr. President,' he ["Michael Morell, the head of the C.I.A.'s bin Laden team"] said, 'if we had a human source who had told us directly that bin Laden was living in that compound, I still wouldn't be above 60 percent.' Morell said he had spent a lot of time on both questions, W.M.D. and Abbottabad. He had seen no fewer than 13 analytical drafts on the former and at least as many on the latter. 'And I'm telling you, the case for W.M.D. wasn't just stronger—it was *much* stronger.' [308]

President Obama said, 'This is 50–50.'[309] He added, 'You guys, I can't base this decision on the notion that we have any greater certainty than that.'[310] In retrospect, President Obama told Bowden, "No issue comes to my desk where there's 100 percent confidence that this is the right thing to do. Because if people were absolutely certain then it would have been decided by someone else."[311]

One option presented to the president was to obliterate the compound, which would pose the smallest number of American casualties.[312] Additionally, if the U.S. went this route, they would not have to worry about running into the Pakistanis.[313] After inquiring about the number of inhabitants at the residence (9 or 10 adults and about 20 children), and effect on surrounding houses, Obama vetoed the plan.[314] "He said the only way he would

---

[307] Bowden, "The Hunt for 'Geronimo.'"

[308] Ibid.

[309] Ibid.

[310] Ibid.

[311] Ibid.

[312] Ibid.

[313] Ibid.

[314] Ibid.

even consider attacking the compound from the air was if the blast area could be drastically reduced."[315] Thus, I suppose civilian casualties were a noncompensatory option. The air force did reassess and reduce the number of bombs however, this would not account for any possible tunnels or bunkers or provide clarity that bin Laden was killed.[316]

Another alternative was the raid. Admiral McRaven said the SEALs could capture or kill bin Laden.[317] 'I can tell you that we can succeed on the raid. What I can't tell you yet is how I get in and how I get out.'[318] There was also another option. General James Cartwright said they could use a "small guided munition" launched from a drone to take out only bin Laden.[319] Cartwright's thinking was that since The Pacer walked in the same area, the missile would kill him alone.[320] "But it was strictly a one-shot deal. If the drone missed, The Pacer and his entourage would vanish."[321] Bowden said those involved in the planning did not provide details but he speculated that this was a new "Raytheon G.P.S.-guided missile, about the length and width of a strong man's forearm" that weighed 13 pounds.[322] "It was a 'fire-and-forget' missile, which meant you could not guide it once it was released."[323] However, this specific weapon had not been used before so Bowden said,

---

[315] Bowden, "The Hunt for 'Geronimo.'"

[316] Ibid.

[317] Ibid.

[318] Ibid.

[319] Ibid.

[320] Ibid.

[321] Ibid.

[322] Ibid.

[323] Ibid.

"did you want to hang such a critical opportunity on a single shot, with a missile that had never been fired in anger?"[324] Additionally, although The Pacer was in the same place, he was not standing still.[325]

President Obama told Admiral McRaven to prepare the helicopter raid option because among the advantages were, a) you would know the fate of The Pacer and b) you could obtain intelligence from the compound.[326] Additionally, this alternative presented the faint chance of bin Laden being captured.[327] Obama said they considered the politics and legalities, "But, frankly, my belief was, if we had captured him, that I would be in a pretty strong position, politically, here, to argue that displaying due process and rule of law would be our best weapon against al-Qaeda, in preventing him from appearing as a martyr."[328]

The SEALs conducted two rehearsals in April.[329] "They would be flying very low and very fast to avoid Pakistani radar."[330] According to reporting in *The New York Times*, the U.S. thought about using a cyberattack "to prevent Pakistani radars from spotting helicopters carrying Navy Seal commandos."[331] This was another option. There is very little information about this alternative but since this was a secret raid, I assumed the U.S.

---

[324] Bowden, "The Hunt for 'Geronimo.'"

[325] Ibid.

[326] Ibid.

[327] Ibid.

[328] Ibid.

[329] Ibid.

[330] Ibid.

[331] Schmitt and Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya."

cared about collateral damage as well as this operation being covert. However, this plan was rejected and "specially modified, radar-evading Black Hawk helicopters ferried the strike team, and a still-secret stealthy surveillance drone was deployed."[332] Nevertheless, I decided to include this cyberattack as a case study since it fits the parameters of a cyberweapon as defined in this dissertation.

On April 28th, a few days before the raid, President Obama, Secretary of Defense Bob Gates, Deputy National Security Adviser Tom Donilon, Chairman of the Joint Chiefs Admiral Mike Mullen, Vice President Joe Biden, C.I.A. Director Leon Panetta, Vice-Chairman James Cartwright, Director of National Intelligence James Clapper, Secretary of State Hillary Clinton and John Brennan, President Obama's Chief of Counterterrorism, met in the Situation Room for a final vote.[333] The options were "a raid, a missile strike, or doing nothing."[334] According to Bowden, almost everyone at this meeting supported the helicopter raid. Vice President Biden was concerned about domestic ramifications. "'Mr. President, my suggestion is: don't go," he said. "We have to do two more things to see if he's there." Biden believed that if the president decided to choose either the air or the ground option, and if the effort failed, Obama could say good-bye to a second term."[335] Defense Secretary Gates voted for the missile strike because of "maintaining the flow of fuel and matériel to American forces fighting in Afghanistan, which depended on Pakistan's goodwill," but he eventually backed the raid.[336] Cartwright also voted for the

---

[332] Schmitt and Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya."

[333] Bowden, "The Hunt for 'Geronimo.'"

[334] Ibid.

[335] Ibid.

missile strike.[337] Secretary Clinton was concerned about the diplomatic ramifications for the State Department "But because the U.S.-Pakistani relationship was built more on mutual dependence than friendship and trust, it would likely survive the crisis."[338] Bowden pointed out that Secretary Clinton "who had faulted Obama during the primary campaign for asserting that he would send forces to Pakistan unilaterally if there was a good chance of getting bin Laden, now said that she favored the raid."[339]

According to Bowden, the President had already decided in favor of the raid. "He had been tempted by the air option, but believed that the importance of certainty was too great."[340] Obama told Bowden 'At that point my estimation was that we weren't going to be able to do it better a month or two months or three months from now. We weren't going to have better certainty about whether bin Laden was there, and so it was just a matter of pulling the trigger.'[341] Plus, Obama believed in McRaven. 'He just never looks like he's surprised by anything.'[342] On the evening of May 1, 2011, President Obama announced that he had authorized a mission that killed Osama bin Laden.[343]

---

[336] Bowden, "The Hunt for 'Geronimo.'"

[337] Ibid.

[338] Ibid.

[339] Ibid.

[340] Ibid.

[341] Ibid.

[342] Ibid.

[343] The White House, "Osama Bin Laden Dead," May 2, 2011, accessed August 8, 2017, https://obamawhitehouse.archives.gov/blog/2011/05/02/osama-bin-laden-dead.

SYRIA

For many policymakers, Obama officials and some journalists, "The signal foreign-policy conundrum of today: whether, when and how the United States should wield its military power in Syria and elsewhere in the Middle East."[344] The debate over using a cyberweapon began in 2011 and continued throughout 2014.

As the conflict in Syria exacerbated in the spring of 2011, the Obama administration debated about using a covert cyberweapon to cripple Syrian airpower and missile production facilities.[345] This was seen as a cheaper and low-casualty way of non-direct American intervention and yet, the U.S. refrained.[346]

A year later, as the U.S. contemplated further action against Syria, U.S. military planners were still reluctant about using cyberweapons. "'We weren't ready to do that in Libya,' one former official said, 'We're not ready to do that now, either.'"[347] Then, the Syrian government threatened that their chemical weapons "are made to be used strictly and only in the event of external aggression against the Syrian Arab Republic."[348] On August 20, 2012, President Obama threatened to intervene in Syria if the Assad regime

---

[344] Becker and Shane, "The Libya Game | Part 1 Hillary Clinton, 'Smart Power' and a Dictator's Fall."

[345] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[346] Ibid.

[347] Ellen Nakashima, "U.S. Accelerating Cyberweapon Research," *The Washington Post,* March 18, 2012, accessed November 29, 2016, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html?utm_term=.a7280c3b0778.

[348] Neil MacFarquhar and Eric Schmitt, "Syria Threatens Chemical Attack on Foreign Force," *The New York Times,* July 23, 2012, accessed December 6, 2016, http://www.nytimes.com/2012/07/24/world/middleeast/chemical-weapons-wont-be-used-in-rebellion-syria-says.html.

was gearing up to use its secretive stockpile of chemical weapons.[349] "We have been very clear to the Assad regime but also to other players on the ground that a red line for us is, we start seeing a whole bunch of weapons moving around or being utilized."[350]

On March 21, 2013, the U.N. announced that it was investigating the purported use of chemical weapons in Syria.[351] In July, General Martin Dempsey sent a letter to Congress spelling out a list of options with costs, the most expensive of which was a no-fly zone that would eventually cost "a billion dollars per month."[352] Notably absent from his list was a cyber option even though in 2012, Dempsey said that in the past, cyber was not a substantial part of military action however, "Cyber is a significant factor today."[353]

By August 2013, reports surfaced that a massive chemical attack occurred in the suburbs of Damascus.[354] The Obama administration continued weighing their options. "The strikes would instead be aimed at military units that have carried out chemical attacks, the headquarters overseeing the effort and the rockets and artillery that have launched the

---

[349] Mark Landler, "Obama Threatens Force Against Syria," *The New York Times,* August 20, 2012, accessed December 6, 2016, http://www.nytimes.com/2012/08/21/world/middleeast/obama-threatens-force-against-syria.html.

[350] Ibid.

[351] "UN chief announces independent probe into allegations of chemical attack in Syria," *The United Nations,* March 21, 2013, accessed December 6, 2016, http://www.un.org/apps/news/story.asp?NewsID=44450.

[352] General Martin E. Dempsey, "General Dempsey's Letter to Senator Levin on the U.S. Military and the Syrian Conflict, July 2013," *Council on Foreign Relations*, July 19, 2013, accessed December 13, 2016, http://www.cfr.org/syria/general-dempseys-letter-senator-levin-us-military-syrian-conflict-july-2013/p31198.

[353] Nakashima, "U.S. accelerating cyberweapon research."

[354] "Syrian opposition: 1,300 killed in chemical attack on Ghouta region," *Al Arabiya,* August 21, 2013, accessed December 6, 2016, http://english.alarabiya.net/en/News/middle-east/2013/08/21/Syrian-activists-at-least-500-killed-in-chemical-attack-on-Eastern-Ghouta.html.

attacks."[355] On August 29th, Britain surprisingly voted against military intervention in Syria.[356] On August 30th, the U.S. released a report (pre-empting the U.N. investigation) declaring that 1,429 civilians, 426 of whom were children were killed and the Syrian government was responsible for the chemical attack.[357] The next day, President Obama announced

> I have decided that the United States should take military action against Syrian regime targets. This would not be an open-ended intervention. We would not put boots on the ground. Instead, our action would be designed to be limited in duration and scope.[358]

However, in a bold turn of events (and contradictory to what we saw in Libya), President Obama said he was seeking Congressional approval even though he simultaneously declared, "I believe I have the authority to carry out this military action without specific congressional authorization."[359] In a letter sent to Congress on August 31st, requesting the authorization to use force ("the modern-day equivalent of a declaration of war")[360] President Obama justified that the president is authorized to use force to

---

[355] Thom Shanker, C. J. Chivers and Michael R. Gordon, "Obama Weighs 'Limited' Strikes Against Syrian Forces," *The New York Times,* August 27, 2013, accessed December 6, 2016, http://www.nytimes.com/2013/08/28/world/middleeast/obama-syria-strike.html.

[356] Nicholas Watt and Nick Hopkins, "Cameron Forced to Rule Out British Attack on Syria After MPs Reject Motion," *The Guardian,* August 29, 2013, accessed December 6, 2016, https://www.theguardian.com/world/2013/aug/29/cameron-british-attack-syria-mps.

[357] "Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013,", August 30, 2013, accessed December 6, 2016, *The White House*, https://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21.

[358] Barack Obama, "Statement by the President on Syria," August 31, 2013c, accessed December 6, 2016, *The White House*, https://www.whitehouse.gov/the-press-office/2013/08/31/statement-president-syria.

[359] Ibid.

> (1) prevent or deter the use of proliferation (including the transfer to terrorist groups or other state or non-state actors), within, to or from Syria, of any weapons of mass destruction, including chemical or biological weapons or components of or materials used in such weapons; or
> (2) protect the United States and its allies and partners against the threat posed by such weapons.[361]

Obama daringly sought congressional approval even though he knew many Republicans did not view the Syrian conflict as a direct threat to the U.S.[362] Even Republicans who advocated for action expressed doubts about this operation.[363] "His decision raises the possibility that he would be the first president in modern times to lose a vote on the use of force."[364] Some journalists suggested that Obama was seeking approval because he had no other support – not from the U.N. or even from long-time U.S. ally, Britain.[365] On September 10, 2013, after seeing a possible diplomatic solution where Assad finally admitted that Syria had chemical weapons and agreed to turn them over, President Obama asked Congress to postpone their vote.[366] However, there were other options.

---

[360] Russell Berman, "The War Against ISIS Will Go Undeclared," *The Atlantic,* April 15, 2015, accessed December 6, 2016, http://www.theatlantic.com/politics/archive/2015/04/the-war-against-isis-will-go-undeclared/390618/.

[361] Barack Obama, "Letter from the President -- Authorization for the Use of United States Armed Forces in Connection with the Conflict in Syria," August 31, 2013a, accessed August 8, 2017, *The White House*, https://obamawhitehouse.archives.gov/sites/default/files/docs/aumfresolutiontext.pdf.

[362] Peter Baker and Jonathan Weisman, "Obama Seeks Approval by Congress for Strike in Syria," *The New York Times,* August 31, 2013, accessed December 6, 2016, http://www.nytimes.com/2013/09/01/world/middleeast/syria.html.

[363] Ibid.

[364] Ibid.

[365] Ibid.

[366] Barack Obama, "Remarks by the President in Address to the Nation on Syria," (speech, Washington, D.C., September 10, 2013b), accessed December 6, 2016, *The White*

Cyber practitioner Jason Healey advocated for the use of cyberweapons against Syria in order to destroy air defenses and temporarily disrupt critical infrastructure.[367] Others cautioned that "it's unlikely that these strikes would provide the US military with a greater tactical advantage than they already have,"[368] echoing the potency argument examined in the Libya case study. However, more importantly Healey argued, was that Stuxnet defined a cyberweapon as evil but Syria was a chance for redemption. "America should take this chance to demystify these weapons to show the world they, and the U.S. military in general, can be used on the battlefield in line with humanitarian principles."[369] Here was the potential to establish a good norm and simultaneously boost the U.S.' image.[370] However, despite the fact that the Syrian government used chemical weapons (a

---

House, https://www.whitehouse.gov/the-press-office/2013/09/10/remarks-president-address-nation-syria.

[367] Jason Healey, "Why the U.S. Should Use Cyber Weapons Against Syria," *Defense One,* August 30, 2013b, accessed December 6, 2016, http://www.defenseone.com/technology/2013/08/why-us-should-use-cyber-weapons-against-syria/69776/.

[368] Mark Clayton, "In any US-Syria conflict, cyberweapons could fly in both directions," *The Christian Science Monitor,* September 6, 2013, accessed December 6, 2016, http://www.csmonitor.com/USA/Military/2013/0906/In-any-US-Syria-conflict-cyberweapons-could-fly-in-both-directions-video.

[369] Healey, "Why the U.S. Should Use Cyber Weapons Against Syria." According to Michael Walzer, one of the foremost scholars of Just War theory, state sovereignty is disregarded when it comes to massacres, secession and counterintervention. Michael Walzer, "The Moral Standing of States: A Response to Four Critics," *Philosophy and Public Affairs* 9, no. 3 (Spring 1980): 217, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/2265115.

[370] Ross M. Rustici, "Cyberweapons: Leveling the International Playing Field," *Parameters* 41, no. 3 (Autumn, 2011): 36, ProQuest via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

crime against humanity[371]) thereby crossing the "red line" that Obama declared,[372] the U.S. did not use a cyberweapon. We do not even know if this was on the menu of options.

In 2014, David Sanger reported about the ongoing cyber discussion within the Obama administration as they once again considered their options for dealing with Syria.[373]

> The Obama administration has been engaged in a largely secret debate about whether cyberarms should be used like ordinary weapons, whether they should be rarely used covert tools or whether they ought to be reserved for extraordinarily rare use against the most sophisticated, hard-to-reach targets.[374]

Caitlin Hayden, the National Security Council spokeswoman stated, "we have been clear that there are a range of tools we have at our disposal to protect our national security, including cyber," noting that in 2012 "the president signed a classified presidential directive relating to cyber operations that establishes principles and processes so that cyber tools are integrated with the full array of national security tools."[375]

Sanger quoted Healey making the same humanitarian arguments he made the year before. However, Sanger also quoted prominent cyber scholar P.W. Singer who said this could 'be viewed as opening up a new realm for warfare.'[376] Additionally, Sanger pointed out that a cyberattack against Syria could result in Russian or Iranian retaliation.[377] Even if

---

[371] "Use of chemical weapons in Syria would be 'crime against humanity' – Ban," *The United Nations,* August 23, 2013, December 9, 2016, http://www.un.org/apps/news/story.asp?NewsID=45684.

[372] Landler, "Obama Threatens Force Against Syria."

[373] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[374] Ibid.

[375] Ibid.

[376] Ibid.

[377] Ibid.

the attack was covert, which the Obama administration wanted it to be, Syria would notice if its lights went out and American military planners said the cyberattack needed to be sustained in order to produce any real results but this could exacerbate the already precarious conditions for Syrian civilians.[378] Thus, they decided this operation was 'of limited utility.'[379]

NORTH KOREA (2014)

On November 24, 2014, North Korean hackers seized control of the computers at Sony Pictures Entertainment displaying terrifying images including a red skeleton warning– 'If you don't obey us, we'll release data shown below to the world'– and graphic photos of severed heads of a few Sony executives.[380] The attacks were allegedly carried out at the behest of North Korea's leader Kim Jong-un and their director of intelligence.[381] The North Koreans were livid about the upcoming release of "The Interview," a comedy about two American journalists recruited by the C.I.A. to assassinate Kim Jong-un.[382] The North Koreans expressed their outrage in June[383] but they denied responsibility for this cyberattack.

---

[378] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[379] Ibid.

[380] Brooks Barnes and Nicole Perlroth, "Sony Films Are Pirated, and Hackers Leak Studio Salaries," The New York Times, December 2, 2014a, accessed June 14, 2016, http://www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html.

[381] David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *The New York Times,* January 18, 2015c, accessed January 28, 2015, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0.

[382] Barnes and Perlroth, "Sony Films Are Pirated, and Hackers Leak Studio Salaries."

Bureau 121, North Korea's hacking unit, began attacking Sony in September 2014 with 'spear phishing' emails.[384] The North Koreans spent two months roaming, mapping and planning the attacks on Sony's networks.[385] The Sony malware used command-and-control servers in Singapore, Thailand and Bolivia[386] to steal one hundred terabytes of information, some of which was leaked, exposing salaries and social security information.[387] Then, the Sony malware used a wiping mechanism to wipe out the data.[388] "By some accounts, it wiped out roughly two-thirds of the studio's computer systems and servers — one of the most destructive cyberattacks on American soil."[389]

The malware spread through stolen administrator logins.[390] A group named "Guardians of Peace" claimed responsibility[391] however; some officials believed that the

---

[383] Choe Sang-Hun, "North Korea Warns U.S. Over Film Mocking its Leader," *The New York Times,* June 25, 2014, accessed June 14, 2016, http://nyti.ms/TvMzsx.

[384] Sanger and Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say."

[385] Ibid.

[386] David E. Sanger and Nicole Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony," *The New York Times,* December 17, 2014d, accessed June 14, 2016, https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

[387] Ibid.

[388] Ibid.

[389] David E. Sanger, "Countering Cyberattacks Without a Playbook," *The New York Times,* December 23, 2014a, accessed November 29, 2016, http://www.nytimes.com/2014/12/24/world/asia/countering-cyberattacks-without-a-playbook.html.

[390] Sanger and Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony."

[391] Brooks Barnes and Nicole Perlroth, "Sony Pictures and F.B.I. Widen Hack Inquiry," *The New York Times,* December 3, 2014b, accessed November 29, 2016, http://www.nytimes.com/2014/12/04/business/sony-pictures-and-fbi-investigating-attack-by-hackers.html.

Sony cyberattack was the work of an insider,[392] or it could have been a false flag to frame North Korea.[393] "Unlike stealth attacks from China and Russia, Sony's hackers not only aimed to steal data, but also to send a clear message."[394] Sony canceled the release of "The Interview" after the North Koreans threatened to attack U.S. theaters.[395] The F.B.I. blamed North Korea because this attack shared 'similarities' to prior attacks that bore North Korea's signature.[396] The F.B.I. did not really explain how it had come to these conclusions however; the media speculated that the evidence came from the N.S.A.'s implants.[397]

According to the "International Strategy for Cyberspace," "the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[398] Thus, Admiral Michael Rogers, head of USCYBERCOM, encouraged President Obama to retaliate.[399] On December 19, 2014, President Obama said the U.S. 'will respond

---

[392] Sanger and Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say."

[393] A 'false- flag' is when a cyberattack "crashes one country's computer infrastructures while making it seem that another nation was at fault." Lucas Kello, "The Virtual Weapon: Dilemmas and Future Scenarios," *Politique Étrangère* 79, no. 4 (Winter 2014-2015): 4, accessed November 29, 2016, https://www.ifri.org/sites/default/files/atoms/files/kello_vanglaise_0.pdf.

[394] Barnes and Perlroth, "Sony Films Are Pirated, and Hackers Leak Studio Salaries."

[395] Brooks Barnes and Michael Cieply, "Sony Drops 'The Interview' Following Terrorist Threats," *The New York Times,* December 17, 2014, accessed November 29, 2016, http://nyti.ms/1GtuCOw.

[396] David E. Sanger, Michael S. Schmidt and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *The New York Times,* December 19, 2014e, accessed November 29, 2016, http://nyti.ms/1Gz1GF9.

[397] Ibid.

[398] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, (2011), 14, accessed March 14, 2016, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[399] David E. Sanger, "U.S. Decides to Retaliate Against China's Hacking," *The New York Times,* July 31, 2015b, accessed November 29, 2016,

proportionally' 'in a place and time and manner that we choose.'[400] President Obama called the Sony attack "cybervandalism."[401] This was the first time the U.S. publicly accused a foreign leader of purposely attacking America (as opposed to stealing information) as well as the first time that the U.S. stated that they would retaliate for a cyberattack. (The U.S. previously issued unenforceable indictments against a Chinese hacking unit for data theft.[402] In 2015, the U.S. also wanted to retaliate against the Chinese [but did not know the best way to do so] for a massive data breach at the Office of Personnel Management that affected over 20 million Americans.)[403]

Three days later, North Korea's entire internet was offline.[404] It is unclear to date what exactly happened and whether the U.S. was involved. The U.S. has not admitted to carrying out a cyberattack against North Korea. In January 2015, the U.S. issued sanctions against North Korea stating this was the 'first aspect of our response' to the cyberattack.'[405] *The New York Times* reported that there was also "a covert element" as a part of the

---

http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0.

[400] Sanger, Schmidt and Perlroth, "Obama Vows a Response to Cyberattack on Sony."

[401] Amy Chozick, "Obama to See if North Korea Should Return to Terror List," *The New York Times,* December 21, 2014, accessed November 29, 2016. http://nyti.ms/1GJUkhU.

[402] Sanger, Schmidt and Perlroth, "Obama Vows a Response to Cyberattack on Sony."

[403] Sanger, "U.S. Decides to Retaliate Against China's Hacking."

[404] Nicole Perlroth and David E. Sanger, "North Korea Loses its Link to the Internet," *The New York Times,* December 22, 2014, accessed January 28, 2015, http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

[405] Zeke J. Miller, "U.S. Sanctions North Korea Over Sony Hack," *Time,* January 2, 2015, accessed December 13, 2016, http://time.com/3652479/sony-hack-north-korea-the-interview-obama-sanctions/.

response.[406] In April 2015, Ashton Carter, the Defense Secretary, "acknowledged that in the biggest case to date — the attack on Sony last November — the president chose to respond with sanctions on North Korea, 'not in cyberspace.'"[407] Despite the U.S.' denial, I decided to label the U.S. responsible for temporarily taking out North Korea's internet. (Although *The New York Times* says it was the Chinese who was behind this.[408]) If I am correct, this is an example of the U.S. using a cyberweapon (because it resulted in a physical effect) for retaliatory purposes.

REGIN (2015)

On January 17, 2015, *Der Spiegel* published an article based on more Snowden documents about "cyberweapons" created by the Five Eyes.[409] The Five Eyes is the epitome of alliances. It began in 1946 with an agreement between the United States and the United Kingdom.[410] In 1948, Canada joined and in 1956, Australia and New Zealand

---

[406] David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony Case," *The New York Times,* January 2, 2015d, accessed December 1, 2016, http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

[407] David E. Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *The New York Times,* April 23, 2015a, accessed December 1, 2016, http://nyti.ms/1ProCKP.

[408] Eric Lipton, David E. Sanger and Shane Scott, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times,* December 13, 2016, accessed December 14, 2016, http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?hp=undefined&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&_r=0.

[409] Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle."

[410] Margaret Warner, "An exclusive club: The 5 countries that don't spy on each other," *PBS,* October 25, 2013, accessed November 19, 2016, http://www.pbs.org/newshour/rundown/an-exclusive-club-the-five-countries-that-dont-spy-on-each-other/.

joined.[411] The Five Eyes is an intelligence sharing alliance, especially electronic intelligence, where spying on one another is off limits.[412] 2010 was the first time that officials spoke of the Five Eyes publicly as Britain's Government Communications Headquarters declassified documents about the alliance. [413] The Five Eyes have been studying foreign cyberattacks for a while with the help of an automated system called Tutelage which can identify and deter attacks.[414] The N.S.A. specifically has a department called Transgression that catalogues foreign cyberattacks.[415] The N.S.A. is also able to very successfully watch other states as they steal information. The N.S.A. calls this "Fourth Party Collection" where the U.S. can hack into China's spying operation against another state for example, thereby having access to whatever China is collecting.[416] If you are not a member of Five Eyes, then you are fair game for spying.[417]

In the Snowden documents, there was talk of Qwerty, a keylogger that is one of the modules of the WARRIORPRIDE program. WARRIORPRIDE is "a kind of universal Esperanto software used by all the Five Eyes partner agencies that at times was even able to break into iPhones, among other capabilities."[418] Der Spiegel published the code for

---

[411] Warner, "An exclusive club: The 5 countries that don't spy on each other."

[412] Ibid.

[413] "Newly Released GCHQ Files: UKUSA Agreement," *The National Archives*, June 2010, accessed November 19, 2016, http://www.nationalarchives.gov.uk/ukusa/.

[414] Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle."

[415] Ibid.

[416] Ibid.

[417] Ibid.

[418] Ibid.

Qwerty[419] which Kaspersky Lab analyzed and concluded was part of Regin, a "cyberweapon" created by the Five Eyes.[420]

At the end of 2014, Symantec published a report about Regin, an advanced "back door-type Trojan," that has spied on researchers, businesses, and government organizations across the globe from 2008 - 2011.[421] Version 2.0 appeared in 2013.[422] *The Intercept* traces Regin back to 2003.[423] Regin has five stages, all of which except the first are hidden and encrypted. Once you unlock the first, you have to keep going in order to piece together the puzzle. Symantec says this modular structure is akin to Stuxnet and its family.[424] Regin propagates by visiting purportedly legitimate sites which are actually spoofed websites that have a browser or application exploit.[425] Once installed, Regin is capable of customizing

---

[419] "Malware from the Five Eyes," *Der Spiegel,* January 17, 2015, accessed November 19, 2016, http://www.spiegel.de/media/media-35668.pdf.

[420] Marcel Rosenbach, Hilmar Schmundt and Christian Stöcker, "Experts Unmask 'Regin' Trojan as NSA Tool," *Der Spiegel,* January 27, 2015, accessed November 19, 2016, http://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html.

[421] Symantec Security Response, "Regin: Top-tier espionage tool enables stealthy surveillance," *Symantec* (blog)*,* November 23, 2014, accessed November 19, 2016, http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance.

[422] Symantec Security Response, *Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance*, (Symantec, August 27, 2015), 5, accessed November 19, 2016, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf.

[423] Morgan Marquis-Boire, Claudio Guarnieri and Ryan Gallagher, "Secret Malware in European Union Attack Linked to U.S. and British Intelligence," *The Intercept,* November 24, 2014, accessed November 19, 2016, https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/.

[424] Symantec Security Response, "Regin: Top-tier espionage tool enables stealthy surveillance," *Symantec* (blog).

[425] Symantec Security Response, *Regin: Top-tier espionage tool enables stealthy surveillance*, 6.

the payload to the target and then using a remote access Trojan (RAT) to take screenshots, sniff traffic, gather data, retrieve deleted files and steal login information.[426]

Symantec claimed that because of Regin's capabilities and the amount of time and resources invested including the modular design to make sure that it remained hidden, the author was a state.[427] Regin has been used against the European Union and Belgacom, a Belgian telecommunications company.[428] The attack on the European Union was carried out by the N.S.A.[429] The Belgacom attack, called Operation Socialist, was carried out by the British.[430] Since the purpose of Regin is espionage, not destruction, Regin is not a cyberweapon. So far, this chapter has mainly discussed alleged U.S. cyberweapons against other states, but unsurprisingly, the U.S. is also using cyberweapons against non-state actors.

---

[426] Symantec Security Response, *Regin: Top-tier espionage tool enables stealthy surveillance*, 5.

[427] Ibid. 18.

[428] Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle."

[429] Laura Poitras et al., "Attacks from America: NSA Spied on European Union Offices," *Der Spiegel,* June 29, 2013, accessed November 29, 2016, http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html.

[430] Marquis-Boire, Guarnieri and Gallagher, "Secret Malware in European Union Attack Linked to U.S. and British Intelligence."

ISIS (2016)

ISIS (the Islamic State in Iraq and Syria), was originally al-Qaeda in Iraq who was fomented by the anarchy of Syria's civil war.[431] However, ISIL (Islamic State of Iraq and the Levant) or ISIS' perverse vision of an Islamic state clashed with the Syrian rebels who were focused on fighting the Assad regime.[432] In February 2014, al-Qaeda disassociated themselves from ISIS after ISIS had essentially gone rogue – refusing to obey al-Qaeda's orders to leave Syria and indiscriminate in its killing.[433] (Even al-Qaeda thought ISIS was callous!) 'ISIS is now officially the biggest and baddest global jihadi group on the planet.'[434] In early June 2014, ISIS alarmingly conquered Iraq's second largest city, Mosul.[435] A few weeks later, ISIS proclaimed itself as the 'Islamic State,' declared its leader, Abu Bakr al-Baghadi, the Caliph,[436] and Raqqa, Syria as its capital.[437] ISIS rose to

---

[431] Suadad al-Salhy and Tim Arango, "Sunni Militants Drive Iraqi Army Out of Mosul," *The New York Times,* June 10, 2014, accessed December 12, 2016, https://www.nytimes.com/2014/06/11/world/middleeast/militants-in-mosul.html.

[432] Ben Hubbard, "Qaeda Branch in Syria Pursues its Own Agenda," *The New York Times,* October 1, 2013, accessed December 12, 2016, http://www.nytimes.com/2013/10/02/world/middleeast/in-pushing-its-own-agenda-for-syria-a-qaeda-franchise-turns-rebels-into-enemies.html.

[433] Ben Hubbard, "Al Qaeda Breaks with Jihadist Group in Syria Involved in Rebel Fighting," *The New York Times,* February 3, 2014, accessed December 12, 2016, https://www.nytimes.com/2014/02/04/world/middleeast/syria.html.

[434] Ibid.

[435] al-Salhy and Arango, "Sunni Militants Drive Iraqi Army Out of Mosul."

[436] Matt Bradley, "ISIS Declares New Islamist Caliphate," *The New York Times,* June 29, 2014, accessed December 12, 2016, http://www.wsj.com/articles/isis-declares-new-islamist-caliphate-1404065263.

[437] Employee of The New York Times and Ben Hubbard, "Life in a Jihadist Capital: Order with a Darker Side," *The New York Times,* July 23, 2014, accessed December 12, 2016, https://www.nytimes.com/2014/07/24/world/middleeast/islamic-state-controls-raqqa-syria.html.

further infamy with its videotaped beheadings of Westerners[438] and increasing terrorist attacks around the world.[439]

In August 2014, the U.S. began airstrikes against ISIS.[440] A month later airstrikes came under the purview of Operation Inherent Resolve, a "broad international coalition to defeat ISIL."[441] In a letter to Congress on February 11, 2015, President Obama sought official authorization to use force against ISIS.

> The authorization I propose would provide the flexibility to conduct ground combat operations in other, more limited circumstances, such as rescue operations involving U.S. or coalition personnel or the use of special operations forces to take military action against ISIL leadership.[442]

Congress never approved this request but in October 2015, the U.S. sent about 50 special operations forces to Syria to advise military operations.[443]

---

[438] Rukmini Callimachi, "The Horror Before the Beheadings," *The New York Times,* October 25, 2014, accessed December 12, 2016, https://www.nytimes.com/2014/10/26/world/middleeast/horror-before-the-beheadings-what-isis-hostages-endured-in-syria.html.

[439] Karen Yourish et al., "How Many People Have Been Killed in ISIS Attacks Around the World," *The New York Times,* July 16, 2016, accessed December 12, 2016, http://www.nytimes.com/interactive/2016/03/25/world/map-isis-attacks-around-the-world.html.

[440] Helene Cooper, Mark Landler and Alissa J. Rubin, "Obama Allows Limited Airstrikes on ISIS." *The New York Times,* August 7, 2014, accessed December 12, 2016, https://www.nytimes.com/2014/08/08/world/middleeast/obama-weighs-military-strikes-to-aid-trapped-iraqis-officials-say.html.

[441] "Combined Joint Task Force - Operation Inherent Resolve (CJTF-OIR)," *U.S. Central Command,* accessed December 13, 2016, http://www.centcom.mil/OPERATIONS-AND-EXERCISES/OPERATION-INHERENT-RESOLVE/.

[442] Barack Obama, "Letter from the President – Authorization for the Use of United States Armed Forces in connection with the Islamic State of Iraq and the Levant," February 11, 2015, accessed December 12, 2016, *The White House*, https://www.whitehouse.gov/the-press-office/2015/02/11/letter-president-authorization-use-united-states-armed-forces-connection.

[443] Greg Jaffe and Thomas Gibbons-Neff, "Obama seeks to intensify operations in Syria with Special Ops troops," *The Washington Post,* October 30, 2015, accessed December 10, 2016, https://www.washingtonpost.com/politics/obame-decides-on-small-special-operations-force-for-syria/2015/10/30/a8f69c0e-7f13-11e5-afce-2afd1d3eb896_story.html?utm_term=.562b8fd2582d.

On November 13, 2015, ISIS killed over 120 people in coordinated terrorist attacks across Paris.[444] On December 2, 2015, a wife and husband loyal to ISIS, killed 14 people in a terrorist attack in San Bernardino, California.[445] Emboldened by ISIS' widening spate of massacres, the Obama administration launched cyberattacks against ISIS in 2016.[446] While this dissertation focuses on the U.S.' proposed cyber deployments against states, it is worth mentioning that the U.S. had started targeting non-state actors. President Obama supposedly asked why these cyberweapons that he has spent millions developing were not being used to fight this scourge upon the world.[447] President Obama issued a statement at C.I.A. headquarters on April 13, 2016, stating that the U.S. had launched over 11,500 airstrikes, had SOF in Syria and "Our cyber operations are disrupting their command-and-control and communications."[448] ISIS has managed to wage attacks and a successful recruitment campaign online.[449] So CYBERCOM installed 'implants' onto ISIS' networks

---

[444] Adam Nossiter, Aurelien Breeden and Katrin Bennhold, "Three Teams of Coordinated Attackers Carried Out Assault on Paris, Officials Say; Hollande Blames ISIS," *The New York Times,* November 14, 2015, accessed December 12, 2016, http://www.nytimes.com/2015/11/15/world/europe/paris-terrorist-attacks.html.

[445] Michael S. Schmidt and Richard Pérez-Peña, "F.B.I. Treating San Bernardino Attack as Terrorism Case," *The New York Times,* December 4, 2015, accessed December 12, 2016, http://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

[446] Brian Bennett, David S. Cloud and W. J. Hennigan, "Pentagon Weighs Cyber Campaign Against Islamic State," *Los Angeles Times,* December 20, 2015, accessed December 12, 2016, http://www.latimes.com/world/la-fg-cyber-isis-20151220-story.html.

[447] David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times,* April 24, 2016c, accessed August 20, 2017, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[448] Barack Obama, "Statement by the President on Progress in the Fight Against ISIL," April 13, 2016, accessed December 10, 2016, *The White House*, https://www.whitehouse.gov/the-press-office/2016/04/13/statement-president-progress-fight-against-isil.

[449] Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat."

in order to change their messages so that the militants were unknowingly lured into going to areas where they could be killed.[450] One official boldly proclaimed, 'We are dropping cyberbombs.'[451] This is a drastic change from just a few years ago when officials were extremely tight-lipped about anything with the prefix of cyber, not even confirming their role in Stuxnet or even admitting to having cyberweapons. The U.S. decided to open up about these operations because "a bit of boasting might degrade the enemy's trust in its communications, jumbling and even deterring some actions."[452] However, National Security Adviser, Susan Rice stated, "It should not be taken out of proportion — it is not the only tool."[453] Another official said, "We are not going to kill our way out of this conflict," "And we are not going to delete our way out of it, either."[454] The ISIS (2016) operation is a cyberweapon and thus, I have included it as a case study in this dissertation.

The Center for Strategic and Budgetary Assessments estimates that the monthly cost of a "lower-intensity air campaign" is $200 - $320 million, a "higher-intensity air campaign" is $350 - $570 million, and boots on the ground is one to two billion.[455] "As of October 15, 2016, the total cost of operations related to ISIL since kinetic operations started on August 8, 2014, is $10 billion and the average daily cost is $12.6 million for 800 days

---

[450] Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat."

[451] Ibid.

[452] Ibid.

[453] Ibid.

[454] Ibid.

[455] Todd Harrison et al., *Estimating the Cost of Operations Against ISIL*, (Center for Strategic and Budgetary Assessments, September 2014), 5, accessed December 13, 2016, http://csbaonline.org/uploads/documents/Estimating-the-Costs-of-Operations-against-ISIL.pdf.

of operations."[456] On December 13, 2016, an airstrike killed three of the ISIS terrorists involved in the November 2015 Paris attacks.[457] Over 45,000 ISIS militants have been killed.[458]

RUSSIA (2016)

After noticing strange activity in its systems in late April 2016, the Democratic National Committee hired cybersecurity firm CrowdStrike who discovered a group they named Cozy Bear, who might work for the Federal Security Service (Russia's equivalent of the C.I.A.)[459] Cozy Bear previously gained unauthorized access into the Joint Chiefs of Staff, State Department and the White House's "unclassified email systems" in 2014.[460] CrowdStrike suspected Cozy Bear had been in the D.N.C.'s network since 2015.[461] A separate group, who CrowdStrike named Fancy Bear, and probably worked for Russia's military intelligence, had gained unauthorized access to the D.N.C. in April 2016.[462] Ellen

---

[456] "Operation Inherent Resolve," *Department of Defense,* accessed December 13, 2016, http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve.

[457] Rukmini Callimachi, "3 ISIS Terrorism Planners Killed in Syria Airstrike, Pentagon Says," *The New York Times,* December 13, 2016, accessed December 13, 2016, http://www.nytimes.com/2016/12/13/world/middleeast/isis-airstrike-raqqa.html.

[458] Mark Thompson, "Former U.S. Commanders Take Increasingly Dim View of War on ISIS," *Time,* August 31, 2016, accessed December 13, 2016, http://time.com/4474910/isis-retired-generals/.

[459] Ellen Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump," *The Washington Post,* June 14, 2016c, accessed August 11, 2017, http://wapo.st/1tuiAUt?tid=ss_tw&utm_term=.664687e10d33.

[460] Ibid.

[461] Ibid.

[462] Ibid.

Nakashima of The Washington Post wrote, "The depth of the penetration reflects the skill and determination of the United States' top cyber-adversary as Russia goes after strategic targets" and Russia's espionage of gaining information about leaders is akin to American espionage.[463] It was unclear how the hackers gained access but CrowdStrike guessed it was because of 'spearfishing' emails.[464] "The hackers constantly switched tactics to maintain a stealthy presence inside the network and used built-in Windows tools so that they didn't have to resort to malicious code that might trigger alerts." [465] CrowdStrike's co-founder said, "They flew under the radar." [466] Perhaps the Russians were angry about sanctions levied by the West for Russia's illegal annexation of Crimea from Ukraine in 2014.[467] However, over the next year, the U.S. would learn that Russia had bigger ambitions.

On May 18, 2016, James Clapper, the Director of National Intelligence stated there were signs that Russian hackers tried to infiltrate the 2016 U.S. presidential campaign.[468] By June 14, 2016, *The Washington Post* reported that Russian hackers breached the presidential campaigns of candidates Donald Trump and Hillary Clinton however, it was the Democratic National Committee's systems that were "thoroughly compromised."[469]

---

[463] Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump."

[464] Ibid.

[465] Ibid.

[466] Ibid.

[467] Ibid.

[468] Ellen Nakashima, "National intelligence director: Hackers have targeted 2016 presidential campaigns," *The Washington Post,* May 18, 2016a, accessed August 20, 2017, https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html?utm_term=.ebd6e7b293ed.

On July 22, 2016, days before the Democratic National Convention, Wikileaks released almost 22,000 emails belonging to the D.N.C.[470] A group called Guccifer 2.0 claimed they gave this information to Wikileaks.[471] Many experts believed Guccifer 2.0 was Russian military intelligence.[472] By July 26, 2016, American intelligence officials stated they had "high confidence" that the Russians had stolen this information but they were unsure whether this was standard espionage or to influence the U.S. presidential election.[473] While espionage is as old as time, 'weaponizing' this information is atypical.[474]

Coincidentally, the Obama administration released Presidential Policy Directive 41, on the same day, which dictates how the U.S. will respond to severe cyberattacks, along with "a cyber incident severity schema"[475] which is a schema for ranking cyberattacks from

---

[469] Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump."

[470] "Search the DNC email database," *Wikileaks*, July 22, 2016, accessed August 12, 2017, https://wikileaks.com/dnc-emails/; Andrea Peterson, "Wikileaks posts nearly 20,000 hacked DNC emails online," *The Washington Post,* July 22, 2016, accessed August 12, 2017, https://www.washingtonpost.com/news/the-switch/wp/2016/07/22/wikileaks-posts-nearly-20000-hacked-dnc-emails-online/?utm_term=.5b46ca985699.

[471] Guccifer 2.0 (@GUCCIFER_2), "@wikileaks published #DNCHack docs I'd given them!!! #HillaryClinton #DonaldTrump #BernieSanders #Guccifer2," Twitter, July 22, 2016, 9:44 a.m., accessed August 12, 2017, https://twitter.com/GUCCIFER_2/status/756530278982684672.

[472] David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C.," *The New York Times,* July 26, 2016f, accessed August 12, 2017, https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.

[473] Ibid.

[474] Ibid.

[475] "FACT SHEET: Presidential Policy Directive on United States Cyber Incident Coordination," *The White House,* July 26, 2016, accessed December 2, 2016, https://www.whitehouse.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1.

Level 0 – 5. Level 5 (Black) is the most egregious since it "poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or to the lives of U.S. persons."[476] Interestingly, "about 2 percent of attacks on American systems, officials say, may rise to the level of prompting a national response."[477] The U.S. said the D.N.C. breach "would qualify as a 'significant cyber incident,' which was defined as one that causes 'demonstrable harm to the national security interests, foreign relations or economy of the United States, or to the public confidence, civil liberties or public health and safety of the American people.'" [478]

On August 16, 2016, a group named the Shadow Brokers claimed that they stole cyberweapons from the N.S.A. and were willing to sell them for one million bitcoins.[479] (The Shadow Brokers did not receive anything close to the one million bitcoins they were seeking.[480]) Edward Snowden said this theft was the work of the Russians.[481] *The Intercept* confirmed that these cyberweapons matched some of those they had previously reported

---

[476] "Cyber Incident Severity Schema," *The White House,* July 26, 2016, accessed December 2, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf.

[477] David E. Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *The New York Times,* April 23, 2015a, accessed December 1, 2016, http://nyti.ms/1ProCKP.

[478] Sanger and Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C."

[479] Andy Greenberg, "No One Wants to Buy Those Stolen NSA-Linked 'Cyberweapons,'" *Wired,* August 16, 2016, accessed November 1, 2016, https://www.wired.com/2016/08/no-one-wants-buy-stolen-nsa-linked-cyberweapons/.

[480] Ibid.

[481] Edward Snowden (@Snowden), "Circumstantial evidence and conventional wisdom indicates Russian responsibility. Here's why that is significant:," Twitter, August 16, 2016, accessed November 29, 2016, https://twitter.com/Snowden/status/765514891813945344.

on as well as those from Snowden's trove.[482] *The New York Times* alluded that the Shadow Brokers were Russians and this was a warning shot to the U.S. that if it retaliated against Russia, bigger American secrets would be exposed.[483] CYBERCOM was unfazed.[484] Most of these "weapons" were tools for espionage, not shutting something off or causing physical damage so it is debatable whether these devices were really weapons. (Wikileaks also tweeted that they were going to release their copy of the N.S.A.'s cyberweapons.[485])

In October 2016, one month before the U.S. presidential election, the Obama administration "formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee."[486] David Sanger of *The New York Times* declared that Russia had used "cyberweapons" against the U.S. in order to influence the 2016 U.S. presidential election.[487] While data theft is not uncommon, "Publishing the documents — what some have called 'weaponizing' them — is a different issue."[488] Two

---

[482] Sam Biddle, "The NSA Leak is Real, Snowden Documents Confirm," *The Intercept,* August 19, 2016, accessed November 10, 2016, https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/.

[483] Lipton, Sanger and Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S."

[484] Ibid.

[485] WikiLeaks (@wikileaks), "We had already obtained the archive of NSA cyber weapons released earlier today and will release our own pristine copy in due course," Twitter, August 15, 2016, 5:20 p.m., accessed November 29, 2016, https://twitter.com/wikileaks/status/765342384821534722.

[486] David E. Sanger, "U.S. Says Russia Directed Hacks to Influence Elections," *The New York Times,* October 7, 2016d, accessed December 1, 2016. http://nyti.ms/2dLddLS.

[487] David E. Sanger, "Under the Din of the Presidential Race Lies a Once and Future Threat: Cyberwarfare," *The New York Times,* November 6, 2016e, accessed November 30, 2016, http://nyti.ms/2etAn66.

[488] Sanger and Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C."

days before the U.S. presidential election, Sanger stated that cyberwarfare is the biggest takeaway of the 2016 election. "It is the first time that a foreign power has unleashed cyberweapons to disrupt, or perhaps influence, a United States election."[489] Since the U.S. has always been preoccupied with a "cyber Pearl Harbor," "this is a very different use of power than what the Obama administration has long prepared the nation for."[490]

While it is debatable whether these Russian cyberattacks were in fact cyberweapons since there was no intended or actual physical damage, the U.S.' response is key. The Obama administration thought about "using economic sanctions to covert action against Russian targets, potentially including the computers used in the hack."[491] Cyber scholar Adam Segal said sanctions was one of the non-cyber responses that the U.S. should have taken.[492] However, Russia had already warned the U.S. not to institute more sanctions against them because of their role in Aleppo.[493] President Obama had not discussed the Russian cyberattacks in great detail but his preference was "to deal with the problem by developing new norms of international behavior or authorizing covert action rather than direct confrontation."[494] Initially, the Obama administration was waiting for the conclusion

---

[489] Sanger, "Under the Din of the Presidential Race Lies a Once and Future Threat: Cyberwarfare."

[490] Ibid.

[491] Sanger, "U.S. Says Russia Directed Hacks to Influence Elections."

[492] Adam Segal, "After Attributing a Cyberattack to Russia, the Most Likely Response Is Non Cyber," *Council on Foreign Relations* (blog), October 10, 2016a, accessed December 13, 2016, http://blogs.cfr.org/cyber/2016/10/10/after-attributing-a-cyberattack-to-russia-the-most-likely-response-is-non-cyber/.

[493] Will Worley, "Russia warns US of 'painful' response if it toughens existing sanctions over Syria," *Independent,* October 20, 2016, accessed December 13, 2016, http://www.independent.co.uk/news/world/europe/russia-us-sanctions-aleppo-syria-putin-obama-sergey-ryabkov-hollande-merkel-a7371096.html.

of the election to figure out a "proportional response."[495] But Sanger says "the announcement itself — an effort to 'name and shame' — will deter further action."[496]

Supposedly, Admiral Rogers (the head of CYBERCOM) wanted to reveal Putin's ties to oligarchs and unshackle Russia's internet thereby enabling protestors to speak.[497] However, other Pentagon officials proposed more indirect options.[498] (None of these suggestions were officially shared with the President.[499]) Other officials worried that these measures would work in Putin's favor or have repercussions on Election Day.[500] "Even something seemingly straightforward — using the president's executive powers, bolstered after the Sony incident, to place economic and travel sanctions on cyberattackers — seemed too risky."[501] At the G20 meeting in China, President Obama allegedly told Putin aside that the U.S. would respond strongly if Russia continued to interfere in the election.[502] President Obama also uncharacteristically mentioned U.S. offensive cyber capabilities saying 'Frankly, both offensively and defensively, we have more capacity.'[503]

---

[494] Sanger, "Under the Din of the Presidential Race Lies a Once and Future Threat: Cyberwarfare."

[495] Ibid.

[496] Sanger, "U.S. Says Russia Directed Hacks to Influence Elections."

[497] Lipton, Sanger and Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S."

[498] Ibid.

[499] Ibid.

[500] Ibid.

[501] Ibid.

[502] Ibid.

[503] Ibid.

According to NBCNews, President Obama asked the C.I.A. to provide him with a covert retaliatory cyber option.[504] Supposedly, this was not the first time the U.S. had considered using offensive cyber capabilities against Russia but in the past, the C.I.A. officers said they allegedly refrained because this was a "political decision," or "none of the options were particularly good, nor did we think that any of them would be particularly effective."[505]

The Russian case is interesting because "Until now, most American cyberattacks on adversaries have been covert operations."[506] But, when asked about the U.S.' response to Russia's attacks during an October 14th interview with *Meet the Press*, Vice President Joe Biden said, "we're sending a message. We have the capacity to do it and he'll [Putin] know it. It will be at the time of our choosing and under the circumstances that have the greatest impact."[507] Biden also said, "We will be proportional in what we do," and when asked whether Americans will know about this operation he said, "hope not."[508] However, other officials argued this operation needed to be unconcealed so that Russia knew the U.S. meant business.[509]

---

[504] William M. Arkin, Ken Dilanian and Robert Windrem, "CIA Prepping for Possible Cyber Strike Against Russia," *NBC News,* October 14, 2016, accessed August 12, 2017, http://www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636.

[505] Ibid.

[506] Sanger, "Pentagon Announces New Strategy for Cyberwarfare."

[507] Chuck Todd, "MTP Exclusive: VP Biden Promises Response to Russian Hacking," *Meet the Press* video*,* October 14, 2016, accessed December 2, 2016, http://www.nbcnews.com/meet-the-press/video/vp-biden-on-russia-and-cyber-warfare-786308675872.

[508] Ibid.

By daybreak of November 9, 2016, Donald Trump was declared the winner of the 2016 U.S. presidential election. On December 9, 2016, the C.I.A. "concluded with 'high confidence' that Russia acted covertly in the latter stages of the presidential campaign to harm Hillary Clinton's chances and promote Donald J. Trump."[510] The President-elect responded by pointing out the severely flawed intelligence on Iraq's W.M.D. program in 2003.[511] Just as with the Pakistan case, the flawed intelligence about Iraq's W.M.D. program once again permeated discussions however, unlike that flawed intelligence, there is mounting evidence that proves Russia influenced the 2016 U.S. presidential election. Although this case is evolving, I have included it as a case study in this dissertation which is one way in which my research is novel.

CONCLUSION

This chapter focused on alleged U.S. cyberweapons from 1994 – 2016 and debunked a few that were wrongly classified as such. As the interest in cyberweapons grows, so will the number of alleged cyberweapons. This is why it is crucial we understand the conditions of their usage. During an interview in March 2016, David Sanger of *The*

---

[509] Lipton, Sanger and Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S."

[510] David E. Sanger and Scott Shane, "Russian Hackers Acted to Aid Trump in Election, U.S. Says," *The New York Times,* December 9, 2016g, accessed December 10, 2016, http://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html.

[511] Mark Mazzetti and Eric Lichtblau, "C.I.A. Judgment on Russia Built on Swell of Evidence," *The New York Times,* December 11, 2016, accessed December 12, 2016, http://www.nytimes.com/2016/12/11/us/politics/cia-judgment-intelligence-russia-hacking-evidence.html?ref=politics.

New York Times asked the Republican presidential nominee Donald Trump **"**how would you envision using cyberweapons?" to which Trump responded

> certainly cyber has to be in our thought process, very strongly in our thought process. Inconceivable that, inconceivable the power of cyber. But as you say, you can take out, you can take out, you can make countries nonfunctioning with a strong use of cyber. I don't think we're there. I don't think we're as advanced as other countries are.[512]

An evasive answer to a very important question, which only the President of the United States has the ultimate authority to answer. Mr. Trump is now the 45th President of The United States so we will see whether he will have more articulate thoughts on the subject forthcoming.

[512] Maggie Haberman and David E. Sanger, "Transcript: Donald Trump Expounds on His Foreign Policy Views," *The New York Times,* March 26, 2016, accessed March 30, 2016, http://www.nytimes.com/2016/03/27/us/politics/donald-trump-transcript.html.

Chapter 5

QUANTITATIVE ANALYSIS

This chapter reports the results of empirical testing of 13 cases where the U.S. used or debated about using an offensive cyberweapon from 2001 – 2016. The cyberweapons were Stuxnet, Iraq (2007), Shotgiant (2007), Quantum (2008), Turbine (2010), Nitro Zeus, Libya (2011), Pakistan (2011), Syria, North Korea (2014), ISIS (2016), Russia (2016), and Iraq (2003). Although there were at least 3 other cases that could have been defined as cyberweapons: the Trans-Siberian pipeline (1982), Haiti (1994) and Serbia (1999) because they caused physical damage or intended to shut things off, I decided not to include these cases. I chose 2001 as the beginning of the timeframe because when Kaspersky Lab analyzed the 50-page N.S.A. catalog of devices published by Der Spiegel, they discovered 'implants' that dated back to 2001.[1]

This dissertation focused on sophisticated operations where the intention was destruction not espionage, website defacements or data theft. Thus, cyber operations such as Regin, Flame and Duqu which may have been deemed "cyberweapons" by others, were not identified as such in this dissertation. Additionally, this dissertation was interested mainly in cyberwarfare between the U.S. and other states, not the U.S. and non-state actors, but ISIS was included since some believe ISIS is an example of the complementary role cyberweapons will play in future military conflicts.[2]

---

[1] Kevin Poulsen, "Surprise! America Already has a Manhattan Project for Developing Cyber Attacks," *Wired,* February 18, 2015, accessed June 1, 2016, https://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/.

This study was also primarily concerned with first-strike deployments by the U.S., not retaliation for an attack, however I included the U.S.' response to North Korea's cyberattack against Sony since the U.S. allegedly responded by shutting off North Korea's Internet.[3] I also included the U.S.' response to Russia's role in the 2016 U.S. presidential election. According to the 2015 DoD Cyber Strategy, one of the purposes of offensive cyber operations is "to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace."[4]

The unit of analysis was the foreign policy decision whether to deploy or not deploy a cyberweapon. I used the STATA program to perform cluster analysis on these 13 cyberweapons in order to uncover patterns and develop an empirical typology of cyberweapon attacks. Next, I examined the correlates associated with the different types of attacks. These results were then assessed against the proposed hypotheses as well as the major themes highlighted in the Literature Review. Quantitative analysis of prior cyberweapons was useful in understanding if the U.S. adhered to their stated procedures as well as proposing future conditions under which the U.S. could use these weapons.

---

[2] David E. Sanger, "*Zero Days* Screening," (discussion, Harvard University, Cambridge, Massachusetts, April 29, 2016a); "U.S. Cyber Policy and Innovation" (discussion, EastWest Institute, New York, N.Y., November 3, 2016).

[3] Nicole Perlroth and David E. Sanger, "North Korea Loses its Link to the Internet," *The New York Times,* December 22, 2014, January 28, 2015, http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

[4] Department of Defense, *The DoD Cyber Strategy*, (April 2015), 5, accessed March 27, 2016, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

CLUSTER ANALYSIS

Cluster analysis is useful for small datasets. "Clustering methods are designed to create homogenous groups of cases or entities called clusters." [5] Cluster analysis detects "structure in data that is not readily apparent by visual inspection or by appeal to other authority."[6] There are four goals of cluster analysis:

(1) "development of a typology or classification,

(2) investigation of useful conceptual schemes of regrouping entities,

(3) hypothesis generation through data exploration, and

(4) hypothesis testing, or the attempt to determine if types defined through other procedures are in fact present in a data set."[7]

In this study, I used cluster analysis to develop a classification, investigate the groups that were formed, and test some of my proposed hypotheses and conditions that were discussed in the Literature Review such as covert, collateral damage and conventional enabler.

The most common rule used in social science is the hierarchical agglomerative clustering procedure[8] where each observation is its own group[9] and cases are added to this cluster instead of forming new groups.[10] By the end of the process, everything is lumped

---

[5] Mark S. Aldenderfer and Roger K. Blashfield, *Cluster Analysis* (Newbury Park, CA: Sage University Paper series on Quantitative Applications in the Social Sciences No. 07-044, 1984), 9.

[6] Ibid., 16.

[7] Ibid., 9.

[8] Ibid., 35.

[9] Ibid., 36.

[10] Ibid., 16.

together into one big group.[11] Thus, "The key to using cluster analysis is knowing when these groups are 'real' and not merely imposed on the data by the method."[12] It is very likely that the researcher can be guilty of 'naïve empiricism' which is "the collection and subsequent analysis of as many variables as possible in hope that the 'structure' will emerge if only enough data are obtained."[13] This was a concern in this dissertation as I tried to piece together this puzzle without a full picture. Therefore, since I took educated guesses to fill in the information I did not know, selection bias was possible. There are probably more cyberweapons that we do not know about and for the ones that we do know of, publicly available information is scarce and the information that we do have is ambiguous. For instance, the initial start date of Nitro Zeus and Shotgiant are unclear. This is important because a limitation of cluster analysis is that if you change the order of the data or if you use a different method, you can wind up with different results.[14]

QUANTITATIVE PROCEDURES

Cluster analysis specifies that first a sample has to be identified.[15] In this study, the cluster sample was Stuxnet, Iraq (2007), Shotgiant (2007), Quantum (2008), Turbine (2010), Nitro Zeus, Libya (2011), Pakistan (2011), Syria, North Korea (2014), ISIS (2016), Russia (2016), and Iraq (2003). Stuxnet was the basis for the cluster analysis since that is

[11] Aldenderfer and Blashfield, 36.

[12] Ibid., 16.

[13] Ibid., 20.

[14] Ibid., 37.

[15] Ibid., 12.

the operation that many scholars labeled as the world's first cyberweapon. The rest of the cyberweapons were listed in chronological order with the exception of Iraq (2003) which I listed last.

Next, variables had to be defined.[16] The variables are presented and operationally defined in Table 5.1. I collected the name of the cyberweapon (if that was not available, I labeled it according to the target country), whether the target was a perceived adversary, whether the target was the military sector (air defense systems, military communications systems, "weapons capabilities,"[17] etc.), whether there were other options that could have achieved the intended goal, whether this cyberweapon was part of a conventional operation, whether collateral damage (casualties, spillover or retaliation) was a concern, whether this operation was covert and whether the cyberweapon was deployed.

Table 5.1: Variables

Variable Name	Operationalization	Coding
PERCEIVED ADVERSARY	Was the cyberweapon targeting a real or perceived adversary (Russia, Iran, China, North Korea)?	1 = Yes 0 = No
MILITARY SECTOR	Was the cyberweapon targeting the military sector (air defense systems, military communications systems, or "weapons capabilities")?	1 = Yes 0 = No
OTHER ALTERNATIVES	Were other alternatives (troops, airstrikes or drones) capable of accomplishing this goal?	1 = Yes 0 = No
CONVENTIONAL ENABLER	Was this cyberweapon a conventional enabler for a	1 = Yes 0 = No

[16] Aldenderfer and Blashfield, 12.

[17] *The DoD Cyber Strategy*, 14.

	conventional military conflict?	
COLLATERAL DAMAGE	Was the U.S. concerned that this cyberweapon could have other consequences?	1 = Yes 0 = No
COVERT	Was the U.S. concerned about this cyberweapon being covert?	1 = Yes 0 = No
DEPLOYED	Was the cyberweapon deployed?	1 = Yes 0 = No

I chose PERCEIVED ADVERSARY as a variable in order to test whether these weapons were being used against Russia, China, Iran, and North Korea, countries the U.S. has listed as their adversaries in this arena.[18] In the cases where the U.S. was at war or about to go to war with that country, PERCEIVED ADVERSARY was also marked Yes. According to Presidential Policy Directive 20, adversaries fall under the Geography category which is a consideration for engaging in offensive cyberwarfare.[19]

I chose MILITARY SECTOR as a variable in order to understand what these cyberweapons were targeting. I chose OTHER ALTERNATIVES as a variable in order to test whether this condition that was discussed in the Literature Review was plausible. I chose CONVENTIONAL ENABLER as a variable because I attended an event at the EastWest Institute on November 3, 2016 called "U.S. Cyber Policy and Innovation" where

[18] Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," *The Washington Post,* August 30, 2013, accessed March 22, 2016, https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[19] "Presidential Policy Directive," 13, in Glenn Greenwald and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian,* June 7, 2013b, accessed November 1, 2014, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

a U.S. Cyber Command employee said offensive cyber operations were a "conventional enabler."[20] This statement coincides with the member of the Special Operations Forces who told Jeffrey Carr in 2011 that the U.S. government was deploying cyberweapons[21] "in combat in Iraq and Afghanistan when they can be employed as part of the U.S. rules of engagement."[22] This statement also coincides with the 2015 DoD Cyber Strategy which states one of the goals of offensive cyber operations is "to support military operations and contingency plans."[23]

This U.S. Cyber Command employee also stressed the role of collateral damage in the decision-making calculus[24] which is a theme that was also discussed in the Literature Review. Collateral damage could be civilian casualties, retaliation, or norms such as in the case of Libya where the U.S. worried that deploying a cyberweapon would set a bad precedent.[25] This employee also mentioned that Christopher Painter, the Coordinator for Cyber Issues at the State Department, was a strong advocate of norms in discussions with USCYBERCOM.[26] Thus, I chose to test COLLATERAL DAMAGE.

---

[20] "U.S. Cyber Policy and Innovation" (discussion, EastWest Institute, New York, N.Y., November 3, 2016).

[21] Jeffrey Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," *Bulletin of the Atomic Scientists* 69, no. 5 (September 1, 2013): 36, EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[22] Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," 35.

[23] *The DoD Cyber Strategy*, 5.

[24] "U.S. Cyber Policy and Innovation."

[25] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times,* October 17, 2011, accessed July 5, 2016, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

[26] "U.S. Cyber Policy and Innovation."

I chose COVERT as a variable because this was another condition discussed in the Literature Review. I also chose DEPLOYED as a variable because not all of these cyberweapons were ultimately deployed. All of the information was culled from public news sources such as *The Washington Post, The New York Times, Wired, The Guardian, The Intercept*, and *Der Spiegel*, as well as government documents such as the 2015 DoD Cyber Strategy and Presidential Policy Directive 20. I also used journal articles, the Snowden archive and technical reports issued by Symantec and Kaspersky Lab.

DATA

Table 5.2: Data

Operation	Was the cyberweapon targeting a real or perceived adversary (Russia, Iran, China, North Korea)?	Was the cyberweapon targeting the military sector (air defense systems, military communications systems, or "weapons capabilities")?	Were other alternatives (troops, airstrikes or drones) capable of accomplishing this goal?	Was this cyberweapon a conventional enabler for a conventional military conflict?	Was the U.S. concerned that this cyberweapon could have other consequences?	Was the U.S. concerned about this cyberweapon being covert?	Was the cyberweapon deployed?
Stuxnet	Yes	Yes	No	No	Yes	Yes	Yes
Iraq (2007)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Shotgiant	Yes	Yes	No	No	No	Yes	Yes
Quantum	No	Yes	No	No	No	Yes	Yes
Turbine	No	No	No	No	No	Yes	Yes
Nitro Zeus	Yes	Yes	No	Yes	Yes	No	No
Libya	Yes	Yes	Yes	Yes	Yes	No	No
Pakistan	No	Yes	Yes	Yes	Yes	Yes	No

Operation	Was the cyberweapon targeting a real or perceived adversary (Russia, Iran, China, North Korea)?	Was the cyberweapon targeting the military sector (air defense systems, military communications systems, or "weapons capabilities")?	Were other alternatives (troops, airstrikes or drones) capable of accomplishing this goal?	Was this cyberweapon a conventional enabler for a conventional military conflict?	Was the U.S. concerned that this cyberweapon could have other consequences?	Was the U.S. concerned about this cyberweapon being covert?	Was the cyberweapon deployed?
Syria	Yes	Yes	Yes	No	Yes	Yes	No
North Korea	Yes	No	Yes	No	Yes	Yes	Yes
ISIS	Yes	Yes	Yes	Yes	No	No	Yes
Russia	Yes	No	Yes	No	Yes	Yes	No
Iraq (2003)	Yes	No	Yes	Yes	Yes	No	No

Stuxnet targeted Iran, a perceived adversary of the United States.[27] So I coded PERCEIVED ADVERSARY Yes. The target sector was nuclear infrastructure which was out of the reach of airstrikes, drones and troops.[28] Thus, I coded MILITARY SECTOR Yes and OTHER ALTERNATIVES No. Stuxnet was not a precursor for a conventional military operation and the U.S. was concerned about collateral damage. [29] Thus, I coded CONVENTIONAL ENABLER No and COLLATERAL DAMAGE Yes. The U.S. was

[27] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012a), 188-191.

[28] Ibid., 193.

[29] Ibid.

very keen on keeping Stuxnet covert which is why they have not officially admitted responsibility. Both COVERT and DEPLOYED were coded Yes.

Although Iraq is not listed as one of the U.S.' perceived adversaries in the cyber realm, I coded PERCEIVED ADVERSARY Yes because at the time, the U.S. was at war with Iraq. Since the target sector was the communication systems of the insurgents, I coded MILITARY SECTOR Yes.[30] I also coded OTHER ALTERNATIVES and CONVENTIONAL ENABLER Yes since this operation was one component of the 'surge.'[31] Harris also discussed the role of spillover and blowback so I coded COLLATERAL DAMAGE Yes even though this cyberweapon would be used to kill insurgents.[32] I also coded COVERT Yes since Harris said this was a "politically sensitive" operation. Since the cyberweapon was deployed, I coded DEPLOYED Yes.

Shotgiant targeted a perceived adversary since it targeted Huawei, a Chinese company, in order to possibly conduct offensive cyber operations against the Chinese army as well as "high priority targets" such as Iran.[33] Thus, I coded both PERCEIVED ADVERSARY and MILITARY SECTOR Yes. There were no other alternatives for achieving this intended goal. Additionally, Shotgiant was not a conventional enabler because it was not conceived as part of a conventional military operation. According to the

---

[30] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing Company, 2014), 8-10.

[31] Harris, 7.

[32] Harris, 9.

[33] David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *The New York Times,* March 22, 2014c, accessed January 28, 2015, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

literature, there was no discussion of collateral damage but the U.S. wanted Shotgiant to be covert. For these reasons, I coded OTHER ALTERNATIVES, CONVENTIONAL ENABLER and COLLATERAL DAMAGE No. I coded COVERT and DEPLOYED Yes.

Since Quantum is so widespread, it is unclear at the moment who the intended target was.[34] For this reason, I coded PERCEIVED ADVERSARY No. Among Quantum's many targets were the Russian and Chinese armies, thus, I coded MILITARY SECTOR Yes. There were no other alternatives for achieving such access and there was no mention of collateral damage in the literature about Quantum. Hence, I coded OTHER ALTERNATIVES and COLLATERAL DAMAGE No. This operation was not conceived as part of a conventional military operation so I coded CONVENTIONAL ENABLER No. However, the U.S. was concerned about keeping Quantum covert so I coded both COVERT and DEPLOYED Yes.

Turbine's eventual goal is to target "millions" of computers[35] which indicates that perhaps Turbine is targeting a wide swath of countries, not solely adversaries; so I coded PERCEIVED ADVERSARY No. We also do not know the specific goals of Turbine so I coded MILITARY SECTOR No. There were no other alternatives that could accomplish such broad access. This capability was not part of a conventional military operation and there was no discussion about collateral damage in the literature about Turbine. Thus, OTHER ALTERNATIVES, CONVENTIONAL ENABLER and COLLATERAL

---

[34] David E. Sanger and Thom Shanker, "N.S.A. Devises Radio Pathway Into Computers," *The New York Times,* January 14, 2014f, accessed January 28, 2015, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html.

[35] Ryan Gallagher and Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers With Malware," *The Intercept,* March 12, 2014, accessed May 13, 2016, https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.

DAMAGE were coded No. The U.S. wanted Turbine to be covert though so I coded COVERT Yes. I also coded DEPLOYED Yes.

Nitro Zeus was a backup plan in case the Iranian nuclear deal was unsuccessful and conflict erupted.[36] So Nitro Zeus was conceived as a conventional enabler. The target was Iran's air defense systems as well as the Fordo nuclear site. Thus, I coded PERCEIVED ADVERSARY, MILITARY SECTOR, and CONVENTIONAL ENABLER Yes. However, the Fordo site could not have been reached by drones, airstrikes or troops so I coded OTHER ALTERNATIVES No even though there were other methods of taking out Iran's air defenses. Collateral damage was a concern so I coded COLLATERAL DAMAGE Yes. Covertness was not mentioned in the literature about Nitro Zeus. So I coded COVERT No. In the end though, Nitro Zeus was not deployed since the U.S. struck a deal with the Iranians so I coded DEPLOYED No.

Libya was not a perceived adversary as defined above however, Libya was an adversary since the U.S. and NATO were about to launch missiles against Libya's air defense systems.[37] Thus, I coded PERCEIVED ADVERSARY, MILITARY SECTOR and OTHER ALTERNATIVES Yes. This operation would have been a conventional enabler since it was conceived as a precursor to NATO's bombing campaign. The U.S. was concerned about setting an unfavorable norm but not about the operation being covert.[38] Hence, I coded CONVENTIONAL ENABLER and COLLATERAL DAMAGE Yes but I

---

[36] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times,* February 16, 2016e, accessed May 10, 2016, http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

[37] Schmitt and Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya."

[38] Ibid.

coded COVERT No. In the end though, the U.S. decided not to deploy a cyberweapon against Libya so I coded DEPLOYED No.

During the May 2011 U.S. raid against Osama bin Laden, the U.S. thought about using a cyberweapon "to prevent Pakistani radars from spotting helicopters carrying Navy Seal commandos."[39] Pakistan was not a perceived adversary as defined above and the U.S. was not at war with Pakistan or about to go to war with Pakistan although they were conducting drone strikes in Pakistan so I coded PERCEIVED ADVERSARY No. Although the U.S. was not about to go to traditional war with Pakistan, I coded CONVENTIONAL ENABLER Yes because this cyberattack was a part of a secret military raid. Since this cyberweapon targeted Pakistan's radars, I coded MILITARY SECTOR Yes. However, this plan was rejected and "specially modified, radar-evading Black Hawk helicopters ferried the strike team, and a still-secret stealthy surveillance drone was deployed."[40] Thus, I coded OTHER ALTERNATIVES Yes. When considering the other options, President Obama cared about collateral damage so I coded COLLATERAL DAMAGE Yes although this was not explicitly stated since there is scarce public information about this operation. Additionally, since the military raid was a top secret operation, I coded COVERT Yes. However, this plan was rejected so I coded DEPLOYED No.

As discussed in the Cyberweapons chapter, the decision to deploy a cyberweapon in Syria first appeared in 2011 and continued throughout 2014. I decided to combine all of these considerations into one case. Syria was not a perceived adversary as defined above

[39] Schmitt and Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya."

[40] Ibid.

but Syria is an adversary because of their ongoing civil war and the spread of ISIS. Thus, I coded PERCEIVED ADVERSARY Yes. In early 2011, the U.S. thought about using a cyberweapon to target Syrian air defenses systems and other Syrian military facilities.[41] So I coded MILITARY SECTOR Yes. These cyber plans would have coincided with airstrikes thus; I coded OTHER ALTERNATIVES Yes. Despite the chemical attack in Syria, the Obama administration was extremely cautious about entangling the U.S. in another Middle Eastern conflict so President Obama stated he was not putting boots on the ground. Thus, I coded CONVENTIONAL ENABLER No (although the U.S. conducted airstrikes in Syria in 2014.[42]) The U.S. was very concerned about civilian casualties and wanted the weapon to remain covert. Hence, I coded COLLATERAL DAMAGE and COVERT Yes. In the end though, the U.S. decided not to deploy a cyberweapon against Syria so I coded DEPLOYED No.

When North Korea hacked Sony and threatened U.S. theaters, President Obama promised a proportional response.[43] Since North Korea is an adversary, I coded PERCEIVED ADVERSARY Yes. Coincidentally, North Korea's Internet went out a few days later.[44] So I coded MILITARY SECTOR No. This operation was not part of a

---

[41] David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times,* February 24, 2014b, accessed December 10, 2016, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?ref=davidesanger.

[42] Dan Roberts and Spencer Ackerman, "Barack Obama authorises air strikes against Isis militants in Syria," *The Guardian,* September 11, 2014, accessed June 1, 2017, https://www.theguardian.com/world/2014/sep/10/obama-speech-authorise-air-strikes-against-isis-syria.

[43] David E. Sanger, Michael S. Schmidt and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *The New York Times,* December 19, 2014e, accessed November 29, 2016, http://nyti.ms/1Gz1GF9.

[44] Perlroth and Sanger, "North Korea Loses Its Link to the Internet."

conventional military operation thus, I coded CONVENTIONAL ENABLER No. Since the U.S. implemented sanctions in January 2015,[45] I coded OTHER ALTERNATIVES Yes. We do not know if the U.S. was concerned about specific collateral damage but President Obama did say the response would be proportional so I coded COLLATERAL DAMAGE Yes. However, the U.S. wanted this operation to be covert, as demonstrated by the fact that they have not admitted responsibility so I coded COVERT Yes. I also coded DEPLOYED Yes even though *The New York Times* says it was the Chinese who took out North Korea's internet.[46]

Although ISIS was not a perceived adversary as defined above, ISIS is an adversary of the U.S. and by December 2015, the U.S. had launched more than 9,000 airstrikes against ISIS.[47] Additionally, the U.S. Cyber Command employee who spoke at the "U.S. Cyber Policy and Innovation" event included ISIS in the list of actors that pose the greatest cyber threat to the U.S.[48] Hence, I coded PERCEIVED ADVERSARY Yes. Just as in the Iraq (2007) operation, this operation targeted ISIS' online command-and-control operations[49] so I coded MILITARY SECTOR Yes. There were other alternatives of

---

[45] David E. Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *The New York Times,* April 23, 2015a, accessed December 1, 2016, http://nyti.ms/1ProCKP.

[46] Eric Lipton, David E. Sanger and Shane Scott, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times,* December 13, 2016, accessed December 14, 2016, http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?hp=undefined&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&_r=0.

[47] "President Obama on U.S. Strategy Against ISIS," *C-SPAN* video, December 14, 2015, accessed November 13, 2016, https://www.c-span.org/video/?402051-1/president-obama-statement-us-strategy-isis.

[48] "U.S. Cyber Policy and Innovation."

[49] David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times,* April 24, 2016c, accessed August 20, 2017,

accomplishing this goal since there were ongoing airstrikes. Hence, I coded OTHER ALTERNATIVES Yes. The U.S. is also at war with ISIS so I coded CONVENTIONAL ENABLER Yes. As far as we know, the U.S. was not concerned about this operation being covert or about collateral damage. Thus, I coded COLLATERAL DAMAGE and COVERT No. The Obama administration operationalized these cyberweapons in April 2016 so I coded DEPLOYED Yes.

Russia is a perceived adversary of the U.S. as defined above and re-emerged as a real adversary after their role in the 2016 U.S. presidential election. Thus, I coded PERCEIVED ADVERSARY Yes. However, I coded MILITARY SECTOR No since the U.S. supposedly wanted to target Russia's internet, its President and/or the computers that hacked the U.S.[50] Since the U.S. went with sanctions,[51] there were other means of accomplishing this goal so I coded OTHER ALTERNATIVES Yes. The U.S. was not about to conduct a military campaign against Russia so I coded CONVENTIONAL ENABLER No. The U.S. was worried about collateral damage related to Election Day[52] so I coded COLLATERAL DAMAGE Yes. The U.S. also wanted the operation to be covert so I coded COVERT Yes. However, I coded DEPLOYED No since the U.S. sanctioned Russia.

---

http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[50] Lipton, Sanger and Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S."

[51] David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *The New York Times,* December 29, 2016b, accessed January 13, 2017, https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=0.

[52] Ibid.

Although Iraq was not a perceived adversary as defined above, the U.S. was gearing up to invade Iraq in early 2003. Thus, I coded PERCEIVED ADVERSARY Yes. However, this offensive cyberweapon targeted the banking sector not the military sector. [53] Thus, I coded MILITARY SECTOR No. There were other alternatives in the works since this operation was a precursor to a conventional military conflict. Thus, I coded OTHER ALTERNATIVES and CONVENTIONAL ENABLER Yes. The Bush administration stated their concerns about collateral damage so I coded COLLATERAL DAMAGE Yes. However, the U.S. was not concerned about this operation being covert so I coded COVERT No. Even though the U.S. engaged in jamming telephone networks, I coded DEPLOYED No since the Bush administration decided against taking out Iraq's financial system.

Table 5.3 illustrates the coded dataset. The data was entered into STATA chronologically in ascending order according to their supposed date of inception with the exception of Iraq (2003) because I wanted Stuxnet to be the basis for the cluster analysis since many experts proclaimed Stuxnet the first cyberweapon.[54] So I listed Iraq (2003) last. As mentioned earlier, cluster analysis is affected by the order in which the data is entered. Thus, if I changed the order of these cyberweapons, I would have gotten different results.

---

[53] John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New York Times,* August 1, 2009, accessed July 5, 2016, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html.

[54] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* June 1, 2012b, accessed March 17, 2014, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

Table 5.3: Dataset

OPERATION	PERCEIVED ADVERSARY	MILITARY SECTOR	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COLLATERAL DAMAGE	COVERT	DEPLOYED
Stuxnet	1	1	0	0	1	1	1
Iraq (2007)	1	1	1	1	1	1	1
Shotgiant	1	1	0	0	0	1	1
Quantum	0	1	0	0	0	1	1
Turbine	0	0	0	0	0	1	1
Nitro Zeus	1	1	0	1	1	0	0
Libya	1	1	1	1	1	0	0
Pakistan	0	1	1	1	1	1	0
Syria	1	1	1	0	1	1	0
North Korea	1	0	1	0	1	1	1
ISIS	1	1	1	1	0	0	1
Russia	1	0	1	0	1	1	0
Iraq (2003)	1	0	1	1	1	0	0
TOTAL	**10**	**9**	**8**	**6**	**9**	**9**	**7**

RESULTS

After the data is entered, you have to use a cluster method.[55] I used STATA to perform the Ward's linkage method. Ward's linkage is a common method.[56] It "is designed to optimize the minimum variance within clusters (Ward, 1963)."[57] This means that Ward's linkage highlights the clusters that are the least different.[58]

[55] Aldenderfer and Blashfield, 12.

[56] Ibid., 38.

[57] Ibid., 43.

> At the first step of the clustering process, when each case is in its own cluster, the ESS [error sum of squares] is 0. The method works by joining those groups or cases that result in the minimum increase in the ESS. The method tends to find (or create) clusters of relatively equal sizes and shapes as hyperspheres.[59]

The command is shown below.

. cluster wardslinkage perceivedadversary militarysector otheralternatives conventionalenabler collateraldamage covert deployed, measure(L2)

cluster name: _clus_1

In order to portray the results, I used a dendrogram. "Dendrograms graphically present the information concerning which observations are grouped together at various levels of (dis)similarity."[60]A dissimilarity measure means cases are similar if "the distance between them is zero."[61] In other words, the greater the distance, the bigger the difference between cases. In a dendrogram, "Vertical lines extend up for each observation, and at various (dis)similarity values, these lines are connected to the lines from other observations with a horizontal line." [62] The longer the vertical line, the more separated those groups are.[63] Thus, "The height of the vertical lines and the range of the (dis)similar axis give visual clues about the strength of the clustering." [64] I used Ward's linkage with a

---

[58] Aldenderfer and Blashfield, 43.

[59] Ibid.

[60] *STATA Multivariate Statistics Reference Manual Release 13* (College Station, TX: STATA Press, 1985-2013), 113, accessed October 25, 2016, http://www.stata.com/manuals13/mv.pdf.

[61] Aldenderfer and Blashfield, 25.

[62] *STATA Multivariate Statistics Reference Manual Release 13*, 113.

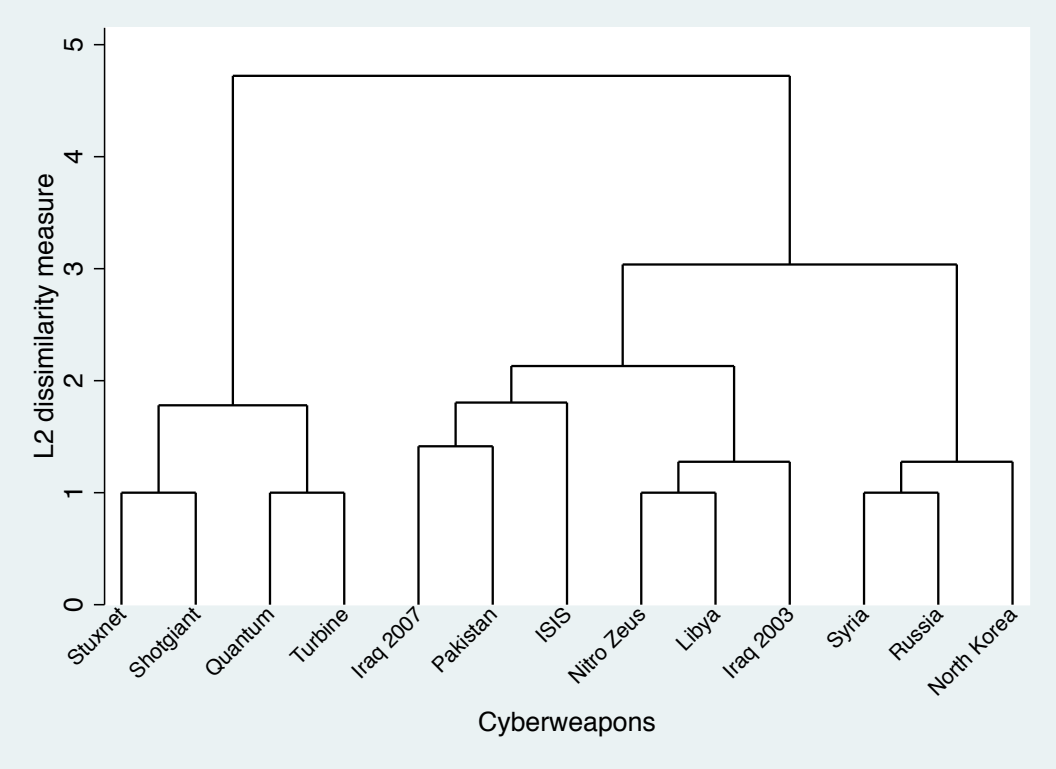
[63] Ibid., 114.

[64] Ibid.

Continuous measure of L2 or Euclidean, which is one of the most used distances.[65] The dendrogram command is shown below.

. cluster dendrogram _clus_1, labels(operation) lcolor(black) ylabel(, labels valuelabel tlcolor(black) glcolor(black)) ymtick(, labels valuelabel) xtitle(Cyberweapons) xlabel(, labels labsize(small) labcolor(black) angle(forty_five) valuelabel tposition(inside) nogrid) xmtick(, ticks tposition(inside))

Figure 5.1: Dendrogram for Cluster Analysis



This dendrogram portrays a dissimilarity measure from 0 – 5 with relatively short vertical lines which means that these clusters are not distinctly separated from each other. One way to determine the number of clusters is to look at the cluster height output.

[65] Aldenderfer and Blashfield, 25.

Table 5.4: Cluster Height

1
1.780239
1
4.7217216
1.4142136
1.8047379
2.1307683
1
1.2761424
3.0373974
1
1.2761424

Upon analyzing the heights, it looks like there is a big jump from 1.78 to 4.72 to 1.41 to 2.13 to 1.28 to 3.04 to 1.28 which indicates that there at least 6 clusters.

There is no definitive way of determining the number of clusters however, the two most common techniques are tests and heuristics.[66] "A hierarchical tree is 'cut' by the subjective inspection of the different levels of the tree."[67] Since heuristics are the most popular method and this dissertation used poliheuristic theory, I used heuristics to cut the dendrogram.[68] If we draw a vertical line to cut through the dissimilarity measure of 4.0, because that is where the biggest gap occurs between the branches, then we would get two

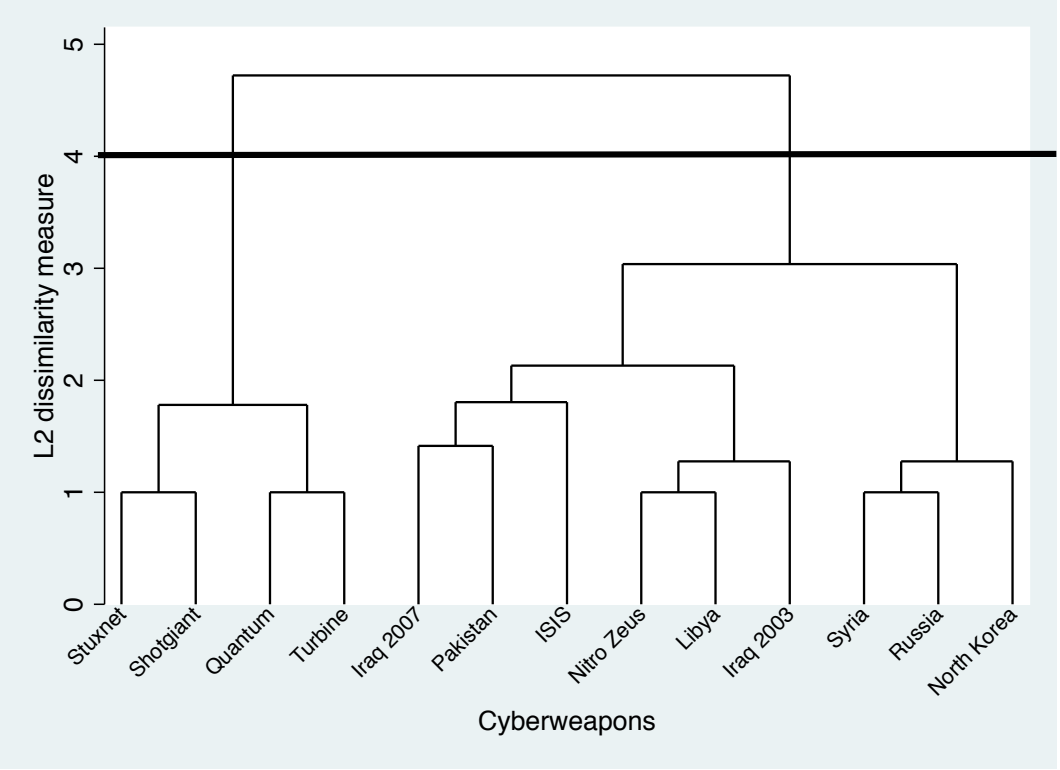
[66] Aldenderfer and Blashfield, 54.

[67] Ibid.

[68] Ibid., 14.

clusters. However, since heuristics are subjective, this is a limitation of using this technique as a way to determine the number of clusters.[69]

Figure 5.2: Cutting the Tree



The first group of clusters is (Stuxnet & Shotgiant) and (Quantum & Turbine). This cluster is grouped together because of OTHER ALTERNATIVES, CONVENTIONAL ENABLER, COVERT and DEPLOYED.

[69] Aldenderfer and Blashfield, 14.

Table 5.5: First Group of Clusters

OPERATION	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COVERT	DEPLOYED
Stuxnet	0	0	1	1
Shotgiant	0	0	1	1
Quantum	0	0	1	1
Turbine	0	0	1	1

This group of clusters is distinctly separated from the second group of clusters which is {[(Iraq 2007 & Pakistan) + ISIS] + [(Nitro Zeus & Libya) + Iraq 2003]} and {[Syria & Russia] + North Korea}. This cluster does not have any values in common so I think it was grouped together because it was distinct from the first group of clusters.

Table 5.6: Second Group of Clusters

OPERATION	PERCEIVED ADVERSARY	MILITARY SECTOR	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COLLATERAL DAMAGE	COVERT	DEPLOYED
Iraq 2007	1	1	1	1	1	1	1
Nitro Zeus	1	1	0	1	1	0	0
Libya	1	1	1	1	1	0	0
Pakistan	0	1	1	1	1	1	0
Syria	1	1	1	0	1	1	0
North Korea	1	0	1	0	1	1	1
ISIS	1	1	1	1	0	0	1
Russia	1	0	1	0	1	1	0
Iraq 2003	1	0	1	1	1	0	0

Another way to determine the number of clusters is via the cluster stop command.

Table 5.7: Cluster Stop

Number of Clusters	Calinski / Harabasz pseudo-F
2	5.56
3	5.25
4	4.72
5	4.54
6	4.65
7	4.5
9	4.54

STATA tells us that there are nine clusters in this dataset. So perhaps there are hidden clusters or false clusters in this dataset. Remember, different methods will produce different results[70] and "The key to using cluster analysis is knowing when these groups are 'real' and not merely imposed on the data by the method."[71] One problem with Ward's linkage is "that clusters with relatively few cases may be inappropriately absorbed into larger clusters."[72]

DISCUSSION

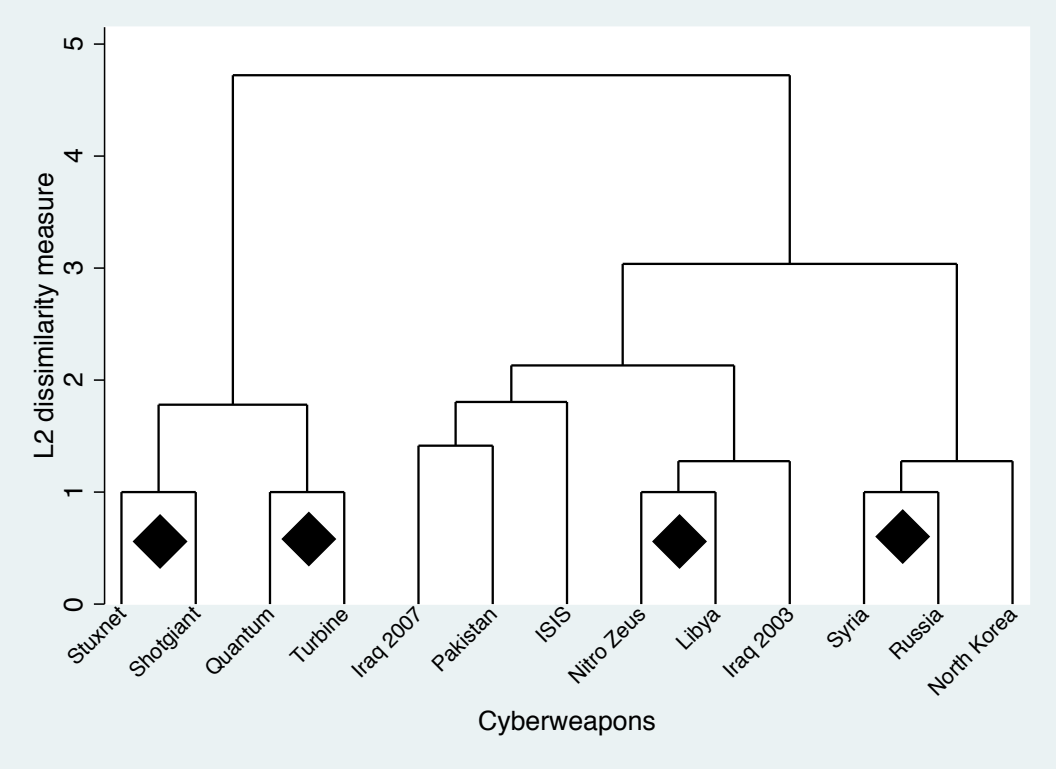
There are four clusters at the dissimilarity scale of 1.0, shown via black diamonds. They are [Stuxnet & Shotgiant]; [Quantum & Turbine]; [Nitro Zeus & Libya]; and [Syria & Russia]. These four clusters are the most similar to each other as indicated by their short vertical lines. Thus, these are the four strongest clusters in the dataset.

[70] Aldenderfer and Blashfield, 15.

[71] Ibid., 16.

[72] Ibid., 60.

Figure 5.3: Single Clusters



I think [Stuxnet & Shotgiant] were clustered because they both targeted a perceived adversary; they both targeted the military sector; there were no other alternatives that could have accomplished the intended goal; the operation was not a conventional enabler; the cyberweapon was covert; and the cyberweapon was deployed. It is interesting that Shotgiant is clustered with Stuxnet when there is scant literature about Shotgiant.

Table 5.8: Stuxnet & Shotgiant

OPERATION	PERCEIVED ADVERSARY	MILITARY SECTOR	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COVERT	DEPLOYED
Stuxnet	1	1	0	0	1	1
Shotgiant	1	1	0	0	1	1

So the typology for deployment here is PERCEIVED ADVERSARY, MILITARY SECTOR, no OTHER ALTERNATIVES, not a CONVENTIONAL ENABLER and COVERT.

[Quantum & Turbine] were clustered because they both did not target a perceived adversary; there were no other alternatives for accomplishing the intended goals; the operation was not a conventional enabler; collateral damage was not a major concern; the operation was covert and the cyberweapon was deployed.

Table 5.9: Quantum & Turbine

OPERATION	PERCEIVED ADVERSARY	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COLLATERAL DAMAGE	COVERT	DEPLOYED
Quantum	0	0	0	0	1	1
Turbine	0	0	0	0	1	1

So the typology for deployment here is not a PERCEIVED ADVERSARY, no OTHER ALTERNATIVES, not a CONVENTIONAL ENABLER, no COLLATERAL DAMAGE and COVERT.

[Nitro Zeus & Libya] were clustered because they both targeted a perceived adversary; they both targeted the military sector; these operations were both conventional enablers; collateral damage was a concern in both cases; both operations did not have to be covert and both cyberweapons were not deployed.

Table 5.10: Nitro Zeus & Libya

OPERATION	PERCEIVED ADVERSARY	MILITARY SECTOR	CONVENTIONAL ENABLER	COLLATERAL DAMAGE	COVERT	DEPLOYED
Nitro Zeus	1	1	1	1	0	0
Libya	1	1	1	1	0	0

So the typology for not deploying here is PERCEIVED ADVERSARY, MILITARY SECTOR, CONVENTIONAL ENABLER, COLLATERAL DAMAGE and not COVERT.

[Syria & Russia] were clustered because they both targeted a perceived adversary; there were other alternatives for accomplishing the intended goals; this operation was not a conventional enabler for a conventional military attack; collateral damage was a concern; the weapon had to be covert and the cyberweapon was not deployed.

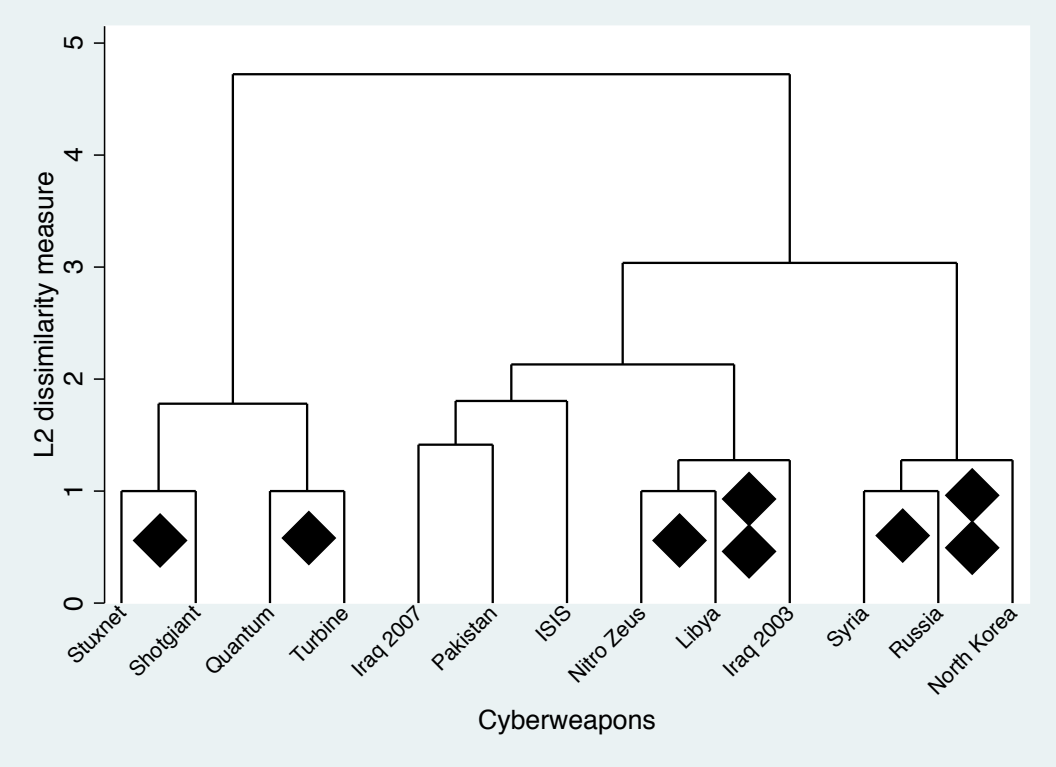
Table 5.11: Syria & Russia

OPERATION	PERCEIVED ADVERSARY	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COLLATERAL DAMAGE	COVERT	DEPLOYED
Syria	1	1	0	1	1	0
Russia	1	1	0	1	1	0

So the typology for not deploying here is PERCEIVED ADVERSARY, OTHER ALTERNATIVES, not a CONVENTIONAL ENABLER, COLLATERAL DAMAGE and COVERT.

These four clusters were then joined to other groups via short vertical lines indicating that these groups were not drastically different from the others.

Figure 5.4: The Fifth & Sixth Clusters

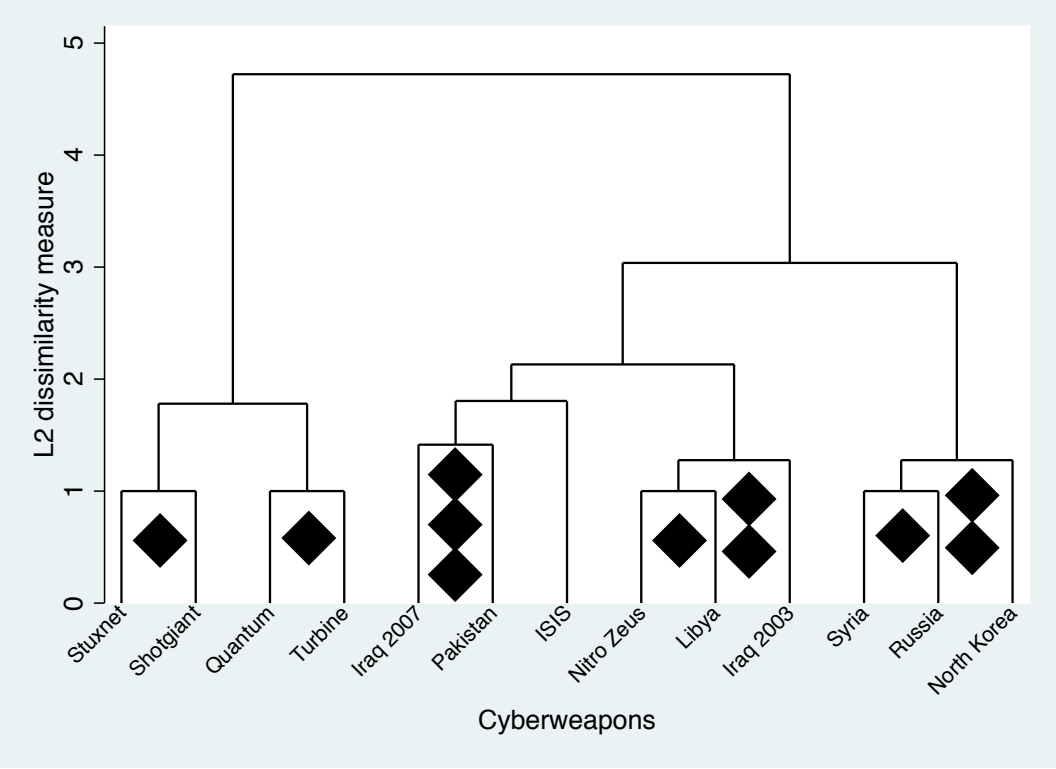


The 5th and 6th clusters, shown via two black diamonds, are [(Nitro Zeus & Libya) + Iraq 2003] and [(Syria & Russia) + North Korea]. These clusters are at the same dissimilarity scale. I think Iraq (2003) was grouped with the [Nitro Zeus & Libya] cluster because like [Nitro Zeus & Libya], the target was a perceived adversary; these operations were conventional enablers; collateral damage was a concern; these cyberweapons did not have to be covert and these cyberweapons were not deployed. However, unlike [Nitro Zeus & Libya], the target for Iraq (2003) was not the military sector. So the typology for not

deploying here is PERCEIVED ADVERSARY, CONVENTIONAL ENABLER, COLLATERAL DAMAGE and not COVERT.

The 6th cluster is [(Syria & Russia) + North Korea]. I think North Korea was grouped with the [Syria & Russia] cluster because like [Syria & Russia], the operation against North Korea targeted a perceived adversary; there were other alternatives for accomplishing the intended goal; this operation was not a conventional enabler; collateral damage was a concern and the weapon had to be covert. However, unlike [Syria & Russia], the cyberweapon was deployed in the North Korean case. So the typology here is PERCEIVED ADVERSARY, OTHER ALTERNATIVES, not a CONVENTIONAL ENABLER, COLLATERAL DAMAGE and COVERT.

Figure 5.5: The Seventh Cluster

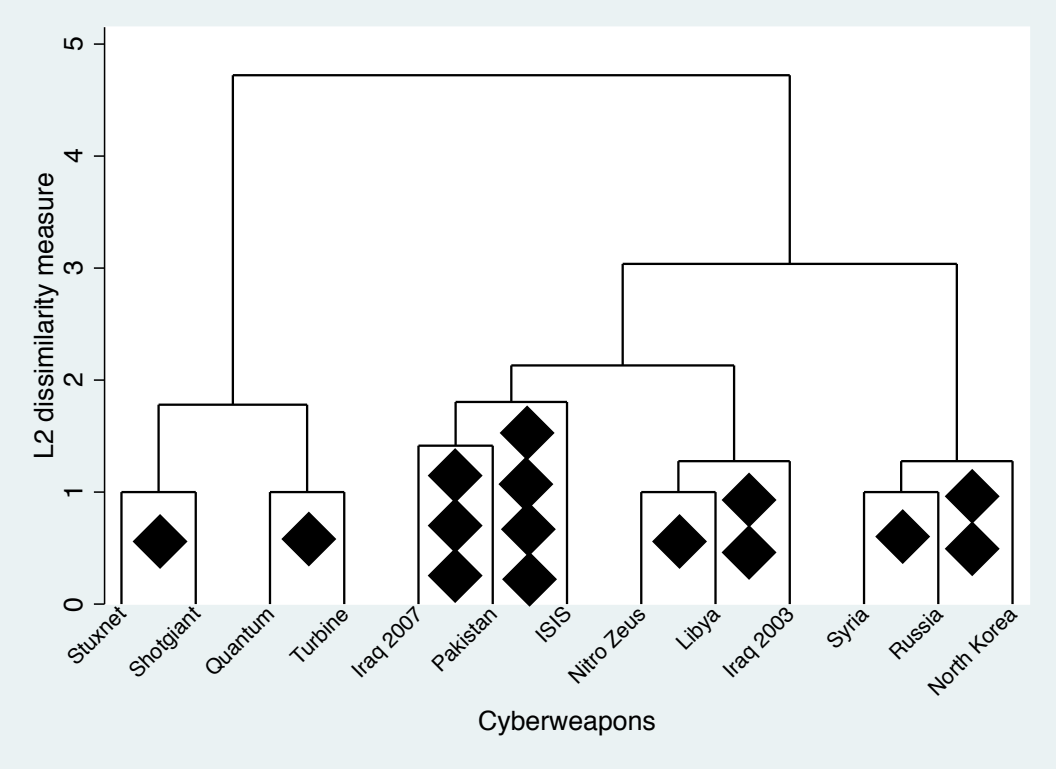


The 7th cluster, shown via three black diamonds, is [Iraq 2007 & Pakistan]. I think [Iraq 2007 & Pakistan] were clustered because the targets were the military sector, there were other alternatives for accomplishing the intended goals; the operations were conventional enablers; collateral damage was a concern; and the cyberweapons had to be covert. So the typology here is MILITARY SECTOR, OTHER ALTERNATIVES, CONVENTIONAL ENABLER, COLLATERAL DAMAGE and COVERT. It is interesting to note that all of the values are Yes.

Table 5.12: Iraq (2007) & Pakistan

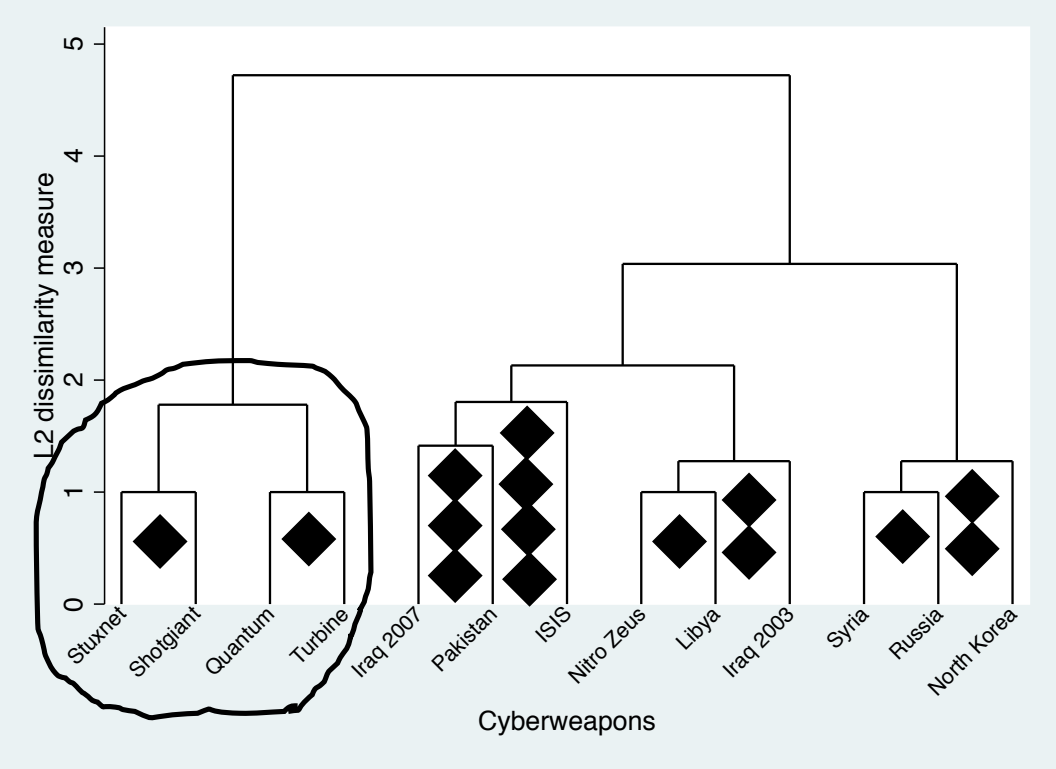
OPERATION	MILITARY SECTOR	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COLLATERAL DAMAGE	COVERT
Iraq (2007)	1	1	1	1	1
Pakistan	1	1	1	1	1

Figure 5.6: The Eighth Cluster



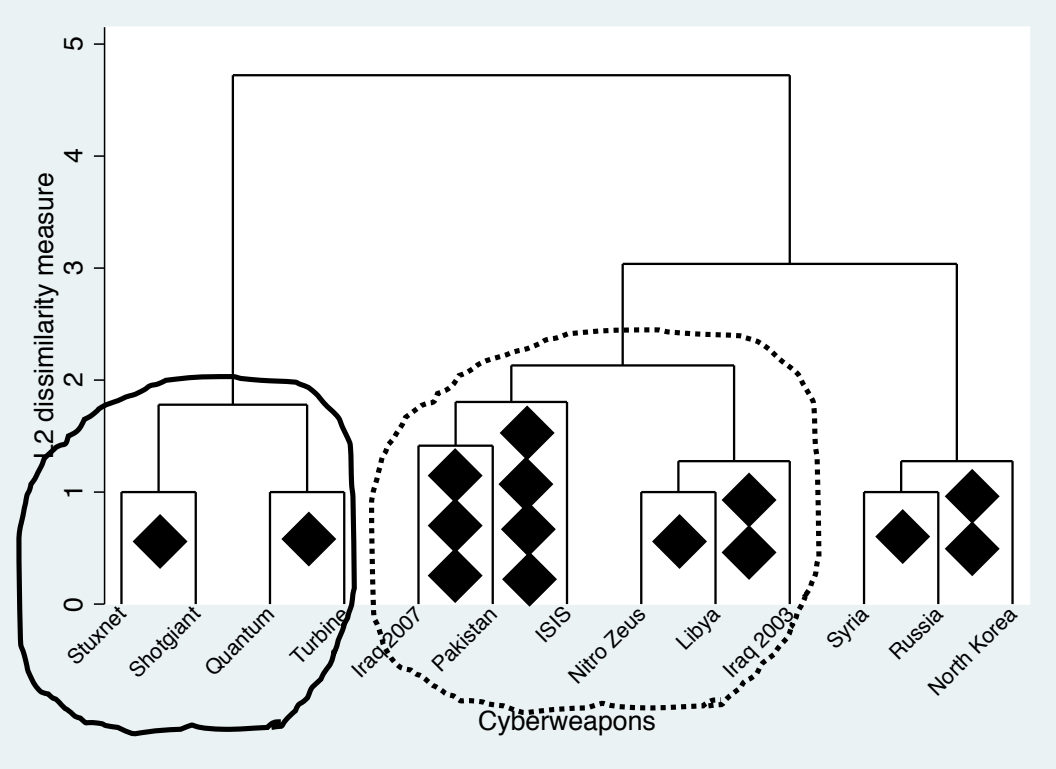
The 8th cluster, shown via 4 black diamonds is [(Iraq 2007 & Pakistan) + ISIS]. I think ISIS was clustered with [Iraq 2007 & Pakistan] because the target was the military sector, there were other alternatives for accomplishing the intended goals; and this cyberweapon was a conventional enabler. However, unlike [Iraq 2007 & Pakistan], collateral damage was not a concern in the ISIS case; and this cyberweapon did not have to be covert. So the typology here is MILITARY SECTOR, OTHER ALTERNATIVES and CONVENTIONAL ENABLER. Again, it is interesting to note that all of the values in this cluster are Yes.

Figure 5.7: The Ninth Cluster



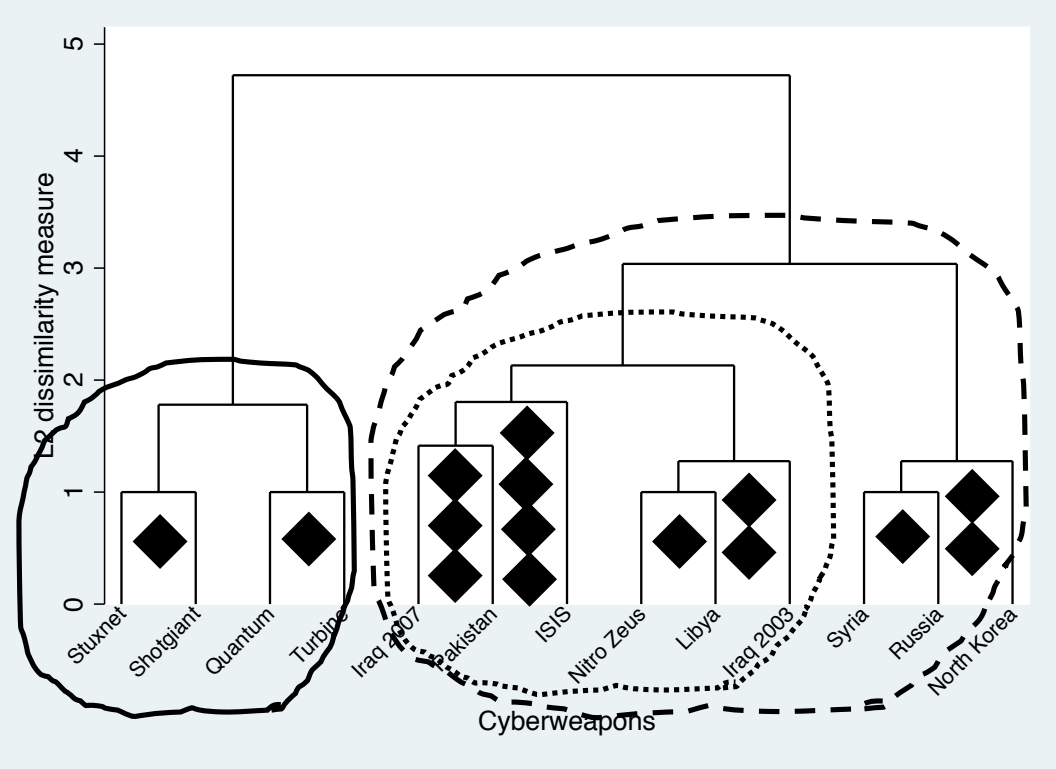
The 9th cluster, shown via the circle, is [Stuxnet & Shotgiant] + [Quantum & Turbine]. I think [Quantum & Turbine] was added to the [Stuxnet & Shotgiant] cluster because in the [Quantum & Turbine] cluster there were no alternatives, these cyberweapons were not conventional enablers; covertness did matter; and the cyberweapon was deployed. However, unlike [Stuxnet & Shotgiant], [Quantum & Turbine] did not target a perceived adversary. So the typology for deploying was no OTHER ALTERNATIVES, not a CONVENTIONAL ENABLER, and COVERT.

Figure 5.8: The Tenth Cluster



The 10th cluster, shown via a black dotted line is [(Iraq 2007 & Pakistan) and ISIS] + [(Nitro Zeus & Libya) and Iraq 2003]. I think this group is a cluster because in all of these cases, the cyberweapon was a conventional enabler.

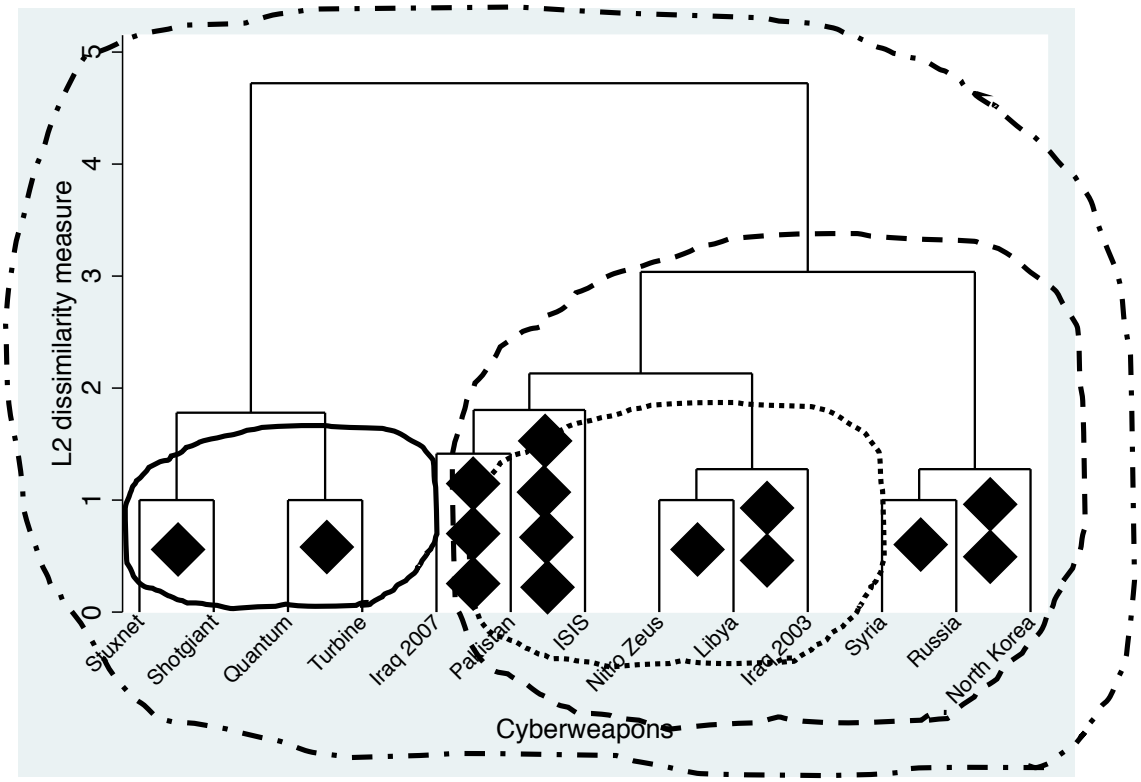
Figure 5.9: The Eleventh Cluster



The 11th cluster, circled in a black dashed line, is {[(Iraq 2007 & Pakistan) and ISIS] + [(Nitro Zeus & Libya) and Iraq 2003]} + [(Syria & Russia) and North Korea]. These clusters have nothing in common. As discussed earlier, one problem with Ward's linkage is "that clusters with relatively few cases may be inappropriately absorbed into larger clusters."[73] I think this is what happened here.

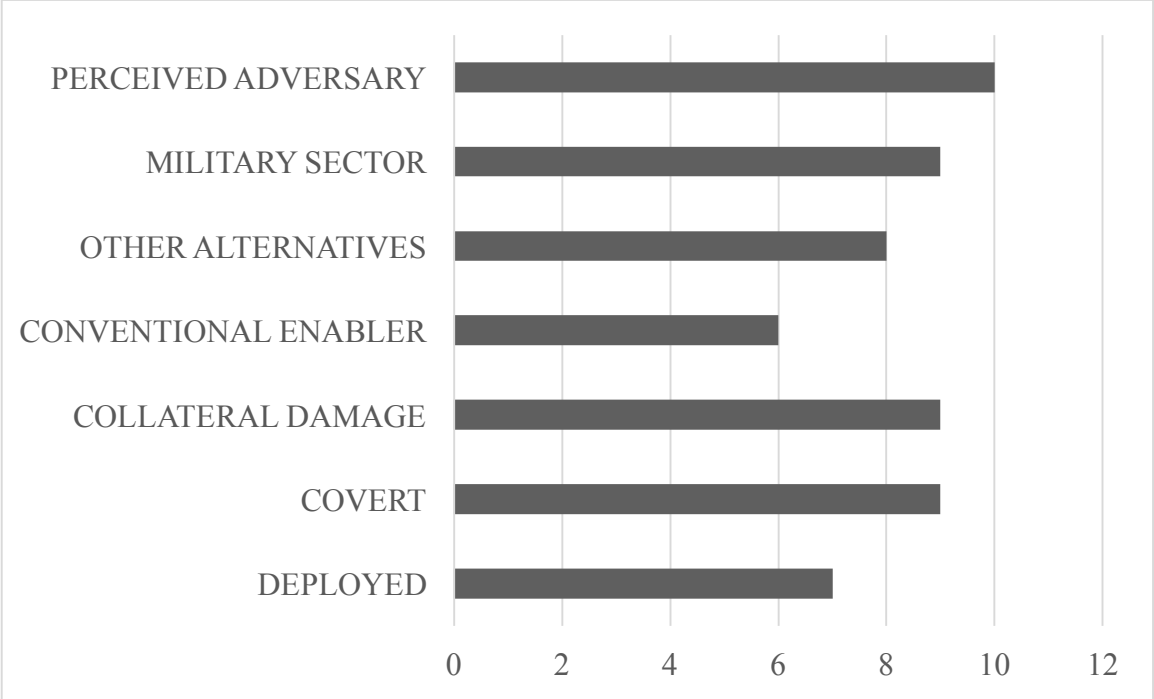
[73] Aldenderfer and Blashfield, 60.

Figure 5.10: The Final Cluster



The 12th and final cluster, circled in a large black dotted and dashed line, is {[Stuxnet & Shotgiant] and [Quantum & Turbine]} + {([(Iraq 2007 & Pakistan) and ISIS] and [(Nitro Zeus & Libya) and Iraq 2003]) and [(Syria & Russia) and North Korea]}. This is the last cluster where everything is grouped together so there is no typology. Now that we know there are 12 clusters, let us look at the frequency and profile of each variable.

Figure 5.11: Variable Frequency



The most important variable based on frequency is PERCEIVED ADVERSARY (n = 10). The second highest total is a three-way tie between COLLATERAL DAMAGE, MILITARY SECTOR with n = 9, and COVERT. Next is OTHER ALTERNATIVES with n = 8 and DEPLOYED with n = 7. CONVENTIONAL ENABLER is the least frequent variable with n = 6. In order to understand whether there is a relationship between the variables, let us look at whether these variables are correlated.

We can use the following command to calculate a pairwise correlation.

. pwcorr perceivedadversary militarysector otheralternatives conventionalenabler collateraldamage covert deployed

Table 5.13: Pairwise Correlation

	PERCEIVED ADVERSARY	MILITARY SECTOR	OTHER ALTERNATIVES	CONVENTIONAL ENABLER	COLLATERAL DAMAGE	COVERT	DEPLOYED
PERCEIVED ADVERSARY	1						
MILITARY SECTOR	0.0304	1					
OTHER ALTERNATIVES	**0.3175**	-0.1845	1				
CONVENTIONAL ENABLER	0.1409	0.2829	**0.4148**	1			
COLLATERAL DAMAGE	**0.426**	-0.0833	**0.5007**	0.2829	1		
COVERT	**-0.3651**	-0.0833	-0.1845	**-0.7201**	-0.0833	1	
DEPLOYED	-0.1409	0.0514	**-0.4148**	**-0.381**	**-0.6172**	**0.3858**	1

The correlation coefficient "ranges from -1 to 1 with 0 meaning no relationship."[74] A correlation of .10 is "small" or weak, a correlation of .30 is "moderate" and a correlation of .50 is "large"[75] or strong. I have bolded the moderate and large correlations.

Let us start with the profile of PERCEIVED ADVERSARY, the most frequent variable with n = 10. COLLATERAL DAMAGE and PERCEIVED ADVERSARY are positively correlated (0.43). Out of the 10 operations that targeted a perceived adversary, eight of them were concerned about collateral damage. This result suggests that if the

[74] Dahlia K. Remler and Gregg G. Van Ryzin, *Research Methods in Practice: Strategies for Description and Causation* (Thousand Oaks, California: SAGE Publications, 2011), 261.

[75] Remler and Van Ryzin, 262.

cyberweapon is targeting a perceived adversary, it is likely that that cyberweapon is concerned about collateral damage. This seems plausible because if the U.S. is preparing to attack a perceived adversary, it is likely that the U.S. will care about collateral damage. Thus, there is a relationship between COLLATERAL DAMAGE and PERCEIVED ADVERSARY.

PERCEIVED ADVERSARY and OTHER ALTERNATIVES were positively correlated (0.32). Out of 10 cyberweapons that targeted a perceived adversary, seven of these cases had other alternatives. This means that if the cyberweapon is targeting a perceived adversary, it is likely there are other alternatives.

On the other hand, COVERT and PERCEIVED ADVERSARY are negatively correlated (-0.37). Out of the 10 cyberweapons that targeted a perceived adversary, six of them were covert. This finding suggests that if the cyberweapon is targeting a perceived adversary, it is unlikely that the cyberweapon is covert. This seems plausible because if the U.S. is targeting someone who is an adversary, then it is possible that this would not be a covert attack. Thus, there is a relationship between COVERT and PERCEIVED ADVERSARY. This finding raised an interesting question in regards to the Five Eyes Alliance that was explored during the interviews: Do you think other countries in the Five Eyes Alliance would be likely to be informed before the US were to use a cyberweapon in a first strike? It is assumed that rivals will attack each other but what about allies?

Another interesting result from this correlation matrix is that DEPLOYED is negatively correlated to PERCEIVED ADVERSARY (-0.14). This finding suggests a small relationship between DEPLOYED and PERCEIVED ADVERSARY. When you look at the frequency totals, out of seven deployments, five targeted a perceived adversary.

This seems like a strong relationship, but the correlation is weak and negative which implies that the U.S. is using these weapons indiscriminately. This means if the cyberweapon is deployed, it is likely that it was not targeting a perceived adversary. Therefore, the following hypothesis might not be true: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary.* This finding raised an interesting question that was explored during the interviews: Can you think of one or more countries (or perceived adversaries) that the U.S. might use a cyberweapon against as a first strike? And why?

MILITARY SECTOR shared a three-way tie with COLLATERAL DAMAGE and COVERT with a frequency total of n = 9. However, MILITARY SECTOR is not strongly positively or negatively correlated to the other variables. This finding suggests that MILITARY SECTOR did not have a significant relationship with the other variables. DEPLOYED and MILITARY SECTOR had a small correlation of 0.05. Thus, perhaps the following hypothesis is null: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they believe they can destroy the intended target(s).* This finding raised an interesting question that was explored during the interviews: Against what sort of target or targets might the U.S. use a cyberweapon as a first strike?

COVERT, tied with MILITARY SECTOR and COLLATERAL DAMAGE, had a frequency total of n = 9. The strongest correlation in this matrix (and strongest negative correlation) is COVERT and CONVENTIONAL ENABLER (-0.72). Out of nine cyberweapons that were covert, two were conventional enablers (Iraq 2007 and Pakistan.) This finding suggests that if the cyberweapon is covert, it is unlikely to be a conventional enabler. This seems plausible because if the U.S. is using a covert cyberweapon, then they

are probably not gearing up for a conventional military conflict (since they are engaging in covert action), hence the cyberweapon would not be a conventional enabler. Thus, there is a relationship between COVERT and CONVENTIONAL ENABLER.

On the other hand, DEPLOYED and COVERT are positively correlated (0.39). Out of seven deployments, six were covert. ISIS was the only case where the operation was not covert and the U.S. deployed. Thus, this finding suggests that there is a relationship between DEPLOYED and COVERT. If the cyberweapon is covert, it is likely that it will be deployed. This seems plausible so perhaps COVERT is a possible condition for deploying these cyberweapons, reinforcing this claim discussed in the Literature Review. This result also raised an interesting question that was explored during the interviews: is cyberwarfare successful if we do not know about it?

However, DEPLOYED and CONVENTIONAL ENABLER are negatively correlated (-0.38). Out of seven deployments, two were conventional enablers. ISIS and Iraq (2007) were the only two cyberweapons that were conventional enablers and the U.S. deployed. So even though in theory the U.S. government states that cyberweapons are a conventional enabler, in practice, that was not the case. Thus, these weapons were not a force multiplier but rather a standalone operation thereby negating the U.S. Cyber Command employee's earlier claim. This finding also raised an interesting question that was explored during the interviews: What role do you think cyberweapons might play in concurrent military operations?

COLLATERAL DAMAGE, tied with COVERT and MILITARY SECTOR, has a strong positive correlation with OTHER ALTERNATIVES (0.50). This is the strongest positive correlation in this matrix. Out of nine cyberweapons that were concerned with

collateral damage, seven had other alternatives. Thus, this finding suggests that there is a relationship between COLLATERAL DAMAGE and OTHER ALTERNATIVES. If the cyberweapon is concerned with collateral damage, it is likely that there will be other alternatives. This seems plausible because if the cyberweapon can result in collateral damage, then it is likely that the U.S. is considering other alternatives as well.

DEPLOYED and COLLATERAL DAMAGE is strongly negatively correlated (-0.62). Out of seven deployments, three were deployed when collateral damage was a concern. Stuxnet, Iraq (2007), and North Korea were the only cases where collateral damage was a concern and the U.S. still deployed. This finding suggests that if a cyberweapon is deployed, it is highly unlikely there were serious concerns about collateral damage. This seems plausible. Thus, the following hypothesis might be true: *The U.S. will deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.*

OTHER ALTERNATIVES is an interesting variable because it was positively and negatively correlated to several other variables. CONVENTIONAL ENABLER and OTHER ALTERNATIVES had a positive correlation of 0.41. Out of six cyberweapons that were conventional enablers, five had other alternatives. Nitro Zeus was the only cyberweapon that was a conventional enabler but there were no other alternatives of accomplishing the intended goal. This finding suggests that if the cyberweapon is a conventional enabler, there are other alternatives. This seems plausible so there is a relationship between OTHER ALTERNATIVES and CONVENTIONAL ENABLER.

DEPLOYED and OTHER ALTERNATIVES had the same correlation except in this case, it was negative (-0.41). Out of seven deployments, three had other alternatives.

Iraq (2007), North Korea, and ISIS were the only cases where the U.S. had other alternatives but still deployed a cyberweapon. This finding suggests that if the cyberweapon was deployed, it is highly unlikely that there are other alternatives. The Literature Review suggested that an advantage of using these weapons is that they can access areas that are out of the reach of other alternatives. Thus, this seems plausible so there is a relationship between DEPLOYED and OTHER ALTERNATIVES and the following hypothesis might be true: *The U.S. will deploy a cyberweapon in a first strike against a perceived adversary if they cannot use troops, drones or airstrikes.*

CONCLUSION

After using STATA to perform cluster analysis on these 13 cases and seven variables, I uncovered that there were 12 clusters in the dataset, four of which had a dissimilarity measure of 1.0: [Stuxnet & Shotgiant]; [Quantum & Turbine]; [Nitro Zeus & Libya]; and [Syria & Russia]. These pairs of cyberweapons were the most similar and there were different typologies for both deployment and non-deployment. So then I ran a pairwise correlation in order to explore the relationship between the variables which revealed that the strongest relationship in this matrix (and strongest negative correlation) was COVERT and CONVENTIONAL ENABLER. This finding suggests that if the cyberweapon is covert, it is unlikely to be a conventional enabler. The strongest positive correlation in this matrix was COLLATERAL DAMAGE and OTHER ALTERNATIVES. This finding suggests that if the cyberweapon is concerned with collateral damage, it is likely that there will be other alternatives.

A result that reinforced themes discussed in the Literature Review was the finding that suggested there is a relationship between DEPLOYED and COVERT. This echoed the notion that COVERT is a possible condition for deploying cyberweapons. This result also raised an interesting question that was explored during the interviews: is cyberwarfare successful if we do not know about it?

A finding that negated claims discussed in the Literature Review was the negative correlation between DEPLOYED and CONVENTIONAL ENABLER. This correlation coefficient indicated that these cyberweapons were not a force multiplier but rather a standalone operation. This finding contradicts the statements by USCYBERCOM and others that cyberweapons are a component of conventional warfare. However, many of these weapons were created before USCYBERCOM and U.S. cyber doctrine. Thus, this finding was explored during the interviews with the question: What role do you think cyberweapons might play in concurrent military operations?

Another unexpectedly weak relationship was between DEPLOYED and PERCEIVED ADVERSARY. Thus, perhaps the following hypothesis might not be true: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary.* My hypotheses are built off of these two premises: first strike and a perceived adversary. So this finding was explored further during the interviews with the question: Can you think of one or more countries (or perceived adversaries) that the U.S. might use a cyberweapon against as a first strike? And why? One other interesting point is that COVERT and PERCEIVED ADVERSARY were negatively correlated which raised an interesting question that was explored during the interviews: Do you think other countries in the Five

Eyes Alliance would be likely to be informed before the US were to use a cyberweapon in a first strike?

Additionally, MILITARY SECTOR did not have a significant relationship with the other variables which suggested that the following hypothesis was null: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they believe they can destroy the intended target(s).* This finding raised an interesting question that was explored during the interviews: Against what sort of target or targets might the U.S. use a cyberweapon as a first strike?

There were two other relationships that suggested some of my hypotheses were true. The strong negative correlation between DEPLOYED and COLLATERAL DAMAGE suggested that if a cyberweapon is deployed, it is highly unlikely there were serious concerns about collateral damage. Thus, the following hypothesis might be true: *The U.S. will deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* The negative relationship between DEPLOYED and OTHER ALTERNATIVES implied that: *The U.S. will deploy a cyberweapon in a first strike against a perceived adversary if they cannot use troops, drones or airstrikes.*

These results are not generalizable because the results can change depending upon the method used. There was also a possibility of sampling bias because the conclusions were based upon the data entered and the coding is subject to interpretation. Additionally, although I combed through the Snowden archive, books, news articles, blogs and journals to cross check all of the cyberweapons I found, there are probably more cyberweapons that we do not know about. The exact number of unknown cyberweapons is hard to determine since there is a tendency to declare everything a cyberweapon. Furthermore, the scarce

knowledge we have about current cyberweapons is constantly changing. This is the nature of a highly classified subject. Thus, there was a cushion of two years to allow this evolving subject of cyberwarfare to unfold. During that time, the Shadow Brokers emerged as cyberweapons dealers, providing the public with access to these weapons.[76] Thus far, these "weapons" that have been deciphered by *The Intercept*[77] are not weapons according to the parameters of this dissertation. However, the Shadow Brokers might be affiliated with those who hacked the D.N.C. and after Trump launched airstrikes against Syria in 2017, the Shadow Brokers released more N.S.A. tools.[78]

Overall, these findings from the quantitative analysis were useful in exploring how the cyberweapons were grouped, developing a typology, understanding the relationships between the variables, testing proposed hypotheses, reinforcing and negating some claims in the Literature Review, and generating interview questions. The next two chapters will qualitatively explore the findings and questions generated in this chapter since there is a responsibility to learn more about these weapons in order to have an informed public discussion about future usage.

---

[76] Andy Greenberg, "No One Wants to Buy Those Stolen NSA-Linked 'Cyberweapons,'" *Wired,* August 16, 2016, accessed November 1, 2016, https://www.wired.com/2016/08/no-one-wants-buy-stolen-nsa-linked-cyberweapons/.

[77] Sam Biddle, "The NSA Leak is Real, Snowden Documents Confirm," *The Intercept,* August 19, 2016, accessed November 10, 2016, https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/.

[78] Nicole Perlroth, "Hacking Group Claims N.S.A. Infiltrated Mideast Banking System," *The New York Times,* April 15, 2017, accessed August 12, 2017, https://www.nytimes.com/2017/04/15/us/shadow-brokers-nsa-hack-middle-east.html.

Chapter 6

DECISION MATRIXES

The previous chapter applied cluster analysis to 13 cyberweapons in order to reveal patterns among the weapons. The results were that OTHER ALTERNATIVES, COVERT, and COLLATERAL DAMAGE were correlated to deployment and the following hypotheses might be true: *The U.S. will deploy a covert cyberweapon in a first strike if they cannot use troops, drones or airstrikes or in order to minimize collateral damage.*

This chapter applies poliheuristic theory to these 13 cyberweapons in order to qualitatively explain the President's past decisions to deploy or not deploy a cyberweapon. Again, the unit of analysis was the foreign policy decision whether to deploy or not deploy a cyberweapon but in this chapter, the explanatory dependent variables were: *THREAT, ACCESS, VIOLENCE,* and *COLLATERAL DAMAGE*. I chose to explore THREAT because the quantitative analysis suggested that these weapons were not being deployed against perceived adversaries so now we will look further to discern if that was because there needed to be a threat. I chose to explore ACCESS because the cluster analysis indicated that these weapons were being used in countries where the U.S. had no other alternatives; hence, was the intended target in a hard-to-reach area? I chose to explore VIOLENCE because in some cases, a cyberweapon was considered as a way to end or avoid war. I chose COLLATERAL DAMAGE because the cluster analysis suggested that cyberweapons were being deployed in order to minimize collateral damage. Therefore, this chapter tested the following hypotheses:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."*[1] [VIOLENCE]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

Since previous studies of poliheuristic theory utilized a decision matrix as their research instrument, I created a decision matrix for each cyberweapon. I used information culled from the government rules of engagement, academic frameworks, leaked N.S.A. documents and news articles discussed in the Literature Review and Cyberweapons chapters to create the dimensions and alternatives. The dimensions that were used in this study were Military, Political, Diplomatic and Economic, respectively, because in poliheuristic theory, order matters.

[1] Barry M. Blechman and Stephen S. Kaplan, *Force without War: U.S. Armed Forces as a Political Instrument* (Washington, D.C.: The Brookings Institution, 1978), 12.

STUXNET

According to Gallup, in January 2006, President Bush had an approval rating of 43% but that plummeted to 38% by the beginning of March.[2] During this time, Iran was considered the U.S.' greatest enemy.[3] 65% of those polled thought Iran posed a long-term threat.[4] 47% were "somewhat worried" about Iran developing a nuclear weapon.[5] In 2006, 41% of those polled were "somewhat concerned" that "the U.S. will not do enough to prevent Iran from developing nuclear weapons."[6] 68% of those polled wanted the U.S. to "use economic/diplomatic efforts" to entice Iran to stop its nuclear program.[7] If those measures were unsuccessful, 49% did not want the U.S. to "take military action against Iran."[8]

When Barack Obama came into office in 2009, he assumed office with a very high approval rating of 66%[9] since Wall Street had collapsed at the end of 2008,[10] propelling

---

[2] *Presidential Approval Ratings -- George W. Bush*, (Gallup), accessed December 10, 2016, http://www.gallup.com/poll/116500/presidential-approval-ratings-george-bush.aspx.

[3] Joseph Carroll, *Americans Say Iran Is Their Greatest Enemy*, (Gallup, February 23, 2006), accessed December 10, 2016, http://www.gallup.com/poll/21607/americans-say-iran-their-greatest-enemy.aspx.

[4] *Iran*, (Gallup), accessed December 10, 2016, http://www.gallup.com/poll/116236/iran.aspx.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] *Presidential Approval Ratings – Barack Obama*, (Gallup), accessed December 10, 2016, http://www.gallup.com/poll/116479/barack-obama-presidential-job-approval.aspx.

the U.S. into 'the worst financial crisis since the Great Depression.'[11] Of those polled in 2009, 56% wanted the U.S. to use diplomacy with Iran.[12]

Thus, using the sources discussed in the Literature Review and Cyberweapons chapters as well as the Gallup polls depicted above, we can create the following choice set for Stuxnet.

(1) do nothing

(2) continue talks

(3) increase sanctions

(4) implement airstrikes

(5) deploy a cyberweapon

Alternative 1: The U.S. can do nothing, anticipating that Iran is not trying to obtain a nuclear weapon.

Alternative 2: The U.S. could continue discussions to get Iran to agree to abandon its nuclear program.

Alternative 3: The U.S. could implement more sanctions to force Iran to agree to abandon its nuclear program.

Alternative 4: The U.S. could launch airstrikes against Iranian nuclear facilities.

---

[10] Andrew Ross Sorkin, "Lehman Files for Bankruptcy; Merrill Is Sold," *The New York Times,* September 14, 2008, accessed December 10, 2016, www.nytimes.com/2008/09/15/business/15lehman.html.

[11] Jon Hilsenrath, Serena Ng and Damian Paletta, "Worst Crisis Since '30s, With No End Yet in Sight," *The Wall Street Journal,* September 18, 2008, accessed December 10, 2016, http://www.wsj.com/articles/SB122169431617549947.

[12] *Iran*, (Gallup).

Alternative 5: The U.S. could use a cyberweapon against Iran to destroy their nuclear facilities.

The decision matrix consists of four dimensions and five alternatives. I listed the dimensions in order of increasing importance.

Table 6.1: Proposed Decision Matrix for Stuxnet

		Alternatives				
		Do nothing	Continue talks	Increase sanctions	Launch U.S. airstrikes	Deploy a cyberweapon
Dimension	Military	If we do nothing, Iran could get a nuclear bomb. This is unacceptable.	There are no implications for the military if the U.S. continues talks but are they really working?	There are no implications for the military if the U.S. increases sanctions but are they really working?	We cannot launch airstrikes since we are unsure of the exact location of Iran's nuclear facilities; the facilities are buried deep underground and an airstrike against Iran could have wider political ramifications such as the potential to start a war and risk retaliation and casualties.	This is the chance to test out a new weapon that could be deployed covertly and precisely and would strike at the heart of the problem without putting troops on the ground. However, there could be repercussions if the weapon leaks out.

		Do nothing	Continue talks	Increase sanctions	Launch U.S. airstrikes	Deploy a cyberweapon
Dimensions	Political	The global balance of power will shift if Iran were to acquire a nuclear bomb. Our greatest ally, Israel would be threatened as would the entire Middle East. This is unacceptable.	We could continue talks but are they really working?	We could increase sanctions. They are working.	We cannot implement airstrikes because we do not know where the facilities are and there can be casualties and retaliation.	We can do this covertly so the public will not know but, there could be repercussions if the weapon leaks out. Plus, do we want to work with the Israelis?
	Diplomatic	If we do nothing, the Israelis said they would launch an airstrike thereby potentially dragging us into a bigger conflict. This is unacceptable.	We should continue talks because this is the best diplomatic solution.	We could increase sanctions. They are working.	We should not launch airstrikes because airstrikes could result in casualties, be inaccurate, or the U.S. could be seen as overreaching.	If we use this option, we could be unleashing a new type of weapon into the world. Are we willing to do that when we do not know exactly how this weapon will work? There could be repercussions if the weapon leaks out.

		Do nothing	Continue talks	Increase sanctions	Launch U.S. airstrikes	Deploy a cyberweapon
Dimension	Economic	There are no economic implications if we do nothing.	There are no economic implications if we continue talks.	We should increase sanctions. They are effective.	Airstrikes cost millions of dollars.	Stuxnet took a lot of time, money and resources to create. (Some say $100 million.[13]) Once it is used, it cannot be used again but, it would be a way to effectively destroy our target.

Doing nothing and allowing Iran to acquire a nuclear weapon is noncompensatory on the military, political and diplomatic dimensions so that alternative is eliminated immediately. So we move to the second stage of the decision-making process with the following options below. In the case of Stuxnet, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in preventing Iran from acquiring a nuclear weapon?* I decided to rate each alternative on a scale of 1 to 4. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

[13] David Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," *International Business Times,* February 6, 2014, accessed December 13, 2016, http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.

Table 6.2: Proposed Decision Matrix for Stuxnet

		Alternatives			
		Continue talks	Increase sanctions	Launch U.S. airstrikes	Deploy a cyberweapon
Dimensions	Military	There are no implications for the military if we continue talks but this option will not fulfill the decision rule so I would score this alternative as 1.	There are no implications for the military if we increase sanctions but at least we are doing something so I would score this alternative as 2.	Airstrikes may be ineffective because we do not know where the facilities are and there can be casualties and retaliation. I would score this alternative as 3.	This is the chance to test out a new weapon that could be deployed covertly and precisely and would strike at the heart of the problem without putting troops on the ground. However, there could be repercussions if the weapon leaks out. I would score this alternative as 4.
	Political	We could continue talks but are they really working? I would score this alternative as 2.	We could increase sanctions but are they really working? I would score this alternative as 3.	We cannot implement airstrikes because we do not know where the facilities are and there can be casualties and retaliation. I would score this alternative as 1.	We can do this covertly so the public will not know but, there could be repercussions if the weapon leaks out. Plus, do we want to work with the Israelis? I would score this alternative as 4.

		Continue talks	Increase sanctions	Launch U.S. airstrikes	Deploy a cyberweapon
Dimensions	Diplomatic	We should continue talks because this is the best diplomatic solution. I would score this alternative as 4.	We could increase sanctions because they are working. I would score this alternative as 3.	The airstrikes could be inaccurate or result in casualties or international backlash because we could be seen as overreaching. I would score this alternative as 1.	Are we willing to unleash a new weapon into the world? There could be repercussions if the weapon leaks out. I would score this alternative as 2.
	Economic	There are no economic implications if we continue talks but this option may not fulfill the decision rule so I would score this alternative as 1.	We should increase sanctions. They are effective. I would score this alternative as 4.	Airstrikes cost millions of dollars. I would score this alternative as 2.	Stuxnet took a lot of time, money and resources to create. (Some say $100 million.[14]) Once it is used, it cannot be used again but, it would be a way to effectively destroy our target. I would score this alternative as 3.
	Final Choice	8	12	7	**13**

We can deductively conclude that a cyberweapon was the preferred choice to prevent Iran from acquiring a nuclear weapon because it had the highest overall score.

[14] Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog."

Since Stuxnet was deployed, this decision matrix is accurate. Thus, the following hypotheses might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [15] [VIOLENCE]

- *The U.S. will deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

In the case of Stuxnet, the U.S. decided to use direct action – since they are not at war with Iran but deployed a cyberweapon – in order to effectively neutralize the threat of a nuclear Iran although the U.S. was worried about spillover and blowback (collateral damage.) Launching a cyberweapon allowed the U.S. to covertly deal with this threat in a way that was relatively cost-free for them[16] while simultaneously stalling the Israelis from launching the Middle East into war. Thus, Stuxnet found that THREAT, ACCESS, VIOLENCE, and COLLATERAL DAMAGE may be conditions of deployment.

---

[15] Blechman and Kaplan, 12.

[16] Sanger says that the U.S. has lost some "moral high ground when it comes to warning the world of the dangers of cyberattacks." David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012a), 207.

IRAQ (2007)

"As of January 2007, 71% of Americans in a Gallup poll said the Iraq war is going badly."[17] When asked in January 2007 "Do you approve or disapprove of the way George W. Bush is handling his job as president?,"[18] President Bush's approval ratings fluctuated between 34 and 37%. In a March/April 2007 article for *Foreign Affairs,* James Fearon questioned, "Is it just a matter of domestic political games and public perceptions, or does the existence of civil war in Iraq have implications for what can be achieved there and what strategy Washington should pursue?"[19] This is a fascinating question which speaks to the domestic dimension of poliheuristic theory. According to a Gallup poll, by April 2007, two out of three Americans viewed the Iraq war as the most important problem.[20] At the time, 41% of those polled said the surge did not provide much difference.[21] Some Democrats proposed "cutting funds for the troops in Iraq as a means of forcing a change in U.S. policy" but 61% of Americans at the time opposed this.[22] Clearly, the U.S. and the American public wanted other options. Enter cyberweapons.

---

[17] Frank Newport et al., *Gallup Poll Review: 10 Key Points About Public Opinion on Iraq*, (Gallup, April 27, 2007), accessed August 12, 2017, http://www.gallup.com/poll/27391/gallup-poll-review-key-points-about-public-opinion-iraq.aspx.

[18] *Presidential Approval Ratings -- George W. Bush*.

[19] James D. Fearon, "Iraq's Civil War," *Foreign Affairs* 86, no. 2 (March - April 2007): 2, JSTOR via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[20] Newport et al., *Gallup Poll Review: 10 Key Points About Public Opinion on Iraq*.

[21] Ibid.

[22] Ibid.

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the polls depicted above, we can create the following choice set for the Iraq (2007) case:

(1) do nothing

(2) increase troops

(3) withdraw troops

(4) deploy a cyberweapon in order to identify and kill insurgents

Alternative 1: The U.S. could continue as is and do nothing.

Alternative 2: The U.S. could send in even more troops.

Alternative 3: The U.S. could withdraw their troops.

Alternative 4: The U.S. could deploy a cyberweapon in order to help identify and kill insurgents.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 6.3: Proposed Decision Matrix for Iraq (2007)

Alternatives

		Do nothing	Send more troops	Withdrawal	Deploy a cyberweapon
Dimensions	Military	In January, Bush said, "Failure in Iraq would be a disaster for the United States." So we cannot afford to do nothing. This is unacceptable.	We have already deployed 20,000 troops so perhaps we could deploy more.	In January, Bush said, "to step back now would force a collapse of the Iraqi government, tear that country apart, and result in mass killings on an unimaginable scale." This is unacceptable.	- We could demonstrate that these weapons can be used to kill people. - This can "provide some breathing space, a zone of security, for Iraq's political factions to settle their quarrels and form a unified state without having to worry about bombs blowing up every day."[23]
	Political	American troops are dying and support for the war is dwindling. We cannot do nothing. This is unacceptable.	41% of those polled at the time said the surge did not provide much difference.[24] So we should not send in additional troops.	In January, Bush said, "This new strategy will not yield an immediate end to suicide bombings, assassinations or IED attacks."[25] So we should withdraw.	We could deploy a cyberweapon but there is a lot of sensitivity surrounding the N.S.A. because the public is weary of their illegal surveillance.

[23] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016a), 160.

[24] Newport et al., *Gallup Poll Review: 10 Key Points About Public Opinion on Iraq*.

		Do nothing	Send more troops	Withdrawal	Deploy a cyberweapon
Dimensions	Diplomatic	In January, Bush said, "Radical Islamic extremists would grow in strength and gain new recruits. They would be in a better position to topple moderate governments, create chaos in the region and use oil revenues to fund their ambitions. Iran would be emboldened in its pursuit of nuclear weapons." So we cannot afford to do nothing. This is unacceptable.	We already have thousands of troops in Iraq so sending in more might not further exacerbate U.S.-Iraqi relations.	In January, Bush said, "to step back now would force a collapse of the Iraqi government, tear that country apart, and result in mass killings on an unimaginable scale." This is unacceptable.	This is sensitive because of the infiltration of Iraqi companies and Iraqi civilians.
	Economic	There are no economic implications if we do nothing.	In January, Bush said, "We will give our commanders and civilians greater flexibility to spend funds for economic assistance."	Some Democrats proposed "cutting funds for the troops in Iraq as a means of forcing a change in U.S. policy" but 61% of Americans at the time opposed this.[26] Thus, this is unacceptable.	These weapons cost time, resources and money but they are cheaper than other methods such as sending additional troops.

[25] George W. Bush, "President Bush Addresses Nation on Iraq War," (speech, Washington, D.C., January 10, 2007), accessed August 12, 2017, *CQ Transcripts Wire*, http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011002208.html.

[26] Newport et al., *Gallup Poll Review: 10 Key Points About Public Opinion on Iraq*.

Doing nothing and allowing Iraq to further implode is noncompensatory on the military, political and diplomatic dimensions so that alternative is eliminated immediately. The withdrawal alternative is noncompensatory on the military, diplomatic and economic dimensions so that alternative is also eliminated. So we move to the second stage of the decision-making process with the following options below. In the Iraq (2007) case, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in stemming the violence in Iraq?* I decided to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.4: Proposed Decision Matrix for Iraq (2007)

		Alternatives	
		Send more troops	Deploy a cyberweapon
Dimensions	Military	We have already deployed 20,000 troops so perhaps we could deploy more. I would score this alternative as 1.	- We could demonstrate that these weapons can be used to kill people. - This can "provide some breathing space, a zone of security, for Iraq's political factions to settle their quarrels and form a unified state without having to worry about bombs blowing up every day."[27] I would score this alternative as 2.
	Political	41% of those polled at the time said the surge did not provide much difference.[28] So we should not send in additional troops.	We could deploy a cyberweapon but there is a lot of sensitivity surrounding the N.S.A. because the public is weary of their illegal surveillance.

[27] Kaplan, *Dark Territory: The Secret History of Cyber War*, 160.

[28] Frank Newport et al., *Gallup Poll Review: 10 Key Points About Public Opinion on Iraq*.

		Send more troops	Deploy a cyberweapon
		I would score this alternative as 1.	I would score this alternative as 2.
Dimensions	Diplomatic	We already have thousands of troops in Iraq so sending in more might not further exacerbate U.S.-Iraqi relations. I would score this alternative as 2.	This is sensitive because of the infiltration of Iraqi companies and Iraqi civilians. I would score this alternative as 1.
	Economic	In January, Bush said, "We will give our commanders and civilians greater flexibility to spend funds for economic assistance." I would score this alternative as 1.	These weapons cost time, resources and money but they are cheaper than other methods such as sending additional troops. I would score this alternative as 2.
	Final Choice	5	**7**

We can deductively conclude that deploying a cyberweapon was the preferred choice to assist in stemming the violence in Iraq because it had the highest overall score. Since cyberweapons were used in this case, this decision matrix is accurate. The decision matrix for the Iraq (2007) case is different from the other decision matrixes since the U.S. was already at war with Iraq when they considered using what this dissertation defines as a cyberweapon so this case was not a first strike. Nevertheless, I think the following hypotheses might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [29] [VIOLENCE]

The ACCESS variable is thought-provoking because the N.S.A. used these cyber capabilities in order to ensnare insurgents into areas where they could then be killed by a drone. In a way, this was a tool to get a target into the reach of troops or drones. So even though a drone could fulfill this goal, I did not include drones as an option. Furthermore, even though the U.S. Predator drone was used in Afghanistan in 2001,[30] in 2007, drones were not yet the preferred tactic for taking out jihadists.[31] Thus, I do not think it was an obvious option at the time as they are today.

The VIOLENCE variable is also thought-provoking because my hypothesis assumes that the U.S. will deploy a cyberweapon in order to prevent or end a war. Well, the U.S. was already at war with Iraq so this operation was not about preventing war. However, U.S. forces eventually withdrew from Iraq, so this tactic contributed to ending a war which suggests this hypothesis may be plausible.

---

[29] Blechman and Kaplan, 12.

[30] Fred Kaplan, "The First Drone Strike," *Slate,* September 14, 2016b, accessed August 12, 2017, http://www.slate.com/articles/news_and_politics/the_next_20/2016/09/a_history_of_the_armed_drone.html.

[31] Ibid.

As for the COLLATERAL DAMAGE variable, the Iraq (2007) case proved the following hypothesis false since this operation resulted in the deaths of militants, whether implicit or not. Thus, the following hypothesis may be false:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

In the case of Iraq (2007), the U.S. deployed a cyberweapon in order to effectively neutralize the threat of roadside bombers and insurgents. Thus, the Iraq (2007) case found that THREAT, ACCESS, and VIOLENCE may be conditions of deployment but COLLATERAL DAMAGE was not a condition of deployment.

SHOTGIANT (2007)

During President Bush's lame duck term, his approval rating throughout 2007 ranged in the 30s[32] so perhaps there was an impetus for this operation. Some scholars have argued that because a lame duck president may not have the same preoccupation with domestic support as when they were first elected, they could now feel free to do as they wished.[33] This is one way in which domestic politics influences the use of force.

Another way in which domestic politics factors into the use of force, is the diversionary theory of war where the President uses "the military to divert attention from

[32] *Presidential Approval Ratings -- George W. Bush*.

[33] Eric Stern, "Contextualizing and Critiquing the Poliheuristic Theory," *The Journal of Conflict Resolution* 48, no. 1 (February, 2004): 111, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

domestic problems" in order to experience a boost in ratings.[34] This is a pessimistic view of American leadership, but some scholars have found evidence that supports this theory. In Charles Ostrom and Brian Job's "The President and the Political Use of Force," they concluded that "the president is more prone to use force in times of economic stress."[35] In 2007, the housing market collapsed[36] and the U.S. economy was tanking so the economy may have factored into Bush's decision-making process about using a cyberweapon.

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the Gallup poll depicted above, we can create the following choice set for Shotgiant.

(1) do nothing

(2) continue traditional surveillance

(3) infiltrate Huawei to install the capability of carrying out future offensive cyber operations

Alternative 1: The U.S. can continue as is and do nothing since there is no imminent threat.

Alternative 2: The U.S. could continue its current ways of conducting surveillance.

Alternative 3: The U.S. could install a backdoor that would enable them to conduct surveillance against those possessing Huawei products and to carry out future offensive cyber operations.

---

[34] Karl DeRouen Jr., "Presidents and the Diversionary Use of Force: A Research Note" *International Studies Quarterly* 44 (2000): 317, Worldwide Political Science Abstracts via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[35] Charles W. Ostrom and Brian L. Job, "The President and the Political Use of Force," *The American Political Science Review* 80, no. 2 (June, 1986): 557, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/1958273.

[36] Jim Zarroli, "The 2007 Economy in Review," *NPR,* December 31, 2007, accessed August 12, 2017, http://www.npr.org/templates/story/story.php?storyId=17716248.

The decision matrix consists of four dimensions and three alternatives. I listed the dimensions in order of increasing importance.

Table 6.5: Proposed Decision Matrix for Shotgiant (2007)

		Alternatives		
		Do nothing	Continue traditional surveillance	Infiltrate Huawei
Dimensions	Military	There are no military implications if we do nothing since there is no imminent threat.	The U.S. should continue its traditional methods of surveillance since this is customary behavior.	We should do this since it is a covert way to get better information and enable the President to authorize a future attack on 'high priority targets.'
	Political	There are no political implications if we do nothing since there is no imminent threat.	The U.S. should continue its traditional methods of surveillance since this is customary behavior.	We could do this since it is a covert way to get better information and enable the President to authorize a future attack on 'high priority targets.'
	Diplomatic	There are no diplomatic implications if we do nothing since there is no imminent threat.	The U.S. could continue its traditional methods of surveillance since this is customary behavior.	If this operation is discovered, there could be diplomatic ramifications.
	Economic	There are no economic implications if we do nothing since there is no imminent threat.	Continuing traditional surveillance incurs the expected costs of such operations.	Shotgiant may be costly in terms of time, money and resources but it can be more accurate than traditional surveillance.

Shotgiant is an interesting case because there was no imminent threat and it was also against a Chinese company, not China per say. Furthermore, there was no noncompensatory alternative here which raised the even more interesting question of – does poliheuristic theory always have a noncompensatory option? This is a possible question for future research about poliheuristic theory. However, I decided to label the Do Nothing option as unacceptable because I do not think U.S. officials would simply do nothing since they were worried about Huawei creating backdoors into the U.S. Thus, we move to the second stage of the decision-making process with the following options below. In the case of Shotgiant, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Does this alternative enable future offensive cyber operations against those possessing Huawei products?* I decided to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.6: Proposed Decision Matrix for Shotgiant (2007)

		Alternatives	
		Continue traditional surveillance	Infiltrate Huawei
Dimensions	Military	The U.S. could continue its traditional methods of surveillance but this option may not fulfill the decision rule thus, I would score this alternative as 1.	This is a covert way to get better information and enable the President to authorize a future attack on 'high priority targets.' I would score this alternative as 2.
	Political	The U.S. could continue its traditional methods of surveillance but this option may not fulfill the decision rule thus, I would score this alternative as 1.	This is a covert way to get better information and enable the President to authorize a future attack on 'high priority targets.'

		Continue traditional surveillance	Infiltrate Huawei
			I would score this alternative as 2.
Dimensions	Diplomatic	The U.S. should continue its traditional methods of surveillance because this option might fulfill the decision rule. I would score this alternative as 2.	If this operation is discovered, there could be diplomatic ramifications. I would score this alternative as 1.
	Economic	The U.S. could continue its traditional methods of surveillance but this option may not fulfill the decision rule thus, I would score this alternative as 1.	Shotgiant may be costly in terms of time, money and resources but it may fulfill the decision rule, so I would score this alternative as 2.
	Final Choice	5	**7**

We can deductively conclude that infiltrating Huawei was the preferred choice to enable future offensive cyber operations because it had the highest overall score. Since Shotgiant was operational, this decision matrix is accurate. So the following hypothesis might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

Since there was no viable threat to the U.S., Shotgiant may have proved this hypothesis false:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

Since there was no looming military conflict with China, VIOLENCE was not tested. COLLATERAL DAMAGE was also not tested since I did not find any discussion

of collateral damage in the literature about Shotgiant though one can assume the U.S. did not want Huawei and those with Huawei products to know about this operation. Shotgiant found that ACCESS might be a condition of deployment.

QUANTUM (2008)

In 2008, President Bush had a very low approval rating ranging from high 20s to the low 30s[37] so again, since he was a lame duck, he could have felt more inclined to proceed as he wished.

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the Gallup polls depicted here, we can create the following choice set for Quantum.

(1) do nothing

(2) continue traditional surveillance

(3) install implants for 'active defense,' or to access difficult areas

Alternative 1: The U.S. can continue as is and do nothing since there is no imminent threat.

Alternative 2: The U.S. could continue its current methods of conducting surveillance.

Alternative 3: The U.S. could carry out missions for 'active defense,' or in order to access hard-to-reach areas.

The decision matrix consists of four dimensions and three alternatives. I listed the dimensions in order of increasing importance.

[37] *Presidential Approval Ratings -- George W. Bush*.

Table 6.7: Proposed Decision Matrix for Quantum (2008)

		Alternatives		
		Do nothing	Continue traditional surveillance	Install implants
Dimensions	Military	There are no military implications if we do nothing since there is no imminent threat.	The U.S. should continue its traditional methods of surveillance since this is customary behavior.	We should do this since it can be done covertly and allow us to conduct 'active defense' in hard-to-reach areas.
	Political	There are no political implications if we do nothing since there is no imminent threat.	The U.S. should continue its traditional methods of surveillance since this is customary behavior.	We could do this since it can be done covertly and allow us to conduct 'active defense' in hard-to-reach areas.
	Diplomatic	There are no diplomatic implications if we do nothing since there is no imminent threat.	The U.S. could continue its traditional methods of surveillance since this is customary behavior.	If this operation is revealed, there can be diplomatic ramifications.
	Economic	There are no economic implications if we do nothing since there is no imminent threat.	Continuing traditional surveillance incurs the expected costs of such operations.	Quantum is costly in terms of time, money and resources but it can be more accurate than traditional surveillance.

Comparable to Shotgiant, Quantum is also an interesting case since there was no imminent threat but again, I decided to label the Do Nothing option as unacceptable because I do not think U.S. officials would simply do nothing. Thus, we move to the second stage of the decision-making process with the following options below. In the case of Quantum, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in accessing hard-to-reach areas?* I decided

to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.8: Proposed Decision Matrix for Quantum (2008)

		Alternatives	
		Continue conventional surveillance	Install implants
Dimensions	Military	The U.S. could continue its traditional methods of surveillance but this option will not fulfill the decision rule thus, I would score this alternative as 1.	This can be done covertly and allow us to conduct 'active defense' in hard-to-reach areas. I would score this alternative as 2.
	Political	The U.S. could continue its traditional methods of surveillance but this option may not fulfill the decision rule thus, I would score this alternative as 1.	This can be done covertly and allow us to conduct 'active defense' in hard-to-reach areas. I would score this alternative as 2.
	Diplomatic	The U.S. should continue its traditional methods of surveillance because this option might fulfill the decision rule. I would score this alternative as 2.	If this operation is revealed, there could be diplomatic ramifications. I would score this alternative as 1.
	Economic	The U.S. could continue its traditional methods of surveillance but this option may not fulfill the decision rule thus, I would score this alternative as 1.	Quantum is costly in terms of time, money and resources but it can be more accurate than traditional surveillance so I would score this alternative as 2.
	Final Choice	5	**7**

We can deductively conclude that installing implants was the preferred choice to achieve access because it had the highest overall score. Since Quantum is operational, this decision matrix is accurate. So the following hypotheses might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

Since there was no viable threat to the U.S., Quantum may have proved this hypothesis false:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

In the case of Quantum, the U.S. decided to use direct action – they are not at war with these countries but deployed a cyberweapon anyway. VIOLENCE was not explored in this scenario since there was no looming conflict with many of these countries. Additionally, COLLATERAL DAMAGE was not tested since there was no mention of collateral damage in the literature about Quantum though presumably, the U.S. wanted this operation to be covert. Quantum found that ACCESS might be a condition of deployment.

TURBINE (2010)

Using the sources discussed in the Literature Review and Cyberweapons chapters we can create the following choice set for Turbine.

(1) do nothing

(2) continue traditional intelligence gathering

(3) deploy millions of implants for possible attack

Alternative 1: The U.S. can continue as is and do nothing since there is no imminent threat.

Alternative 2: The U.S. could continue its current ways of gathering intelligence.

Alternative 3: The U.S. could install millions of implants with the capability of waging attacks.

The decision matrix consists of four dimensions and three alternatives. I listed the dimensions in order of increasing importance.

Table 6.9: Proposed Decision Matrix for Turbine (2010)

		Alternatives		
		Do nothing	Continue traditional intelligence gathering	Install implants
Dimensions	Military	There are no military implications if we do nothing since there is no imminent threat.	The U.S. should continue its traditional methods of intelligence gathering since this is customary behavior.	We should do this since it can be done covertly and allow us to conduct future attacks.
	Political	There are no political implications if we do nothing since there is no imminent threat.	The U.S. could continue its traditional methods of intelligence gathering since this is customary behavior.	We could do this since it can be done covertly and allow us to conduct future attacks.
	Diplomatic	There are no diplomatic implications if we do nothing since there is no imminent threat.	The U.S. could continue its traditional methods of intelligence gathering since this is customary behavior.	This can be done covertly and allow us to conduct future attacks but this is an automated system so there could be mishaps.
	Economic	There are no economic implications if we do nothing since there is no imminent threat.	Continuing traditional intelligence gathering incurs the expected costs of such operations.	Turbine costs hundreds of millions of dollars but it requires less personnel since this is part of an automated system.

Similar to Shotgiant and Quantum, Turbine is also an interesting case since there was no imminent threat but I also decided to label the Do Nothing option as unacceptable because I do not think U.S. officials would simply do nothing. Thus, we move to the second stage of the decision-making process with the following options below. In the case of Turbine, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in enabling attacks?* I decided to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.10: Proposed Decision Matrix for Turbine (2010)

		Alternatives	
		Continue traditional intelligence gathering	Install implants
Dimensions	Military	The U.S. could continue its traditional methods of intelligence gathering but this option will not fulfill the decision rule thus, I would score this alternative as 1.	This can be done covertly and allow us to conduct future attacks. I would score this alternative as 2.
	Political	The U.S. could continue its traditional methods of intelligence gathering but this option may not fulfill the decision rule thus, I would score this alternative as 1.	This can be done covertly and allow us to conduct future attacks. I would score this alternative as 2.
	Diplomatic	The U.S. should continue its traditional methods of intelligence gathering because this option might fulfill the decision rule. I would score this alternative as 2.	This can be done covertly and allow us to conduct future attacks but this is an automated system so there can be mishaps. I would score this alternative as 1.
	Economic	The U.S. could continue its traditional methods of	Turbine costs hundreds of millions of dollars but it

		Continue traditional intelligence gathering	Install implants
		intelligence gathering but this option may not fulfill the decision rule thus, I would score this alternative as 1.	requires less personnel since this is part of an automated system so I would score this alternative as 2.
	Final Choice	5	**7**

We can deductively conclude that installing implants was the preferred choice to enable attacks because it had the highest overall score. Since Turbine is operational, this decision matrix is accurate. So the following hypotheses might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

Since there was no viable threat to the U.S., Turbine may have proved this hypothesis false:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

In the case of Turbine, the U.S. decided to use direct action –they are not at war with these countries but deployed a cyberweapon anyway. VIOLENCE was not explored in this scenario since there was no looming conflict with many of these countries. Additionally, COLLATERAL DAMAGE was not tested since there was no mention of collateral damage in the literature about Turbine though presumably, the U.S. wanted this operation to remain covert. Turbine found that ACCESS might be a condition of deployment.

NITRO ZEUS

There were no Gallup polls conducted in 2009 asking about Iran's nuclear program but Americans had a high unfavorable rating of Iran from 2009 – 2013.[38] In 2010, 42% of those polled approved of the way President Obama handled Iran but a few months after the nuclear deal with Iran, that rating fell to 33%.[39] From 2013 – 2016, 83% - 75% of those polled said Iran was a critical threat to the U.S.[40]

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the Gallup polls depicted above, we can create the following choice set for Nitro Zeus.

(1) do nothing

(2) use military force

(3) deploy cyberweapons

Alternative 1: The U.S. could wait and see how events unfold in Iran.

Alternative 2: The U.S. can use military force if conflict erupts with Iran.

Alternative 3: The U.S. can use covert cyberweapons to destroy Fordo as well as parts of Iran's communications systems, air defenses and power grid in case the pending nuclear deal fell through and war erupted.

The decision matrix consists of four dimensions and three alternatives. I listed the dimensions in order of increasing importance.

---

[38] *Iran*, (Gallup).

[39] *Presidential Ratings -- Issues Approval*, (Gallup), accessed December 10, 2016, http://www.gallup.com/poll/1726/presidential-ratings-issues-approval.aspx.

[40] *Iran*, (Gallup).

Table 6.11: Proposed Decision Matrix for Nitro Zeus

		Alternatives		
		Do nothing	Use military force	Deploy a cyberweapon
Dimensions	Military	The U.S. cannot afford to wait and see if there is a looming conflict with Iran. This is unacceptable.	The U.S. should use military force if a military conflict is on the horizon.	The U.S. should deploy a cyberweapon as part of a 'hybrid' attack.[41]
	Political	The U.S. cannot afford to do nothing if there is a looming conflict with Iran and Israel is preparing to strike. This is unacceptable.	The U.S. public will not support another war in the Middle East.	This is "a way to turn off critical elements of the Iranian infrastructure without firing a shot."[42]
	Diplomatic	If we do nothing, the Israelis may launch an airstrike thereby potentially dragging us into a bigger conflict.	The international community may not support another war in the Middle East.	"Depending on how the conflict unfolded, there could be significant effects on civilians, particularly if the United States had to cut vast swaths of the country's electrical grid and communications networks."[43]
	Economic	There are no economic	Sending in troops is costly in terms of time,	This plan costs tens of millions of dollars and

[41] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times,* February 16, 2016e, accessed May 10, 2016, http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

[42] Ibid.

[43] Ibid.

		Do nothing	Use military force	Deploy a cyberweapon
		implications if we do nothing.	money and casualties.	thousands of personnel. Is it worth it?

Doing nothing is unacceptable on the military and political dimensions so that alternative is eliminated immediately. Therefore, in the second stage of the decision-making process, we are left with the following options below. In the case of Nitro Zeus, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is this alternative expected to result in preventing Iran from acquiring a nuclear weapon?* I decided to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.12: Proposed Decision Matrix for Nitro Zeus

		Alternatives	
		Use military force	Deploy a cyberweapon
Dimensions	Military	The U.S. should use military force if a military conflict is on the horizon. I would score this alternative as 1.	The U.S. should deploy a cyberweapon as part of a 'hybrid' attack.[44] I would score this alternative as 2.
	Political	The U.S. public will not support another war in the Middle East.	This is "a way to turn off critical elements of the Iranian infrastructure without firing a shot."[45]

[44] Sanger and Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict."

[45] Ibid.

		Use military force	Deploy a cyberweapon
		I would score this alternative as 1.	I would score this alternative as 2.
Dimensions	Diplomatic	The international community may not support another war in the Middle East. I would score this alternative as 1.	"Depending on how the conflict unfolded, there could be significant effects on civilians, particularly if the United States had to cut vast swaths of the country's electrical grid and communications networks."[46] I would score this alternative as 2.
	Economic	Sending in troops is costly in terms of time, money and casualties. I would score this alternative as 1.	This plan costs tens of millions of dollars and thousands of personnel but it may be the best option we have. I would score this alternative as 2.
	Final Choice	4	**8**

We can deductively conclude that deploying a cyberweapon against Iran was the preferred choice to prevent them from obtaining a nuclear weapon because it had the highest overall score. However, the pending nuclear deal with Iran was approved so Nitro Zeus was not operationalized. Nevertheless, the following hypotheses might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

[46] Sanger and Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict."

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

However, since Nitro Zeus was conceived as a part of a kinetic attack, the following hypothesis may be false:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [47] [VIOLENCE]

Thus, Nitro Zeus suggests that while THREAT, ACCESS and COLLATERAL DAMAGE may be conditions of deployment, VIOLENCE may not be a condition of deployment. Although, since this cyberweapon was never deployed because a deal was reached, perhaps one could argue that these hypotheses are null.

[47] Blechman and Kaplan, 12.

LIBYA (2011)

When Operation Odyssey Dawn began,[48] President Obama's approval rating was 48%.[49] A few days after the operation began, 47% of those polled approved of military action in Libya.[50] This is known as 'rally 'round the flag' where "international crises and similar phenomena will give a President a short-term boost in popularity."[51] This is another way in which domestic politics influences the use of force. Sometimes the use of force helps decisionmakers in the short run because the public will initially support such actions.[52] However, when this poll was conducted, Obama's approval rating dropped to 45%.[53] It went back up to 48% the week after.[54] Thus, Obama received a slight boost in popularity. However, I do not think Obama chose to intervene just to raise his popularity a smidge.

---

[48] David D. Kirkpatrick, Steven Erlanger and Elisabeth Bumiller, "Allies Open Air Assault on Qaddafi's Forces in Libya," *The New York Times,* March 19, 2011a, accessed December 5, 2016, http://www.nytimes.com/2011/03/20/world/africa/20libya.html?pagewanted=all.

[49] *Presidential Approval Ratings – Barack Obama*.

[50] Jeffrey M. Jones, *Americans Shift to More Negative View of Libya Military Action*, (Gallup, June 24, 2011a), accessed December 10, 2016, http://www.gallup.com/poll/148196/americans-shift-negative-view-libya-military-action.aspx.

[51] John E. Mueller, "Presidential Popularity from Truman to Johnson," *The American Political Science Review* 64, no. 1 (March, 1970): 20, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/1955610; Karen Tumulty, "Pressure Building on Obama to Specify Scope, Goals of U.S. Action in Libya," *The Washington Post,* March 24, 2011, accessed December 10, 2016, https://www.washingtonpost.com/politics/pressure-building-on-obama-to-specify-scope-goals-of-us-action-in-libya/2011/03/24/ABE9G6RB_story.html?utm_term=.2603ee22b176.

[52] Alex Mintz, "The Decision to Attack Iraq: A Noncompensatory Theory of Decision Making," *The Journal of Conflict Resolution* 37, no. 4 (December 1993): 602, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/174541.

[53] *Presidential Approval Ratings – Barack Obama*.

[54] Ibid.

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the polls depicted above, we can create the following choice set for Libya.

(1) do nothing

(2) continue talks

(3) send in Special Operations Forces (SOF)

(4) implement airstrikes

(5) deploy a cyberweapon

Alternative 1: The U.S. can do nothing, anticipating that Qaddafi does not carry out his promise of slaughtering Libyans in Benghazi.[55]

Alternative 2: The U.S. could continue discussions, anticipating that there could be a diplomatic resolution to the Libyan crisis.

Alternative 3: The U.S. could send in Special Operations Forces as was the case in Afghanistan.[56]

Alternative 4: The U.S. could launch airstrikes against Libyan military targets.

Alternative 5: The U.S. could deploy a cyberweapon against Libyan military targets.

The decision matrix consists of four dimensions and five alternatives. I listed the dimensions in order of increasing importance.

---

[55] Helene Cooper, "Obama Cites Limits of U.S. Role in Libya," *The New York Times,* March 28, 2011, accessed December 5, 2016, http://www.nytimes.com/2011/03/29/world/africa/29prexy.html

[56] Thom Shanker, "U.S. Weighs Options, on Air and Sea," *The New York Times,* March 6, 2011, accessed December 9, 2016, http://www.nytimes.com/2011/03/07/world/middleeast/07military.html.

Table 6.13: Proposed Decision Matrix for Libya (2011)

Alternatives

		Do nothing	Continue talks	Implement airstrikes	Send in SOF	Deploy a cyberweapon
Dimensions	Military	If we do nothing, the conflict can spill over into the region. This is unacceptable.	There are no military implications if the U.S. continues talks but are they really working?	We should implement airstrikes.	We could send in SOF, but this is risky.	We could effectively attack Libya's air defenses.
	Political	If we do nothing, we will have again failed to prevent the massacre of civilians. This is unacceptable.	We could continue talks but are they really working?	We should implement airstrikes.	The public may not support SOF in Libya.	This option may not be fast enough and we are unsure whether the President needs Congressional approval.
	Diplomatic	If we do nothing, the Europeans could act without us thereby potentially dragging us into a bigger conflict.[57] This is unacceptable.	We should continue talks because this is the best diplomatic solution.	We could implement airstrikes since the U.N. has instituted a no-fly zone.	We cannot send SOF into Libya because there are military, political and diplomatic risks involved.	These weapons may set a new norm for adversaries such as Russia and China. Are we willing to do that?

[57] Jo Becker and Scott Shane, "The Libya Game | Part 1 Hillary Clinton, 'Smart Power' and a Dictator's Fall," *The New York Times,* February 27, 2016, accessed December 6, 2016, http://www.nytimes.com/2016/02/28/us/politics/hillary-clinton-libya.html.

		Do nothing	Continue talks	Implement airstrikes	Send in SOF	Deploy a cyberweapon
Dimension	Economic	There are no economic implications if we do nothing.	There are no economic implications if we continue talks.	A Tomahawk missile costs over one million dollars each and we are going to need to fire a lot.[58]	Troops cost more than airstrikes.	We could be wasting this superior capability that cost a lot of time and money on Libya's archaic defense systems.

Doing nothing when Qaddafi threatened to slaughter civilians is unacceptable on the military, political and diplomatic dimensions so that alternative is eliminated immediately. Therefore, in the second stage of the decision-making process, we are left with the following options below. In the case of Libya, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in preventing Qaddafi from attacking civilians?* I decided to rate each alternative on a scale of 1 to 4. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

[58] Alexander, "Cost of a U.S. strike against Syria could top Hagel's estimate."

Table 6.14: Proposed Decision Matrix for Libya (2011)

		Alternatives			
		Continue talks	Implement airstrikes	Send in SOF	Deploy a cyberweapon
Dimensions	Military	There are no military implications if the U.S. continues talks but this option will not accomplish the decision rule. I would score this alternative as 1.	We should implement airstrikes. I would score this alternative as 3.	We could send in SOF to assist the rebels but this is risky and could result in casualties. I would score this alternative as 2.	We could effectively attack Libya's air defenses. I would score this alternative as 4.
	Political	We could continue talks but this option may not accomplish the decision rule. I would score this alternative as 3.	We should implement airstrikes along with the rest of the international coalition. I would score this alternative as 4.	We should not send SOF into Libya because there are military and political risks involved. I would score this alternative as 1.	This option may not be fast enough and we are unsure whether the President needs Congressional approval. I would score this alternative as 2.

		Continue talks	Implement airstrikes	Send in SOF	Deploy a cyberweapon
Dimensions	Diplomatic	We should continue talks because this may accomplish the decision rule. I would score this alternative as 4.	We could implement airstrikes along with the rest of the international coalition. I would score this alternative as 3.	We cannot send SOF into Libya because there are military, political and diplomatic risks involved. I would score this alternative as 1.	These weapons may set a new norm for adversaries such as Russia and China. I would score this alternative as 2.
	Economic	There are no economic implications if we continue talks but this option may not accomplish the decision rule. I would score this alternative as 1.	A Tomahawk missile costs over one million dollars each and we are going to need to fire a lot.[59] I would score this alternative as 4.	Troops cost more than airstrikes. I would score this alternative as 2.	We could be wasting this superior capability that cost a lot of time and money on Libya's archaic defense systems. I would score this alternative as 3.
	Final Choice	9	**14**	6	11

We can deductively conclude that implementing airstrikes in Libya was the preferred choice to prevent Qaddafi from attacking civilians because it had the highest overall score. Since this is the alternative that the U.S. chose, this decision matrix is accurate. So the following hypotheses might not be true:

[59] Alexander, "Cost of a U.S. strike against Syria could top Hagel's estimate."

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [60] [VIOLENCE]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

Since these targets were not out of the reach of airstrikes and the U.S. did not deploy, I think the following hypothesis might still be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

In the case of Libya, the U.S. decided not to deploy a cyberweapon even though there was a threat, and deploying a cyberweapon could have helped avoid the violence of airstrikes as well as minimize casualties. Thus, perhaps THREAT, VIOLENCE and COLLATERAL DAMAGE are not conditions of deployment but ACCESS might be a condition of deployment. These considerations would reverberate during U.S. deliberations about deploying a cyberweapon in Syria.

[60] Blechman and Kaplan, 12.

PAKISTAN (2011)

After the raid, President Obama received a bump in ratings from 46% pre-raid to 52% post-raid.[61] Gallup pointed out that presidential support increases after a 'rally event' which is the 'rally round the flag effect'[62] discussed earlier in this chapter. Additionally, this gave some Americans more confidence in President Obama as a commander in chief.[63] 54% of those polled felt safer as a result of bin Laden's death.[64] Although 62% were worried about increased terrorism as a result.[65] Nevertheless, 9/10 of those polled approved "of the U.S. military action that killed Osama bin Laden" but 89% gave most of the credit to the military.[66] 33% of those polled preferred bin Laden to have been captured.[67]

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the Gallup polls depicted above, we can create the following choice set for the Pakistan case:

---

[61] Jeffrey M. Jones, *Obama Approval Rallies Six Points to 52% After Bin Laden Death*, (Gallup, May 5, 2011b), accessed June 2, 2017, http://www.gallup.com/poll/147437/obama-approval-rallies-six-points-bin-laden-death.aspx.

[62] Tumulty, "Pressure building on Obama to specify scope, goals of U.S. action in Libya."

[63] Lydia Saad, *Majority in U.S. Say Bin Laden's Death Makes America Safer*, (Gallup, May 4, 2011b), accessed August 8, 2017, http://www.gallup.com/poll/147413/majority-say-bin-laden-death-makes-america-safer.aspx.

[64] Ibid.

[65] Ibid.

[66] Frank Newport, *Americans Back Bin Laden Mission; Credit Military, CIA Most*, (Gallup, May 3, 2011), accessed August 8, 2017, http://www.gallup.com/poll/147395/americans-back-bin-laden-mission-credit-military-cia.aspx.

[67] Ibid.

(1) do nothing

(2) helicopter raid

(3) launch a missile

(4) deploy a cyberweapon

Alternative 1: The U.S. could do nothing, since they are not very confident that bin Laden is there.

Alternative 2: The U.S. could conduct a helicopter raid to capture or kill bin Laden.

Alternative 3: The U.S. could launch a precision guided munition to kill only bin Laden.

Alternative 4: The U.S. could deploy a covert cyberweapon against Pakistan's radar systems.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 6.15: Proposed Decision Matrix for Pakistan (2011)

		Alternatives			
		Do nothing	Launch a missile	Helicopter raid	Deploy a cyberweapon
Dimension	Military	"What would the average American say if he knew we had the best chance of getting bin Laden since Tora Bora and	-This is good for "maintaining the flow of fuel and matériel to American forces fighting in Afghanistan, which depended on	-We are not sure if OBL is there. -We will know the fate of OBL. -There could be casualties.	-We could use this covertly "to prevent Pakistani radars from spotting helicopters carrying Navy Seal commandos."[71]

[71] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times,* October 17, 2011, accessed July 5, 2016, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

		Do nothing	Launch a missile	Helicopter raid	Deploy a cyberweapon
		we didn't take a shot?"[68] This is unacceptable.	Pakistan's goodwill."[69] -We won't know the fate of OBL. -Fewer casualties. - "The Pacer, after all, was moving. The missile could not be guided. You have one shot, they reminded Gates, and if you miss, you've blown it. Imagine the criticism of the president that would follow: You got the chance of a lifetime and you blew it with something untried?" [70] - Do we really want to reveal	-Can we get in and out undetected? -Do we really want to reveal the stealth helicopter?	-There would be less risk of retaliation from Pakistan's army or police.

[68] Mark Bowden, "The Hunt for 'Geronimo,'" *Vanity Fair,* October 12, 2012, accessed April 22, 2017, http://www.vanityfair.com/news/politics/2012/11/inside-osama-bin-laden-assassination-plot.

[69] Ibid.

[70] Bowden, "The Hunt for 'Geronimo.'"

		Do nothing	Launch a missile	Helicopter raid	Deploy a cyberweapon
			this new weapon?		
Dimensions	Political	"What would the average American say if he knew we had the best chance of getting bin Laden since Tora Bora and we didn't take a shot?"[72] This is unacceptable.	-Biden was concerned about this failing and costing them a second term. -We won't definitively know the fate of OBL. -There could be fewer casualties. -This missile has never been tried before so we could miss.	-Biden was concerned about this failing and costing them a second term. -If OBL was captured, we could try him in court. -There could be casualties.	We could maintain plausible deniability.
	Diplomatic	Doing nothing will not exacerbate U.S.-Pakistani relations.	Perhaps this alternative is better than a raid since there are less casualties involved.	-Secretary Clinton was concerned about the diplomatic ramifications of a raid. -This violates Pakistan's sovereignty.	This may alleviate diplomatic concerns.
	Economic	There are no economic implications if we do nothing.	This weapon costs a lot of money, time and resources.	Stealth helicopters cost a lot of money, time	A cyberweapon costs a lot of time, money and resources.

[72] Bowden, "The Hunt for 'Geronimo.'"

		Do nothing	Launch a missile	Helicopter raid	Deploy a cyberweapon
			Do we really want to reveal this capability?	and resources. Do we really want to reveal this capability?	Do we really want to reveal this capability?

Although doing nothing was an option here, Panetta told Obama that he ought to ask himself this question: "What would the average American say if he knew we had the best chance of getting bin Laden since Tora Bora and we didn't take a shot?"[73] I think the average American would be angry, to say the least thus, the Do Nothing option is noncompensatory on the military and political dimensions so this alternative is eliminated immediately. So we move to the second stage of the decision-making process with the following options below. In the case of Pakistan, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in killing Osama bin Laden and minimizing casualties?* I decided to rate each alternative on a scale of 1 to 3. The higher the score, the more likely that alternative will be able to fulfill the decision rule. On the Economic dimension, I assumed that cyberweapons were the cheapest option followed by the missile and then the helicopter raid.

[73] Bowden, "The Hunt for Geronimo."

Table 6.16: Proposed Decision Matrix for Pakistan (2011)

		Alternatives		
		Launch a missile	Helicopter raid	Deploy a cyberweapon
Dimension	Military	-This is good for "maintaining the flow of fuel and matériel to American forces fighting in Afghanistan, which depended on Pakistan's goodwill."[74] -We won't know the fate of OBL. -Fewer casualties. - "The Pacer, after all, was moving. The missile could not be guided. You have one shot, they reminded Gates, and if you miss, you've blown it. Imagine the criticism of the president that would follow: You got the chance of a lifetime and you blew it with something untried?"[75] - Do we really want to reveal this new weapon? I would score this alternative as 2.	-We are not sure if OBL is there. -We will know the fate of OBL. -There could be casualties. -Can we get in and out undetected? -Do we really want to reveal the stealth helicopter? I would score this alternative as 3.	-We could use this covertly "to prevent Pakistani radars from spotting helicopters carrying Navy Seal commandos."[76] -There would be less risk of retaliation from Pakistan's army or police. I would score this alternative as 1.

[74] Bowden, "The Hunt for Geronimo."

[75] Ibid.

[76] Schmitt and Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya."

		Launch a missile	Helicopter raid	Deploy a cyberweapon
Dimensions	Political	-Biden was concerned about this failing and costing them a second term. -We won't definitively know the fate of OBL. -There could be fewer casualties. -This missile has never been tried before so we could miss. I would score this alternative as 1.	-Biden was concerned about this failing and costing them a second term. -If OBL was captured, we could try him in court. -There could be casualties. I would score this alternative as 2.	We could maintain plausible deniability. I would score this alternative as 3.
	Diplomatic	Perhaps this alternative is better than a raid since there are less casualties involved. I would score this alternative as 2.	-Secretary Clinton was concerned about the diplomatic ramifications of a raid. -This violates Pakistan's sovereignty. I would score this alternative as 1.	This option may alleviate diplomatic concerns. I would score this alternative as 3.
	Economic	This weapon costs a lot of money, time and resources. Do we really want to reveal this capability? I would score this alternative as 2.	Stealth helicopters cost a lot of money, time and resources. Do we really want to reveal this capability?	A cyberweapon costs a lot of time, money and resources. Do we really want to reveal this capability? I would score this alternative as 3.

		Launch a missile	Helicopter raid	Deploy a cyberweapon
			I would score this alternative as 1.	
	Final Choice	7	7	**10**

We can deductively conclude that deploying a cyberweapon in Pakistan was the preferred choice to kill Osama bin Laden and minimize casualties because it had the highest overall score. However, we know that this was not the choice that the Obama administration went with therefore, this decision matrix is inaccurate. This makes sense because the cyberweapon was not about killing Osama bin Laden, but about evading detection. So the following hypotheses might not be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [77] [VIOLENCE]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

Since this target was not out of the reach of other alternatives and the U.S. did not deploy, I think the following hypothesis might still be true:

[77] Blechman and Kaplan, 12.

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

In the case of Pakistan, the U.S. decided not to deploy a cyberweapon even though Osama bin Laden was a big threat, and deploying a cyberweapon could have helped avoid a possible scuffle with the Pakistanis as well as minimize collateral damage. Additionally, this was a chance to use a cyber capability with a military operation (though not for a conventional war) and yet the U.S. refrained. So will cyber capabilities be utilized alongside military missions in the future? This will be explored during the next chapter. Perhaps THREAT, VIOLENCE and COLLATERAL DAMAGE are not conditions of deployment but ACCESS might be a condition of deployment.

SYRIA

As explained in previous chapters, the U.S. first considered using an offensive cyberweapon in Syria as early as 2011. These deliberations continued in 2014. I decided to combine all of these considerations into one decision matrix.

According to a Gallup poll conducted September 3 – 4, 2013, American support for intervention in Syria was only 36%, which is among the lowest of all Gallup polls conducted about intervention in the past two decades.[78] This number is higher than the May poll suggesting that Americans were swayed by the use of chemical weapons however, it

[78] Andrew Dugan, *U.S. Support for Action in Syria Is Low vs. Past Conflicts*, (Gallup, September 6, 2013b), accessed December 6, 2016, http://www.gallup.com/poll/164282/support-syria-action-lower-past-conflicts.aspx.

is not nearly as high as Libya. (To be fair though, the Libyan poll was conducted after the operation began which means people could have felt the 'rally round the flag effect.[79])

The Pentagon said this intervention would cost 'tens of millions'[80] but others said the price tag was at least $100 million because the U.S. used 221 Tomahawks in Libya that cost over one million dollars each so if the U.S. used a comparable number of Tomahawks in Syria, the total cost of just the Tomahawks would be over $100 million.[81] This cost does not include other military components such as B-2 planes (over $60,000/hour) or warships ($25 million - $40 million per week.)[82]

Since Americans did not support Obama's plans for intervention, many disapproved of his management of the Syrian conflict. The following week's Gallup poll stated 61% of those polled disapproved of President Obama's handling of Syria.[83] For the first time, the "situation in Syria" made Gallup's "most important U.S. problem" list.[84]

Using the considerations discussed in the Literature Review and Cyberweapons chapters and the polls depicted above, we can create the following choice set for Syria.

---

[79] Dugan, *U.S. Support for Action in Syria Is Low vs. Past Conflicts*.

[80] David Alexander, "Hagel Estimates Cost of Syria Strike at 'Tens of Millions' of Dollars," *Reuters,* September 4, 2013b, accessed December 13, 2016, http://www.reuters.com/article/us-syria-crisis-usa-cost-idUSBRE98312N20130904.

[81] Ibid.

[82] Alexander, "Cost of a U.S. strike against Syria could top Hagel's estimate."

[83] *Presidential Ratings -- Issues Approval*.

[84] Andrew Dugan, *In U.S., Syria Emerges as a Top Problem, but Trails Economy*, (Gallup, September 11, 2013a), accessed August 20, 2017, http://www.gallup.com/poll/164348/syria-emerges-top-problem-trails-economy.aspx.

(1) do nothing

(2) continue talks

(3) implement airstrikes

(4) deploy a cyberweapon

Alternative 1: The U.S. could wait and see if there are other methods or countries that can assist with stemming the violence in Syria.

Alternative 2: The U.S. could continue discussions to stem the violence in Syria.

Alternative 3: The U.S. could launch airstrikes against Syrian targets.

Alternative 4: The U.S. could preemptively use a cyberweapon against specific Syrian facilities in order to stem the violence.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 6.17: Proposed Decision Matrix for Syria

		Alternatives			
		Do nothing	Continue talks	Implement airstrikes	Deploy a cyberweapon
Dimension	Military	If we do nothing, the crisis in Syria worsens and the conflict can spill over into the region. This is unacceptable.	There are no military implications if the U.S. continues talks but are they really working?	The U.S. should implement airstrikes since President Obama previously threatened the use of force.	An attack on Syria could result in Russian or Iranian retaliation.[85]

[85] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

		Do nothing	Continue talks	Implement airstrikes	Deploy a cyberweapon
Dimensions	Political	If we do nothing, the crisis in Syria worsens. We cannot afford to do nothing. This is unacceptable.	We could continue talks but are they really working?	The U.S. could implement airstrikes.	If we deploy a cyberweapon, we would be doing something to contain Syria's civil war without putting troops on the ground.[86]
	Diplomatic	Syria is imploding so we cannot afford to do nothing. This is unacceptable.	We should continue talks because this is the best diplomatic solution.	Airstrikes could result in international backlash because they can result in casualties, be inaccurate, or the U.S. can be seen as overreaching since we do not have U.N. support.	We could demonstrate that these weapons can be used for humanitarian purposes.[87]
	Economic	There are no economic implications if we do nothing.	There are no economic implications if we continue talks.	Airstrikes will cost hundreds of millions of dollars.	A cyberweapon is costly in terms of time and money but it may be cheaper than other alternatives.

[86] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[87] Ibid.

Doing nothing and allowing Syria to further implode is noncompensatory on the military, political and diplomatic dimensions so that alternative is eliminated immediately. So in the second stage of the decision-making process, we are left with the following options below. In the case of Syria, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in stopping Assad from further attacking civilians?* I decided to rate each alternative on a scale of 1 to 3. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.18: Proposed Decision Matrix for Syria

		Alternatives		
		Continue talks	Implement airstrikes	Deploy a cyberweapon
Dimensions	Military	There are no military implications if the U.S. continues talks but this option will not accomplish the decision rule. I would score this alternative as 1.	The U.S. should implement airstrikes since President Obama previously threatened the use of force. I would score this alternative as 3.	An attack on Syria could result in Russian or Iranian retaliation.[88] I would score this alternative as 2.
	Political	We could continue talks but this option may not accomplish the decision rule. I would score this alternative as 1.	The U.S. could implement airstrikes. I would score this alternative as 2.	If we deploy a cyberweapon, we would be doing something to contain Syria's civil war without putting troops on the ground.[89]

[88] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[89] Ibid.

		Continue talks	Implement airstrikes	Deploy a cyberweapon
				I would score this alternative as 3.
Dimensions	Diplomatic	We should continue talks since this is the best diplomatic solution. This option may accomplish the decision rule. I would score this alternative as 3.	Airstrikes could result in international backlash because they can result in casualties, be inaccurate, or the U.S. can be seen as overreaching since we do not have U.N. support. I would score this alternative as 1.	We could demonstrate that these weapons can be used for humanitarian purposes.[90] I would score this alternative as 2.
	Economic	There are no economic implications if we continue talks. I would score this alternative as 1.	Airstrikes will cost hundreds of millions of dollars. I would score this alternative as 2.	A cyberweapon is costly in terms of time and money but it may be cheaper than other alternatives. I would score this alternative as 3.
	Final Choice	6	8	**10**

We can deductively conclude that deploying a cyberweapon in Syria is the preferred choice to stop Assad from further attacking civilians since it has the highest overall score. However, the U.S. ultimately refrained from deploying a cyberweapon so, this decision matrix is inaccurate. Thus, the following hypotheses might not be true:

[90] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [91] [VIOLENCE]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

Since these targets were not out of the reach of airstrikes and the U.S. did not deploy, I think the following hypothesis might still be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

Additionally, since some Republicans thought Syria was not a threat and the U.S. did not deploy, I think the following hypothesis might still be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

In the case of Syria, the U.S. decided not to deploy a cyberweapon even though deploying a cyberweapon could have helped stem the violence and minimize casualties. Thus, perhaps VIOLENCE and COLLATERAL DAMAGE are not conditions of deployment but THREAT and ACCESS might be conditions of deployment. Some of these results are similar to the Libya findings but there are differences between the two scenarios.

As mentioned earlier, Obama sought congressional approval in Syria but not in Libya. Second, Libya was seen as a mild threat whereas Syria was not seen as a threat. Third, when Qaddafi threatened to massacre Libyans in Benghazi, the international

[91] Blechman and Kaplan, 12.

community felt compelled to act and Americans supported the subsequent military action. The intent in Libya was to prevent violence. However, in Syria, where over a thousand people were killed by chemical weapons – which are a considered a crime against humanity[92] – Britain vetoed military intervention and American support for intervention was only 36%. In Syria, it seems there was sparse political will to act since lives were already lost.

Another difference between Libya and Syria is that the Libyan operation occurred in 2011, a year before the 2012 U.S. presidential election and the crisis in Syria increasingly worsened in the run-up to and after the 2012 U.S. presidential election. According to the lame duck notion, President Obama could have felt more free to act in 2014, and yet he refrained. So perhaps the lack of domestic support was an overwhelming factor. I think the more likely reason though is that the Libyan operation dominated the decision-making calculus in Syria. A Gallup poll conducted after Operation Odyssey Dawn, which was initially declared "a model intervention" by the Commander of NATO,[93] stated 39% of those polled disapproved of Obama's handling of Libya[94] since Libya was subsequently overrun by militants.[95]

---

[92] "Use of chemical weapons in Syria would be 'crime against humanity' – Ban," *The United Nations,* August 23, 2013, accessed December 9, 2016, http://www.un.org/apps/news/story.asp?NewsID=45684.

[93] Ivo H. Daalder and James G. Stavridis, "NATO's Victory in Libya," *Foreign Affairs* 91, no. 2 (March/April, 2012): 2, JSTOR via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

[94] *Presidential Ratings -- Issues Approval.*

[95] Scott Shane and Jo Becker, "The Libya Gamble | Part 2, A New Libya, with 'Very Little Time Left,'" *The New York Times,* February 27, 2016, accessed August 20, 2017, https://www.nytimes.com/2016/02/28/us/politics/libya-isis-hillary-clinton.html.

NORTH KOREA (2014)

According to a Gallup poll, in 2014 North Korea was tied with Iran for the second 'greatest enemy' of the U.S.[96] Therefore, when North Korea hacked Sony Pictures Entertainment on November 24, 2014 and threatened violence against U.S. theaters,[97] the U.S. decided to respond. President Obama's approval rating from Dec 8 – 14 was 43%, from Dec 15 – 21, 45% and from Dec 22 – 28, 44%.[98]

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the polls mentioned above, we can create the following choice set for responding to North Korea's hacking of Sony.

(1) do nothing

(2) increase sanctions

(3) deploy a cyberweapon

Alternative 1: The U.S. could do nothing since Sony only lost $35 million.

Alternative 2: The U.S. could implement additional sanctions against North Korea to punish them for attacking Sony.

Alternative 3: The U.S. could deploy a cyberweapon against North Korea.

The decision matrix consists of four dimensions and three alternatives. I listed the dimensions in order of increasing importance.

---

[96] Jim Norman, *Four Nations Top U.S.'s Greatest Enemy List*, (Gallup, February 22, 2016), accessed December 10, 2016, http://www.gallup.com/poll/189503/four-nations-top-greatest-enemy-list.aspx.

[97] Brooks Barnes and Michael Cieply, "Sony Drops 'The Interview' Following Terrorist Threats," *The New York Times,* December 17, 2014, accessed November 29, 2016, http://nyti.ms/1GtuCOw.

[98] *Presidential Approval Ratings – Barack Obama*.

Table 6.19: Proposed Decision Matrix for Attacking North Korea (2014)

		Alternatives		
		Do nothing	Increase sanctions	Deploy a cyberweapon
Dimensions	Military	We cannot afford to do nothing because the North Koreans threatened violence against our theaters. This is unacceptable.	We could increase sanctions but will they be effective since the North Koreans are already heavily sanctioned?[99]	We should do this since it can be done covertly and precisely. Tit-for-tat.
	Political	We cannot afford to do nothing because the North Koreans have attacked our freedom of speech and threatened violence against our theaters. This is unacceptable.	We could increase sanctions.	We could do this since it can be done covertly and precisely. Tit-for-tat.
	Diplomatic	If we do nothing, the North Koreans get away with attacking us. This is unacceptable.	We could increase sanctions as long as they do not exacerbate the already dire situation for North Korean civilians.	We could do this covertly but will it trigger a wider conflict?
	Economic	The North Korean attack cost Sony $35 million. So we cannot do nothing. This is unacceptable.	We should increase sanctions. They are effective.	Deploying a cyberweapon against North Korea may be costly in terms of time and money.

[99] David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony Case," *The New York Times,* January 2, 2015d, accessed December 1, 2016, http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

Doing nothing and allowing North Korea to get away with attacking Sony and threatening violence is unacceptable on all dimensions so that alternative is eliminated immediately. (This is the only case where an option was noncompensatory on all dimensions.) Thus, in the second stage of the decision-making process, we are left with two options. In the case of North Korea, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is this alternative a proportional response?* I decided to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.20: Proposed Decision Matrix for Attacking North Korea (2014)

		Alternatives	
		Increase sanctions	Deploy a cyberweapon
Dimensions	Military	We could increase sanctions but will they be effective since the North Koreans are already heavily sanctioned?[100] I would score this alternative as 1.	This is a proportional response to North Korea's attack. Tit-for-tat. I would score this alternative as 2.
	Political	We could increase sanctions. I would score this alternative as 1.	We could do this covertly and precisely. Tit-for-tat. I would score this alternative as 2.
	Diplomatic	We could increase sanctions as long as they do not exacerbate the already dire situation for North Korean civilians. I would score this alternative as 1.	We could do this covertly but will it trigger a wider conflict? I would score this alternative as 2.
	Economic	We should increase sanctions. They are effective.	Deploying a cyberweapon against North Korea may be

[100] Sanger and Schmidt, "More Sanctions on North Korea After Sony Case."

		Increase sanctions	Deploy a cyberweapon
		I would score this alternative as 2.	costly in terms of time and money. I would score this alternative as 1.
	Final Choice	5	**7**

We can deductively conclude that deploying a cyberweapon against North Korea for their attack on Sony was the preferred choice for responding to North Korea's hacking of Sony because it had the highest overall score. Since the Internet went out in North Korea, this decision matrix is accurate. (Although the opposite could also be argued since the U.S. imposed ineffective sanctions on North Korea in January 2015.[101]) Although this cyber operation was not about a first strike, the following hypotheses might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

There was no looming military conflict with North Korea so VIOLENCE was not tested.

[101] Sanger and Schmidt, "More Sanctions on North Korea After Sony Case."

In the case of North Korea, the U.S. decided to use direct action – since they are not at war with North Korea but deployed a cyberweapon – in order to covertly deal with a threat and strike a hard-to-reach area. The North Korean case suggests that THREAT, ACCESS, and COLLATERAL DAMAGE may be conditions of deployment.

ISIS (2016)

In December 2015, 16% of those polled said terrorism was the number one threat facing the U.S.[102] "This is the highest percentage of Americans to mention terrorism in a decade, although it is still lower than the 46% measured after 9/11."[103]

Using the sources discussed in the Literature Review and Cyberweapons chapters, as well as the polls cited above, we can create the following choice set for the ISIS case.

(1) continue current methods

(2) implement more airstrikes

(3) send in additional SOF

(4) deploy a cyberweapon

Alternative 1: The U.S. could continue its current methods of fighting ISIS.

Alternative 2: The U.S. could launch additional airstrikes against ISIS.

Alternative 3: The U.S. could send in additional SOF to deal with ISIS on the ground.

Alternative 4: The U.S. could deploy a cyberweapon against ISIS targets.

---

[102] Rebecca Riffkin, *Americans Name Terrorism as No. 1 U.S. Problem*, (Gallup, December 14, 2015), accessed December 12, 2016, http://www.gallup.com/poll/187655/americans-name-terrorism-no-problem.aspx.

[103] Ibid.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 6.21: Proposed Decision Matrix for ISIS (2016)

		Alternatives			
		Continue current methods	Implement additional airstrikes	Send in additional SOF	Deploy a cyberweapon
Dimensions	Military	The U.S. could continue its current methods but ISIS is still wreaking havoc. This is unacceptable.	We should implement additional airstrikes against ISIS.	There are already SOF in Syria so perhaps we could send more.	We should do this since it could disrupt the Islamic State's operations without putting more boots on the ground.
	Political	The U.S. could continue its current methods but ISIS is still wreaking havoc.	We could implement additional airstrikes against ISIS.	We should not send more troops to the Middle East.	We should do this since it could disrupt the Islamic State's operations without putting more boots on the ground.
	Diplomatic	The U.S. could continue its current methods but ISIS is still wreaking havoc.	We could implement additional airstrikes against ISIS.	We should not send more troops to the Middle East.	We could do this since it could disrupt the Islamic State's operations without putting more boots on the ground or launching more airstrikes.
	Economic	Current methods have cost us $10 billion.	The estimated cost of monthly airstrikes against ISIS ranges from	The estimated cost of monthly boots on the ground is over one	We have spent millions of dollars on these weapons so we could use them especially if they may be cheaper than other options.

		Continue current methods	Implement additional airstrikes	Send in additional SOF	Deploy a cyberweapon
			$200 - $570 million.[104]	billion dollars.[105]	

Continuing current methods while ISIS is still wreaking havoc is unacceptable on the military dimension but I did not classify this as noncompensatory on the political dimension because in February 2015, President Obama sent a request to Congress for an Authorization to Use Military Force against ISIS but as of December 2015, Congress had not yet voted.[106] Nevertheless, I eliminated this alternative immediately. Thus, in the second stage of the decision-making process, we are left with the following options below. In the case of ISIS, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is this alternative expected to result in disrupting ISIS' command-and-control operations?* I decided to rate each alternative on a scale of 1 to 3. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

[104] Harrison et al., 5.

[105] Ibid.

[106] Jennifer Bendery, "Obama Pleads Again For Congress To Authorize His ISIS War," *Huffington Post,* December 7, 2015, accessed August 20, 2017, http://www.huffingtonpost.com/entry/obama-war-authorization-isis_us_5661d411e4b08e945fef455c. The Authorization for Use of Military Force was a resolution that President George W. Bush signed in 2001 authorizing the President to use force against those who were responsible for 9/11. Authorization for Use of Military Force, S.J. Res. 23, 107th Congress, (September 18, 2001), accessed August 20, 2017, https://www.gpo.gov/fdsys/pkg/PLAW-107publ40/pdf/PLAW-107publ40.pdf.

Table 6.22: Proposed Decision Matrix for ISIS (2016)

		Alternatives		
		Implement additional airstrikes	Send in additional SOF	Deploy a cyberweapon
Dimensions	Military	We should implement additional airstrikes against ISIS. I would score this alternative as 2.	There are already SOF in Syria so perhaps we could send more. I would score this alternative as 1.	We should do this since it could disrupt the Islamic State's operations without putting more boots on the ground. I would score this alternative as 3.
	Political	We could implement additional airstrikes against ISIS. I would score this alternative as 2.	We should not send more troops to the Middle East. I would score this alternative as 1.	We should do this since it could disrupt the Islamic State's operations without putting more boots on the ground. I would score this alternative as 3.
	Diplomatic	We could implement additional airstrikes against ISIS. I would score this alternative as 2.	We should not send more troops to the Middle East. I would score this alternative as 1.	We could do this since it could disrupt the Islamic State's operations without putting more boots on the ground or launching more airstrikes. I would score this alternative as 3.
	Economic	The estimated cost of monthly airstrikes against ISIS ranges from $200 - $570 million.[107]	The estimated cost of monthly boots on the ground is over one billion dollars.[108]	We have spent millions of dollars on these weapons so we could use them especially if they may be cheaper than other options. I would score this alternative as 3.

[107] Harrison et al., 5.

[108] Ibid.

		Implement additional airstrikes	Send in additional SOF	Deploy a cyberweapon
		I would score this alternative as 2.	I would score this alternative as 1.	
	Final Choice	8	4	**12**

We can deductively conclude that deploying a cyberweapon against ISIS targets was the preferred choice to disrupt their command-and-control operations because it had the highest overall score. Since the U.S. did deploy cyberweapons against ISIS targets, this decision matrix is accurate. Although this cyber operation was not about a first strike, the following hypothesis might be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

However, since this operation was happening alongside airstrikes, the following hypotheses might not be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [109] [VIOLENCE]

[109] Blechman and Kaplan, 12.

Additionally, since this cyberweapon was used to kill militants, the following hypothesis might not be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

This case is different from the Iraq (2007) case because in the Iraq (2007) case, the U.S. said they were concerned about collateral damage whereas collateral damage was not a stated concern in regards to the ISIS (2016) case. However, just as in the Iraq (2007) case, the U.S. was already at war when they thought about using a cyberweapon. Thus, the ISIS (2016) case suggests that THREAT might be a condition of deployment.

RUSSIA (2016)

Using the sources discussed in the Literature Review and Cyberweapons chapters, we can create the following choice set for responding to Russia's actions in the 2016 U.S. presidential election:

(1) do nothing

(2) implement sanctions

(3) covert action

(4) deploy a cyberweapon

Alternative 1: The U.S. could do nothing because any option may work in Putin's favor.

Alternative 2: The U.S. could implement sanctions against Russia.

Alternative 3: The U.S. could engage in "covert action against Russian targets."[110]

Alternative 4: The U.S. could use a cyberweapon against Russian facilities.

[110] David E. Sanger, "U.S. Says Russia Directed Hacks to Influence Elections," *The New York Times,* October 7, 2016d, accessed December 1, 2016, http://nyti.ms/2dLddLS.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 6.23: Proposed Decision Matrix for Russia (2016)

		Alternatives			
		Do nothing	Implement sanctions	Engage in covert action	Deploy a cyberweapon
Dimensions	Military	The U.S. cannot allow Russia to go unpunished for meddling in the U.S. presidential election so this option is unacceptable.	We could implement sanctions against Russia.	We cannot engage in covert action in Russia because the military risks are great and the Russians will probably retaliate. Thus, this option is unacceptable.	We should deploy a cyberweapon against Russian facilities because this is an effective way of retaliating against a hard-to-reach target and we could do it covertly so we avoid a wider conflict. Tit-for-tat.
	Political	The U.S. cannot allow Russia to go unpunished for meddling in the U.S. presidential election so this option is unacceptable.	We could implement sanctions against Russia but this may result in political repercussions.	We cannot engage in covert action in Russia because the military and political risks are great and the Russians will probably retaliate. Thus, this option is unacceptable.	We should deploy a cyberweapon against Russian facilities because this is an effective and proportional way of retaliating against a hard-to-reach target and we could do it covertly so we avoid a wider conflict. Tit-for-tat.

		Do nothing	Implement sanctions	Engage in covert action	Deploy a cyberweapon
Dimensions	Diplomatic	The U.S. should not allow Russia to go unpunished for meddling in the U.S. presidential election.	We could implement sanctions against Russia but this may result in diplomatic repercussions.	We cannot engage in covert action in Russia because the political risks are great and the Russians will probably retaliate. Thus, this option is unacceptable.	We could deploy a cyberweapon against Russian facilities because this is a proportional way of retaliating against a hard-to-reach target and we could do it covertly so we avoid a wider conflict however, there could be diplomatic ramifications.
	Economic	There are no economic implications if the U.S. decides to do nothing.	We could increase sanctions but this may result in economic repercussions for the U.S.	Covert action is costly in terms of time, money and possibly casualties.	We have spent millions of dollars on these weapons so we should use them if they are more effective than other options.

Doing nothing and allowing Russia to go unpunished for interfering in the 2016 U.S. presidential election is unacceptable on the military and political dimensions so this alternative is eliminated immediately. Since we do not really know what covert action in Russia entails, this alternative is unacceptable on the military, political and diplomatic dimensions so this option is also eliminated immediately. Thus, in the second stage of the decision-making process, we are left with the following options below. In the case of Russia, the decision rule that the U.S. could use for choosing among the alternatives can

be posed as: *Is this alternative a proportional response that will minimize retaliation?* I decided to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 6.24: Proposed Decision Matrix for Russia (2016)

		Alternatives	
		Implement sanctions	Deploy a cyberweapon
Dimensions	Military	We could implement sanctions against Russia. I would rate this alternative as 1.	We should deploy a cyberweapon against Russian facilities because this is an effective way of retaliating against a hard-to-reach target and we could do it covertly so we avoid a wider conflict. Tit-for-tat. I would rate this alternative as 2.
	Political	We could implement sanctions against Russia but this may result in political repercussions. I would rate this alternative as 1.	We should deploy a cyberweapon against Russian facilities because this is an effective and proportional way of retaliating against a hard-to-reach target and we could do it covertly so we avoid a wider conflict. Tit-for-tat. I would rate this alternative as 2.
	Diplomatic	We could implement sanctions against Russia but this may result in diplomatic repercussions. I would rate this alternative as 1.	We could deploy a cyberweapon against Russian facilities because this is a proportional way of retaliating against a hard-to-reach target and we could do it covertly so we avoid a wider conflict however, there could be diplomatic ramifications. I would rate this alternative as 2.
	Economic	We could increase sanctions but this may result in economic repercussions for the U.S.	We have spent millions of dollars on these weapons so we should use them if they are more effective than other options. I would rate this alternative as 2.

		Implement sanctions	Deploy a cyberweapon
		I would rate this alternative as 1.	
	Final Choice	4	**8**

We can deductively conclude that deploying a cyberweapon against Russia was the preferred choice for responding to their role in the 2016 U.S. presidential election because it had the highest overall score. However, the Obama administration decided to sanction a few Russian intelligence agencies and organizations, seize a couple of U.S. properties that were being used by the Russians and expel 35 Russian spies from the U.S. so perhaps this decision matrix is inaccurate.[111] Although this cyber operation was not about a first strike, I still think the following hypotheses may not be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]
- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they cannot use troops, drones or airstrikes.* [ACCESS]
- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

[VIOLENCE] was not tested since this cyberweapon was not for preventing or ending a war.

[111] David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *The New York Times,* December 29, 2016b, accessed January 13, 2017, https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=0.

IRAQ (2003)

At the time, 64% of those polled approved of military action in Iraq in 2003 before military action even began[112] and Bush had extremely high approval ratings of 79 – 81%.[113]

Using the sources discussed in the Literature Review and Cyberweapons chapters as well as the polls depicted above, we can create the following choice set for the Iraq (2003) case:

(1) do nothing

(2) use military force

(3) deploy a cyberweapon

Alternative 1: The U.S. could refrain from engaging in conflict since Iraq's W.M.D.s have not been found and we do not have U.N. authorization to use force.[114]

Alternative 2: The U.S. could use military force against Iraq.

Alternative 3: The U.S. could use a cyberweapon to obliterate Iraq's financial system.

The decision matrix consists of four dimensions and three alternatives. I listed the dimensions in order of increasing importance.

---

[112] Dugan, *U.S. Support for Action in Syria Is Low vs. Past Conflicts*.

[113] *Presidential Approval Ratings -- George W. Bush*.

[114] David E. Sanger and with John F. Burns, "Bush Orders Start of War on Iraq; Missiles Said to Be Aimed at Hussein," *The New York Times,* March 19, 2003, accessed December 11, 2016, http://www.nytimes.com/2003/03/19/international/bush-orders-start-of-war-on-iraq-missiles-said-to-be-aimed-at.html.

Table 6.25: Proposed Decision Matrix for Iraq (2003)

		Alternatives		
		Do nothing	Use military force	Deploy a cyberweapon
Dimensions	Military	We cannot do nothing when "Intelligence gathered by this and other governments leaves no doubt that the Iraq regime continues to possess and conceal some of the most lethal weapons ever devised."[115] This is unacceptable.	"Now that conflict has come, the only way to limit its duration is to apply decisive force." [116]	We should use a cyberweapon to obliterate Saddam Hussein's finances.
	Political	We cannot afford to do nothing when "the mercy of an outlaw regime that threatens the peace with weapons of mass murder"[117] exists. This is unacceptable.	The U.S. public supports military action in Iraq.	We could use a cyberweapon to cripple Iraq's financial system but we are unsure of the implications.
	Diplomatic	"The United Nations Security Council has not lived up to its responsibilities, so we will rise to ours." [118]	We do not have U.N. authorization to use force.[119]	We should not use a cyberweapon to cripple Iraq's financial system since we are

[115] "Full Text: Bush's Speech," *The Guardian,* March 17, 2003, accessed December 10, 2016, https://www.theguardian.com/world/2003/mar/18/usa.iraq.

[116] George W. Bush, "President Bush Addresses the Nation," (speech, Washington, D.C., March 19, 2003), accessed December 10, 2016, *The White House*, https://georgewbush-whitehouse.archives.gov/news/releases/2003/03/20030319-17.html.

[117] Ibid.

[118] "Full text: Bush's speech."

[119] Sanger with Burns, "Bush Orders Start of War on Iraq; Missiles Said to Be Aimed at Hussein."

		Do nothing	Use military force	Deploy a cyberweapon
				unsure of the implications.
Dimension	Economic	There are no economic implications if we do nothing.	This will cost $50 to $60 billion.[120]	If this is cheaper than a full scale war, we should use it.

Doing nothing is unacceptable on the military and political dimensions so that alternative is eliminated immediately. Therefore, in the second stage of the decision-making process, we are left with the following options below. In the case of using a cyberattack against Iraq, the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is this alternative expected to result in obliterating the Iraqi financial system?* I decided to rate each alternative on a scale of 1 to 2. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

[120] Elisabeth Bumiller, "Threats and Responses: The Cost; White House Cuts Estimate of Cost of War with Iraq," *The New York Times,* December 31, 2002, accessed December 11, 2016, http://www.nytimes.com/2002/12/31/us/threats-responses-cost-white-house-cuts-estimate-cost-war-with-iraq.html.

Table 6.26: Proposed Decision Matrix for Iraq (2003)

Alternatives

		Use military force	Deploy a cyberweapon
Dimensions	Military	"Now that conflict has come, the only way to limit its duration is to apply decisive force."[121] I would score this alternative as 1.	We should use a cyberweapon to obliterate Saddam Hussein's finances. I would score this alternative as 2.
	Political	The U.S. public supports military action in Iraq. I would score this alternative as 2.	We could use a cyberweapon to cripple Iraq's financial system but we are unsure of the implications. I would score this alternative as 1.
	Diplomatic	We do not have U.N. authorization to use force.[122] I would score this alternative as 1.	We should not use a cyberweapon to cripple Iraq's financial system since we are unsure of the implications. I would score this alternative as 2.
	Economic	This will cost $50 to $60 billion.[123] I would score this alternative as 1.	If this is cheaper than a full scale war, we should use it. I would score this alternative as 2.
	Final Choice	5	**7**

[121] Bush, "President Bush Addresses the Nation."

[122] Sanger with Burns, "Bush Orders Start of War on Iraq; Missiles Said to Be Aimed at Hussein."

[123] Bumiller, "Threats and Responses: The Cost; White House Cuts Estimate of Cost of War With Iraq."

We can deductively conclude that deploying a cyberweapon against Iraq was the preferred choice to obliterate Iraq's finances since it had the highest overall score. However, the U.S. refrained even though history would show that the invasion of Iraq would cost them so much more than anticipated. I think the U.S. refrained from deploying a cyberweapon since the public supported intervention. So in the end, domestic politics may have influenced the outcome. Since this decision matrix is inaccurate, the following hypotheses might not be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* [THREAT]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* [124] [VIOLENCE]

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* [COLLATERAL DAMAGE]

Since these targets were not out of the reach of airstrikes and the U.S. did not deploy, I think the following hypothesis might still be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.* [ACCESS]

The Iraq case study suggests that THREAT, VIOLENCE and COLLATERAL DAMAGE may not be conditions of deployment but ACCESS may be a condition of deployment.

---

[124] Blechman and Kaplan, 12.

RESULTS

We can summarize the results from the decision matrixes as follows:

Table 6.27: Summary of Results

WEAPON	PREFERRED DECISION	DEPLOYED	THREAT	ACCESS	VIOLENCE	COLLATERAL DAMAGE
Stuxnet	Cyberweapon	Yes	True	True	True	True
Iraq (2007)	Cyberweapon	Yes	True	True	True	False
Shotgiant (2007)	Cyberweapon	Yes	False	True	Not tested	Not tested
Quantum (2008)	Cyberweapon	Yes	False	True	Not tested	Not tested
Turbine (2010)	Cyberweapon	Yes	False	True	Not tested	Not tested
Nitro Zeus	Cyberweapon	NULL	True	True	False	True
Libya (2011)	Airstrikes	Yes	False	True	False	False
Pakistan (2011)	Cyberweapon	No	False	True	False	False

WEAPON	PREFERRED DECISION	DEPLOYED	THREAT	ACCESS	VIOLENCE	COLLATERAL DAMAGE
Syria	Cyberweapon	No	True	True	False	False
North Korea (2014)	Cyberweapon	Yes	True	True	Not tested	True
ISIS (2016)	Cyberweapon	Yes	True	False	False	False
Russia (2016)	Cyberweapon	No	False	False	Not tested	False
Iraq (2003)	Cyberweapon	No	False	True	False	False

These 13 decision matrixes revealed the process in which the decision to deploy or not deploy a cyberweapon was made. THREAT and ACCESS were the two variables that were tested in all 13 cases. ACCESS was true in 11/13 cases. Thus, the following hypothesis is true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they cannot use troops, drones or airstrikes.*

This result supports the finding in Chapter 5 that suggested DEPLOYED and OTHER ALTERNATIVES were negatively correlated.

THREAT was true 6/13 times which builds on the weak finding from the previous chapter that suggested PERCEIVED ADVERSARY and DEPLOYED were correlated. Now, it might be true that

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.*

COLLATERAL DAMAGE was only tested in 10 cases and out of those 10 cases, it was true three times so perhaps the following hypothesis might not be true:

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize casualties.*

This result seems to contradict the finding in Chapter 5 that implied COLLATERAL DAMAGE and DEPLOYED were strongly negatively correlated. Thus, I will explore collateral damage further during the interviews.

As for VIOLENCE, this variable was tested eight times and was true twice. Thus, it is probably unlikely that

- *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."*[125]

Only in four cases was the preferred choice to deploy a cyberweapon but the U.S. refrained, (Syria, Russia, Iraq (2003) and Pakistan). Nitro Zeus was a null case since the Iranian nuclear deal went through but I did not label the hypotheses null. In the case of Libya, the proposed decision matrix was accurate in describing that the preferred choice was airstrikes, not deploying a cyberweapon. In the case of North Korea, even though the

[125] Blechman and Kaplan, 12.

decision matrix was accurate in explaining that deploying a cyberweapon was the preferred choice, the U.S. may not have committed this act. Additionally, the U.S. sanctioned North Korea in January 2015 so it can be argued that this decision matrix was inaccurate.

We might also be able to infer that 7/13 of the decision matrices were accurate in explaining the decision to deploy a cyberweapon. Of course it can be argued that perhaps the decision matrixes were created so that they would pan out in favor of the known outcome. After all, I could have labeled more alternatives on the diplomatic dimension noncompensatory and some cases have more in-depth explanations than others. However, I portrayed all available information that I found. Nevertheless, these are the ways in which to falsify these results.

Another way to falsify these results is to remove some of the cases. For instance, ISIS could be removed since this operation was against a non-state actor. North Korea (2014) and Russia (2016) could also be removed since these were acts of retaliation. Shotgiant (2007) could be removed since this operation was against a Chinese company not the Chinese government per say. Iraq (2003) could also be removed if it is argued that this cyberweapon did not intend to physically destroy anything.

Based on these results as well as those of Chapter 5, I propose that the two questions to ask respectively, when thinking about deploying a cyberweapon are:

(1) Is there a threat?

(2) Is the intended target out of the reach of troops, drones or airstrikes?

If the answers are Yes, then it is likely that the U.S. will consider deploying a cyberweapon.

CONCLUSION

This chapter retroactively applied poliheuristic theory to the 13 case studies analyzed in this dissertation in order to assess the process validity of previous U.S. decisions about using a cyberweapon. Through the use of a decision matrix, I was able to understand the conditions that factored into the U.S.' decision-making calculus when it came to deploying or not deploying a cyberweapon. We were able to reveal that access is a condition in the U.S. decision-making process. *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they cannot use troops, drones or airstrikes.* This outcome supports the finding in Chapter 5 that suggested OTHER ALTERNATIVES and DEPLOYMENT were negatively correlated.

This chapter also established that *the U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.* This outcome clarifies the weak finding in Chapter 5 that suggested the U.S. may deploy a cyberweapon against a perceived adversary.

Additionally, contrary to the arguments of some scholars and U.S. officials, it is unlikely that *the U.S. will deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in full-scale conflict* or that *the U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize collateral damage.* This outcome contradicts the finding in Chapter 5 that implied collateral damage and deployment were strongly negatively correlated. Thus, I explored this discrepancy during the interviews.

Now we move from explaining past decisions to speculating about future ones. In the next chapter, we will hear from 22 officials who speculated about other conditions

under which the U.S. will likely deploy a cyberweapon. Some of the interviewees also discussed these cases, so in the final chapter, I applied their answers to my proposed decision matrixes and tweaked the matrixes accordingly.

Chapter 7

INTERVIEWS

"Hammers aren't much good hanging on the wall."

–A Legal Advisor

From January 2017 – March 2017, I conducted 22 confidential semi-structured interviews in-person, over the phone, on Skype, and one via email. I discussed arranging an interview with almost 50 people but not everyone responded and some declined. First, I used purposive sampling to target certain interviewees. I also cold-emailed some prospects. If I did not have someone's email address, I attempted to contact them through LinkedIn. I even messaged people on Twitter. I also contacted former colleagues and asked them to connect me with certain government officials. I also sought their advice as to who else they would recommend I speak with. I also sought the advice and assistance of a former government official whom I met through the Rutgers Institute for Emergency Preparedness and Homeland Security. Not all of their contacts ultimately agreed to an interview. In a way, I also utilized simple random sampling because one individual sent out an email blast to his network and some people expressed interest but not all of them ended up responding to an interview request. If individuals agreed to an interview, I then used snowball sampling by asking at the end of the interview, "Whom else do you think it might be useful for me to interview? Would you be so kind as to help me make contact?"

The breakdown of the interviewees was: three journalists, seven former government officials, one current government official, one legal advisor, five cybersecurity specialists, four academics (although one says he is a practitioner) and one think tank

member. Many interviewees in the government and cybersecurity sectors overlapped. Some of these cybersecurity and former government officials are also aligned with organizations such as New America and the Truman National Security Project. I interviewed one person who used to work for the N.S.A.'s elite cyberwarfare division, Tailored Access Operations (T.A.O.) as well as one person who used to work for the N.S.A.'s Remote Operations Center (R.O.C.). I also interviewed someone who used to work for U.S. Cyber Command, a former Senior Cyber Policy Advisor for the government, and a Legal Advisor at a collective security organization.

On the academic side, I spoke with the directors of cyber programs at Stanford University, Columbia University and Harvard University as well as the Naval Postgraduate School. On the cybersecurity front, I spoke with people from major cybersecurity companies including someone who used to work for Kaspersky Lab. One thing to note is that Kaspersky Lab has come under fire for their alleged Russian ties. Currently, they may not be granting interviews, but I interviewed one of their former employees before the curtain came down.

As for the media category, I spoke with journalists from *The New York Times*, *The Washington Post* as well as someone who used to work for *Wired*. I tried to interview at least 1 female in each category but most of the interviewees were men. I spent a lot of time in Washington. I also travelled to Boston and California. I spoke with each person one time, although I did follow-up with a few people on email mostly about additional persons to interview. Most of the interviews lasted 30-60 minutes although one interview lasted about two hours. I had a list of IRB-approved questions as an interview guide, and I took handwritten notes during the interview.

The interview process was extremely interesting. Many people praised my project while a few academics wanted to shift my focus in other directions. However, my dissertation chair was right- the interviews were the fun part. I even enjoyed the coding! I used the Nvivo for Mac software to first code the interviews and then perform a content analysis of the data. I used *Research Methods in Practice: Strategies for Description and Causation*,[1] *Qualitative Data Analysis with Nvivo,*[2] and the "Nvivo for Mac Help" online manual[3] as reference guides for how to use the Nvivo for Mac software to handle the data. Unfortunately, not all of the features are available in Nvivo for Mac. Nevertheless, I utilized many of the queries that were available to describe and interpret the interviews.

I coded mainly according to the topics discussed during the interviews. The codes were "Advantages and Disadvantages," "Adversaries," "Cases," "Conditions," "Cost," "Decision-making," "Definitions," "Five Eyes," "Future," "ISIS," "North Korea," "Proxy War," "Russia," "Situation," "Stuxnet," and "Targets." A new theme that emerged from the interviews was "Influence Operations." I also coded for "Split Role" and "Trump," both of which were based on current events. I also had a category called "Interesting Findings" which was basically a catchall for content that I found interesting but did not fit neatly into the other nodes. As you can imagine, I had to do some more research which included digging further into *Technology, Policy, Law, and Ethics Regarding U.S.*

---

[1] Dahlia K. Remler and Gregg G. Van Ryzin, *Research Methods in Practice: Strategies for Description and Causation* (Thousand Oaks, California: SAGE Publications, 2011).

[2] Patricia Bazeley and Kristi Jackson, *Qualitative Data Analysis with Nvivo* (London: SAGE Publications, 2013).

[3] Nvivo for Mac, "Nvivo for Mac Help," *QSR International*, accessed March 14, 2017, http://help-nv11mac.qsrinternational.com/desktop/welcome/welcome.htm.

Acquisition and Use of Cyberattack Capabilities, by William A. Owens, Kenneth W. Dam, and Herbert S. Lin as well as *Joint Publication 3-12 (R) Cyberspace Operations*.

This chapter is organized around these themes, which, in turn, reflected the questions I asked. The questions themselves were drawn from the Literature Review, hypotheses and poliheuristic theory. What follows is a narrative based on each theme interspersed with the query results, visualizations and interpretations. The next and final chapter is the Discussion and Conclusion where I explain how all the information I gathered and analyzed ties together.

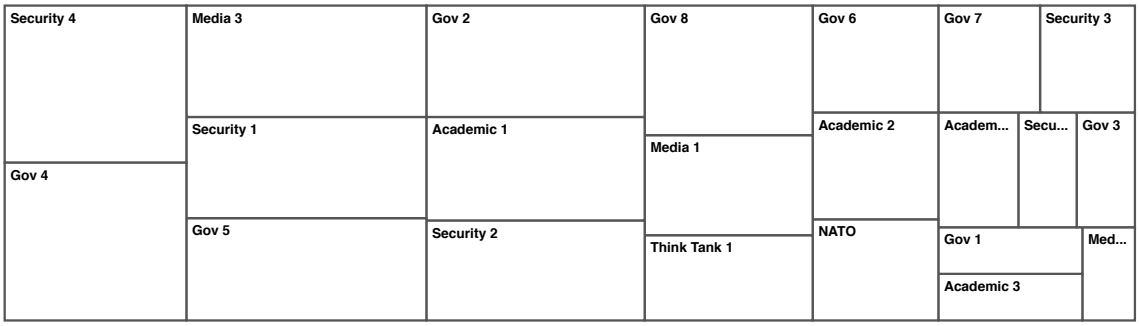
NVIVO FINDINGS

In order to understand what interviews were coded the most, I used a hierarchy chart which depicts all of the interviews arranged by size.[4] This is visualized via a treemap which shows all the hierarchies at once.[5] The following treemap indicates the sources that were coded the most were Security 4, Gov 4 and Media 3 with over 30 references each. Gov 4 and Security 4 tied for 34 references each. I spent two hours speaking with Security 4. Gov 4 represents a former T.A.O. official.

[4] Nvivo for Mac, "About hierarchy charts," *QSR International*, accessed March 22, 2017, http://help-nv11mac.qsrinternational.com/desktop/concepts/about_hierarchy_charts.htm.

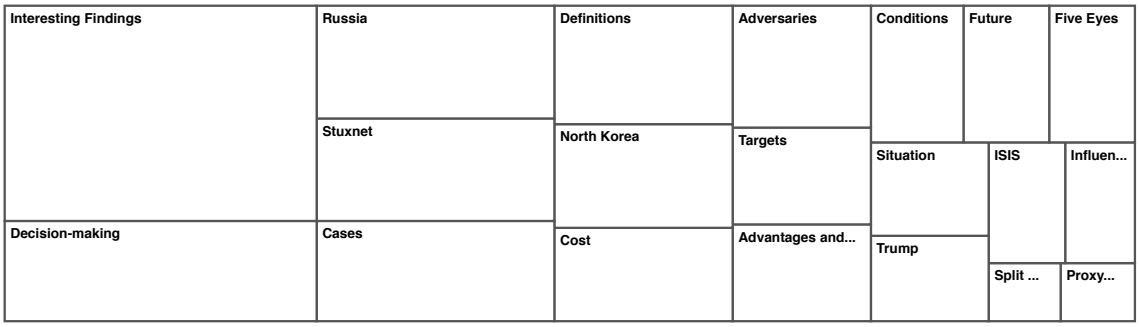
[5] Ibid.

Figure 7.1 Treemap of Sources



The following hierarchy chart shows the coding for the nodes. This treemap indicates that "Interesting Findings" was coded the most with about 80 references followed by "Decision-making," "Russia," "Stuxnet," and "Cases" with about 30 or so references each.

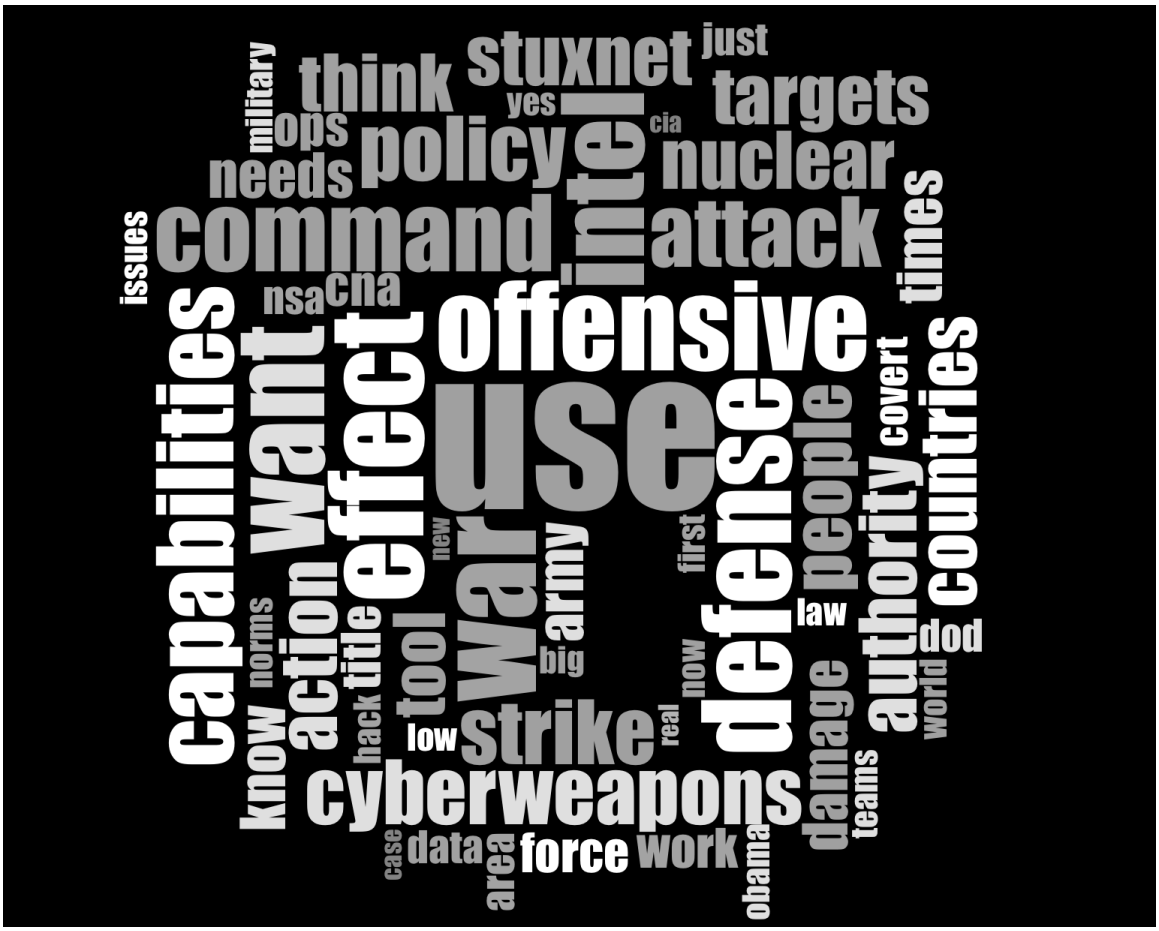
Figure 7.2 Treemap of Nodes



We can take a deeper look at the "Interesting Findings" node by utilizing a Word Frequency query. "A word frequency query catalogues the words used most often in the data or a subset of the data."[6] I visualized this via a Word Cloud diagram.

[6] Bazeley & Jackson, 249.

Figure 7.3 Word Cloud of Interesting Findings



In order to understand how often each category of interviewees spoke about these different themes, I used a Matrix Coding query which is useful for comparing content.[7] "In a matrix coding query, pairs of items are cross-tabulated and displayed as a matrix."[8] In Nvivo, you can click on each cell and see all of the coding references. I highlighted all the instances where the coding was greater than 1. The following table depicts the matrix coding for the government interviews. It indicates that "Interesting Findings" was the most coded theme followed by "Decision-making."

[7] Bazeley & Jackson, 251.

[8] Ibid., 250.

Table 7.1 Matrix Coding Query of Government Interviews

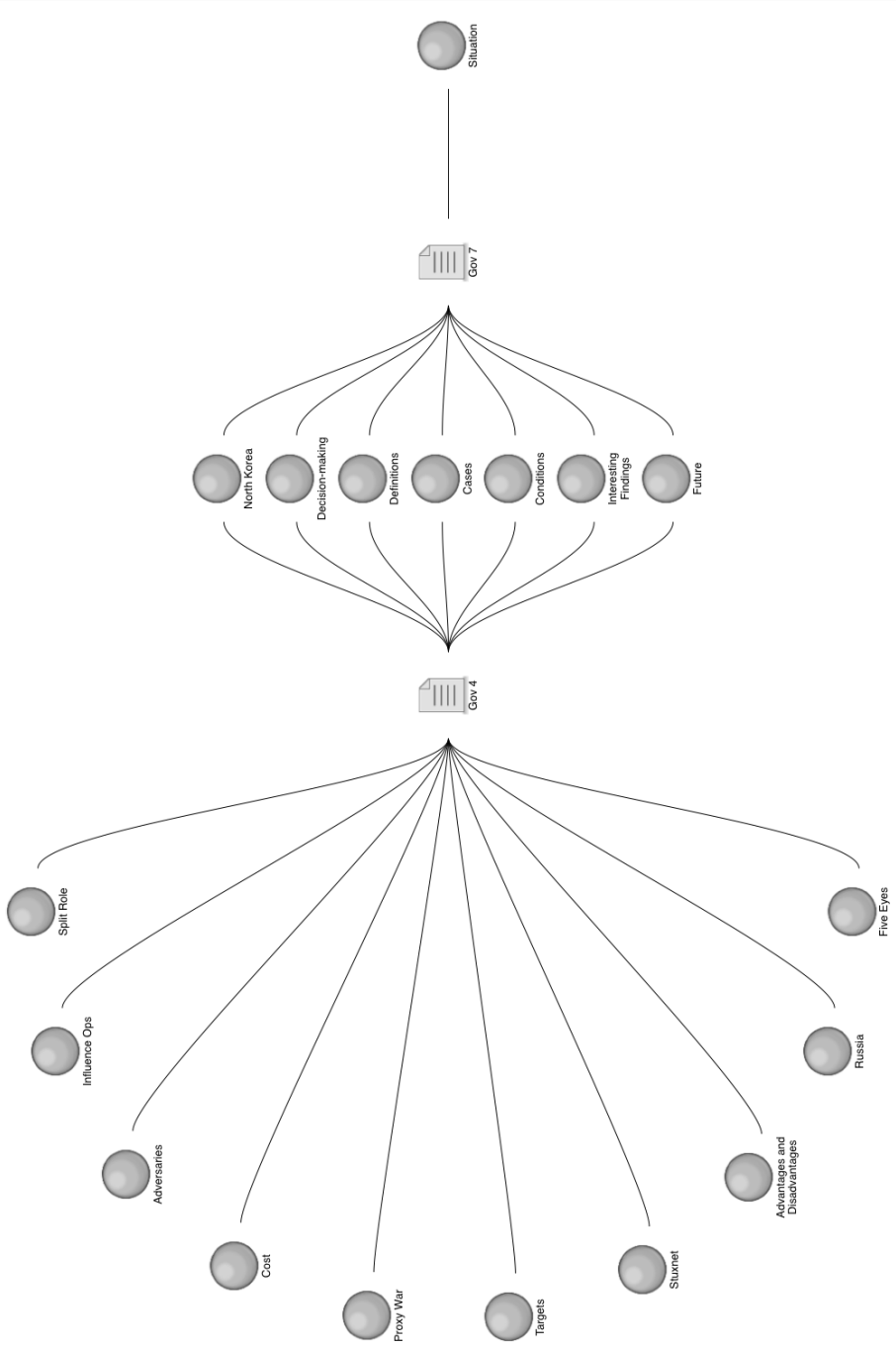
	A : Gov 1	B : Gov 2	C : Gov 3	D : Gov 4	E : Gov 5	F : Gov 6	G : Gov 7	H : Gov 8
1 : Advantages and Disadvantages	0	1	1	1	1	1	0	1
2 : Adversaries	0	1	0	1	**4**	0	0	0
3 : Cases	0	**2**	0	**2**	**2**	**3**	**2**	**3**
4 : Conditions	0	1	1	**3**	1	1	1	0
5 : Cost	0	1	1	**2**	1	0	0	1
6 : Decision-making	0	**3**	0	**3**	**3**	**4**	**2**	**3**
7 : Definitions	1	**2**	0	**2**	1	1	1	**2**
8 : Five Eyes	0	0	1	1	1	0	0	1
9 : Future	0	1	1	1	1	0	1	1
10 : Influence Ops	0	0	0	1	1	0	0	**2**
11 : Interesting Findings	**3**	**6**	1	**9**	**8**	**2**	**4**	**5**
12 : ISIS	0	1	0	0	0	0	0	**2**
13 : North Korea	1	1	0	**2**	**2**	**2**	1	0
14 : Proxy War	0	0	0	1	1	0	0	0
15 : Russia	0	**5**	0	**2**	**2**	1	0	1
16 : Situation	1	**0**	1	0	0	0	1	1
17 : Split Role	0	0	0	1	0	1	0	1
18 : Stuxnet	1	**2**	0	1	0	0	0	0
19 : Targets	1	1	0	1	0	0	0	1
20 : Trump	0	1	1	0	0	0	0	1

I also used a Comparison Diagram in order to explore the two former N.S.A. interviewees so that I could decipher shared commonalities.[9] The following visualization

[9] Nvivo for Mac, "About comparison diagrams," *QSR International*, accessed March 22, 2017, http://help-nv11mac.qsrinternational.com/desktop/concepts/About_comparison_diagrams.htm.

indicates that these two interviews had the “North Korea,” “Definitions,” “Cases,” “Conditions,” “Interesting Findings,” “Future” and “Decision-making” nodes in common.

Figure 7.4 Comparison Diagram of Former N.S.A. Interviewees



The following table depicts the matrix coding query for the cybersecurity interviews. It indicates that “Interesting Findings” was the most coded theme.

Table 7.2 Matrix Coding Query of Cybersecurity Interviews

	A : Security 1	B : Security 2	C : Security 3	D : Security 4	E : Security 5
1 : Advantages and Disadvantages	1	**2**	0	**3**	1
2 : Adversaries	**2**	**3**	**2**	**2**	1
3 : Cases	**2**	0	0	1	0
4 : Conditions	1	0	1	1	0
5 : Cost	**3**	**2**	1	1	0
6 : Decision-making	1	1	1	0	1
7 : Definitions	1	1	1	**3**	1
8 : Five Eyes	**2**	0	0	**2**	0
9 : Future	1	0	1	1	0
10 : Influence Ops	0	**2**	1	**3**	0
11 : Interesting Findings	**5**	**3**	1	**3**	1
12 : ISIS	1	1	0	1	0
13 : North Korea	**2**	1	0	1	0
14 : Proxy War	0	0	0	0	0
15 : Russia	1	**4**	1	**4**	0
16 : Situation	0	**2**	1	1	1
17 : Split Role	0	0	0	0	0
18 : Stuxnet	**3**	**2**	1	**4**	1
19 : Targets	1	1	0	**3**	0
20 : Trump	**2**	1	0	0	1

The following table depicts the matrix coding query for the media interviews. It indicates that “Stuxnet” was the most coded theme.

Table 7.3 Matrix Coding Query of Media Interviews

	A : Media 1	B : Media 2	C : Media 3
1 : Advantages and Disadvantages	0	0	1
2 : Adversaries	1	0	1
3 : Cases	**3**	1	0
4 : Conditions	0	**2**	1
5 : Cost	1	0	1

	A : Media 1	B : Media 2	C : Media 3
6 : Decision-making	0	1	**2**
7 : Definitions	1	0	1
8 : Five Eyes	1	0	1
9 : Future	1	0	1
10 : Influence Ops	0	0	0
11 : Interesting Findings	**4**	0	**4**
12 : ISIS	0	1	1
13 : North Korea	**3**	0	**2**
14 : Proxy War	0	0	1
15 : Russia	**4**	0	**2**
16 : Situation	0	0	1
17 : Split Role	0	0	0
18 : Stuxnet	0	1	**9**
19 : Targets	0	0	1
20 : Trump	1	0	**2**

The following table depicts the matrix coding query for the academic interviews. It indicates that “Interesting Findings” was the most coded theme.

Table 7.4 Matrix Coding Query of Academic Interviews

	A : Academic 1	B : Academic 2	C : Academic 3	D : Academic 4
1 : Advantages and Disadvantages	1	0	0	0
2 : Adversaries	0	1	0	0
3 : Cases	**2**	1	1	0
4 : Conditions	1	0	0	0
5 : Cost	1	1	0	0
6 : Decision-making	**5**	1	**2**	**4**
7 : Definitions	1	1	0	1
8 : Five Eyes	1	1	0	0
9 : Future	0	1	0	0
10 : Influence Ops	0	0	0	0
11 : Interesting Findings	**9**	**2**	**2**	**5**
12 : ISIS	0	0	0	1
13 : North Korea	0	0	**2**	0
14 : Proxy War	0	0	0	0
15 : Russia	**2**	1	1	0
16 : Situation	1	0	0	0
17 : Split Role	0	1	0	0

	A : Academic 1	B : Academic 2	C : Academic 3	D : Academic 4
18 : Stuxnet	**2**	**2**	0	0
19 : Targets	0	**3**	0	0
20 : Trump	1	0	0	0

Overall, these queries and visualizations were useful in understanding the most referenced interviews and topics. Now we will turn to each theme.

SEARCHING FOR DEFINITIONAL CONSENSUS

When I asked the question "What do you think is the best definition of a *cyberweapon*?," a few of the journalists and government officials I spoke with liked the term "cyberweapon" whereas many of the academics and cybersecurity officials I spoke with expressed that they hated this term because they found it ambiguous. Some definitions interviewees offered include "malware that is physically destructive or significantly interferes with the system." A journalist defined a cyberweapon as the "use of malware to accomplish a result you previously could not do by physical attack." A former T.A.O. employee defined a cyberweapon as a "tool that can be used to conduct a cyber effect." A cybersecurity official told me "I leave the definition to policymakers" but he defined a cyberweapon as "a piece of malicious code that gained unauthorized intrusion." He said once it passes the intrusion bar, it counts. "Whether it is a cyberweapon or not makes zero difference to our purposes but that matters to others because it is about declaring war– I was attacked by a weapon."

Some of the other interviewees I spoke with had an issue with the weapon classification, arguing that a weapon kills or destroys. This was a squabble discussed in the Literature Review. A couple of interviewees expressed they do not like the use of the term

"cyber" anything. A Legal Advisor I spoke with said he uses the term cyberweapon colloquially. "It is not in the taxonomy of NATO," he stated. They use "offensive cyber capability." He explained they do not talk about offense unless they are talking about the theory of an attack. So they talk more about cyber defense because only two, maybe three, out of 28 NATO countries have cyber capabilities, he said. "You are an idiot if you do not know the U.S. has a massive cyber arsenal which is anathema to 25/26 nations," he pronounced.

One journalist said she uses the term "digital weapon" because "cyber" is overused. This journalist defined a digital weapon as a means to delivering a weapon that causes some kind of destruction. She also said wiping out data is destruction so that would classify as a cyberweapon, or in her terms, a digital weapon. Hence, some of the interviewees argued that this is really a question of "what counts below the use of force threshold?" When you read media reports, it seems as if everything is an attack because "a cyberattack is subjective," said one academic.

A former T.A.O. employee I spoke with said what we are talking about here is "software that was weaponized." He described North Korea's attack on Sony and Stuxnet as examples of cyberweapons and described any supposed Russian efforts as "bull****." However, while he does not use the term cyberweapon, he thinks it is a good term. An Army reservist also said that the term cyberweapon is applicable; however, he said there is no reason to say we have cyberweapons because the military does not develop a weapon unless there is a mission space. So there is no reason not to say the same for the cyber realm, he explained. This is an interesting point which I will revisit in later sections. One academic said he did not like the term cyberweapon because you cannot count

cyberweapons. Thus, he found this term useless. I disagree with this claim though, because in my view, quantity should not determine whether it is in fact a weapon.

I also spoke with a colonel who once worked for U.S. Cyber Command. He explained that in 2010, the Department of Defense (DoD) liked the term Computer Network Operations, which was classified at the time. Then the DoD came up with Computer Network Defense, Computer Network Attack and Computer Network Exploitation, which is the gathering of information (often conducted by the intelligence community). This explanation lines up with the discussion in Chapter 1. He conveyed that these operations are often similar and the only difference is intent. If you corrupt the information or have an effect on it, then that is a Computer Network Attack, he explained. Computer Network Attack includes Offensive Cyber Operations and Defensive Cyber Operations. He said he found it interesting that Computer Network Exploitation disappeared from this definition. A cybersecurity official I spoke with told me that all of this falls under Computer Network Attack because the end result is the same. He explained that a Computer Network Attack is sabotage and if you can take a country offline, that is a cyberweapon.

Some interviewees did not like the term cyberweapon because of its conflation with espionage. Additionally, a couple of interviewees communicated that they do not use the term cyberweapon because they do not know what it means. One current government official complained that cyberweapon is a messy term like "cyberterrorism." He also rejected any notion that the U.S. is engaged in cyberwarfare because of espionage since every country conducts espionage, he said. So he asked, "Who are we at war with?"

Several former government officials confirmed that "capabilities" is the terminology used by the defense community. Indeed, "capability" was the term used throughout *Joint Publication 3-12 (R) Cyberspace Operations*. According to one former government official, it is always called a capability. "Cyberweapon" is not used by the Department of Defense, declared a former Senior Cyber Policy Advisor. A cybersecurity official who is a former government employee said, we could say Stuxnet was a cyberweapon but most of what we have seen do not qualify as weapons. It is a "capability," "tool" or "suite of tools," he stated. An academic said capabilities means the potential to weaponize. An attack is based on impact and a weapon is based on means, he explained. A former R.O.C. employee stated, 99% of offensive action is Computer Network Exploitation so it is all about access. He illustrated that if you want to attack the power grid of country X, you have to go through content management system servers. So you do not have to develop a capability, he said. You can just shut something off. He articulated that most of the time you can do this via tools, exploits or implants. Tools perform actions or disrupt and destroy data. Exploits gain access and implants leave behind sustained access. A Senior Cyber Policy Advisor I spoke with further clarified that the weapons for cyber operations are: "platform, access, and payload." "You need all three." A former T.A.O. employee said an effective cyberattack is covert, has real-world measurable effects and results in someone experiencing pain.

There was at least one interviewee in each category that pointed to Stuxnet as the proof-of-concept for the type of destruction that a cyberweapon inflicts. However, one academic who says he is a practitioner encouraged me to be careful asking if I am talking about a weapon, am I controlling for primary and secondary effects? He said militants, as

in the ISIS or Iraq (2007) cases, were secondary compared to Stuxnet. I did not control for primary and secondary effects. To me, an effect is an effect. Additionally, when Owens, Dam, and Lin talked about direct and indirect effects of cyberweapons, they claimed that indirect effects "are often the primary goal of a cyberattack."[10]

I. Legality

Since there were differing opinions about whether these attacks were cyberweapons, there were also differing opinions about how to carry out these attacks. A former Remote Operations Center employee explained that there are three ways in which offensive action occurs according to U.S. Code: [11]

- Title 10- military action
- Title 50- covert action under the C.I.A.
- Title 18- offensive action under law enforcement (such as the F.B.I.) to protect against immediate (often criminal) attack.

During the interviews, many academics, government and cybersecurity specialists pointed out the ambiguity between Title 10 and Title 50 in U.S. Code. "The Title 10-Title 50 debate is essentially a debate about the proper roles and missions of U.S. military forces and intelligence agencies."[12] The breakdown is as follows:

---

[10] William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, D.C.: The National Academy of Sciences, 2009), 112-113, accessed March 7, 2017, http://www3.nd.edu/~cpence/eewt/Owens2009.pdf.

[11] Applicable U.S. codes were discussed in *Joint Publication 3-12 (R) Cyberspace Operations*, (Department of Defense, February 5, 2013), III-3, accessed March 15, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[12] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3 (2011): 87, accessed March 18, 2017, http://www.soc.mil/528th/PDFs/Title10Title50.pdf.

> Unconventional[13] and cyber warfare, are conducted by SOF [Special Operations Forces] and U.S. Cyber Command, respectively. Neither special operations nor U.S. Cyber Command are elements of the Intelligence Community, so if an unconventional or cyber warfare activity is conducted pursuant to tasking from the Secretary of Defense, then there can be little question it is a military operation. Military operations authorized and funded under Title 10 authorities are properly labeled military operations subject to the exclusive oversight of the armed services committees, even if those activities are related to intelligence gathering—so long as they are in response to tasking from the Secretary of Defense and remain under military direction and control. Yet Title 50 includes one provision that would place even military operations meeting these criteria under the jurisdiction of the intelligence committees: the intelligence committees retain jurisdiction over all covert action.[14]

Confused yet? One practitioner said, the U.S. should be "upfront" and do this as warfare under Title 10. A former Remote Operations Center employee said, so far, the only ones to conduct actions are the N.S.A. under Title 10 authority. At the time, Cyber Command was not effective or fast enough to protect systems because they were ill-equipped to do this, he explained. So this really is an authority question and thus, my dissertation is "cutting to the heart of this," because "the N.S.A. has the capability but no authority."

A former Cyber Command person I spoke with told me that a Computer Network Attack is "a point of contention between the intelligence community and the war-fighting community." The N.S.A. conducts surveillance centered on intelligence capabilities and the C.I.A. conducts covert cyber operations, he said. So the "intel gain/loss" [15] calculus is

---

[13] According to the U.S. Department of Defense, unconventional warfare is "Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area." *DOD Dictionary of Military and Associated Terms*, s.v. "unconventional warfare," March 2017, 243, accessed April 1, 2017, http://www.dtic.mil/doctrine/dod_dictionary/.

[14] Wall, 126.

a deliberation between burning assets (sources and methods), he explained. The intelligence community leans on monitoring but the war-fighting community wants to break things, he clarified. Thus, another cybersecurity official said, it is a "tug-of-war" between the intelligence community who likes low, slow and quiet versus the military who likes impactful and loud. Additionally, no other domain depends so heavily on intelligence capabilities. For example, if you want to position an aircraft carrier, you do not need to execute an exploit, he explained. This is a unique challenge to cyberspace. A cybersecurity official said, there is a distinction between enabling access versus disruption and that distinction is dictated based on national security priorities.

Another point of contention is the autonomous vs. remote operator consideration. One cybersecurity official pointed out that Stuxnet did not need outside commands but then it was uncontrollable once it was released into the wild. However, the dependence on a human operator implies that someone is issuing a directive. Or in other words, the operator needs authority to issue a destructive command. Thus, some interviewees questioned where this legality is coming from. According to the documentary, *Zero Days,* lawyers were involved in the Stuxnet operation. (This was also mentioned by a journalist I interviewed.) In the documentary, the N.S.A. representative said, "For Natanz [Stuxnet], it was a C.I.A.-led operation so we had to have agency signoff. Someone from the agency stood behind the operator and the analyst and gave the order to launch every attack."[16]

---

[15] "An Intelligence Gain/Loss assessment is required prior to executing a CO [cyberspace operation] to the maximum extent practicable." *Joint Publication 3-12 (R) Cyberspace Operations*, II-9.

[16] *Zero Days*, Amazon Video, (2016; Magnolia Pictures, 2017), accessed February 6, 2017, https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2EKYTC.

Another challenge is that when moving this tool across the Internet, it has to pass through other countries. Thus, a Legal Advisor said, when the C.I.A. and N.S.A. do these covert operations, it is a conceivable violation of international law. (He also explained that the legal authorization for a cyberattack falls under Chapter VII of the U.N. Charter.) A cybersecurity official explained that with a strike, you have to get permission to fly over the airspace but here is the "gray space of the internet." Hence, another cybersecurity official stated, President Obama loved covert operations that were "lightweight" and where the U.S. was "in and out."

For some of these reasons, the Legal Advisor professed that he does not use the term "cyberwar." He said either we were attacked or we were not attacked. So to call it a cyberwar is meaningless. "We do not contemplate the existence of cyberwar," he declared. He explained that Article 5 of NATO is triggered in response to an armed attack but "war" does not appear in the NATO treaty. Furthermore, there are no judicial procedures about the use of offensive cyberweapons in court, he explained. So this is almost in essence a political question, he said. Cyber is too new for a ruling on the offensive use of cyberweapons so they accede to government guidelines for their usage, he stated. A current government official told me that his office is advancing a framework that says international law (so the U.N. Charter and the Law of Armed Conflict) applies in cyberspace. (According to *Joint Publication 3-12 (R) Cyberspace Operations*, the law of war must be upheld during armed conflicts.)[17] This means that distinction, proportionality and legal constraints all matter. In Chapter 2, I discussed the Tallinn Manual, but this interviewee said governments do not endorse it. The manual is academic, he said. Nevertheless, he has been able to get

[17] *Joint Publication 3-12 (R) Cyberspace Operations*, III-10.

some countries to affirm that legality applies in the cyber realm. Some of the norms that he has been promoting are:

1. Do not attack critical infrastructure absent in peacetime.
2. Do not attack CERTs (Community Emergency Response Teams) because then you are essentially going after ambulances.

He stated that norms are voluntary akin to the Treaty on the Non-Proliferation of Nuclear Weapons, so if a country violates it, they can be sanctioned. Thus, there is accountability, he said. While the U.S. is more transparent about their offensive cyber capabilities, there are doctrines of restraint, he said. “People think we engage in cyber activities,” he said, “but look at the objective.” “Whether it is cyber or not cyber, it is not a specialty,” he explained.

In summary, there were some mixed feelings about the term cyberweapon. In all of the interview categories there were people who either opposed or supported the term. Overall, I think almost no one said they used this term in their line of work. This is interesting because I have used this term in this dissertation. Additionally, this section also highlighted the lack of consensus surrounding the legal justification for using these capabilities. The legal obscurity is due in part to the intent and target of the operation. The next section looks at the countries that are on the receiving end of these weapons.

ADVERSARIES

In order to get a better idea as to who the U.S. is likely to use these weapons against, I asked the interviewees “Can you think of one or more countries (or perceived adversaries) that the U.S. might use a cyberweapon against as a first strike?” PERCEIVED

ADVERSARY was one of the variables tested in Chapter 5. Many of the people I spoke with confirmed that Russia, China, Iran and North Korea were the U.S.' main adversaries in the cyber arena.

One of the 22 interviewees was a former Senior Cyber Policy Advisor for the government. He explicated that his office executed civilian oversight over U.S. Cyber Command and any organization that had a cyber role. He coordinated cyberwarfare policy and focused on "classic" national security issues such as deterrence policy. He also worked on "classified operations with an architecture for cyber operations." He said he coordinated the department's strategy versus one major non-adversary. I did not ask him who the non-adversary was but this is fascinating because it challenges my first hypothesis– "*The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary."* A cybersecurity official advanced a parallel claim that the U.S. is attacking everyone. Even allies can be attacked, he suggested.

A cybersecurity official proposed that the next breed of cyber players is likely to be the Middle Eastern or Gulf countries because if they cannot develop a nuclear weapon, they can develop a cyber capability. A journalist included Israel, France and the U.K. (through their collaboration with the U.S.) on the list of top offensive cyber players. She clarified that Iran is a small player and anyone else is far behind.

There was disagreement as to who poses the biggest cyber threat to the U.S. Some interviewees maintained that a decline in Chinese attacks against the U.S. was due to several meetings between President Obama and President Xi in 2015. These resulted in the adoption of a United Nations accord to the effect that critical infrastructure is off-limits during peacetime (fortifying the norms discussion earlier) and that the U.S. and China

would not "engage in state-sponsored cyber intrusions to poach intellectual property, and that they would together seek 'international rules of the road for appropriate conduct in cyberspace.'"[18] Some attributed this "success" to diplomacy but one cybersecurity official said China was supposedly about to reorganize their cyber operations. An N.S.A. advisor I spoke with disagreed that there are fewer attacks coming from China. Additionally, a cybersecurity official said Russia is sophisticated but long-term China holds far more cards so China is the U.S.' biggest adversary in the cyber arena. Another cybersecurity official also said long-term, China is the more important player.

Other interviewees proclaimed that Russia was the U.S.' biggest adversary in cyberspace. A cybersecurity official declared, "if it is geopolitical, it is Russia." Another cybersecurity specialist said that the Russians are the most capable and stealthy and the U.S. government is not interested in striking back like President Obama did in regards to the Chinese' intellectual property theft. He added, "The U.S. has a lot to learn about how an information operation works." He said, "Russia has learned a lot because they are trying their tactics elsewhere." Another cybersecurity official said right now, it is a covert chess game with Russia. (COVERT was one of the variables tested in Chapter 5.) He believed this was an example of hybrid warfare, where there is a conflict but not a full-scale conflict. I discussed this notion of proxy warfare with the interviewees.

I. Proxy Warfare

I asked the interviewees "Do you think a cyberweapon might be particularly useful as a tool for initiating, sustaining or ending a proxy war?" An academic I spoke with quoted

[18] Julie Hirschfeld and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *The New York Times,* September 25, 2015, accessed March 10, 2017, https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

Kenneth Waltz, "mutual fear of big weapons may produce, instead of peace, a spate of smaller wars"[19] suggesting that cyberweapons may result in smaller wars. A government official stated, it is clear that countries should not engage in proxy warfare. He said the U.S. does not engage in proxy warfare because we work with allies differently so we cannot escape the legal parameters. A journalist said these tools can be used when you want to avoid an all-out war, echoing the cybersecurity official's point above. In fact, a former T.A.O. official stated, this was a condition for using these weapons in a first strike since these weapons are mainly to prevent war although he acknowledged that proxy war is still war. However, a prominent think tank member disagreed, claiming this is "proxy conflict" not war. He said the U.S. is unlikely to do what Russia did in Crimea or to do an Iran-Contra situation since the U.S. has tight control of their cyberweapons. One journalist disagreed, arguing "the U.S. struts around as if they are in full control but other players are the wild card."

One interviewee proposed that the U.S. is likely to use these capabilities against a "rogue nation engaging in imminent dangerous behavior." A journalist said these capabilities are useful for "any place with illicit nuclear activity." She pointed out North Korea as an example although, she said it is harder to have an effect in North Korea since they are less open. Many other interviewees also repeated this thought claiming that a highly-networked country makes a big difference. I will revisit this argument later in this chapter. A former T.A.O. employee also claimed that the U.S. uses offensive cyber operations against weapons of mass destruction and "nasty people." Although, if I recall correctly, I think he said the N.S.A. would qualify this as Computer Network Defense since

[19] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 1959), 236.

they are protecting the U.S. government. (A R.O.C. employee clarified that if someone attacks us, while this is an offensive act, it is an emergency act so that is the difference between "active defense" and an offensive action.)

One journalist that I interviewed was David Sanger of *The New York Times*. He is the only interviewee I will name in this dissertation (my committee has seen the full list) and this is the only instance where I will specifically identify him. He said there are deep political motives to use offensive cyberweapons against Iran and North Korea but not in Russia and China. "Would the U.S. want to take out Chinese and Russian nuclear facilities?," he asked. "No," he said. "Iran and North Korea are a different story." A former government official also concurred that Iran and North Korea are a different calculus. I interviewed Mr. Sanger in January. In March, he and a colleague wrote an article about President Obama's secret covert cyber war against North Korea's nuclear program.[20] So thus far, one of the overarching findings emerging from the interviews is that these weapons will be used covertly against nuclear programs of adversaries.[21] Another journalist also mentioned that cyberweapons can be targeted against chemical weapons and weapons systems that pose a threat to the world. Therefore, perhaps my second hypothesis

[20] David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *The New York Times,* March 4, 2017, accessed March 5, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

[21] In "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," Austin Long cited a news article that said a Chinse defector shared Chinese nuclear information with the U.S. so Long says the U.S. could possibly develop an offensive cyber operation against Chinese nuclear facilities although this is impractical given the high possibility of retaliation. Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," *SRRN*, (June 15, 2016): 16, accessed March 25, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836204.

is plausible: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests.*

SITUATION

In order to further understand what is a viable threat, I asked the interviewees, "Can you think of a situation in which the U.S. might use a cyberweapon as a first strike?" THREAT was a variable tested in the Decision Matrixes chapter. Some interviewees suggested that if the U.S. were to act offensively it would be because of "some dramatic incident in foreign theater" or as mentioned earlier, a "rogue nation engaging in imminent or dangerous behavior." One interviewee suggested an example of such an incident would be "Russia seizing a bigger part of Ukraine." Some academics and former government officials claimed they could see these weapons being used during a conflict over the South China Sea or Taiwan. One cybersecurity official thought these weapons might be used for tactical purposes if there was a war in the Middle East. He gave the example of Israel's Operation Orchard (which was discussed in earlier chapters.)

Other interviewees spoke about a whole sphere of psychological operations. For example, there are a number of cyber operations that do not destroy physical infrastructure such as changing the shipping of bullets or production orders for the military so these materials are redirected elsewhere. A former R.O.C. employee suggested the U.S. might use these capabilities as a first strike in order to support a military or strategic operation or even as direct action.[22] He said this is a good idea in order to "prep the battlefield" where

[22] According to the Department of Defense, "direct action entails short-duration strikes and other small-scale offensive actions conducted with specialized military capabilities to seize destroy, capture, exploit, recover, or damage designated targets in hostile, denied, or diplomatically and/or politically sensitive environments." *Joint Publication 3-05 Special*

before troops moved in, there is a suppression of military infrastructure. The DoD term for this is "operational preparation of the environment."[23] However, in 2010, there was a document that attempted to develop "a standard joint cyber operations lexicon." This document defined a "Cyber Operational Preparation of the Environment."[24] The interesting part of this definition is a bolded statement that says "Replaces: CNE or CNA when used specifically as an enabling function for another military operation."[25] This document had more information than the 2013 *Joint Publication 3-12 (R) Cyberspace Operations* which had a section about "Cyberspace Operational Preparation of the Environment" but it did not provide many details.

This former R.O.C. employee suggested that a cyber capability could take out another country's air forces without physically taking them out. One academic conveyed a similar thought that the U.S. can do this in order to take out another country's command-and-control.[26] One journalist explained via email,

---

Operations, (Department of Defense, July 16, 2014), x, accessed March 15, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf.

[23] "OPE consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations." *Joint Publication 3-12 (R) Cyberspace Operations*, II-5.

[24] "C-OPE includes but is not limited to identifying data, system/network configurations, or physical structures connected to or associated with the network or system (to include software, ports, and assigned network address ranges or other identifiers) for the purposes of determining system vulnerabilities; and actions taken to assure future access and/or control of the system, network, or data during anticipated hostilities." James E. Cartwright, *Joint Terminology for Cyberspace Operations*, (Washington D.C.: Department of Defense, 2010), 7, accessed March 18, 2017, http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[25] *Joint Terminology for Cyberspace Operations*, 7.

[26] Some of these ideas were discussed by Owens, Dam, and Lin on page 179.

> I think the US government would be very reluctant to use a cyber weapon that has the impact of something like Stuxnet — destroying uranium centrifuges —on a first strike basis unless there is a significant strategic benefit. In this case, the Obama administration decided there was. But I think such operations remain very rare. When it comes to more tactical effects, as on the battlefield in Iraq and Afghanistan, the military has deployed cyber weapons or tools to jam IEDs, and confuse the enemy by sending cell phone messages that led them right into an ambush.

However, according to one academic, "when the U.S. uses these capabilities, it becomes non-cyber factors." He explained "If there was a China incident, then regional experts would analyze that" so there is no generalizable answer as to a situation in which these capabilities would be used. It is case by case, he said. This statement echoes the assertions made by a former Senior Cyber Policy Advisor that will be discussed later.

One cybersecurity official said for a government, the target has to be a level of criticality. Another cybersecurity official who used to work for the government explained that the "lifelines" or critical infrastructure of a country are "energy, water, telecommunications, emergency services, financial services and information technology." (MILITARY SECTOR was a variable tested in Chapter 5.) He stated, attacks against these would be a nation-state level attack but again, this is subjective. This is a problem in the cyber realm because the targets are largely unknown whereas in the real world, if a hospital was bombed, you would know.

In summary, this section indicated that the situations in which the U.S. will be likely to use a cyberweapon might have to do with a conflict over the South China Sea or a dramatic and dangerous event in the international arena. These answers may seem vague because some interviewees argued that the situations under which the U.S. uses these weapons should not be generalizable. One interesting finding was in regards to using a

cyber capability to prepare the battlefield, which in 2010, may have replaced Computer Network Attack but was still lumped under cyberwarfare.[27]

CONDITIONS

So far we have assessed what are cyberweapons, who are the adversaries, when will they be used and what are the targets. Now we turn to why and how these weapons will be used. Since this dissertation focused upon the key question of the conditions under which the United States would be likely to use a cyberweapon in a first strike, I asked the interviewees "Can you think of any conditions under which the U.S. might use a cyberweapon as a first strike?" As mentioned above, many interviewees talked about the strategic and tactical benefits of these weapons, reinforcing Libicki's arguments discussed in earlier chapters. A former Cyber Command official stated there are three different levels of a cyberweapon– tactical battlefield, operational level and national level.[28] The following conditions fall under these different levels.

I. Access

One tactical condition for using a cyberweapon is that these capabilities are useful in places where you do not have access, said some interviewees. ACCESS was a variable tested in the Decision Matrixes chapter. One former R.O.C. employee echoed this thought stating that a cyberweapon can have an impact on bothersome targets where the U.S. does not have a physical chance to attack. Thus, these thoughts suggest that my fourth hypothesis might be plausible– *The U.S. will likely deploy a cyberweapon in a first strike*

---

[27] *Joint Terminology for Cyberspace Operations*, 8.

[28] A similar thought was discussed in *Joint Publication 3-12 (R) Cyberspace Operations*, II-10.

against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.

II. Collateral Damage

A condition many interviewees discussed was collateral damage. This was an argument that I addressed in the Literature Review where I said collateral damage includes retaliation, norms or civilian casualties. COLLATERAL DAMAGE was a variable tested in both the Quantitative Analysis and Decision Matrix chapters.

One cybersecurity official expressed "I am not surprised that the U.S. has taps on all major networks" because "other countries do the same." "What is interesting is that countries are willing to accept the collateral damage." "I would be surprised if the U.S. decided to take out a whole country and target everyone" (so if the cyberweapon was deployed 100%) but, the U.S.' goal is to minimize civilian casualties, he stated. A Legal Advisor I spoke with shared if for example, an "adversary puts their command-and-control in a densely populated area, kinetic weapons would cause a loss of life so cyberweapons would be good here." He added, "If political conditions are such that these weapons can result in zero civilian casualties, then yes" they will be used. A Senior Cyber Policy Advisor I spoke with proposed that cyber capabilities should be used as a "humane alternative." A former T.A.O. employee disclosed that he is a proponent of using these capabilities because these tools can save lives on both sides of the conflict. This was Dorothy Denning's argument noted in the Literature Review. A journalist I interviewed also shared similar beliefs stating you can achieve your goals without a long-drawn out process. "So from an international relations perspective, it presents a real option to achieve aims." Thus, these findings suggest that my 5th hypothesis might be plausible– *The U.S.*

will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize casualties.

III. Retaliation

Interrelated with collateral damage is the concern over retaliation. One cybersecurity specialist explained "In the past, there was great hesitance to use offensive capabilities because of retaliation." An "eye for eye is dangerous," he said. Additionally, he quoted the Director of National Intelligence, James Clapper, who when testifying about Russia's role in the 2016 U.S. presidential election expressed he was "a bit reticent about people who live in glass houses shouldn't throw publicly too many rocks."[29]

One cybersecurity specialist said, "In cyber, you can conduct an attack and achieve goals with relatively little attribution and there is this line where you could signal but you do not want to trigger retaliation." "The bar is higher for retaliation," he explained. During the interview, we also discussed the Shadow Brokers and he alleged this "was Russia signaling that hey if you retaliate, we will unleash this." Owens, Dam and Lin said sending signals are "more problematic when cyberattacks are involved."[30]

A former government official told me that the U.S. would not attack unprovoked. "It has to be a 9/11 event or higher," he clarified, and "it has to be against an adversary." However, another cybersecurity official said the U.S. is inclined to retaliate against smaller countries.[31] If the U.S. is attacked, many of the interviewees I spoke with stated, "a cyber response is not necessarily the best response" claiming the "right reaction to a cyberattack

---

[29] James Clapper, "Russia's Hacking of U.S. Elections," *C-SPAN* (video), January 5, 2017, accessed March 12, 2017, https://www.c-span.org/video/?c4641807/living-nsa-glass-house.

[30] Owens, Dam and Lin, 308.

[31] Owens, Dam and Lin shared a similar thought on page 309.

is a non-cyber response." One government official said, "If we get hit with cyber we do not have to respond with cyber." "There are other means outside of the cyber domain," said a cybersecurity official. "You just have to look at what is most effective." Another cybersecurity specialist said, "There is no playbook for a response situation" because "you do not want an adversary setting the parameters for the kind of targets." A Senior Cyber Policy Advisor agreed expressing "one thing we pushed back on was the notion that we need to set red lines to respond to any specific cyberattack." He disclosed "these are all political determinations made by political leadership." "There is no if this happens then we will do that," he professed. "We never want there to be." "We want to preserve flexibility." It "does no good to generalize," he avowed. We "always want to look at this situation by situation." This was a key finding in this dissertation since I incorrectly presumed I could generalize to some extent.

In order to further understand the conditions behind deploying a cyberweapon, I asked the interviewees "What are the advantages of using a cyberweapon rather than U.S. troops, special forces, drones or airstrikes? Disadvantages?" Their responses were similar to many of the conditions discussed in earlier chapters.

IV. Reversibility

One advantage of using these weapons is the potential for reversibility. A Senior Cyber Policy Advisor said if we want to knock out air defenses, then we can use cyber tools instead of bombs because of the diminished collateral damage a cyberweapon produces. So he does not view these weapons as a last resort but rather they "should be closer to a first resort" since it is often reversible.[32] He claims this is as simple as loading

[32] Owens, Lin and Dam suggested these capabilities could be used at the beginning of a conflict. Owens, Dam and Lin, 309.

a backup drive. The localized effects are not permanent, he explained. So this should be viewed as being closer to electronic warfare, he said. For instance, if you want to strike a jet in Syria, you can use electronic warfare to suppress the systems, he said. A former R.O.C. employee I spoke with shared similar views. An Army reservist also echoed this arguing it "could have been awesome to use cyber keystrokes in Iraq to damage some of the infrastructure that was blown up by bombs that the U.S. now has to rebuild."[33] He also suggested these capabilities might have been useful for taking out the lights in the recent failed counterterrorism raid in Yemen that resulted in the deaths of one American commando and Yemeni civilians.[34] However, when Owens, Dam, and Lin discussed indirect effects, they said they "are generally not reversible."[35]

V. Reliability

A possible disadvantage of using these capabilities is reliability. First of all, there is the autonomous vs. remote operator consideration where you are not 100% sure how the cyberweapon will work on its own and if you are depending on a human operator, there are also risks. Although, one cybersecurity official pointed out that it can be beneficial to be able to modify these capabilities, and more attractive than an aircraft carrier, which you cannot upgrade.

Another interviewee said there are "problems with guaranteeing effects" as compared to using a laser-guided bomb or missile where you know what the impact is.

---

[33] Owens, Dam and Lin made a similar argument on page 225.

[34] Eric Schmitt and David E. Sanger, "Raid in Yemen: Risky from the Start and Costly in the End," *The New York Times,* February 1, 2017, accessed March 1, 2017, https://www.nytimes.com/2017/02/01/world/middleeast/donald-trump-yemen-commando-raid-questions.html.

[35] Owens, Dam, and Lin, 112 – 113.

Thus, this "might dampen commanders' capabilities." Another interviewee stated since cyber is a one-hit wonder, it "might not keep up the pressure." A former T.A.O. employee I spoke with shared a similar thought claiming a disadvantage is that you have to attack for a long time in order to deploy effectively. Furthermore, an academic said that if you can re-use the tool, it may not be as great the second time around so in some respects "cyber is a wasting aspect." (A government official also said the second-order effects of cyber are harder.[36]) This academic claimed there are only so many exploits so do you want to show your hand? This is a "problem of capability revelation," he stated.[37] Therefore, a former Cyber Command official said in many ways, cyber capabilities are harder because this is probabilistic. For example, you think you could turn out the lights but what if someone patches right before?, he questioned. "Warfighters do not like uncertainty." One cybersecurity official shared a similar viewpoint– "capabilities in cyberspace are perishable" because "all people have to do is release a software patch" and if they do, that "million-dollar cyber tool is now worthless." A government official added, "Countries are constrained because of uncertainty."[38]

VI. Attribution

Another disadvantage of deploying a cyberweapon is that you may only get one shot if this is attributable. In the cyber realm, the prevailing thinking is that a state can direct an attack and achieve its goals with relatively little attribution. Some interviewees said you do not want to trigger retaliation.

---

[36] *Joint Publication 3-12 (R) Cyberspace Operations*, also mentioned this on page II-10.

[37] *Joint Publication 3-12 (R) Cyberspace Operations*, also mentioned this on page I-7.

[38] Owens, Lin and Dam discussed uncertainty on page 227.

Another problem with attribution is that you can frame someone else. This is the false flag argument discussed earlier. Furthermore, it is not too difficult to lead people astray since in the cyber realm, you also have proxies that wage warfare. Therefore, many interviewees urged "we need to set a high bar for attribution" because "We are setting an example when we attribute cyberattacks to North Korea and Russia."

Of course, if you are at war, then you probably do not care about people knowing about this capability and actually want to flex your muscles, said one interviewee. Although, a cybersecurity official I spoke with stated, "random malware is preferable because of plausible deniability." (Plausibility deniability was discussed in earlier chapters.) Thus, he said he did "not see why anyone would want to give up plausible deniability because people can take the code and replicate it." Therefore, he said he "could see more stuff attributed to the U.S."

VII. Cost

Cost is both an advantage and a disadvantage. Interviewees across the spectrum said these weapons are cheaper. One journalist said the Russian cyberattack on the D.N.C. cost hundreds of thousands to execute whereas another interviewee said these weapons cost hundreds of millions. However, this pales in comparison to the four or five billion that an aircraft carrier costs, said one cybersecurity official. Regardless, "the cost of the attack does not indicate the damage," explained one journalist.

One disadvantage that a few interviewees spoke about was the familiar argument that once a cyber capability is used, it is burned. Another disadvantage is the "process to request a battlefield effect and time were not aligned." One government official said a complication is that cyber tools take pre-planning so you have to look at the immediacy of

the operation. A cybersecurity official told me that a cyberweapon takes about four months from order to build. Another cybersecurity official simply said the delivery takes a long time. In other words, it takes time to create a "tailored capability." (However, one cybersecurity official claimed moving this capability is faster than moving a carrier.) An Army reservist I spoke with said, "Stuxnet was not done in one day" so "what are the acceptable areas of mission space and lead time?" There is no "consistent timeframe," he said. This can impact the likelihood of deployment.

In summary, this section demonstrated that access, collateral damage, retaliation, reversibility, reliability, attribution and cost were the considerations involved in deploying a cyberweapon. Now that we have discussed the conditions for deployment, we will focus on real cases to see if in fact, these were the actual considerations.

CASES

Discussing the targets, situations and conditions under which practitioners in this field think the U.S. will likely deploy a cyberweapon is a hypothetical approach. So in order to bring in an empirical perspective, I also spoke to the interviewees about the 13 perceived cyberweapons that were the case studies of this dissertation. Well, I tried to speak to the interviewees about these cases but as expected, not many people were very chatty about all of these cyberweapons. First, I asked the interviewees whether the U.S. has actually used cyberweapons and one person said yes, two times. A current advisor for the N.S.A. said I think we have. "It is already public," he stated. Other interviewees claimed the U.S. is using cyber tools every day but a couple of interviewees pushed back against this notion, raising the earlier point about whether these cases were weapons.

Next, I asked the interviewees about each case. The consensus appeared to be that Stuxnet, Libya, Syria and Pakistan were cyberweapons but Quantum and Turbine were not cyberweapons. Not many people knew about Quantum or Turbine so they did not really address these cases in depth. Many people I spoke with deemed Shotgiant to be Computer Network Exploitation or espionage. One former T.A.O. employee asked, "What the hell is Shotgiant?" and after I explained, he assured that Shotgiant was not a cyberweapon. A R.O.C. employee said, "let's not talk about those specifically" in regards to Shotgiant, Quantum and Turbine.

In *Zero Days,* the T.A.O. representative explained "inside T.A.O. headquarters is the R.O.C. (Remote Operations Center.)" "If the U.S. government wants to get in somewhere, it goes to the R.O.C." She said they "could only do about 30% of missions" "through the web but also by hijacking shipments of parts." She added "sometimes the C.I.A. would assist in putting implants in machines. So once inside a target network, we could just watch or we could attack."[39] This statement confirms that the U.S. engages in interdiction and has the potential to attack. Therefore, Shotgiant, Quantum and Turbine could be cyberweapons. However, a practitioner claimed "anything with N.S.A. in front of it is not offensive. They do espionage." He said if the cyberweapon was a T.A.O. tool, then maybe it was entirely espionage. He added, even if it was T.A.O., a "weapon implies Geneva Conventions" which are the international rules applicable to people in armed conflict. Thus, he was skeptical about some of these cases being cyberweapons.

[39] *Zero Days*, Amazon Video, (2016; Magnolia Pictures, 2017), accessed February 6, 2017, https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2EKYTC.

There were also differing opinions about the ISIS case, the U.S.' response to North Korea's attack on Sony as well as Russia's role in the 2016 U.S. presidential election. Some interviewees said the Iraq (2003) case could have been a cyberweapon or a cyberattack if it drained bank accounts but not if it was solely about breaking in and collecting intelligence. One journalist wrote to me in an e-mail that "Notably, the Bush administration declined to conduct a cyberattack that would have disrupted Iraq's banking system out of a fear that it would have unwanted collateral effects on the European banking system."

Intriguingly, I also heard some "no comments." A former T.A.O. employee declined to comment about Nitro Zeus whereas another interviewee said yes, Nitro Zeus is a cyberweapon. When I asked a former T.A.O. employee if The Equation Group was T.A.O., he said, "no comment." He also said, "no comment" in regards to the Five Eyes. Another government official said, "no comment" in regards to Syria.

A government official explained that maybe some of these cases were cyberweapons however, people are reluctant to label it as such because there are other implications. He pointed out that General Electric claims in the past, they did not have to defend against intercontinental ballistic missiles so why should they have to defend against cyberattacks? But, he said this was too simplistic, because "in a way we are talking about cyberespionage which companies should guard against because this is espionage." One journalist said, "a complication of leaning on the Pentagon is that you encourage companies not to take cybersecurity insurance when there should be an expectation that you are responsible for your company." A cybersecurity official said in terms of defense, private companies are responsible for cyberattacks. In a nuclear attack, the government would have been responsible but in the cyber arena, the private sector owns most of the critical

infrastructure, he explained. So this is a different paradigm where private companies are defending the U.S. from other countries, he stated. I thought this was fascinating.

I. Stuxnet

According to the documentary *Zero Days*, the N.S.A. representative declared that the U.S. created Stuxnet but the N.S.A. called this operation "Olympic Games."[40] So while there is still some lingering doubt as to whether the U.S. was involved in Stuxnet, I think I can say that yes, they were. However, several government officials and academics cautioned that there still has been no official attribution from the U.S. as to their involvement in Stuxnet whereas the journalists I spoke with and some other government officials stated otherwise. A journalist stated, "We didn't do Stuxnet is not a discussion." "We did it." "People can be coy but we did it," she declared.

Some people I spoke with declared that Stuxnet was a "precedent setting event." It was a "first use" explained a former Cyber Command official. A cybersecurity specialist claimed "Stuxnet opened Pandora's box." (This term was also used in *Zero Days*.) Another interviewee said it was the "only option" based on the operational parameters. A journalist said Stuxnet was "a precision weapon" that "takes a lot of skill." "Stuxnet was sophisticated and targeted." "Stuxnet did not need outside commands." "It was autonomous."[41] However, a cybersecurity official said that it does not matter whether the cyberweapon is autonomous or if there is a remote operator because the end result is the same– all of this

[40] *Zero Days*, Amazon Video, (2016; Magnolia Pictures, 2017), accessed February 6, 2017, https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2EKYTC.

[41] Owens, Dam and Lin discussed automation on page 230. According to *Joint Publication 3-12 (R) Cyberspace Operations*, cyber capabilities that "allow the operator to reconfigure the capability on-the-fly are preferred." *Joint Publication 3-12 (R) Cyberspace Operations*, IV-4.

falls under Computer Network Attack. However, he said obviously, this matters to the military though because it depends whether this is a Title 10 or Title 50 operation and who is giving that human operator the directive to attack.

One point of contention was whether Stuxnet was successful. Some interviewees were displeased with the limited amount of damage while others argued that Stuxnet had a destructive effect because it impacted Iran's nuclear program and prevented Israel from launching an airstrike. An academic told me Stuxnet was a good idea but the Israelis f***** it up. A journalist claimed two underground halls of 50,000 centrifuges never got fueled thereby delaying the enrichment process. Stuxnet caused confusion and sowed doubt, she explained. Natanz was shut down for six days and sabotaging attempts continue to this day. The goal was never to destroy Iran's program but to buy time for diplomacy and sanctions, she claimed. A cybersecurity official expressed a similar thought claiming Stuxnet could have been used as leverage. This reasoning seems possible since other interviewees also claimed Stuxnet brought Iran to the negotiating table. However, this cybersecurity official said Stuxnet may have achieved its desired outcome but the process itself was not desired. Thus, he declared Stuxnet a disaster because it was not supposed to go public.

After Stuxnet, the threat intelligence community began paying more attention to what nations were doing. A cybersecurity official told me that before Stuxnet, there were maybe four "campaigns" from nation-states but now there are hundreds. He said there are millions of new samples so the bigger goal for him is to find the needle in the haystack. Hence, understanding world events is important and geopolitics matters, he stated. A cybersecurity official commented that post-Stuxnet there were a lot of sophisticated attacks. Now you see low sophistication but high impact, he said, because there are

numerous players since the barriers to entry are low. While there is a sophistication of subverting systems, if it is old software, odds are it has not been patched, or you can use a zero-day or old code, he added. The same attack code could be used today because the Industrial Control Systems are the same. It is the research that is expensive, not the code, he clarified. A journalist observed that Stuxnet was expensive because of the construction of a testing lab but the cost was between $500,000 to one million, which is cheaper than other military tools. A cybersecurity official stated there is no direct correlation between sophistication and impact, but there may be a correlation between sophistication and discoverable. For instance, he said wiping attacks such as what North Korea did to Sony or the attack against Ukraine's power grid in December 2015, did not use zero-days but they were effective. An academic shared a similar point of view when he cited Rob Joyce's admission about not relying on zero-days in order to break into a network.[42] Rob Joyce is the head of T.A.O.

One interviewee told me that future cyberweapons "will never be as clean as Stuxnet." A cybersecurity official declared that Stuxnet remains the most advanced cyberweapon we have seen. We have seen some Stuxnet-things such as Flame, Duqu and Gauss but very little is related to Stuxnet now, he said. Another cybersecurity specialist explained that he looked at Stuxnet and Flame as platforms, not weapons. A journalist said she sees Duqu, Flame and Gauss as spy tools. Gauss was an Israeli spy tool that was used to create Stuxnet. There is a difference between the entry tool versus the payload, she said.

[42] Kim Zetter, "NSA Hacker Chief Explains How To Keep Him Out Of Your System," *Wired,* January 28, 2016, accessed February 20, 2017, https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/.

Thus, the interviews suggest that the key findings from the Stuxnet case in regards to conditions for using a cyberweapon were operational parameters, geopolitics, and leverage.

1. Five Eyes

In *Zero Days*, the N.S.A. representative declared that the C.I.A., N.S.A., U.S. Cyber Command, GCHQ (British intelligence) and Unit 8200 were all involved in Stuxnet.[43] Thus, I asked the interviewees about allies. "Do you think other countries in the Five Eyes alliance would be likely to be informed before the U.S. were to use a cyberweapon in a first strike?" An academic said in regards to the Five Eyes, not all allies are created equal meaning cyber tools are closely guarded so the U.S. is reluctant to share. Another academic speculated that maybe the Five Eyes would be informed however, he does not know the extent to which there is collusion and he would be surprised if there was collusion. (The word "collusion" is currently dominating news headlines but in regards to the Trump administration and Russia's role in the 2016 U.S. presidential election.) A former T.A.O. official said, "no comment."

A former Senior Cyber Policy Advisor stated the Five Eyes is a signals intelligence partnership so it does not mean any other type of operation will be shared. He said Iraq, Afghanistan and Syria were all coalition operations where we are right there alongside coalition troops, but as we build out Cyber Command, this relationship needs to be renewed. A journalist claimed that the U.S. and the Five Eyes have a cyber spying collaboration but the U.S. does not bring in partners unless they need to.

---

[43] *Zero Days,* Amazon Video, (2016; Magnolia Pictures, 2017), accessed February 6, 2017, https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2EKYTC.

Another cybersecurity official stated under traditional agreements, yes, the Five Eyes would probably know if the U.S. were to launch a cyberattack. “Up until January 20, 2017, yes.” “Now, who knows,” he said. A prominent think tank member stated the Five Eyes would know if the campaign was against Russia. However, if it is against China, the U.S. would notify the Brits, he said. He also confirmed that the N.S.A. and GCHQ work together. A cybersecurity official asserted the Snowden documents showed us that Regin (discussed in Chapter 4) was developed by the Five Eyes. However, another cybersecurity official alleged Regin was carried out by the U.K. not the Five Eyes. It is possible that the code could have been developed by the U.S. but maybe Canada or New Zealand modified it for their purposes, explained a cybersecurity official. Another cybersecurity official said this is why codes appear elsewhere and why it is hard to assess if there is a coordination of malware amongst countries. He suggested perhaps these countries are buying zero-days from the same person.

A current advisor to the N.S.A. advanced a related opinion that we do have close relations with the Five Eyes where we have members sitting in their organizations and they have members sitting in ours and the Five Eyes indeed might be aware “all things being equal.” Another government official said he suspects that the Five Eyes might be informed or at least maybe they should be due to the collective nature of cyberspace. He said there are “diplomatic démarches where the botnets are located” so “how you build alliances and the use of tools complicates that.” A Legal Advisor said NATO may be informed before a NATO country were to use a cyberweapon in a first strike if it was a partner country. For example, if the U.S. decides to deploy a cyberweapon against Serbia, NATO would probably be informed because Serbia is in the middle of NATO countries, he explained.

II. Iraq (2007)

An Army reservist told me that the Iraq (2007) case was another instance in which the U.S. was able to accomplish a physical effect through cyber means. However, he labeled this as an information operation campaign as opposed to a cyber capability. He said the purpose of an information technology campaign is for intelligence whereas a cyberattack is a "deliberate intrusion into closed networks like financial networks." Draining accounts is a cyberattack whereas stealing funds is an information technology operation, he explained. This is confusing, however, since the Iraq (2007) case was about gaining intelligence but also led militants to their death. Thus, I think this falls under his own description of a cyber capability.

There were some other interviewees who also did not view the Iraq (2007) case as a cyberweapon. A prominent think tank member said this was not a cyberweapon. A journalist also said Iraq (2007) "does not count" because at the time, the N.S.A. was concerned with surveillance. "The N.S.A. was messing around," he stated. The U.S. did not know how to use these capabilities for offense, he said, and hence, this case "was child's play." Moreover, he noted, this operation was before the formation of U.S. Cyber Command.

In summary, the interviews suggest that the key finding from the Iraq (2007) case in regards to conditions for using a cyberweapon was purpose.

III. Libya (2011)

Libya (2011) was one of the few cases that some interviewees elaborated on and labeled as a cyberweapon. I inquired why was this offensive cyber capability not deployed? After all, this operation would have fulfilled the 'prep the battlefield' rational proposed

above. A think tank member I spoke with did not know about the Libya (2011) or Syria case but after explaining the circumstances, he said yes, the Libya (2011) and Syria cases would have been examples of cyberweapons. A cybersecurity official proposed that the U.S. may have refrained "because it is noticeable." This is an interesting argument though because the U.S. was preparing to join the airstrikes against Libya[44] so why would they care if a cyberweapon was noticeable?

A journalist said some of these targets are antiquated so using an offensive cyber capability did not make sense because cyberweapons work best against highly integrated societies. (This point was reviewed in earlier chapters.) A former Army official said, "in order to have strong value for the military," the cyberweapon has to be more sophisticated than other operations. "The adversary needs to be vulnerable" even though it is "hard to kill something with cyber," he stated. A former Cyber Command official reiterated "it is easier to kill a human than it is to kill a computer."

Another interviewee suggested that maybe the U.S. refrained because the cyberweapon would have knocked something else out. A Legal Advisor I spoke with echoed these sentiments asking whether the cyberweapon has the intended design effects. Interestingly, this official as well as a few government interviewees told me that whether the U.S. did or did not use a capability does not mean the reporting is accurate. In other words, just because the media said the U.S. did not use a cyberweapon does not mean the U.S. did not use a cyberweapon. For example, when I asked about Libya (2011), Syria and ISIS (2016), a Senior Cyber Policy Advisor said, "whatever is in the news is not true." A

[44] "Remarks by the President on the Situation in Libya," *The New York Times,* March 18, 2011, accessed December 5, 2016, https://www.whitehouse.gov/the-press-office/2011/03/18/remarks-president-situation-libya.

Legal Advisor said he knows these tools were employed in Syria. As mentioned earlier, an academic I spoke with said, a cyberweapon "could have a profound effect" on the "proxy wars" in Syria and Yemen.

In summary, the interviews suggest that the key findings from the Libya (2011) case in regards to conditions for using a cyberweapon were covert, vulnerability and reliability.

IV. Pakistan (2011)

Several interviewees proclaimed that if it had occurred, the Pakistan case would have been an example of a cyberweapon. This operation also would have fulfilled the 'prep the battlefield' rationale described above. A cybersecurity official explained that this incident was concerned about exposure. A former Cyber Command official clarified that the dilemma was "how do you fly in and out without no one knowing you were there?" He said it came down to probabilities of success and optics because there were "high-level political ramifications."

A cybersecurity official said using these capabilities means the loss of these capabilities, echoing the one-time use argument discussed earlier. So he asked, "what is the cost of this loss?" In this situation, the U.S. decided to reveal that they had a stealth helicopter instead of using a cyberweapon. "So there are very isolated scenarios" in which these capabilities are deployed.

In summary, the interviews suggest that the key findings from the Pakistan case in regards to conditions for using a cyberweapon were risk of exposure, probabilities of success, capability loss, high-level political ramifications and flying under the radar (literally).

V. Syria

According to one academic, President Bill Clinton was "extremely reluctant to use cyber" capabilities in 1999 against Serbia because he did not want to set a precedent for others. He said this was fascinating because at the time, the defense was weak and the offense was dominant. So even though the perceived utility of this tool was high in 1999, President Clinton "stepped back." According to one journalist, more than ten years later precedence was still a concern as President Obama deliberated about using a cyberweapon in Syria. There was "high politics in play," said a former Cyber Command official.

One reason for non-deployment could have been due to the availability of the technology. "Were the assets available?," asked one interviewee. A former Cyber Command official told me that the decision to not use a cyberweapon in Syria could have been due to cost. "Was there a cheaper solution?" However, this contradicts the argument that cyberweapons are cheaper than other military tools. Additionally, a journalist said, if the Trump administration decides to use these capabilities today (as they have indicated) then the only thing probably stopping them is legality, not money. Another journalist told me that the U.S. "subcontracted the stuff with Syria" to GCHQ, who he said often do not get credit even though they are good. He said the U.S. went this route in order to get away from the problem of authorization. "Obama did not want to go through another Authorization for the Use of Military Force request," he explained.

Another interesting finding was that a former Cyber Command official proclaimed the Snowden disclosures showed us the intel gained/lost from an offensive cyber operation in Syria. This was news to me so I looked into it. Apparently in 2012, T.A.O. mistakenly took out Syria's internet and was unable to repair the router so they joked 'If we get caught,

we can always point the finger at Israel.'[45] (This might have been what the Legal Advisor was referring to when he said he knows these capabilities were used in Syria.) This is fascinating because it means the U.S. was attempting to install cyber espionage tools onto Syria's networks and they might have been willing to frame an ally if they got caught, which means the U.S. could have been guilty of using a false flag.

In summary, the interviews suggest that the key findings from the Syria case in regards to conditions for using a cyberweapon were precedence, politics, availability and legality.

VI. North Korea (2014)

There were varying degrees of responses about whether the U.S. retaliated against North Korea for their attack on Sony. First of all, a former Cyber Command official said that perhaps North Korea did not carry out the attack on Sony because this could have been a false flag where someone said let us work together to point the finger at North Korea. However, a government official said North Korea was a "big splash" since the President attributed it (a first) and took action.

An Army reservist told me that the U.S. did carry out a DDoS attack against North Korea in order to restore confidence in the U.S. He labeled this DDoS attack as a cyber capability. A journalist claimed that the U.S. went to the Chinese and said, "hey, we cannot do anything because this violates your sovereignty, so can you do it for us?" And the Chinese did, he alleged. A former T.A.O. official attributed the North Korean case to a Computer Network Attack that made use of a cyberweapon. However, a practitioner told me "only kids would use a DDoS attack" thus in his view, the U.S. did not turn off North

[45] James Bamford, "Edward Snowden: The Untold Story," *Wired,* August 22, 2014, accessed March 22, 2017, https://www.wired.com/2014/08/edward-snowden/.

Korea's Internet. He emphasized he had "positive confirmation that North Korea was not us." He explained that China stopping the sale of coal was a part of the response to North Korea's attack on Sony. Some interviewees believe that these capabilities are more effective against highly-networked societies. This echoes the claims discussed previously. A journalist said, "if we went to war with Singapore, we could wipe the floor with them. If we went to war with North Korea: good luck."

What we do know is that the Obama administration decided to enact sanctions and a former T.A.O. official thought these sanctions "were a waste of time" because they had no effect.[46] He proposed "we should have wiped out North Korea's systems." However, a cybersecurity official stated, North Korea was a special case because if you respond, are you willing to risk escalation? As I was finishing the interviews, *The New York Times* published an article about the U.S.' covert cyberwar against North Korea's nuclear program.[47] A former R.O.C. official stated, this article is "really good" and that this "is a really good example" of using these capabilities. A cybersecurity official who used to work for the government told me that they saw these capabilities possibly being used to manipulate missiles. This new article details that this was exactly the manner in which the U.S. used these capabilities against North Korea.

While digging a little deeper, I also came across a 2015 Reuters article that disclosed the U.S. failed in their attempts to deploy a Stuxnet-type operation against North

[46] Owens, Lin and Dam said "economic sanctions are almost always the first actively adversarial action taken against nations that offend the international order. Owens, Lin and Dam, 300.

[47] Sanger and Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles."

Korea's nuclear program in 2009 and 2010.[48] Perhaps this is a case I should have included in this dissertation. I have not seen much written about it and no one really discussed this case per se although as pointed out earlier, they indicated North Korea is a target of these weapons.

In summary, the interviews suggest that the key findings from the North Korea case in regards to conditions for using a cyberweapon were escalation, sovereignty, vulnerability, and restoring confidence.

VII. ISIS (2016)

In regards to ISIS (2016), there was no consensus among the interviewees as to whether this case was a cyberweapon. Additionally, there was no clear differentiation between the ISIS (2016) and Iraq (2007) cases among the interviewees. However, some interviewees stated yes, the ISIS (2016) case is a cyberweapon. A cybersecurity specialist declared this is the first time we have seen this – where the U.S. is using a cyber tactic to go after militants in a kinetic manner. (However, there was the cyber offensive in Iraq in 2007. Additionally, a journalist said in the past, the C.I.A. operated forums to track Al-Qaeda militants. This operation interfered with communications.)

Other interviewees stated no, the ISIS case is not a cyberweapon. "Do you need a cyberweapon when you can pinpoint someone? Is that a weapon?," probed a cybersecurity official. A journalist expressed she had "no idea" what was going on with the cyber offensive against ISIS. She stated, "it is hard to talk about offensive weapons against an asymmetric war like this." Another journalist explained via email,

---

[48] Joseph Menn, "Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed – sources," *Reuters,* May 29, 2015, accessed April 9, 2017, http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529.

> Cyber Command has been conducting a cyber offensive against ISIS with mixed results, according to military sources. Part of the issue is that ISIS does not have a lot of infrastructure to go after, and when you take out a server, the operators can move operations to another. Another issue is that the government has not fully worked out to what degree the military can take actions in a third non-belligerent country —outside Syria or Iraq, for instance—in order to get to the targeted server or computer. There are questions of sovereignty that have not been settled.

A former Senior Cyber Policy Advisor recapped some of these claims. He stated, "ISIS has no air defense systems to attack through cyber means" so the types of targets are different which means the gain/loss calculus is different. Therefore, perhaps my third hypothesis is null– *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they believe they can destroy the intended target(s).*

"There are a variety of considerations" when it comes to deployment, stated a Senior Cyber Policy Advisor. Perhaps the other operations were more difficult or the U.S. did not have the capability, he expounded. "What is important is that the U.S. government felt the need to say that they are using these capabilities." "This is the first time they have said that so this is significant for the U.S.," he pronounced.

In summary, the interviews suggest that the key findings from the ISIS case in regards to conditions for using a cyberweapon were targets, sovereignty, difficulty, and legality.

VIII. Russia (2016)

Russia's role in the 2016 U.S. presidential election was a passionate discussion topic for some of the interviewees. First of all, there was no consensus about whether the Russians carried out a cyberattack against the U.S. A government official believed the theft of information is not a cyberattack. An academic stated, it is "not clear that Russia's actions were illegal" and in fact, "cyber had very little to do" with Russia. A journalist said the

Russians stole data and made it public, which is standard espionage, not warfare or a weapon. However, if they had wiped out the data, that would have been destruction and thus a weapon, she claimed. An academic argued the opposite insisting the Russian release of information was a "virtual weapon." A cybersecurity official attributed the Democratic National Convention hacks to Computer Network Exploitation. Another cybersecurity specialist said this was fundamentally an intelligence operation to influence the election which is no different from what the C.I.A. did in Latin America in the 1950s and 60s. However, a Senior Cyber Policy Advisor rejected this interpretation, exclaiming, "we have not conducted those meddling operations for a long time." "We are long past those days," he stated. It does not matter whether this is "moral equivalence," he argued, it does not mean we should not respond. "We should combat threats," he urged. "We are playing into Russia's hands."

1. "Influence Operations"

One thought-provoking finding when discussing Russia was the notion of "influence operations."[49] Owens, Dam, and Lin mentioned the idea of influence in their 2009 report claiming "cyberwarfare provides tools that can be focused directly on messaging and influencing the leadership of an adversary."[50] Additionally, this term was

[49] According to the Air Force, "Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle, which aligns with the commander's objectives." "Cyberspace & Information Operations Study Center," *Air University*, accessed March 8, 2017, http://www.au.af.mil/info-ops/influence.htm#top. "These activities of influence operations allow the commander to prepare and shape the operational battlespace by conveying selected information and indicators to target audiences, shaping the perceptions of decision-makers," etc. "Cyberspace & Information Operations Study Center," *Air University*, accessed March 8, 2017, http://www.au.af.mil/info-ops/influence.htm#top.

[50] Owens, Dam, and Lin, 224.

mentioned in news accounts at the time. But the term "influence operations" was used by several interviewees when expounding on Russia's actions in the 2016 U.S. presidential election. Perhaps some of the interviewees might have been swayed by *Background to 'Assessing Russian Activities and Intentions in Recent Elections': The Analytic Process and Cyber Incident Attribution*, which was a declassified intelligence report released on January 6, 2017 by the F.B.I., C.I.A and N.S.A. about Russia's role in the 2016 U.S. presidential election. One of the key judgments of this report was "We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election."[51] (I started interviewing people at the end of January 2017.) So I ran a Text Search query (a search for specific words)[52] in order to see how often this phrasing came up.

At least three cybersecurity officials as well as two former and one current government employee used this term. The Russia case was a "supporting operation for a greater campaign which is influence operations," declared a cybersecurity official. He added "This created an environment for the public to be receptive." However, he cautioned that "influence operations are not cyberweapons" because a cyberweapon is measured by its impact or destructiveness. A government official also repeated that "Influence operations are not cyber operations." "So how do you counter?," he probed. "It is not a cyber issue."

---

[51] Office of the Director of National Intelligence, *Background to 'Assessing Russian Activities and Intentions in Recent US Elections,': The Analytic Process and Cyber Incident Attribution*, (National Intelligence Council, January 6, 2017): ii, accessed February 18, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[52] Bazeley & Jackson, 250.

A cybersecurity specialist attributed the confusion over Russia's actions to media coverage, which he said tends to label everything as a cyberweapon. A former T.A.O. employee also repeated that the media lacks an understanding when it comes to cyber matters. (This was an opinion discussed in earlier chapters.) He claimed Russia was an offensive operation "but by and large these were tools of backdoors not a cyberweapon." He said, a "cyberweapon is being conflated with espionage." A government official restated these opinions saying, there was penetration but the difference is that this was an influence operation. "Cybersecurity is different than espionage," he maintained. An Army reservist echoed that the Russia case was an information operation campaign but it "was more cyber espionage than an attack."

A former T.A.O. official clarified that the Russians call this "foreign intelligence," so he advocated "I would be telling them to hack the data too." "This was a psychological operation with a covert influence over the election," he stated. In 2008, there was information that indicated the presidential campaigns of Barack Obama and John McCain were breached so maybe the Russians manipulated the 2008 election, he suggested. I am somewhat doubtful about the 2008 hacking claim though because first of all, the F.B.I. and Secret Service said this hack could have been the work of the Russians or the Chinese.[53] Second, this incident was about the theft of data to understand policy positions, not the theft of data to influence an election.[54] Thus, the 2008 episode was not a cyberweapon

[53] Lee Glendinning, "Obama, McCain computers 'hacked' during election campaign," *The Guardian,* November 7, 2008, accessed February 28, 2017, https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa.

[54] Kevin Bohn and Brian Todd, "Obama, McCain campaigns' computers hacked for policy data," *CNN*, November 6, 2008, accessed February 28, 2017, http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/.

which is possibly why the U.S. probably would not have considered using a cyber capability to respond, or even that a response was warranted at the time. Russia's actions in 2016 were about influencing an election, or at the very least sharing the stolen D.N.C. information with the Trump campaign in order to help them anticipate the other side's policy positions and tactics.

There are two concepts to unpack here. First of all, some interviewees blurred the terms psychological warfare, information warfare and electronic warfare. A former Cyber Command employee said what we are seeing more of is information that is being collected and disclosed publicly– "cyber-enabled information operations." "The line also intersects with electronic warfare," he explained. "For instance, maybe you can jam a drone and turn it around." He classified this as both electronic and cyber warfare. Signals intelligence, electronic warfare– they all blend together, he stated, and this is the future.

However, these terms mean different things in the U.S. military. "Cyberspace Operations" defines cyber operations as using "cyberspace capabilities to create effects which support operations across the physical domains and cyberspace."[55] Information operations "influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[56] This document states cyberspace operations are a subset of information operations.[57]

A Senior Cyber Policy Advisor commented that electronic warfare deals with the electromagnetic spectrum and jammers. Psychological warfare is similar to information

---

[55] *Joint Publication 3-12 (R) Cyberspace Operations*, I-5.

[56] Ibid.

[57] Ibid.

warfare in terms of manipulating the information environment to favor the outcome. He said information warfare is not a term that the military uses anymore. The term today is influence operations although it used to be psychological operations, irrespective of the medium. An Army reservist expressed that this is "gamesmanship" where you have to decide which one is more important. These opinions blend the seven layers of information warfare expounded by Martin Libicki in Chapter 1. However, a cybersecurity official insisted "It does not matter if it is information or psychological operations." "Real influence operations last much longer." Another cybersecurity official underscored this point claiming Russia's role in the election is only the beginning step. "This will be ongoing," he proclaimed.

The second point to note is that some interviewees also blended the terms political warfare and hybrid warfare. A cybersecurity specialist remarked that "This was a big deal but this is not a new playbook." "This is hybrid warfare," he declared. "It started visibly in 2008 with Estonia." Another interviewee pointed to Ukraine as the test case so he claimed what happened in the U.S. is not that surprising. An academic said, this was an example of the use of cyber for political warfare. A Legal Advisor I spoke with used both terms saying "there will be skirmishes and proxies" but "intelligence operations do not invoke military concerns." "So this will not escalate to NATO," he explained, and "NATO will not opine until there is a joint investigation." For example, Estonia v. Russia was not claimed by NATO, he said, in fact, NATO tends to talk around Russia. A practitioner supported this statement explaining that the Russia case is an awesome Article 4 but not Article 5 for NATO.[58]

[58] Article 4 of NATO says "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is

Regardless of what the Russia case was labeled, several interviewees stressed that Russia's actions were significant. A Senior Cyber Policy Advisor argued while Russia's role in the 2016 U.S. presidential election "was not the offensive cyber operation we think about," it was a big deal. This was a successful covert action, he pronounced. "Who cares about the means they do it." "We should be focused on our core interests and values which this was a threat to." "U.S. officials drew a red line about tampering with voting machines." "That is asinine," he declared. "The U.S. is worrying about high-end attacks but the horse gets out of the barn with low-tech methods."

A legal advisor indicated, "eventually it is going to be clear that Russia put a finger on the scale through cyber." A government official stated, "This incident changed the conversation." "It raised awareness." "Russia made it real for a lot of people," said a cybersecurity specialist. "This was a tangible thing," he explained. "Before people were scared about a power grid attack such as what happened in Ukraine." "Now you see the real-world effects from Russia." The "Russian cyberattack changed the course of history," he pronounced. A journalist declared just as "9/11 showed us vulnerabilities, Russia was like a 9/11 moment" "because we were focusing on a cyber-Pearl Harbor and this revealed

---

threatened." The North Atlantic Treaty art. 4, (Washington, D.C.: NATO, April 4, 1949), accessed March 13, 2017, http://www.nato.int/cps/en/natohq/official_texts_17120.htm. Article 5 says "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area." The North Atlantic Treaty art. 5, (Washington, D.C.: NATO, April 4, 1949), accessed March 13, 2017, http://www.nato.int/cps/en/natohq/official_texts_17120.htm.

something totally different." A former Senior Cyber Policy Advisor agreed stating "we were way too focused on a cyber-Pearl Harbor which has not been proven successful."

2. Cyber-Pearl Harbor

Many interviewees discussed the notion of a cyber-Pearl Harbor. So I ran a Text Search for "Pearl Harbor" and at least six government interviewees, two journalists and three cybersecurity specialists used this term. One government official asked "why haven't we seen a cyber-Pearl Harbor?" He then answered his own question stating "it has to be sustained," which means this action ends up being attributable and that allows the U.S. to take measures to prevent or stop such an attack. Owens, Dam, and Lin also discussed this concept of sustainability.[59]

Another interviewee expressed that he hated the term cyber-Pearl Harbor because Pearl Harbor was a complete surprise whereas with a cyberattack, it is not that we do not know it is coming, "we are just not prepared." We are focused on big operations such as the Chinese turning off our power grid but the flip side is that a non-rational actor like North Korea or a terrorist might not care. "We don't have the capability to do so [not care]." A Senior Cyber Policy Advisor reaffirmed this stating it is "never realistic" to think of conducting a Pearl Harbor-type action against another country. You will hear military planners argue against this, he said.

3. The U.S.' Response

Although there was no consensus as to whether Russia carried out a cyberattack against the U.S., almost no one was happy with the Obama administration's response to Russia's role in the 2016 U.S. presidential election. One journalist contended "The Obama

[59] Owens, Dam, and Lin, 112.

administration acted slowly and incorrectly in the Russia case." A cybersecurity specialist echoed this belief alleging the "U.S. was way too late in their response" to Russia. One interviewee declared the U.S. is "behind the curve in understanding the threat and domain." A former T.A.O. employee asserted, "Obama's response to Russia was a classic waste of time." "It was an ineffective response," he proclaimed. An Army reservist expressed he was "not pumped about the U.S.' response." A practitioner acknowledged that he understood why President Obama acted the way he did however, he insisted that he would have acted differently. He added "When President Obama said the next president will have options to respond at their choosing, he meant "her" choosing." This intriguing interpretation was also advanced by an Army reservist who said, "all those decisions were predicated on Secretary Hillary Rodham Clinton winning the presidency." A cybersecurity specialist pronounced, "Russia was more successful than they hoped for." "They weakened Secretary Clinton's presidency but it was not their objective to get Trump elected." However, the declassified report *Background to 'Assessing Russian Activities and Intentions in Recent Elections': The Analytic Process and Cyber Incident Attribution* says the Russians favored Trump.[60]

A government official explained that indicting people sends a message but it does not really do anything. Hence, this government official as well as a former Cyber Command official suggested that the U.S. should have issued sanctions; however, a practitioner said sanctions are ineffective against Putin. A former Cyber Command official also recommended turning off the lights. He urged that there should at the very least have

[60] Office of the Director of National Intelligence, *Background to 'Assessing Russian Activities and Intentions in Recent US Elections,': The Analytic Process and Cyber Incident Attribution*, ii.

been a response since Russia's actions were significant. However, he decreed you "just do not see that pain." "There were no repercussions so why not do it again?" A former T.A.O. employee shared similar sentiments expressing "we were weak." He asserted, "We should have hacked Russia." "We should have done something against Putin which would have been effective." He insisted "Expelling diplomats was not effective." It was the "dumbest thing I ever heard," he uttered. "The U.S. did not hack back because they had no plan," he divulged. "They were caught flat-footed." He boldly stated, "Obama's response to cyberattacks has been pathetic." "The U.S. has failed to respond effectively to a single cyberattack over the last 8 years," he avowed. "The most basic government function failed."

A journalist assumed that President Obama was concerned about escalation with Russia. A government official conveyed "we are in an unstable environment" especially since we "have not figured out how to communicate." Thus, he cautioned "tit-for-tat might not be the best for the U.S. even if our tools are better." Some interviewees said it is debatable who is better in cyberspace. A former government official expressed that he sleeps well at night knowing what the N.S.A. can do whereas one cybersecurity official told me that Russia is better than the U.S. in cyberspace. Nevertheless, some interviewees said a cyber option should have been on the table. A prominent think tank member told me that a cyber response to dismantle infrastructure was indeed on the menu, but the U.S. refrained because the Russian case was not sabotage. In fact, one interviewee who used to work for the government as an intelligence analyst and worked on cyber matters said the U.S. had cyber options but they had simply run out of time [since a new President was about to assume office.]

A cybersecurity specialist explained "Russian military doctrine views cyberspace as national security so they could respond with nuclear weapons." "There are no norms in cyberspace," he stated. I disagree with this assertion because there are some norms in cyberspace as evidenced by President Xi and President Obama's agreements in 2015. Also, I wrestle with the idea that Russia could respond with nuclear weapons. Instead, the question has been the likelihood of hacking a nuclear system. "I know the talk has been that someone would be able to push the red button but it is highly unlikely that someone would be able to hack the nuclear arsenal system." However, in his view, "they could breach the radar systems and that could then cause a reaction where someone decides to shoot off a nuke."

4. Nuclear Threads

I discussed some of the nuclear comparisons in earlier chapters of this dissertation but naturally, these comparisons also surfaced during the interviews. One journalist explained that cyberwarfare is relatively casualty-free and you can dial it up or down unlike the situation with nuclear weapons. A former T.A.O. employee said if we take out power grids, we start approaching nuclear warfare. "Disclosing emails is not nuclear warfare," he stated. "The tradeoff is a real-world effect– thousands impacted versus stealing documents." A cybersecurity official said an advantage of having cyberweapons is that this is not a nuclear weapon where it is only useful if everyone knows you have one. Nevertheless, some interviewees emphasized the importance of signaling and the fact that a deterrent value has military value. Thus, a former government official claimed these capabilities are not unlike Mutually Assured Destruction. However, an academic insisted it is wrong to conflate cyberweapons with Mutually Assured Destruction. Additionally, a

journalist noted that deterrence is highly problematic since behavior is based on arms that states admit to. One interviewee pointed out that unlike nuclear weapons, the U.S. does not have cyberweapons in storage. Even if the U.S. could have zero-days in storage, as mentioned previously, the head of T.A.O. said he does not need a zero-day to conduct operations. Another academic said the U.S. was more worried about escalation and stability than deterrence. One cybersecurity official explained that "people do not ascribe to forced cyber deterrence because of escalation." "It is about motivation." "The next big thing has not happened yet because of motivation not because of zero-days or repercussions."

5. Motivation

Regarding motivation, a cybersecurity official described three trajectories. The first trajectory is cybercrime. The second trajectory began in 2010, with nation-states and the third trajectory is censorship by China and Russia. He alleged that Stuxnet was a catalyst but he also believed that Russia's activities in the 2016 U.S. presidential election would have happened with or without Stuxnet. Another cybersecurity official voiced that four to seven years ago he would have said the motivation was espionage. Stuxnet is the only instance of sabotage, he stated, and he has not seen more of that. Now, he said governments are doing a mix of things where there is a potential for sabotage. He suggested that in the case of Russia potentially swaying an election, political disruption was a motivation. Cyber is a tool that can serve a wide variety of motivations, he divulged.

One journalist designated four waves of cyberwarfare. The first wave is Cyber Mission Teams who are trying to embed with traditional military operations such as boots on the ground. He declared this to be an extension of electronic warfare. The second wave is data alteration. He described the Russian case as data alteration. The third wave is a

smaller set of covert actions such as Olympic Games or Nitro Zeus. He proposed "The Russian hack opened up something in between cyber and warfare," which is the fourth wave. This is the future, he predicted.

In summary, the interviews suggest that the key findings from the Russia case in regards to conditions for using a cyberweapon were intent, time, escalation, destructiveness and motivation. Furthermore, there were connotations with nuclear warfare. Thus, one academic I spoke with encouraged me to look at first-strike literature. So, I turned to Robert C. Aldridge's *First Strike! The Pentagon's Strategy for Nuclear War*. Aldridge defines a first strike as "a capability to inflict a *disarming* or *unanswerable* first strike against a rival nation."[61] In retrospect, perhaps I should have defined first strike at the outset of my dissertation especially since a former Cyber Command official claimed first use can be hard to assess.

NUCLEAR VS. CYBER FIRST-STRIKE

Commissioned by President Jimmy Carter in 1980, Presidential Policy Directive 59 provided guidance about nuclear policy and had some dire instructions which included eliminating "the USSR as a functioning national entity."[62] In the Introduction, Richard Falk writes "As Aldridge explains, a first strike capacity allows leaders to 'use' nuclear weapons as an instrument of foreign policy, rather than just as an ultimate hedge against either nuclear blackmail or attack by a rival." [63] Thus, Falk argued nuclear weapons were

[61] Robert C. Aldridge, *First Strike!: The Pentagon's Strategy for Nuclear War* (Boston: South End Press, 1983), 25.

[62] Aldridge, 35.

[63] Ibid., 4.

"perceived by strategists and bureaucrats as a vital American 'asset'."[64] I think the same can be said today of cyberweapons as seen by the huge investment into cyberspace (at least until January 2017) and especially when some interviewees mentioned that a cyberweapon is a tool of international diplomacy. However, at that time, Falk said one could doubt that the U.S. was pursuing a first strike capability because

1.) "It defies common sense;"
2.) "It involves genocidal planning of the most extreme sort, and seems inconsistent with the minimum sort of morality that has guided America's behavior in the world;"
3.) "It contradicts official descriptions of United States national security policy, maintained by leaders of both political parties, and would require us to conclude that the entire leadership of the country was lying or somehow self-deceived."[65]

Well, the ghosts of 1983, which is when this book was written, are still around today. Considering James Clapper's quote about glass houses cited earlier, as well as how connected the U.S. is, Falk's arguments are still valid. Falk believes that Aldridge makes a convincing argument "that we are being governed in a grossly anti-democratic manner by leaders who are incompetent or depraved."[66] Why does this sound so familiar?

Aldridge also reviewed a few conditions in regards to nuclear weapons that were also discussed by the interviewees in regards to cyberweapons. First, Aldridge highlighted the role of geopolitics[67] as did many of the interviewees. Aldridge also discussed readiness and reliability[68] which are concerns with cyberweapons. Additionally, Aldridge points out

---

[64] Aldridge, 7.

[65] Ibid., 5.

[66] Ibid.

[67] Ibid., 7.

[68] Ibid., 56.

that no one asked why Russia would want to launch a nuclear attack against the U.S. "The hypothesis was blindly accepted by an unquestioning people."[69] However, with cyberweapons, the U.S. knows why other countries would want to launch cyberattacks against the U.S. The North Korean and Russian cases in this dissertation are examples of these reasons.

Falk said, "The United States as the first and only use of nuclear weaponry has a definite psycho-political stake in maintaining the *legitimacy* of this technology of mass destruction. It is not only the denial of guilt that is operative, it is also the sense of imperial predominance."[70] Since the U.S. (and others) were the first to launch Stuxnet, perhaps Falk's claim also applies to cyberweapons. Or if the U.S. desires to maintain the legitimacy and predominance of these capabilities, then this is why there needs to be more conversations about cyberweapons. The next section addresses the huge nuclear imprint on the cyber decision-making process. This is one of the most significant findings of this dissertation.

DECISION-MAKING PROCESS

Now that we have ascertained possible scenarios and conditions for deployment as well as acquired some further details about actual cases, this section will focus on how the decision to deploy a cyberweapon is made. An Army reservist I spoke with explained that each service has a different approach. When the Chairman of the Joint Chiefs of Staff wants to take out communications, he goes to the Air Force. If he wants to do a large scale

[69] Aldridge, 33.

[70] Ibid., 6.

operation, he goes to the Navy. If he wants to attack on land, he goes to the Army. However, the "battlefield effect" of cyber is largely undefined and hence it is unclear which service to go to for a cyber effect. This is one of the constraining factors of a cyber capability, he declared.

As mentioned in earlier chapters, "A single chain of command runs from the U.S. president to the secretary of defense to the commander of Strategic Command to the commander of Cyber Command and on to the individual military units around the world."[71] According to *Joint Publication 3-12 (R) Cyberspace Operations*, the Secretary of Defense provides guidance;[72] the Chairman of the Joint Chiefs of Staff translates this guidance into an operational order;[73] the commander of Strategic Command "has overall responsibility"[74] and the commander of Cyber Command "when directed," can "conduct full-spectrum military cyberspace operations."[75] This is basically the process that some interviewees repeated. For instance, one academic said the Army Cyber Command and the Fleet Cyber Command present their forces to U.S. Cyber Command who deliberate and then advise the Secretary of Defense. Nevertheless, I asked the interviewees "What do you think might have been especially noteworthy about the conditions or decision-making involved in these important cases?" I used a Text Search query to find any instance where "decision" was

---

[71] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October, 2010): 102, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/20788647.

[72] *Joint Publication 3-12 (R) Cyberspace Operations*, III-2.

[73] Ibid., III-4.

[74] Ibid.

[75] Ibid., III-6.

mentioned in the interviews. The following diagram shows the most frequent words in the Decision-making node.

Figure 7.5 Word Cloud of Decision-making

A former Remote Operations Center employee explained that Defense Secretary Robert Gates told General Keith Alexander that he wanted the offensive (Joint Functional Component Command- Network Warfare,) defensive (Joint Task Force- Global Network Operations) and exploit divisions to work together. He explained that Joint Functional Component Command- Network Warfare was a subcomponent under U.S. Strategic Command (USSTRATCOM) because at the time, USSTRATCOM had the authority to do

cyber strikes. USSTRATCOM was the joint forces command for nukes, space and cyber. This explanation coincides with what was discussed in Chapter 1.

Since a lot of military and air force were involved, he said a lot of the thinking about offensive cyber actions was modeled after strategic thinking around nuclear warfare. This interviewee, who was previously an Army Mission Commander and worked on signals intelligence, stated that they did hypothetical offensive cyber actions "modeled after the nuclear strike process." This is a major finding of this dissertation. He explained that U.S. Cyber Command generates the strike package against cyber targets. First, an intelligence and target package is developed. There is also a collateral damage assessment and a rating level assigned to each option.[76] He said, "nothing was taboo right off the bat" but if there was a link to the possibility of loss of life, they would stay away from that." He said, they were "so trepidatious about anything."

I briefly investigated the nuclear strike process. What follows is a simplified version of what is a very complex approval process but it resonates with what the interviewees disclosed. The Single Integrated Operational Plan for Fiscal Year 1962 (SIOP-62) was the first U.S. nuclear strike plan. Needless to say, this was and still remains highly classified.[77] In 2003, the SIOP nomenclature was re-named to Operations Plan.[78] The first Operations

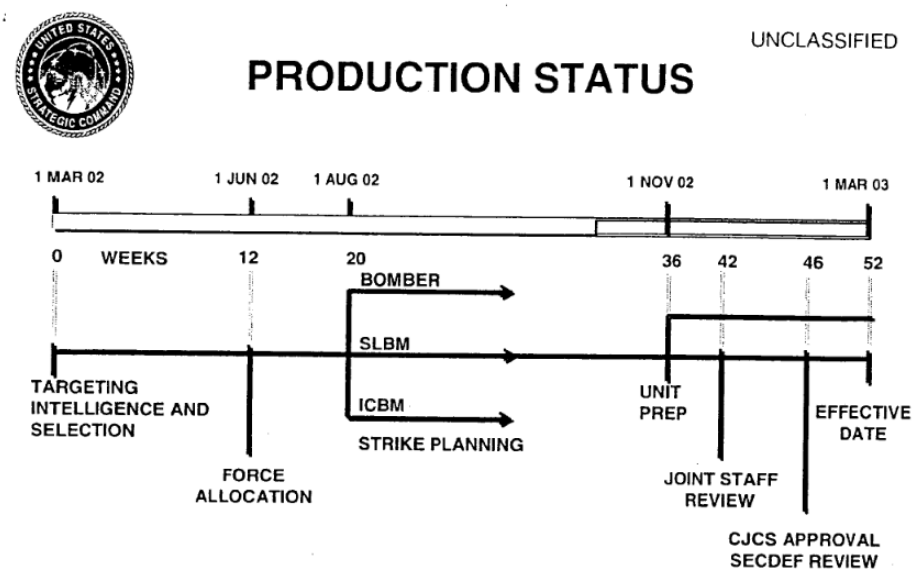
---

[76] "A collateral effects analysis to meet policy limits is separate and apart from the proportionality analysis required by the law of war. Even if a proposed CO is permissible after a collateral effects analysis, the proposed CO must also be permissible under a law of war proportionality analysis." *Joint Publication 3-12 (R) Cyberspace Operations*, IV-4.

[77] Scott D. Sagan, "SIOP-62: The Nuclear War Plan Briefing to President Kennedy," *International Security* 12, no. 1 (Summer, 1987): 22, accessed March 16, 2017, http://www.belfercenter.org/sites/default/files/legacy/files/CMC50/ScottSaganSIOP62TheNuclearWarPlanBriefingtoPresidentKennedyInternationalSecurity.pdf. In 1987, Scott Sagan wrote "SIOP-62: The Nuclear War Plan Briefing to President Kennedy" based on a 1961 declassified SIOP briefing.

Plan was called OPLAN 8044 Revision 03.[79] This new plan was revealed thanks to a declassified STRATCOM document from a 2003 Freedom of Information Act request. Some of the content contained in this 26-page document is strikingly similar to the process outlined above. First is targeting and intelligence. Next is force allocation, followed by strike planning and then reviews and approvals.

Figure 7.6 Process of A Nuclear Strike



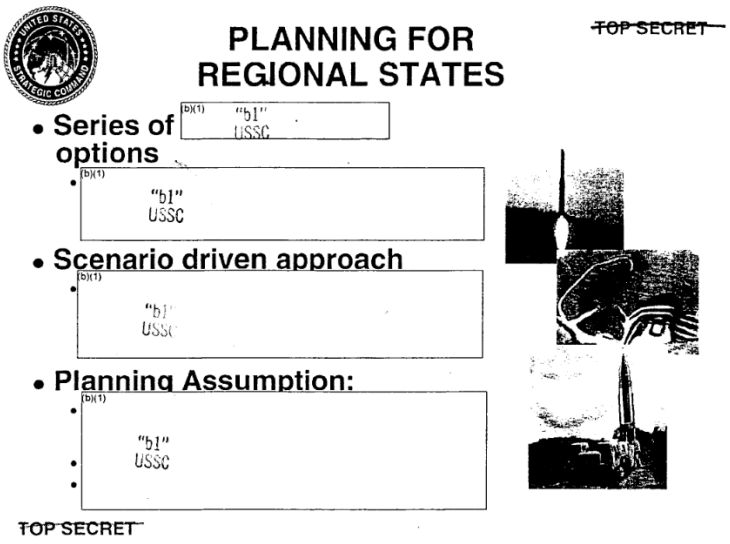
[78] An operation plan is **"**1. Any plan for the conduct of military operations prepared in response to actual and potential contingencies. 2. A complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data." *Joint Publication 5-0 Joint Operation Planning*, (Department of Defense, August 11, 2011), GL-13, accessed March 15, 2017, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

[79] Hans M. Kristensen, "White House Guidance Led to New Nuclear Strike Plans Against Proliferators, Document Shows," *Federation of American Scientists* (blog), November 5, 2007, accessed April 1, 2017, https://fas.org/blogs/security/2007/11/white_house_guidance_led_to_ne/#more.

[80] *Revision 03 Periodic Update*, (United States Strategic Command, November 5, 2007), 3, accessed April 1, 2017, https://fas.org/wp-content/uploads/2007/11/revision03.pdf.

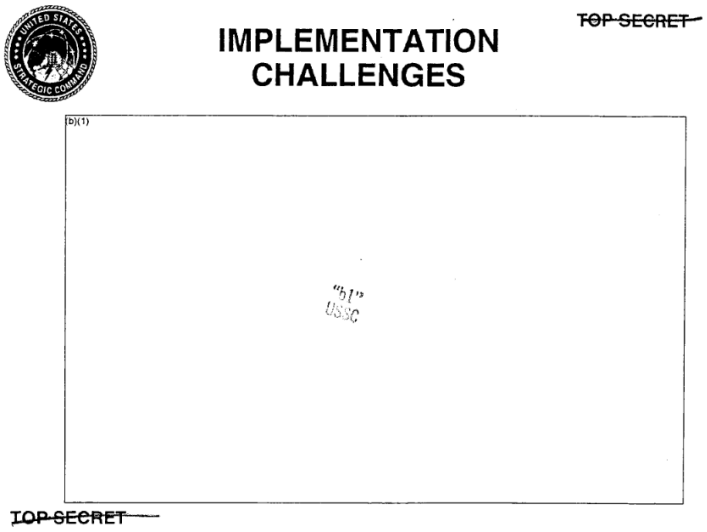
This document also had a slide that shed some insight as to how nuclear plans were formed. Perhaps this is also the thinking behind the deployment of cyberweapons.

Figure 7.7 Planning of A Nuclear Strike



There was also a slide allocating for difficulties. I imagine there is a similar slide when discussing cyberweapons.

Figure 7.8 Challenges of A Nuclear Strike



[81] *Revision 03 Periodic Update*, 11.

[82] Ibid., 106.

OPLAN 8044 Revision 03 also indicated that now the U.S. was targeting W.M.D. programs of seven 'regional states.'[83] The *Federation of American Scientists* determined that these countries were Russia, China, North Korea, Libya, Iraq, and in later reports, Syria and Iran were included.[84] Many interviewees identified China, North Korea, Iran, and Russia as the U.S.' adversaries in the cyber arena and one of the overarching findings from the interviews is that these weapons will be used covertly against nuclear programs of adversaries. *The New York Times* article about the covert cyberwar against North Korea further reinforces these statements.

After some modifications, by 2008, OPLAN 8044 Revision 03 was called "OPLAN 8010." Some of the options for nuclear weapons included "Basic Attack Options" and Selective Attack Options" which can take hours to months to alter.[85] These plans were ranked according to four 'levels' with a classification of Level 4 indicating that the plan was "fully executable."[86] This timeframe of a few months coincides with one interviewee who said a cyberweapon could take about four months to develop. Additionally, the ranking coincides with the ranking pointed out by some interviewees.

Owens, Dam, and Lin proposed what a "cyber-SIOP" might look like.[87]

---

[83] Kristensen, "White House Guidance Led to New Nuclear Strike Plans Against Proliferators, Document Shows."

[84] Ibid.

[85] Hans M. Kristensen, *Obama and the Nuclear War Plan*, (Washington, D.C.: Federation of American Scientists, February 2010), 5, accessed April 1, 2017, https://fas.org/programs/ssp/nukes/publications1/WarPlanIssueBrief2010.pdf.

[86] Ibid.

[87] There is also Austin Long's "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning."

> Translated into the cyberattack domain, a cyber-SIOP could similarly include a list of targets, a timetable on which the targets are to be attacked, and the cyberweapons that are to be used in the attack on those targets. Large-scale attack options might involve large attacks intended to create far-reaching effects, while small-scale options might be narrowly tailored to address a particular target set. Depending on the rules of engagement and the authorizations needed to execute such a plan, either STRATCOM or the geographic combatant command could carry out any one of these options, though it is likely that STRATCOM is largely responsible for planning regional attack options as well as attack options relevant to the entire globe.[88]

They explain that a key difference between a cyber-SIOP and a nuclear SIOP is that nuclear targets are fixed whereas cyber targets are not. "The operational implication of a cyber-SIOP is that a static planning process is unlikely to be effective, and both intelligence gathering and attack planning on possible targets in the various attack options would have to be done on a frequent if not continuous basis."[89] Thus, Owens, Dam, and Lin stated, "nuclear strategy does not provide guidance for cyber targeting."[90] However, some interviewees argued the opposite.

A former R.O.C. employee explained that after the plan is configured, these options are passed to U.S. Cyber Command. Then, they are passed to the Joint Task Force- Global Network Operations – Cyber, which he explained, is a committee with a lot of deputy meetings that goes through the packages. A former U.S. Cyber Command employee echoed this procedure stating that there is a "pretty refined process board that looks at this." "These decisions are made at the Deputies Committee, Principals Committee and White House." The Deputies Committee is "the senior sub-Cabinet interagency forum for consideration

---

[88] Owens, Dam, and Lin, 183 - 184.

[89] Ibid.

[90] Ibid., 224. *Joint Publication 3-12 (R) Cyberspace Operations* discusses the target development process on page IV-4.

of, and where appropriate, decision-making on, policy issues that affect the national security interests of the United States."[91] Its members are the deputies of the cabinet-level officials on the Principals committee. The Principals Committee is "the Cabinet-level senior interagency forum for considering policy issues that affect the national security interests of the United States."[92] The typical members are the Secretary of State, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff and the Director of National Intelligence. (The Trump administration changed this setup in January 2017 and again in April 2017.)[93]

This decision-making chain is related to the decision-making chain highlighted by the *Federation of American Scientists* that says first the White House commissions Presidential Study Directives.[94] The next level is the Office of the Secretary of Defense who conducts the "Guidance for the Employment of the Force,"[95] which is one strategic guidance document that combines the planning and objectives of several combatant commanders.[96] Then comes the Joint Strategic Capability Plan by the Joint Chiefs of

---

[91] Barack Obama, "Presidential Memorandum Organization of the National Security Council and the Homeland Security Council," January 28, 2017, accessed February 2, 2017, *The White House*, https://www.whitehouse.gov/the-press-office/2017/01/28/presidential-memorandum-organization-national-security-council-and.

[92] Ibid.

[93] Heather Landy, "With Bannon Out, Here's Trump's New National Security Council," *Defense One,* April 6, 2017, accessed August 11, 2017, http://www.defenseone.com/politics/2017/04/bannon-out-heres-trumps-new-national-security-council/136805/.

[94] Kristensen, "Obama and the Nuclear War Plan."

[95] Ibid.

[96] Patrick Sweeney, *A Primer for: The Joint Strategic Planning System (JSPS), Guidance for Employment of the Force (GEF), Joint Strategic Capabilities Plan (JSCP), the Adaptive Planning and Execution (APEX) System, and Global Force Management (GFM)*, (The United

Staff.[97] The Joint Strategic Capabilities Plan[98] encompasses the Guidance for Employment of the Force as well as other documents such as the National Military Strategy and the National Security Strategy to offer further detailed direction to the military and certain DoD agencies about how to meet the requests of the Secretary of Defense.[99] Next, Strategic Command weighs in with further guidance for the combatant commanders.[100] Last is the Joint Functional Component Command for Global Strike which provides "target development" and "strike planning."[101] For the cyber realm, a practitioner explained that if the cyberattack was carried out by the N.S.A., then it might have been carried out by the Joint Functional Component Command- Network Warfare unit.[102]

A former Remote Operations Center employee said, the cyber package needs unilateral signoff which was "difficult to get because the State Department and the C.I.A.

States Naval War College Joint Military Operations Department, January 22, 2016), 3, accessed April 2, 2017, https://wss.apan.org/s/JSOFUN/Shared%20Documents/GuidingDocuments/Guidance_for_Employment_for_the_Force_GEF_2016.pdf. Combatant commanders are "one of the unified or specified combatant commands" such as Africa Command, Central Command, European Command, Northern Command, Pacific Command, Southern Command, Special Operations Command, Strategic Command and Transportation Command. *DOD Dictionary of Military and Associated Terms*, 41. They are responsible for integrating cyber capabilities into military plans. *Joint Publication 3-12 (R) Cyberspace Operations*, III-6.

[97] Kristensen, "Obama and the Nuclear War Plan."

[98] The DoD defines this as "A plan that provides guidance to the combatant commanders and the Joint Chiefs of Staff to accomplish tasks and missions based on current military capabilities." *DOD Dictionary of Military and Associated Terms*, 134.

[99] Sweeney, *A Primer for: The Joint Strategic Planning System (JSPS), Guidance for Employment of the Force (GEF), Joint Strategic Capabilities Plan (JSCP), the Adaptive Planning and Execution (APEX) System, and Global Force Management (GFM)*.

[100] Kristensen, "Obama and the Nuclear War Plan."

[101] Ibid.

[102] This is what Owens, Dam, and Lin said on page 65.

were involved" "so they did not want to create negative implications for countries where we have diplomatic relations." One government official also discussed the "diplomatic impact of escalation." A former Remote Operations Center official stated that final approval can come from three places depending on the factors. If there were lower stipulations, General Alexander or the Secretary of Defense could give the final approval. He explained that the Director of Cyber Command can also take action unilaterally if the risk is low enough, but he noted this is considered active defense. If you recall from earlier, active defense means finding and stopping a threat. This broad definition is why it blurs with offense. However, he said, in most cases President Obama (and then he corrected himself to say the President) gives the final approval.

A Senior Cyber Policy Advisor reiterated that cyber operations require lots of approvals. "You will hear a lot at the DoD people saying 'authorities have not been delegated down to lower echelons' for cyber operations." He explained "If you are a company commander who is deployed to Helmand, you do not need to ask permission in order to shoot back." This is different for cyber operations. He stressed that authorization for a cyber operation is "closer" to nuclear authorization than say "a raid in Afghanistan"; however, as to when it is authorized, he said, "I think when it is authorized is not as a last resort" [because it is a humane alternative].

Be that as it may, once approved, according to a former Remote Operations Center employee, an Air Tasking Order (ATO), now called a Cyber Tasking Order (CTO), is issued. He explained that an ATO contains information regarding how to conduct the strike. He disclosed that this is identical to how the nuclear strike process is conducted under Title 10 authority. Owens, Dam, and Lin, proposed what a CTO might look like. "A cyberattack

tasking order could support other combat operations and other combat operations could support cyber operations which could be their principal role."[103] They said first intent has to be established. Next is target development followed by a weapons assessment. Next is "force execution" where everything is integrated. The last step is a "combat assessment" where effectiveness is weighed against objectives.[104] Their proposals, which were made in 2009, seem consistent with the process outlined above.

In summary, according to the interviewees, the decision-making process for deploying a cyberweapon is somewhat defined and not unlike the decision-making process involved in nuclear warfare, although crossing the nuclear threshold would almost certainly constitute more drastic action than a cyberattack. Furthermore, unsurprisingly, more serious cyberwarfare requires higher-level clearances which is complicated by many advisers and considerations. So perhaps the convoluted decision-making process has blockaded the U.S. from deploying its cyberweapons or perhaps the U.S. is getting better at handling their covert cyberweapons.

LOOKING AHEAD

Although there are currently 27 Combat Mission Teams that "provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations,"[105] I asked the interviewees, "What role do you think cyberweapons might play in concurrent military operations?" In this dissertation,

---

[103] Owens, Dam, and Lin, 183.

[104] Ibid.

[105] "The Department of Defense Cyber Strategy," *Department of Defense*, accessed April 2, 2017, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

I used "force multiplier" and "conventional enabler" interchangeably since the academic term was "force multiplier" and "conventional enabler" was the U.S. Cyber Command term. CONVENTIONAL ENABLER was a variable tested in Chapter 5.

One cybersecurity official answered, "There will not be a single future military campaign that does not have a cyber component." He added, "Whether we are going in beforehand," "conducting espionage, propaganda or staging." A prominent think tank member reiterated this same notion– there will "not be military operations without cyber operations." He alluded it may not be destructive but there will be disruptions. One academic advanced a corresponding idea that this is a "cool war" which means more disruption and less destruction. (The notion of a 'cool war' was discussed in Chapter 1.)

A Senior Cyber Policy Advisor said, "Cyber should support the full spectrum."[106] It is a "multi-domain engagement." A current advisor to the N.S.A. commented that cyberweapons are "one of many tools in a toolkit"[107] and cyber's combination with other tools is increasing. Another government official said he would be surprised if these weapons were not integrated into the toolset. A cybersecurity official predicted cyberweapons will be used in actual engagements like Iraq or Afghanistan if troops are on the ground. A former T.A.O. employee suggested in future invasions the U.S. should use cyber capabilities first in order to disable the infrastructure so afterwards they could re-enable this infrastructure instead of spending billions to rebuild it. This is similar to the idea (and advantage) of reversibility discussed earlier.

---

[106] *Joint Publication 3-12 (R) Cyberspace Operations* also called for integration. *Joint Publication 3-12 (R) Cyberspace Operations*, I-6. In fact, this document said cyberweapons are most effective in conjunction, not stand-alone. *Joint Publication 3-12 (R) Cyberspace Operations*, II-10.

[107] Owens, Dam and Lin discussed this on page 163.

A Legal Advisor I spoke with pronounced, “hammers are not much good hanging on the wall.” In his opinion, while there is an unpredictability of the effects of cyber tools, governments are growing more comfortable with them, which suggests they have better collateral damage estimates. One academic observed that cyberweapons can be used for a shorter, swifter and less bloody conflict, so he was a proponent of “bitzkreig” rather than “blitzkrieg.” However, a journalist believed that, although cyberweapons are revolutionary because they changed the landscape of warfare, these capabilities will “not replace kinetic warfare.” A government official also cautioned that these weapons are “not total game-changers.”

Nevertheless, some interviewees envisaged these weapons being used more visibly and frequently. One academic said, “Personally, I would like it if the U.N. blue helmets sat at screens and could have stopped the hate radio in Rwanda in 1994” but he said the U.N. is not on the verge of anything like that. A former Remote Operations Center employee said, these capabilities “should be more prevalent.” “Right now it is a cherry on top of military operations.” “It is almost an afterthought.” A former Cyber Command official said, there is increasing usage of tactical cyber capabilities on the battlefield. However, he claimed these tools are still in the nascent stages.

I. Dual-Hat Split

Some of the interviewees and I also discussed the split of the dual-hatted structure of the N.S.A. and Cyber Command that the Obama administration established in December 2016. One academic told me he did not support a split because the technical expertise that the N.S.A. has is relevant. A former T.A.O. official termed this “stupid” because it will “take Cyber Command a decade to develop the manpower with the right technical

intelligence." He stated, "the U.S. does not go to cyber tools every minute of every day so they will lag behind those doing espionage." An Army reservist predicted this will "hurt the N.S.A. financially because the DoD has endless pockets" and it will also limit operational flexibility since the N.S.A. is not the military.

However, a former Senior Cyber Policy Advisor urged not to overstate the dual-hat role because the only personnel that the N.S.A. and Cyber Command shares is the director. Additionally, Cyber Command does not use all of the N.S.A.'s stuff, he said. He judges that at its inception, the dual-hat structure was a good idea because Cyber Command is a "young and immature organization" and "is being asked to do a lot." "It is the first organization of its kind dedicated to both defense and offense globally." He explained that if Cyber Command had been asked to be by itself, it would have been further behind. So the goal was to avoid investing "two times to get the same capabilities." He claims officials agreed that this was never supposed to be a permanent arrangement. The two agencies should in due course be separate because it is better for the ethos of the N.S.A., which operates clandestinely and takes ten years to develop capabilities whereas the military needs to move fast, he explained. Moreover, the military creates a "loud" impact and does not care about losing tools. Thus, he proposed we should "think of cyber tools as ammunition." One prominent think tank member also believed in splitting the dual-hatted role.

CONCLUSION

This chapter showcased the major findings of my field research. After interviewing 22 people, I confirmed that although there were some mixed feelings about the term cyberweapon, there is a "typology of cyber policy options." A former T.A.O. official summed it up best when he said an effective cyberattack is covert, has a real-world effect and results in inflicting pain. The decision-making process is based at least loosely on the nuclear strike process. Additionally, the president does retain control over most cyber activities and there is "high politics at play."

One interviewee said, the impact of the Snowden leaks was significant because it showed other countries that there was a capability gap so it energized them. (He also said the Snowden leaks "devastated multi-billion dollar programs from which we are still recovering.") A cybersecurity official recapped this claim stating Stuxnet resulted in a multiplying effect because all these countries are now involved and the ensuing chaos could be a nightmare. "There is a concern of the knock-on effect," he said.

Some interviewees confirmed that proxy wars may be waged and a few interviewees pointed out specifically in Syria and Yemen. Iran, China, Russia and North Korea were confirmed as the U.S.' adversaries in the cyber arena as well as possible targets of U.S. cyberweapons. Furthermore, any adversary that poses a viable threat especially those with a weapons of mass destruction program are potential targets of these weapons. Additionally, cyberweapons will continue to be integrated into conventional military plans.

All of the proposed conditions that the interviewees mentioned (access, legality, collateral damage, retaliation, reversibility, reliability, attribution, and cost), were discussed in previous chapters but the interviews demonstrated that there were many

different conditions associated with the case studies. The considerations were operational parameters, geopolitics, leverage, purpose, vulnerability, reliability, covert, availability, legality, probabilities of success, capability loss, escalation, sovereignty, time, and restoring confidence. The interviews also generated some interesting ideas about influence operations and made me delve further into Title 10 versus Title 50 of U.S. code as well as the nuclear strike process. Additionally, these findings tested many of the variables in both the qualitative and quantitative chapters as well as many of the hypotheses.

When I interviewed an academic in February, he cautioned about my level of analysis, claiming that I needed to speak to "the guys at the top." From the outset, I did attempt to interview a range of individuals from different professional settings so that my findings would be representative of a wider population. Nevertheless, I considered his advice and did end up interviewing a number of relatively high-ranking individuals on the frontiers of cyber capabilities. One thing to note however, is that the one "current" government official I spoke with in March 2017 no longer works for the government.

One of the benefits of doing mixed-methods research is to reinforce or see if there are discrepancies in the results. At the end of the previous chapter, I stated I would update my proposed decision board based on the interviews. I will do this in the next chapter. However, some of the interviewees stressed that these capabilities are supposed to be specific, not generalizable. Thus, this is one way in which the findings impacted my research. Additionally, I think almost no one said they used the term cyberweapon in their line of work and clearly this dissertation utilizes this term.

These findings were largely based on the actions of the Obama administration. Obviously, the U.S. now has a new administration. When I began this project I assumed

that rational decision-making would continue to prevail. A former Cyber Command official told me the "intelligence community does not want ham-handed people." However, as I spoke with people, read about the Yemen raid and reviewed Aldridge's book, this absence of rationality kept sticking out like a sore thumb. A Senior Cyber Policy Advisor I spoke with said, "something to watch in the new administration is their decision-making and authority to delegate will be greater." "So it is entirely different," he stated. I think the Yemen raid proved that as the article claimed the Trump administration "has said that it wants to speed the decision-making when it comes to such strikes, delegating more power to lower-level officials so that the military may respond more quickly."[108] The Trump administration has also expressed their desire to use more offensive cyber capabilities, so will the decision-making process be hastened?

The interviewees and I did attempt to discuss the new administration. One journalist claimed, "the Trump administration is over-militarizing cyber" which leads to the possibility of blowback and retaliation. It will be interesting to see how the decision-making and conditions change. Although the new administration does not seem to be all that forthcoming about its actions, if there is increased usage, perhaps that is how we will learn more about the conditions of deployment.

The next and final chapter in this dissertation is the Discussion and Conclusion where I explain how the interviews relate to the findings generated from the Quantitative Analysis and Decision Matrixes chapters as well as how the interviews apply to poliheuristic theory overall. For instance, now that we know deployment is based on the nuclear strike process, does this mean poliheuristic theory is an inadequate lens to analyze

[108] Schmitt and Sanger, "Raid in Yemen: Risky From the Start and Costly in the End."

the decision-making process? I wrap up with some policy implications, final reflections and suggested future research.

Chapter 8

DISCUSSION AND CONCLUSION

At the beginning of this dissertation, I proposed that in order for the U.S. to deploy a cyberweapon in a first strike, there has to be a combination of conditions. The target country has to be an adversary or at least a perceived adversary. There also has to be a perceived threat to the U.S. or its interests. The cyberweapon has to have the potential to destroy the intended target which cannot be reached by other conventional means and the cyberweapon has to minimize collateral damage. I also proposed that the U.S. will likely deploy a cyberweapon in a first strike in order to avoid a conventional war. These six hypotheses were tested in chapters 5 & 6 and explored further during the interviews. The following charts summarize the variables, operationalization, and findings across all chapters.

Table 8.1: Comparing Hypothesis 1 Across Chapters

Hypothesis	**Chapter 5- Quantitative Analysis**	**Chapter 6- Decision Matrixes**	**Chapter 7- Interviews**
Hypothesis 1: The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary.	Variable Name: PERCEIVED ADVERSARY Operationalization: Was the cyberweapon targeting a real or perceived adversary (Russia, Iran, China, North Korea)? Finding: False	Variable Name: NOT TESTED	Variable Name: PERCEIVED ADVERSARY Operationalization: "Can you think of one or more countries (or perceived adversaries) that the U.S. might use a cyberweapon against as a first strike?"

Hypothesis	Chapter 5- Quantitative Analysis	Chapter 6- Decision Matrixes	Chapter 7- Interviews
			Finding: Challenged

Chapter 5 surprisingly suggested that there was a weak relationship between DEPLOYED and PERCEIVED ADVERSARY which meant the following hypothesis might not have been true: *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary.* This result was explored during the interviews with the question: Can you think of one or more countries (or perceived adversaries) that the U.S. might use a cyberweapon against as a first strike? And why? The interviews challenged this finding since one of the interviewees revealed that he was coordinating the government's cyber policy strategy for one major non-adversary. Additionally, even though many of the people I spoke with confirmed that Russia, China, Iran and North Korea were the U.S.' main adversaries in this arena, even allies can be attacked. Thus, these statements reinforce this finding from Chapter 5 which means perhaps the weak relationship between DEPLOYED and PERCEIVED ADVERSARY was not that surprising after all. Even though the hypotheses were built off of the basic premise that the U.S. will use a cyberweapon against an adversary, I do not think these findings invalidate the rest of the hypotheses. I think this result implies that it is not enough to use a cyberweapon against an enemy. There has to be other conditions, which leads me to the second hypothesis.

Table 8.2: Comparing Hypothesis 2 Across Chapters

Hypothesis	Chapter 5- Quantitative Analysis	Chapter 6- Decision Matrixes	Chapter 7- Interviews
Hypothesis 2: The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its perceived interests.	Variable Name: NOT TESTED	Variable Name: THREAT Operationalization: Did these adversaries pose a threat? Finding: Plausible	Variable Name: THREAT Operationalization: "Can you think of a situation in which the U.S. might use a cyberweapon as a first strike?" Finding: Plausible

THREAT was not tested in Chapter 5 but it was tested in both the Decision Matrixes and Interviews chapters. In the Decision Matrixes chapter, THREAT was tested in all 13 cases and THREAT was true 6/13 times. This outcome clarified the finding in Chapters 5 & 7 that suggested it is unlikely that the U.S. will deploy a cyberweapon against a perceived adversary. There has to be a threat. In fact, one of the overarching findings from the interviews was that these weapons will be used against W.M.D. programs of adversaries. Therefore, perhaps the following hypothesis might be plausible– *the U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary that poses a viable threat to the U.S. or its interests*.

Table 8.3: Comparing Hypothesis 3 Across Chapters

Hypothesis	Chapter 5- Quantitative Analysis	Chapter 6- Decision Matrixes	Chapter 7- Interviews
Hypothesis 3: The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they believe they can destroy the intended target(s).	Variable Name: MILITARY SECTOR Operationalization: Was the cyberweapon targeting the military sector (air defense systems, military communications systems, or "weapons capabilities")? Finding: Null	Variable Name: This is the Military dimension in the decision matrix. Operationalization: The military dimension considers "capabilities, logistics, and the likelihood of success." [1] Finding: Plausible	Operationalization: Against what sort of target or targets might the U.S. use a cyberweapon against as a first strike? Finding: Plausible

In the Quantitative Analysis chapter, MILITARY SECTOR did not have a significant relationship with the other variables. Thus, the result was null. In the Decision Matrixes chapter, the Military dimension represented the military's considerations. In 7/12 cases, a cyberweapon was the preferred choice and it was deployed. Thus, I claimed this hypothesis might be plausible. These findings raised an interesting question that was explored during the Interviews chapter: "Against what sort of target or targets might the U.S. use a cyberweapon against as a first strike?" The interviewees said, a cyber capability can take out another country's air forces, command-and-control, jam IEDs, and confuse the enemy. One cybersecurity official said, for a government, the target has to be a level of criticality. Another cybersecurity official who used to work for the government explained

[1] David J. Brulé, "The Poliheuristic Research Program: An Assessment and Suggestions for further Progress," *International Studies Review* 10, no. 2 (June 2008): 271, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/25481960.

that the "lifelines" or critical infrastructure of a country are "energy, water, telecommunications, emergency services, financial services and information technology." He stated attacks against these would be a nation-state level attack but again, this is subjective. This is a problem in the cyber realm because the targets are largely unknown whereas in the real world, it would be clear if a hospital was bombed. Additionally, military attacks are only allowed against "military targets."[2] I will discuss the Military dimension in more detail later but, the Interviews chapter suggested that this hypothesis was plausible– *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they believe they can destroy the intended target(s)*. Since there were differences in the findings, I think further research is needed to confirm whether this hypothesis is indeed plausible.

Table 8.4: Comparing Hypothesis 4 Across Chapters

Hypothesis	**Chapter 5- Quantitative Analysis**	**Chapter 6- Decision Matrixes**	**Chapter 7- Interviews**
Hypothesis 4: The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if they cannot use troops, drones or airstrikes.	Variable Name: OTHER ALTERNATIVES Operationalization: Were other alternatives (troops, airstrikes or drones) capable of accomplishing this goal? Finding: Plausible	Variable Name: ACCESS Operationalization: Was the intended target in a hard-to-reach area? Finding: Plausible	Variable Name: ACCESS Operationalization: "Can you think of any conditions under which the U.S. might use a cyberweapon as a first strike?" Finding: Plausible

[2] *Joint Publication 3-12 (R) Cyberspace Operations*, (Department of Defense, February 5, 2013), III-10, accessed March 15, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Chapter 5 suggested there was a negative relationship between DEPLOYED and OTHER ALTERNATIVES implying that this hypothesis was plausible. In the Decision Matrixes chapter, ACCESS was tested in all 13 cases and it was true in 11/13 cases. This outcome was further supported by the Interviews chapter where interviewees said, a cyberweapon can have an impact on bothersome targets where the U.S. does not have a physical chance to attack and where you cannot send troops. Thus, I can state with some confidence that this hypothesis is plausible– *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary if the intended target(s) are out of the reach of troops, drones or airstrikes.*

Table 8.5: Comparing Hypothesis 5 Across Chapters

Hypothesis	**Chapter 5- Quantitative Analysis**	**Chapter 6- Decision Matrixes**	**Chapter 7- Interviews**
Hypothesis 5: The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize casualties.	Variable Name: COLLATERAL DAMAGE Operationalization: Was the U.S. concerned that this cyberweapon could have other consequences? Finding: Plausible	Variable Name: COLLATERAL DAMAGE Operationalization: Will this minimize casualties? Finding: False	Variable Name: COLLATERAL DAMAGE Operationalization: "Can you think of any conditions under which the U.S. might use a cyberweapon as a first strike?" Finding: Plausible

Chapter 5 also suggested there was a strong negative relationship between DEPLOYED and COLLATERAL DAMAGE. This finding suggests that if a cyberweapon is deployed, it is highly unlikely there were serious concerns about collateral damage. This seems plausible because the Literature Review stated that one of the benefits of using these

weapons is to minimize collateral damage. So if there are other alternatives, naturally one will consider the collateral damage in order to decide whether the use of a cyberweapon will be more effective. However, in the Decision Matrixes chapter, COLLATERAL DAMAGE was only tested in 10 cases and out of those 10 cases, it was true three times. Thus, I asked the interviewees "Can you think of any conditions under which the U.S. might use a cyberweapon as a first strike?" Many interviewees claimed, the U.S.' goal is to minimize civilian casualties and that cyber capabilities should be used as a "humane alternative." A Legal Advisor I spoke with stated, if for example, an "adversary puts their command-and-control in a densely populated area, kinetic weapons would cause a loss of life so cyberweapons would be good here." He added, "If political conditions are such that these weapons can result in 0 civilian casualties, then yes" they will be used. A former T.A.O. employee I spoke with disclosed that he is a proponent of using these capabilities because these tools can save lives on both sides of the conflict. This was Dorothy Denning's argument noted in the Literature Review. Thus, even though the Decision Matrixes chapter suggested that COLLATERAL DAMAGE was false, both the Quantitative Analysis and Interviews chapters suggested that the following hypothesis might be plausible– *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary in order to minimize casualties.* Since there were differences in the findings, I think further research is needed to confirm whether this hypothesis is indeed plausible.

Table 8.6: Comparing Hypothesis 6 Across Chapters

Hypothesis	Chapter 5- Quantitative Analysis	Chapter 6- Decision Matrixes	Chapter 7- Interviews
Hypothesis 6: The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."	Variable Name: NOT TESTED	Variable Name: VIOLENCE Operationalization: Was the cyberweapon a way to end or avoid violence? Finding: False	Variable Name: PROXY WAR Operationalization: "Do you think a cyberweapon might be particularly useful as a tool for initiating, sustaining or ending a proxy war?" Finding: Plausible

This variable was not tested in Chapter 5. In the Decision Matrixes chapter, this variable was tested eight times and was true twice. Thus, it is probably unlikely that this hypothesis is plausible. But in the Interviews chapter, many interviewees said these tools can be used when you want to avoid an all-out war. In fact, a former T.A.O. official stated this was a condition for using these weapons in a first strike since these weapons are mainly to prevent war although he acknowledged that proxy war is still war. However, a prominent think tank member disagreed, claiming this is "proxy conflict" not war. One academic quoted Kenneth Waltz, "mutual fear of big weapons may produce, instead of peace, a spate of smaller wars"[3] suggesting that cyberweapons may result in smaller wars. Therefore, the Interviews chapter suggested this hypothesis was plausible. I would like to point out that I used the term proxy warfare to mean warfare short of a conventional use of force however,

[3] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 1959), 236.

the interviewees said proxies are used to wage warfare. Since there were differences in the findings, I think further research is needed to confirm whether this hypothesis is indeed plausible.

Although my hypotheses were carefully formulated and well-supported overall, they could not fully capture the nuances or complexities of the responses I elicited from professionals during the interviews. So future research may require more refined hypotheses, but this is almost impossible because the "real world" does not fit neatly into if/then propositions. Furthermore, the more complex a hypothesis is, the more difficult it is to test, confirm, or prove. Nevertheless, I would like to have conducted more interviews in order to explore hypotheses 1, 3, 5 and 6 in more detail.

COMPARING THE INTERVIEWS TO THE QUANTITATIVE ANALYSIS

Now that we have discussed how the findings compare across chapters, let us dig deeper to explore how the interviews compared to the quantitative findings. First of all, the interviewees and I did not discuss all of the cases in great depth. Thus, the interviews do not have any significant impact on the coding except for possibly changing the DEPLOYED values for Libya and Syria which in that case, would be a big deal because this would re-group the clusters.

One finding specific to both the Quantitative Analysis and Interviews chapters was in regards to the CONVENTIONAL ENABLER variable. In Chapter 5, the cluster analysis uncovered a negative correlation between DEPLOYED and CONVENTIONAL ENABLER. This correlation coefficient indicated that these cyberweapons were not a force multiplier but rather a standalone operation. Therefore, this finding contradicted the

statements by USCYBERCOM and others that cyberweapons are a component of conventional warfare. However, many of these weapons were created before USCYBERCOM and U.S. cyber doctrine. Thus, this finding was explored during the interviews with the question: "What role do you think cyberweapons might play in concurrent military operations?" A former R.O.C. employee suggested cyberweapons are a good idea in order to "prep the battlefield" where before troops moved in, there is a suppression of military infrastructure. The DoD term for this is "operational preparation of the environment." A "Cyber Operational Preparation of the Environment," "Replaces: CNE or CNA when used specifically as an enabling function for another military operation."[4] Thus, the interviews negated the finding from the Quantitative Analysis chapter. Again, since there are discrepancies in the findings, I think this is another area for suggested future research.

Another negative correlation revealed in Chapter 5 was the relationship between COVERT and PERCEIVED ADVERSARY. This finding suggests that if the cyberweapon is targeting a perceived adversary, it is likely that the cyberweapon is not covert. This seems plausible because if the U.S. is targeting someone who is an adversary, then it is possible that this would not be a covert attack. This finding raised an interesting question in regards to the Five Eyes alliance that was explored during the interviews: "Do you think other countries in the Five Eyes alliance would be likely to be informed before the U.S. were to use a cyberweapon in a first strike?" The interviews were split between those who thought the Five Eyes would be informed and those who thought the Five Eyes would not be

[4] James E. Cartwright, *Joint Terminology for Cyberspace Operations*, (Washington D.C.: Department of Defense, 2010), 7, accessed March 18, 2017, http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

informed. One of the interesting responses was when a former T.A.O. official said, "no comment," which might imply yes, the Five Eyes would be informed. What is somewhat clear, at the very least, there is some collaboration between the U.S. and the U.K. One government official said, he suspects that the Five Eyes might be informed or at least maybe they should be due to the collective nature of cyberspace. He stated there are "diplomatic démarches where the botnets are located" so "how you build alliances and the use of tools complicates that." This notion speaks to the diplomacy dimension of poliheuristic theory that will be discussed in the next section. As I was writing this chapter, *The Washington Post* reported that there was bickering among U.S. officials over the extent of informing allies during the U.S. offensive cyber operation against ISIS in 2016 (apparently called "Operation Glowing Symphony.")[5] Thus, I suppose my research was asking a few right questions. One other thing to note is that when I started this project, the U.K. was still a part of the European Union. Now, it is unclear if there will be implications for the Five Eyes because of the Brexit referendum. I suspect there will not be significant implications for the Five Eyes but this is another area for suggested future research.

A result from the Quantitative Analysis chapter that reinforced themes discussed in the Literature Review was the finding that suggested there is a positive relationship between DEPLOYED and COVERT. This echoed the notion that COVERT is a possible condition for deploying cyberweapons. The interviews supported this finding. One former T.A.O. official summed it up best when he said an effective cyberattack is covert, has a

[5] Ellen Nakashima, "U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies," *The Washington Post,* May 9, 2017, accessed May 10, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.b4d7df09ba88.

real-world effect and results in someone experiencing pain. Of course if you are at war, then you probably do not care about people knowing about this capability and actually want to flex your muscles, said one interviewee. This was an interesting thought that emerged and was explored further during the interviews with the question– "Is cyberwarfare successful if we do not know about it?" One cybersecurity official said, it does not matter if people know or not whereas an academic said, part of the perfection of a cyberweapon is that the victim may not know if it was a country who was the attacker. You cannot anticipate the situation, he said. However, another interviewee stated, it is not that we do not know it is coming, "we are just not prepared." He said, we are focused on big operations such as the Chinese turning off our power grid but the flip side is that a non-rational actor like North Korea or a terrorist might not care. "We don't have the capability to do so [not care]."

In summary, I think the interviews helped clarify some of the quantitative findings and raised some interesting ideas for future research. Thus, there was a significant benefit to using mixed- methods.

COMPARING THE INTERVIEWS WITH POLIHEURISTIC THEORY

An Army reservist explained the decision over deploying a cyberweapon is "gamesmanship" where you have to decide which option is more important. This thought coincided with poliheuristic theory, the main theory behind this dissertation. The interviews were helpful in providing additional information for the alternatives, dimensions and consequences delineated by poliheuristic theory. Since I spoke with former military officers, I was able to glean a few military perspectives for the Military dimension.

A former Cyber Command official said, in many ways, cyber capabilities are harder to use because they are probabilistic. You think you could turn out the lights but what if someone patches right before? "Warfighters do not like uncertainty," he stated. Similarly, another point of contention was the autonomous vs. remote operator consideration since you are not 100% sure how the cyberweapon will work on its own and if you are depending on a human operator, there are also risks, not to mention the legal ambiguities involved. Furthermore, there is the "problem of capability revelation" where once a capability is used, it becomes mostly obsolete.

Another consideration from the Interviews chapter that applied to the Military dimension was the "process to request a battlefield effect and time were not aligned." A government official said, a complication is that a cyber tool takes pre-planning so you have to look at the immediacy of the operation. A cybersecurity official explained that it takes time to create a "tailored capability." However, another cybersecurity official claimed, moving this capability is faster than moving a carrier. Another cybersecurity official told me that a cyberweapon takes about 4 months from order to build. An Army reservist I spoke with said, "what are the acceptable areas of mission space and lead time?" There is no "consistent timeframe," he said. This can impact the likelihood of deployment.

Other interesting findings from the Interviews chapter in regards to the Military dimension arose from discussion of the cases. I will deliberate on this below but overall, the interviewees talked about the goals of Stuxnet and the capabilities of the Iraq (2007) case. In the Libyan, Pakistani and Syrian cases, the interviewees discussed the likelihood of success. As for the North Korean and Russian cases, many interviewees wanted the U.S. to use their cyber capabilities. As for ISIS, a former Senior Cyber Policy Advisor stated,

"ISIS has no air defense systems to attack through cyber means" so the types of targets are different which means the gain/loss calculus is different.

The economic dimension of poliheuristic theory weighs the cost of carrying out a decision, not only the cost of implementation but also its likely financial and economic impact.[6] I covered this dimension by asking the interviewees, "Is it possible in any meaningful sense to estimate "the cost" of developing a cyberweapon?" Many interviewees saw cyberweapons as a cheaper alternative but some pointed out "the cost of the attack does not indicate the damage." This means that while the cost of implementation is lower than other military methods, the economic and financial impact can be hefty. One interviewee I spoke with who works in the cybersecurity insurance market explained that right now cyber insurance is $3.5 billion and will go up to $20 billion by 2025. The asking cost for underwriting some critical infrastructure is $500 billion to one trillion, he said. This is a big amount for cybersecurity insurance companies to underwrite which is why cyberattacks must be taken seriously. I think the cybersecurity insurance market is another area for future research.

Sanctions are one of the preferred tools in the decision-making apparatus. A former Cyber Command official said sanctions might be a possible response to a cyberattack and another government official agreed, arguing cyber sanctions can be effective. However, one cybersecurity official stated that sanctions are out of the cyber domain. One academic was certain that sanctions would be ineffective against Putin, and a former T.A.O. employee frankly declared that U.S. sanctions against North Korea were a waste of time.

---

[6] Kanishkan Sathasivam, "'No Other Choice': Pakistan's Decision to Test the Bomb," in *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making* (New York: Palgrave Macmillan, 2002): 68.

The most interesting findings in regards to the Interviews and Decision Matrixes chapters dealt with the diplomatic and political dimensions. The diplomatic dimension highlights the distribution of power and interactions among "major actors on the world stage."[7] Many interviewees mentioned diplomatic considerations as being very important when it comes to the decision-making process surrounding the deployment of a cyberweapon. An Army reservist said a cyberweapon is a diplomacy tool. Some other interviewees said cyberweapons can bring countries to the table. Interestingly, in the Decision Matrixes chapter, the diplomacy dimension was the least important dimension, but the interviews provided a compelling counterargument.

Some variables that are used to evaluate the political dimension are "public opinion polls, the leader's popularity, the state of the economy, [and] domestic opposition."[8] In order to evaluate the political dimension, which focuses on domestic politics, I asked the subjects "Do you think public opinion polls might factor into the U.S.' decision to use a cyberweapon as a first strike? The current state of the U.S. economy?" Most of the interviewees said public opinion polls did not matter very much. However, the Senior Cyber Policy Advisor I spoke with said, "public opinion is on the mind of the president and his top political advisors when using force" but in his capacity, public opinion was not among their considerations. "We try to provide the best advice" so it "does not factor into our work." Thus, perhaps this statement contradicts the assumption of poliheuristic theory that domestic politics is an influential dimension in the decision-making process.

---

[7] Sathasivam, "'No Other Choice': Pakistan's Decision to Test the Bomb," 65.

[8] Alex Mintz, "The Decision to Attack Iraq: A Noncompensatory Theory of Decision Making," *The Journal of Conflict Resolution* 37, no. 4 (December 1993): 600, http://www.jstor.org.proxy.libraries.rutgers.edu/stable/174541.

Therefore, is the poliheuristic theory of decision-making still a relevant theory to use for explaining the conditions under which the U.S. did and will likely deploy a cyberweapon? Yes, because as we will see below, there are other ways of measuring the political dimension.

One of the research instruments of poliheuristic theory is a decision matrix. In Chapter 6, I retroactively applied poliheuristic theory to the 13 case studies analyzed in this dissertation in order to assess the process validity of previous U.S. decisions about using a cyberweapon. Through the use of a decision matrix, I was able to understand the conditions that factored into the U.S.' decision-making calculus when it came to deploying or not deploying a cyberweapon. The following decision matrixes compares the content of the proposed decision matrixes to the information gathered from the interviews. During the interviews, I asked the participants, "What are the advantages of using a cyberweapon rather than U.S. troops, special forces, drones or airstrikes? Disadvantages?" This question was particularly helpful in explaining the consequences that resulted from each alternative. The interview content is bolded in order to differentiate between my proposals and the interviewees. Unfortunately, we did not discuss all of the cases in great detail so there are some gaps. For instance, I do not have updated decision matrixes for Nitro Zeus, Shotgiant, Turbine, Quantum or Iraq (2003).

I. Stuxnet

In Chapter 6, I created the following choice set for Stuxnet and I think the interviews did not alter this choice set.

(1) do nothing

(2) continue talks

(3) increase sanctions

(4) implement airstrikes

(5) deploy a cyberweapon

Alternative 1: The U.S. could do nothing, anticipating that Iran is not trying to obtain a nuclear weapon.

Alternative 2: The U.S. could continue discussions to get Iran to agree to abandon its nuclear program.

Alternative 3: The U.S. could implement more sanctions to force Iran to agree to abandon its nuclear program.

Alternative 4: The U.S. could launch airstrikes against Iranian nuclear facilities.

Alternative 5: The U.S. could use a cyberweapon against Iran to destroy their nuclear facilities.

The decision matrix consists of four dimensions and five alternatives. I listed the dimensions in order of increasing importance.

Table 8.7: Updated Decision Matrix for Stuxnet

Alternatives

Dimension		Do nothing	Continue talks	Increase sanctions	Launch U.S. airstrikes	Deploy a cyberweapon
	Military	If we do nothing, Iran could get a nuclear bomb. This is unacceptable.	There are no implications for the military if we continue talks but are they really working?	There are no implications for the military if the U.S. increases sanctions but are they really working?	We cannot launch airstrikes since we are unsure of the exact location of Iran's nuclear facilities; the facilities are buried deep underground and an airstrike against Iran could have wider political ramifications such as the potential to start a war and risk retaliation and casualties.	This is the chance to test out a new weapon that could be deployed covertly and precisely and would strike at the heart of the problem without putting troops on the ground. However, there could be repercussions if the weapon leaks out. **-This is the "only option" based on the operational parameters.** **-We can use this to destroy uranium centrifuges.** **-There is a correlation between sophisticated and discoverable.** **-Will this be effective?** **-What is the goal?** **-Is there a strategic benefit?**

Dimensions		
Diplomatic	Political	
If we do nothing, the Israelis said they would launch an airstrike thereby potentially dragging us into a bigger conflict.	The global balance of power will shift if Iran were to acquire a nuclear bomb. Our greatest ally, Israel would be threatened as would the entire Middle East.	Do nothing
We should continue talks because this is the best diplomatic solution.	We could continue talks but are they really working?	Continue talks
We could increase sanctions because they are working.	We could increase sanctions but are they really working?	Increase sanctions
We should not launch airstrikes because airstrikes could result in casualties, be inaccurate, or the U.S. could be seen as overreaching.	We cannot implement airstrikes because we do not know where the facilities are and there could be casualties and retaliation.	Launch U.S. airstrikes
Are we willing to unleash a new weapon when we do not know exactly how this weapon will work? There could be repercussions if the weapon leaks out. **-The goal was never to destroy Iran's program but to buy time for diplomacy and sanctions.** **-This can be used as leverage to bring Iran to the negotiation table.**	We could do this covertly so the public will not know but, there could be repercussions if the weapon leaks out. Plus, do we want to work with the Israelis? **-This was not supposed to go public.**	Deploy a cyberweapon

		Do nothing	Continue talks	Increase sanctions	Launch U.S. airstrikes	Deploy a cyberweapon
Dimension	Economic	There are no economic implications if we do nothing.	There are no economic implications if we continue talks.	We should increase sanctions. They are effective.	Airstrikes cost millions of dollars.	Stuxnet took a lot of time, money and resources to create. (Some say $100 million.[9]) Once it is used, it cannot be used again but, it would be a way to effectively destroy our target. **-This costs $500,000 - one million.**

When comparing the interview content with my proposals, one thing that is different is cost. One million dollars is significantly less than $100 million dollars. I think the more important point though, is that there were different goals across the dimensions. For instance, in the military dimension, the goal was for Stuxnet to destroy centrifuges. In the diplomatic dimension, Stuxnet's goal was to bring Iran to the negotiation table. In the political dimension, Stuxnet was not supposed to go public. This is fascinating because it suggests that perhaps there were different decision rules used by officials for choosing among the alternatives. This reinforces the tenet in poliheuristic theory that decisionmakers can use different decision rules. This is an area for future exploration and another way in which this dissertation contributes to poliheuristic theory. Of course some of this

[9] David Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," *International Business Times,* February 6, 2014, accessed December 13, 2016, http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.

information overlaps with other dimensions but I think the Do Nothing option was an unacceptable alternative to many interviewees. Although I did not assign new evaluations, I think the final choice to deploy a cyberweapon is still the same.

II. Iraq (2007)

In Chapter 6, I created the following choice set for the Iraq (2007) case study and I think the interviews did not alter this choice set.

(1) do nothing

(2) increase troops

(3) withdraw troops

(4) deploy a cyberweapon in order to identify and kill insurgents

Alternative 1: The U.S. could continue as is and do nothing.

Alternative 2: The U.S. could send in even more troops.

Alternative 3: The U.S. could withdraw their troops.

Alternative 4: The U.S. could deploy a cyberweapon in order to help identify and kill insurgents.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 8.8: Updated Decision Matrix for Iraq (2007)

Alternatives

		Do nothing	Send more troops	Withdrawal	Deploy a cyberweapon
Dimension	Military	In January, Bush said, "Failure in Iraq would be a disaster for the United States." So we cannot afford to do nothing. This is still unacceptable.	We have already deployed 20,000 troops so perhaps we could deploy more.	In January, Bush said, "to step back now would force a collapse of the Iraqi government, tear that country apart, and result in mass killings on an unimaginable scale." This is still unacceptable.	- We could demonstrate that these weapons can be used to kill people. - This can "provide some breathing space, a zone of security, for Iraq's political factions to settle their quarrels and form a unified state without having to worry about bombs blowing up every day."[10] **-This can achieve a physical effect.** **-This can confuse the enemy.** **-This can jam IEDs.**

[10] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016a), 160.

		Do nothing	Send more troops	Withdrawal	Deploy a cyberweapon
Dimension	Political	American troops are dying and support for the war is dwindling. We cannot do nothing. This is unacceptable.	41% of Americans at the time said the surge did not provide much difference.[11] So we should not send in additional troops.	In January, Bush said, "This new strategy will not yield an immediate end to suicide bombings, assassinations or IED attacks."[12] So we should withdraw.	We could deploy a cyberweapon but there is a lot of sensitivity surrounding the N.S.A. because the public is weary of their illegal surveillance.

[11] Frank Newport et al., *Gallup Poll Review: 10 Key Points About Public Opinion on Iraq*, (Gallup, April 27, 2007), accessed August 12, 2017, http://www.gallup.com/poll/27391/gallup-poll-review-key-points-about-public-opinion-iraq.aspx.

[12] George W. Bush, "President Bush Addresses Nation on Iraq War," (speech, Washington, D.C., January 10, 2007), accessed August 12, 2017, *CQ Transcripts Wire*, http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011002208.html.

		Do nothing	Send more troops	Withdrawal	Deploy a cyberweapon
Dimensions	Diplomatic	In January, Bush said, "Radical Islamic extremists would grow in strength and gain new recruits. They would be in a better position to topple moderate governments, create chaos in the region and use oil revenues to fund their ambitions. Iran would be emboldened in its pursuit of nuclear weapons." So we cannot afford to do nothing. This is unacceptable.	We already have thousands of troops in Iraq so sending in more might not further exacerbate U.S.-Iraqi relations.	In January, Bush said, "to step back now would force a collapse of the Iraqi government, tear that country apart, and result in mass killings on an unimaginable scale." This is unacceptable.	This is sensitive because of the infiltration of Iraqi companies and Iraqi civilians.
	Economic	There are no economic implications if we do nothing.	In January, Bush said, "We will give our commanders and civilians greater flexibility to spend funds for economic assistance."	Some Democrats proposed "cutting funds for the troops in Iraq as a means of forcing a change in U.S. policy" but 61% of Americans at the time opposed this.[13] Thus, this is unacceptable.	These weapons cost time, resources and money but they are cheaper than other methods such as sending additional troops.

[13] Newport et al., *Gallup Poll Review: 10 Key Points About Public Opinion on Iraq*.

Looking at the interview content juxtaposed with the proposals, a cyberweapon was used for jamming IEDs, which is something that was not considered in the proposed decision matrix. So the interviews added a useful nugget of information to this decision matrix. However, the interviewees did not discuss the Iraq (2007) case in depth because some thought this was not an example of a cyberweapon. One academic pushed back on the Iraq (2007) case saying the effect on militants was second-hand. The Iraq (2007) operation did not directly kill insurgents but aided in getting insurgents killed. Thus, this case does not belong in my universe of cases, he said. I did not differentiate between second-hand and first-hand effects, so perhaps I could for future research, although this would decrease the number of cases.

A journalist also said Iraq (2007) "does not count" because at the time, the N.S.A. was concerned with surveillance. "The N.S.A. was messing around." The U.S. did not know how to use these capabilities for offense. Thus, in his view, this case "was child's play" and, moreover, occurred before the formation of U.S. Cyber Command. This notion of "child's play" was echoed by a practitioner in regards to the North Korea case.

III. Libya (2011)

In Chapter 6, I created the following choice set for the Libya (2011) case study and I think the interviews did not alter this choice set.

(1) do nothing

(2) continue talks

(3) send in Special Operations Forces (SOF)

(4) implement airstrikes

(5) deploy a cyberweapon

Alternative 1: The U.S. could do nothing, anticipating that Qaddafi does not carry out his promise of slaughtering Libyans in Benghazi.[14]

Alternative 2: The U.S. could continue discussions, anticipating that there could be a diplomatic resolution to the Libyan crisis.

Alternative 3: The U.S. could send in Special Operations forces as was the case in Afghanistan.[15]

Alternative 4: The U.S. could launch airstrikes against Libyan military targets.

Alternative 5: The U.S. could deploy a cyberweapon against Libyan military targets.

The decision matrix consists of four dimensions and five alternatives. I listed the dimensions in order of increasing importance.

---

[14] Helene Cooper, "Obama Cites Limits of U.S. Role in Libya," *The New York Times,* March 28, 2011, accessed December 5, 2016, http://www.nytimes.com/2011/03/29/world/africa/29prexy.html

[15] Thom Shanker, "U.S. Weighs Options, on Air and Sea," *The New York Times,* March 6, 2011, accessed December 9, 2016, http://www.nytimes.com/2011/03/07/world/middleeast/07military.html.

Table 8.9: Updated Decision Matrix for Libya (2011)

Alternatives

Dimension		Do nothing	Continue talks	Implement airstrikes	Send in Special Operations Forces (SOF)	Use a cyberweapon
	Military	If we do nothing, the conflict can spill over into the region. This is unacceptable.	There are no military implications if the U.S. continues talks but are they really working?	We should implement airstrikes.	We could send in SOF, but this is risky.	**-This can be useful for preparing the battlefield.** **-This is noticeable.** **-What if the targets are antiquated?** **-The cyberweapon has to be more sophisticated.** **"The adversary needs to be vulnerable" even though it is "hard to kill something with cyber."** **"It is easier to kill a human than it is to kill a computer."**

Dimensions		Do nothing	Continue talks	Implement airstrikes	Send in Special Operations Forces (SOF)	Use a cyberweapon
	Political	If we do nothing, we will have again failed to prevent the massacre of civilians. This is unacceptable.	We could continue talks but are they really working?	We should implement airstrikes.	The public may not support SOF in Libya.	This option may not be fast enough and we are unsure whether the President needs Congressional approval. **-This might have knocked something else out.**
	Diplomatic	If we do nothing, the Europeans could act without us thereby potentially dragging us into a bigger conflict.[16] This is unacceptable.	We should continue talks because this is the best diplomatic solution.	We could implement airstrikes since we have U.N. approval.	We cannot send SOF into Libya because there are military, political and diplomatic risks involved.	-These weapons may set a new norm for adversaries such as Russia and China. Are we willing to do that? **-This might have knocked something else out.**

[16] Jo Becker and Scott Shane, "The Libya Game | Part 1 Hillary Clinton, 'Smart Power' and a Dictator's Fall," *The New York Times,* February 27, 2016, accessed December 6, 2016, http://www.nytimes.com/2016/02/28/us/politics/hillary-clinton-libya.html.

		Do nothing	Continue talks	Implement airstrikes	Send in Special Operations Forces (SOF)	Use a cyberweapon
Dimension	Economic	There are no economic implications if we do nothing.	There are no economic implications if we continue talks.	A Tomahawk missile costs over one million dollars each and we are going to need to fire a lot.[17]	Troops cost more than airstrikes.	We could be wasting this superior capability that cost a lot of time and money on Libya's archaic defense systems.

Like the Iraq (2007) case, there was some discussion about whether the Libya case was a cyberweapon, but unlike the Iraq (2007) case, more interviewees seemed to agree that the Libya case was a cyberweapon. A prominent think tank member I spoke with did not know about this case (or the Syria case) but after I explained the circumstances, he concluded that the Libya (and Syria) cases would have been examples of cyberweapons.

Looking at the interview content juxtaposed with the proposals, the interviewees had the most insights about the military considerations. However, one of the most interesting comparisons between the proposed matrix and the interview content is that I claimed the preferred choice in this case was to implement airstrikes and since this is what the U.S. did, I stated that this decision matrix was accurate. However, a few interviewees

[17] David Alexander, "Cost of a U.S. strike against Syria could top Hagel's estimate," *Reuters,* September 5, 2013a, accessed December 13, 2016, http://www.reuters.com/article/us-syria-crisis-usa-costs-idUSBRE98415K20130905.

pointed out that just because the media said the U.S. did not use a cyberweapon does not mean the U.S. did not use a cyberweapon. So perhaps my decision matrix is null if the U.S. used both a cyberweapon and airstrikes. This statement came from someone who works on behalf of a collective of countries; hence if a cyberweapon was used, perhaps it was not the U.S.' Furthermore, upon looking at the interview content, it seems there were more hesitations than support for using a cyberweapon, so I think more information is needed in order to better assess whether this decision matrix was accurate.

IV. Pakistan (2011)

In Chapter 6, I created the following choice set for the Pakistan (2011) case study and the interviews did not alter this choice set.

(1) do nothing

(2) helicopter raid

(3) launch a missile

(4) deploy a cyberweapon

Alternative 1: The U.S. could do nothing, since they are not very confident that bin Laden is there.

Alternative 2: The U.S. could conduct a helicopter raid to capture or kill bin Laden.

Alternative 3: The U.S. could launch a precision guided munition to kill only bin Laden.

Alternative 4: The U.S. could deploy a covert cyberweapon against Pakistan's radar systems.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 8.10: Updated Decision Matrix for Pakistan (2011)

Alternatives

		Do nothing	Launch a missile	Helicopter raid	Deploy a cyberweapon
Dimension	Military	"What would the average American say if he knew we had the best chance of getting bin Laden since Tora Bora and we didn't take a shot?"[18] This is unacceptable.	-This is better because of "maintaining the flow of fuel and matériel to American forces fighting in Afghanistan, which depended on Pakistan's goodwill."[19] -We won't know the fate of OBL. -Fewer casualties. - "Imagine the criticism of the president that would follow: You got the chance	- We are not sure if OBL is there. -We will know the fate of OBL. -There could be casualties. -Can we get in and out undetected? -Do we really want to reveal the stealth helicopter?	-We could use this covertly "to prevent Pakistani radars from spotting helicopters carrying Navy Seal commandos."[21] -There would be less risk of retaliation from Pakistan's radars, army or police. **-This can be useful for prepping the battlefield.** **-There is a risk of exposure. 'How do you fly in and out without no one**

[18] Mark Bowden, "The Hunt for 'Geronimo,'" *Vanity Fair,* October 12, 2012, accessed April 22, 2017, http://www.vanityfair.com/news/politics/2012/11/inside-osama-bin-laden-assassination-plot.

[19] Ibid.

[21] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times,* October 17, 2011, accessed July 5, 2016, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

		Do nothing	Launch a missile	Helicopter raid	Deploy a cyberweapon
			of a lifetime and you blew it with something untried?"[20] - Do we really want to reveal this new weapon?		**knowing you were there?'**
Dimensions	Political	"What would the average American say if he knew we had the best chance of getting bin Laden since Tora Bora and we didn't take a shot?"[22] This is unacceptable.	-Biden was concerned about this failing and costing them a second term. -We won't definitively know the fate of OBL. -There could be fewer casualties. -This missile has never been tried before so we could miss.	-Biden was concerned about this failing and costing them a second term. -If OBL was captured, we could try him in court. -There could be casualties.	-We could maintain plausible deniability. **-There are "high-level political ramifications."**
	Diplomatic	Doing nothing will not exacerbate U.S.-Pakistani relations.	Perhaps this alternative is better than a raid since there are less	-Secretary Clinton was concerned about the diplomatic	This may alleviate diplomatic concerns.

[20] Bowden, "The Hunt for 'Geronimo.'"

[22] Ibid.

		Do nothing	Launch a missile	Helicopter raid	Deploy a cyberweapon
			casualties involved.	ramifications of a raid. -This violates Pakistan's sovereignty.	
Dimension	Economic	There are no economic implications if we do nothing.	This weapon costs a lot of money, time and resources. Do we really want to reveal this capability?	Stealth helicopters cost a lot of money, time and resources. Do we really want to reveal this capability?	A cyberweapon costs a lot of time, money and resources. Do we really want to reveal this capability? **-"What is the cost of this loss?"**

When comparing the proposed decision matrix to the interview content, the little information that I do have is mostly in relation to the military dimension. As with the Libya (2011) case, the interviewees thought a cyberweapon was useful for prepping the battlefield but, there was the risk of exposure. As with the Syria case, there were high-level political ramifications. A difference between the Pakistan (2011) case and the Syria case is along the economic dimension, where in the Syria case one interviewee was concerned that a cyberweapon was expensive and in the Pakistan (2011) case a different interviewee was concerned about capability loss.

As mentioned earlier, a cybersecurity official stated, President Obama loved covert operations that were "lightweight" and where the U.S. was "in and out." A former Cyber Command official said in this case, 'How do you fly in and out without no one knowing

you were there?' I think these statements suggest a decision rule used by the Obama administration. I will discuss decision rules later, but this is the first case where the interviews may have helped uncover a potential decision rule used for choosing among the alternatives, once again highlighting the benefits of utilizing mixed-methods. In Chapter 6, I stated that the preferred decision was to deploy a cyberweapon but this was inaccurate since the U.S. went with other options. Thanks to the interviews, now we know a little more about why the U.S. chose those other options.

V. Syria

In Chapter 6, I created the following choice set for the Syria case study.

(1) do nothing

(2) continue talks

(3) implement airstrikes

(4) deploy a cyberweapon

Alternative 1: The U.S. could wait and see if there are other methods or countries that can assist with stemming the violence in Syria.

Alternative 2: The U.S. could continue discussions to stem the violence in Syria.

Alternative 3: The U.S. could launch airstrikes against Syrian targets.

Alternative 4: The U.S. could preemptively use a cyberweapon against specific Syrian facilities in order to stem the violence.

However, the interviews revealed that there may have been another option, which was to work with GCHQ in order to avoid authorization. Thus, the new decision matrix consists of four dimensions and five alternatives. I listed the dimensions in order of increasing importance.

Table 8.11: Updated Decision Matrix for Syria

Alternatives

		Do nothing	Continue talks	Implement airstrikes	Deploy a cyberweapon	Work with GCHQ
Dimension	Military	If we do nothing the crisis in Syria worsens and the conflict can spill over into the region. This is unacceptable.	There are no military implications if the U.S. continues talks but are they really working?	The U.S. should implement airstrikes since President Obama previously threatened the use of force.	An attack on Syria could result in Russian or Iranian retaliation.[23] **- "Were the assets available?"** **-What is the intel gain/lost?**	**We can subcontract "the stuff with Syria" to GCHQ in order to get away from the problem of authorization.**

[23] David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times,* February 24, 2014b, accessed December 10, 2016, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?ref=davidesanger.

		Do nothing	Continue talks	Implement airstrikes	Deploy a cyberweapon	Work with GCHQ
Dimensions	Political	If we do nothing the crisis in Syria worsens. We cannot afford to do nothing. This is unacceptable.	We could continue talks but are they really working?	The U.S. could implement airstrikes.	If we deploy a cyberweapon, we would be doing something to contain Syria's civil war without putting troops on the ground.[24] **-There was "high politics in play."**	**We can subcontract "the stuff with Syria" to GCHQ in order to get away from the problem of authorization.**
	Diplomatic	Syria is imploding so we cannot afford to do nothing. This is unacceptable.	We should continue talks because this is the best diplomatic solution.	Airstrikes could result in international backlash because they can result in casualties, be inaccurate, or the U.S. could be seen as overreaching since we do not have U.N. support.	We could demonstrate that these weapons can be used for humanitarian purposes.[25]	**We can subcontract "the stuff with Syria" to GCHQ.**

[24] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[25] Ibid.

		Do nothing	Continue talks	Implement airstrikes	Deploy a cyberweapon	Work with GCHQ
Dimension	Economic	There are no economic implications if we do nothing.	There are no economic implications if we continue talks.	Airstrikes will cost hundreds of millions of dollars.	A cyberweapon is costly in terms of time and money but here is a chance to set a good precedent. **- "Was there a cheaper solution?"**	There are fewer economic implications if we decide to work with others.

Doing nothing about the Assad regime's use of chemical weapons and allowing Syria to further implode is noncompensatory on the military, political and diplomatic dimensions so that alternative is eliminated immediately. Thanks to the interviews, in the second stage of the decision-making process, we are now left with four options. Using the same decision rule from the proposed decision matrix (although I will suggest a new rule later), the decision rule used by the U.S. for choosing among the alternatives can be posed as: *Is the alternative expected to result in stopping Assad from further attacking civilians?* I decided to rate each alternative on a scale of 1 to 4. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 8.12: Updated Decision Matrix for Syria

		Alternatives			
		Continue talks	Implement airstrikes	Deploy a cyberweapon	Work with GCHQ
Dimensions	Military	There are no military implications if the U.S. continues talks but are they really working? I would score this alternative as 1.	The U.S. should implement airstrikes since President Obama previously threatened the use of force. I would score this alternative as 4.	An attack on Syria could result in Russian or Iranian retaliation.[26] **- "Were the assets available?"** **-What is the intel gain/lost?** I would score this alternative as 3.	**We can subcontract "the stuff with Syria" to GCHQ in order to get away from the problem of authorization.** I would score this alternative as 2.
	Political	We could continue talks but are they really working? I would score this alternative as 1.	The U.S. could implement airstrikes. I would score this alternative as 2.	If we deploy a cyberweapon, we would be doing something to contain Syria's civil war without putting troops on the ground.[27] **-There was "high politics in play."**	**We can subcontract "the stuff with Syria" to GCHQ in order to get away from the problem of authorization.** I would score this alternative as 3.

[26] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

[27] Ibid.

		Continue talks	Implement airstrikes	Deploy a cyberweapon	Work with GCHQ
				I would score this alternative as 4.	
Dimensions	Diplomatic	We should continue talks because this is the best diplomatic solution. I would score this alternative as 4.	Airstrikes could result in international backlash because they can result in casualties, be inaccurate, or the U.S. could be seen as overreaching since we do not have U.N. support. I would score this alternative as 1.	We could demonstrate that these weapons can be used for humanitarian purposes.[28] I would score this alternative as 3.	**We can subcontract "the stuff with Syria" to GCHQ.** I would score this alternative as 2.
	Economic	There are no economic implications if we continue talks. I would score this alternative as 1.	Airstrikes will cost hundreds of millions of dollars. I would score this alternative as 2.	A cyberweapon is costly in terms of time and money but here is a chance to set a good precedent. **- "Was there a cheaper solution?"** I would score this alternative as 3.	There are fewer economic implications if we decide to work with others. I would score this alternative as 4.

[28] Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks."

		Continue talks	Implement airstrikes	Deploy a cyberweapon	Work with GCHQ
	Final Choice	7	9	**13**	11

In Chapter 6, I said the preferred choice for the Syria case was to deploy a cyberweapon but since the U.S. refrained, I stated that this decision matrix was inaccurate. After updating this decision matrix with the interview content, deployment remains the preferred choice. However, as with the Libya case, the interviewees noted that just because the media said the U.S. did not deploy a cyberweapon does not mean the U.S. did not use a cyberweapon. A Senior Cyber Policy Advisor said, "whatever is in the news is not true." Thus, perhaps my proposed decision matrix is accurate, although again I need more information before I can better understand whether this decision matrix was accurate. Furthermore, it can be argued that working with GCHQ outranked deploying a cyberweapon, so the preferred choice could have been to work with GCHQ.

In Chapter 6, I stated that the Libyan operation dominated the decision-making calculus in Syria. Based on the interviews, I believe this is an accurate statement since one journalist said the Obama administration tried to work around the legalities and there was "high politics" involved. (One government official said "no comment" in regards to Syria.) However, in the Syria case, the interviewees said some of the concerns were whether the assets were available, as well as authorization. These are concerns that I did not have in the proposed decision matrix for Syria, so here again was a benefit of conducting interviews. Availability of assets was also a concern in the Libya (2011) case; however, in the Syria case, I cited reports that the Obama administration was worried about a cyberweapon

knocking something else out and further punishing Syrian civilians. (This was also a concern in the North Korea case.) This consideration was mentioned in the interviews, but in regards to the Libya case. There was also the surprising concern of cost in this decision matrix where one interviewee wondered if there was a cheaper solution. Much of the literature and many of the interviewees regarded cyberweapons as usually being a cheaper alternative, so this is curious. The relative cost of these weapons is a suggested area for continued research.

An academic I spoke with said, a cyberweapon "could have a profound effect" on the "proxy wars" in Syria and Yemen. This is key for several reasons. First, perhaps Yemen is a potential new adversary to add to the universe of cases for future research. Second, this statement refers to a proxy war in Syria. Hypothesis 6 stated– *The U.S. will likely deploy a cyberweapon in a first strike against a perceived adversary so that they do not have to engage in "a continuing contest of violence."* While this hypothesis was exploring whether cyberweapons will be used to wage proxy war, it was also exploring whether cyberweapons could help end conflicts. Since there was already a proxy war in Syria, I think this academic's statement attests that cyberweapons can be used to end a conflict. Once again the interviews yielded additional useful information.

Another tidbit of information provided by the interviews was an assertion by a Legal Advisor who said he knows these tools were employed in Syria. A former Cyber Command official stated that the Snowden disclosures showed us the intel gained/lost from an offensive cyber operation in Syria. Apparently in 2012, T.A.O. mistakenly took out Syria's internet and was unable to repair the router.[29] This might have been what the Legal

[29] James Bamford, "Edward Snowden: The Untold Story," *Wired,* August 22, 2014, accessed March 22, 2017, https://www.wired.com/2014/08/edward-snowden/.

Advisor was referring to when he said he knows these capabilities were used in Syria. This incident is fascinating because it indicates that the N.S.A. was inside Syria's networks, and if they were there a year ago when the Obama administration first thought about using a cyberweapon, then it calls into further question why the U.S. refrained again in 2013 and 2014. This incident also speaks to the concern expressed by the interviewees in the Libya case, that a cyberweapon "might have knocked something else out." However, this 2012 incident in Syria should not be added to my universe of cases since T.A.O. unintentionally knocked out Syria's internet. But, if I were re-doing this project, perhaps I would split these operations, since this decision matrix combined all of the various events in regards to Syria.

VI. North Korea (2014)

In Chapter 6, I created the following choice set for the North Korea case study.

(1) do nothing

(2) increase sanctions

(3) deploy a cyberweapon

Alternative 1: The U.S. could do nothing since Sony only lost $35 million.

Alternative 2: The U.S. could implement additional sanctions against North Korea to punish them for attacking Sony.

Alternative 3: The U.S. could deploy a cyberweapon against North Korea.

However, I think the interviews revealed that there may have been another option which was to work with the Chinese in order to have them apply pressure against the North Koreans. So, the new decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 8.13: Updated Decision Matrix for North Korea (2014)

Alternatives

		Do nothing	Increase sanctions	Deploy a cyberweapon	Work with the Chinese
Dimension	Military	We cannot afford to do nothing because the North Koreans threatened violence against our theaters. This is unacceptable. **One former Cyber Command official said that perhaps North Korea did not carry out the attack on Sony. He said this could have been a false flag where someone said let us work together to point the finger at North Korea.**	-We could increase sanctions but will they be effective since the North Koreans are already heavily sanctioned?[30] **-This is a "waste of time."**	We should do this since it can be done covertly and precisely. Tit-for-tat. **- "We should have wiped out North Korea's systems."** **-We should carry out a DDoS attack against North Korea in order to restore confidence in the U.S.** **- "Only kids would use a DDoS attack" thus, the U.S. did not turn off North Korea's Internet.** **-It is harder to have an**	**-It is harder to have an effect in North Korea because it is less open.**

[30] David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony Case," *The New York Times,* January 2, 2015d, accessed December 1, 2016, http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

		Do nothing	Increase sanctions	Deploy a cyberweapon	Work with the Chinese
				effect in North Korea because it is less open.	
Dimensions	Political	We cannot afford to do nothing because the North Koreans have attacked our freedom of speech and threatened violence against our theaters. This is unacceptable. **One government official said North Korea was a "big splash" since the President attributed it (a first) and took action.**	We could increase sanctions.	We could do this since it can be done covertly and precisely. Tit-for-tat. **-If we respond, are we willing to risk escalation?**	**If we respond, are we willing to risk escalation?**
	Diplomatic	If we do nothing, the North Koreans get away with attacking us. This is unacceptable.	We could increase sanctions as long as they do not exacerbate the already dire situation for North Korean civilians.	We could do this covertly but will it trigger a wider conflict?	**We can go to the Chinese and ask "hey, we cannot do anything because this violates your sovereignty, so can you do it for us?"**

		Do nothing	Increase sanctions	Deploy a cyberweapon	Work with the Chinese
Dimension	Economic	The North Korean attack cost Sony $35 million. So we cannot do nothing. This is unacceptable.	We should increase sanctions. They are effective.	Deploying a cyberweapon against North Korea may be costly in terms of time and money.	**China stopping the sale of coal was a part of the response to North Korea's attack on Sony.**

Doing nothing and allowing North Korea to get away with attacking Sony and threatening violence was unacceptable on all dimensions so that alternative is eliminated immediately. In Chapter 6, I stated this is the only case where an option was noncompensatory on all dimensions. That statement still stands. Thanks to the interviews, in the second stage of the decision-making process, we are now left with three options. Additionally, the interviews also provided a possible decision rule used by the U.S. for choosing among the alternatives which can be posed as: *If you respond, are you willing to risk escalation?* However, I am going to apply the decision rule I originally posed which was: *Is this alternative a proportional response?* I decided to rate each alternative on a scale of 1 to 3. The higher the score, the more likely that alternative will be able to fulfill the decision rule.

Table 8.14: Updated Decision Matrix for North Korea (2014)

Alternatives

		Increase sanctions	Deploy a cyberweapon	Work with the Chinese
Dimensions	Military	-We could increase sanctions but will they be effective since the North Koreans are already heavily sanctioned?[31] **-This is a "waste of time."** I would score this alternative as 2.	This is a proportional response to North Korea's attack. Tit-for-tat. **- "We should have wiped out North Korea's systems."** **-We should carry out a DDoS attack against North Korea in order to restore confidence in the U.S.** **- "Only kids would use a DDoS attack" thus, the U.S. did not turn off North Korea's Internet.** **-It is harder to have an effect in North Korea because it is less open.** I would score this alternative as 3.	**-It is harder to have an effect in North Korea because it is less open.** I would score this alternative as 1.
	Political	We could increase sanctions.	We could do this since it can be done covertly and	**If we respond, are we willing to risk escalation?**

[31] Sanger and Schmidt, "More Sanctions on North Korea After Sony Case."

		Increase sanctions	Deploy a cyberweapon	Work with the Chinese
		I would score this alternative as 2.	precisely. Tit-for-tat. **-If we respond, are we willing to risk escalation?** I would score this alternative as 3.	I would score this alternative as 1.
Dimensions	Diplomatic	We could increase sanctions as long as they do not exacerbate the already dire situation for North Korean civilians. I would score this alternative as 1.	We could do this covertly but will it trigger a wider conflict? I would score this alternative as 2.	**We can go to the Chinese and ask "hey, we cannot do anything because this violates your sovereignty, so can you do it for us?"** I would score this alternative as 3.
	Economic	We should increase sanctions. They are effective. I would score this alternative as 3.	Deploying a cyberweapon against North Korea may be costly in terms of time and money. I would score this alternative as 2.	**China stopping the sale of coal was a part of the response to North Korea's attack on Sony.** I would score this alternative as 1.
	Final Choice	8	**10**	6

When comparing the proposed decision matrix to the interview content, it looks like the interviewees had a lot to say about the North Korea case. Naturally, some of this content overlaps with other dimensions. In Chapter 6, I stated that in the case of North Korea, the U.S. decided to use direct action. A former R.O.C. employee suggested that the

U.S. might use these capabilities as a first strike in order to support a military or strategic operation or even as direct action. Although this was not a first strike scenario, this former R.O.C. employee's statement aligns with the finding from my proposed decision matrix.

Additionally, I said the preferred choice was deploying a cyberweapon and I claimed that this was correct since North Korea's Internet went out and despite the fact that the U.S. also implemented sanctions. After updating the decision matrix, deployment remains the preferred choice. However, there was no consensus among the interview participants as to whether the U.S. carried out a cyberattack against North Korea. A former Cyber Command official said this could have been a false flag. One of the interesting insights that added to this decision matrix was the alleged conversation between the U.S. and China and China's response to the Sony hack. Unlike with some other countries, in this case, the U.S. was concerned about violating China's sovereignty. Furthermore, one interviewee declared, "Only kids would use a DDoS attack" and he had "positive confirmation that North Korea was not us." (This calls to mind the "child's play" comment in regards to the Iraq (2007) operation discussed earlier.) A journalist stated it is harder to have an effect in North Korea because it is less open (a similar concern in the Libya case.) This hints at the notion that perhaps cyberattacks require Stuxnet-like concepts and capabilities, but perhaps the more likely scenario here was the concern over escalation.

Whether or not the U.S. deployed a cyberweapon, one government official said North Korea was a "big splash" since the President named North Korea as the attacker (the first time the U.S. specifically attributed a cyberattack to another country) and took action. Nonetheless, some interviewees thought sanctions were a waste of time, and that the U.S. should have used a cyberweapon to restore confidence. These ideas of confidence,

escalation and tit-for-tat (mentioned in this decision matrix) are interesting because they resurfaced a year later in the Russian case.

VII. ISIS (2016)

In Chapter 6, I created the following choice set for the ISIS (2016) case study and I think the interviews did not alter this choice set.

(1) continue current methods

(2) implement more airstrikes

(3) send in more SOF

(4) deploy a cyberweapon

Alternative 1: The U.S. could continue its current methods of fighting ISIS.

Alternative 2: The U.S. could launch more airstrikes against ISIS.

Alternative 3: The U.S. could send in additional SOF to deal with ISIS on the ground.

Alternative 4: The U.S. could deploy a cyberweapon against ISIS targets.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 8.15: Updated Decision Matrix for ISIS (2016)

		Alternatives			
		Continue current methods	Implement additional airstrikes	Send in additional SOF	Deploy a cyberweapon
Dimension	Military	The U.S. could continue its current methods but ISIS is still wreaking havoc.	We should implement additional airstrikes against ISIS.	There are already SOF in Syria so perhaps we could send more.	We should do this since it could disrupt the Islamic State's operations without putting more boots on the ground.

		Continue current methods	Implement additional airstrikes	Send in additional SOF	Deploy a cyberweapon
		This is unacceptable.			**- "Part of the issue is that ISIS does not have a lot of infrastructure to go after, and when you take out a server, the operators can move operations to another. Another issue is that the government has not fully worked out to what degree the military can take actions in a third non-belligerent country -outside Syria or Iraq, for instance- in order to get to the targeted server or computer. There are questions of sovereignty that have not been settled."** **- "ISIS has no air defense systems to attack through cyber means" so the types of targets are different which means the gain/loss calculus is different.** **-We can pinpoint militants and go after their communications systems or take them out kinetically.** **-Do we have the capability to do this?**

		Continue current methods	Implement additional airstrikes	Send in additional SOF	Deploy a cyberweapon
Dimensions	Political	The U.S. could continue its current methods but ISIS is still wreaking havoc.	We could implement additional airstrikes against ISIS.	We should not send more troops to the Middle East.	We should do this since it could disrupt the Islamic State's operations without putting more boots on the ground. **- "There are a variety of considerations" when it comes to deployment.** **- "This is the first time they have said that so this is significant for the U.S."**
	Diplomatic	The U.S. could continue its current methods but ISIS is still wreaking havoc.	We could implement additional airstrikes against ISIS.	We should not send more troops to the Middle East.	We could do this since it could disrupt the Islamic State's operations without putting more boots on the ground or launching more airstrikes.
	Economic	Current methods have cost us $10 billion.	The estimated cost of monthly airstrikes against ISIS ranges from $200 - $570 million.[32]	The estimated cost of monthly boots on the ground is over one billion dollars.[33]	We have spent millions of dollars on these weapons so we could use them especially if they may be cheaper than other options.

[32] Todd Harrison et al., *Estimating the Cost of Operations Against ISIL*, (Center for Strategic and Budgetary Assessments, September 2014), 5, accessed December 13, 2016, http://csbaonline.org/uploads/documents/Estimating-the-Costs-of-Operations-against-ISIL.pdf.

[33] Ibid.

When comparing the proposed decision matrix to the interview content, there was no consensus among the interviewees as to whether the ISIS (2016) case study was a cyberweapon. However, they did advocate for cyberweapons to be used against ISIS. Therefore, I think the interviews reinforced this decision matrix. As with a few previous cases, U.S. decisionmakers wondered if they had the cyber capability. It is interesting to note that in this case, the U.S. had the capability and they decided to deploy. "What is important is that the U.S. government felt the need to say that they are using these capabilities," said a Senior Cyber Policy Advisor. "This is the first time they have said that so this is significant for the U.S."

The interviews also reinforced that there are a lot of considerations including sovereignty, which was a concern in the North Korea case. Therefore, the interviews added crucial information to this decision matrix. As mentioned earlier, when I was writing this chapter, *The Washington Post* reported that there was bickering among U.S. officials over the extent of informing allies during this cyber operation which was apparently called "Operation Glowing Symphony."[34] So future research will involve adding this information to this decision matrix. Another area for future research is to explore the differences between the ISIS (2016) and Iraq (2007) cases, which the interviewees did not address.

VIII. Russia (2016)

In Chapter 6, I created the following choice set for the Russia (2016) case study and the interviews did not alter this choice set.

(1) do nothing

(2) implement sanctions

[34] Nakashima, "U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies."

(3) covert action

(4) deploy a cyberweapon

Alternative 1: The U.S. could do nothing because any option may work in Putin's favor.

Alternative 2: The U.S. could implement sanctions against Russia.

Alternative 3: The U.S. could engage in "covert action against Russian targets."[35]

Alternative 4: The U.S. could use a cyberweapon against Russian facilities.

The decision matrix consists of four dimensions and four alternatives. I listed the dimensions in order of increasing importance.

Table 8.16: Updated Decision Matrix for Russia (2016)

		Alternatives			
		Do nothing	Increase sanctions	Engage in covert action	Deploy a cyberweapon
Dimension	Military	The U.S. cannot allow Russia to go unpunished for meddling in the U.S. presidential election so this option is unacceptable. **-This is unacceptable. There needs to be "pain."** **- We did not have a plan.**	We could implement sanctions against Russia. **-This is not effective.** **-This is effective.**	We cannot engage in covert action in Russia because the military risks are great and the Russians will probably retaliate. Thus, this option is unacceptable.	We should covertly deploy a cyberweapon against Russian facilities because this is an effective way of retaliating against a hard-to-reach target without starting a full-scale conflict. Tit-for-tat. **-"Tit-for-tat might not be the best for the U.S. even if our**

[35] David E. Sanger, "U.S. Says Russia Directed Hacks to Influence Elections," *The New York Times,* October 7, 2016d, accessed December 1, 2016, http://nyti.ms/2dLddLS.

		Do nothing	Increase sanctions	Engage in covert action	Deploy a cyberweapon
		-This is unacceptable because what the Russians did was a big deal.			**tools are better."** **-We can turn off the lights.** **-We can dismantle infrastructure.** **-Time was a concern.**
Dimension	Political	The U.S. cannot allow Russia to go unpunished for meddling in the U.S. presidential election so this option is unacceptable. **-Was this a cyberattack?** **-Was this illegal?** **-Is this new?** **-This will be ongoing.** **- "When President Obama said the next president will have options to respond at**	We could implement sanctions against Russia but this may result in political repercussions. **Indicting people sends a message but it does not really do anything.**	We cannot engage in covert action in Russia because the military and political risks are great and the Russians will probably retaliate. Thus, this option is unacceptable.	We should covertly deploy a cyberweapon against Russian facilities because this is an effective and proportional way of retaliating against a hard-to-reach target without starting a full-scale conflict. Tit-for-tat. **-"Tit-for-tat might not be the best for the U.S. even if our tools are better."**

		Do nothing	Increase sanctions	Engage in covert action	Deploy a cyberweapon
		their choosing, he meant "her" choosing." **-This is unacceptable because what the Russians did was a big deal.**			
Dimension	Diplomatic	The U.S. should not allow Russia to go unpunished for meddling in the U.S. presidential election. **-Was this a cyberattack?** **-Was this illegal?** **-Is this new?** **- This was fundamentally an intelligence operation to influence the election which is no different from what the C.I.A. did in Latin America in the 1950s and 60s.**	We could implement sanctions against Russia but this may result in diplomatic repercussions.	We cannot engage in covert action in Russia because the political risks are great and the Russians will probably retaliate. Thus, this option is unacceptable.	We could deploy a cyberweapon against Russian facilities because this is a proportional way of retaliating against a hard-to-reach target and we could do it covertly so we avoid a wider conflict however, there could be diplomatic ramifications. **-"Tit-for-tat might not be the best for the U.S. even if our tools are better."** **-This is an "unstable environment."**

		Do nothing	Increase sanctions	Engage in covert action	Deploy a cyberweapon
		- "We should combat threats." "We are playing into Russia's hands."			
Dimension	Economic	There are no economic implications if the U.S. decides to do nothing.	We could increase sanctions but this may result in economic repercussions for the U.S.	Covert action is costly in terms of time, money and possibly casualties.	We have spent millions of dollars on these weapons so we should use them if they are more effective than other options.

When comparing the proposed decision matrix to the interview content, the interviewees had many thoughts about the Russia case. First of all, I pronounced tit-for-tat in the proposed decision matrix, arguing that the U.S. should deploy a cyberweapon under these circumstances. (I made this argument in the North Korea case as well.) Some interviewees expressed a similar opinion but they said President Obama was concerned about escalation with Russia. (Escalation was also a concern in the North Korea case.) A government official stated, "we are in an unstable environment" especially since we "have not figured out how to communicate." Thus, he cautioned "tit-for-tat might not be the best for the U.S. even if our tools are better."

Second, I speculated that the preferred choice was to deploy a cyberweapon but, the Obama administration's response was sanctions, expulsions and property seizures so my proposed decision matrix was inaccurate. In retrospect, perhaps I could have pulled out indictments as another option, but since they were announced with the sanctions, I decided

to lump them together. However, nearly every interviewee I spoke with was unhappy about the Obama administration's choice of action. Many interviewees wanted the U.S. to use their cyberweapons to demonstrate strength and to also retaliate for what they thought was a serious offense and threat. (Demonstrating confidence was also mentioned during the interview discussions about North Korea.) Many interviewees thought sanctions were ineffective (which was the same thought in the North Korea case) and that indictments were largely symbolic. However, there was confusion, or at least a lack of consensus about Russia's actions, which is probably why the U.S. did not know how or whether to respond. One interviewee claimed this was fundamentally an intelligence operation to influence the election, which is no different from what the C.I.A. did in Latin America in the 1950s and 60s. However, a Senior Cyber Policy Advisor rejected this comparison, exclaiming, "we have not conducted those meddling operations for a long time." "We are long past those days," he stated. It does not matter whether this is "moral equivalence," he argued, it does not mean we should not respond. "We should combat threats," he urged. "We are playing into Russia's hands." This is one of many reasons why definitional consensus is important.

The interviews also provided some important new information for this decision matrix. First of all, according to a former government official, the U.S. did not have a plan which is why they did not respond. Second, "When President Obama said the next president will have options to respond at their choosing, he meant "her" [Hillary Clinton] choosing." Third, time was of the essence, since this happened during a presidential election. As you can see, the interviews were tremendously helpful here and since the Russia case is new and unfolding in real-time, this is another way in which this dissertation adds to the literature about offensive U.S. cyberwarfare.

IX. Decision Rules

Another tenet of poliheuristic theory is the decision rule. Now that we know a little bit more about the options, we can turn to analyzing the decision rule that was used for choosing among the alternatives. During the content analysis of the interviews, I realized that perhaps the interviews may have revealed some of the decision rules used in these cases. Therefore, I decided to compare the decision rule that I proposed to what I learned from the interviews.

Table 8.17: Comparing the Decision Rules

CASE	PROPOSED DECISION RULE	DECISION RULE DISCERNED FROM INTERVIEWS
Stuxnet	Is this alternative expected to result in preventing Iran from acquiring a nuclear weapon?	Does this alternative fulfill the operational parameters [which differed based on the dimension]?
Iraq (2007)	Is this alternative expected to result in stemming the violence in Iraq?	Does this alternative fulfill the purpose of this operation?
Shotgiant (2007)	Does this alternative enable future offensive cyber operations against those possessing Huawei products?	Not really discussed
Quantum (2008)	Is this alternative expected to result in accessing hard-to-reach areas?	Not really discussed
Turbine (2010)	Is this alternative expected to result in enabling attacks?	Not really discussed
Nitro Zeus	Is this alternative expected to result in preventing Iran from acquiring a nuclear weapon?	Not really discussed
Libya (2011)	Is this alternative expected to result in preventing Qaddafi from attacking civilians?	Is this alternative covert, reliable and will it be effective against the target?

CASE	PROPOSED DECISION RULE	DECISION RULE DISCERNED FROM INTERVIEWS
Pakistan (2011)	Is this alternative expected to result in killing Osama bin Laden and minimizing casualties?	"How do you fly in and out without no one knowing you were there?"
Syria	Is this alternative expected to result in stopping Assad from further attacking civilians?	"Are high politics at play?"
North Korea (2014)	Is this alternative a proportional response?	"If you respond, are you willing to risk escalation?"
ISIS (2016)	Is this alternative expected to result in disrupting ISIS' command-and-control operations?	Does this alternative fulfill the purpose of this operation?
Russia (2016)	Is this alternative a proportional response that will minimize retaliation?	Will this alternative inflict pain?
Iraq (2003)	Is this alternative expected to result in obliterating the Iraqi financial system?	Not really discussed

Upon analyzing the decision rules gleaned from the interviews, I have the same decision rule for both the Iraq (2007) and ISIS cases. I could have also had the same decision rule for the Syria and Libya cases but the interviewees discussed the Libya case a bit more, so I was able to craft a more tailored decision rule for the Libya case. There were some gaps since we did not discuss all of the cases and overall, the decision rules gleaned from the interviews were generic. This is not surprising since we did not go into a great deal of detail about each case during the interviews. It is interesting to note that the supposed decision rule from the interviews for the North Korea case was similar to my proposed decision rule for the Russia case. I also find the supposed decision rule for the Russia case fascinating. As discussed earlier, one interviewee essentially suggested the decision rule for the Pakistan case. However, one of the most intriguing findings regarding

the interviews and the decision rules concerns the Stuxnet case, where there were possibly several decision rules, which in turn presents another path of future research for poliheuristic theory.

X. Additional Reflections

Originally, I thought I could conclude with a future decision board. However, some of the interviewees stressed that these capabilities are supposed to be specific, not generalizable. A cybersecurity specialist said, "There is no playbook for a response situation" because "you do not want an adversary setting the parameters for the kind of targets." A Senior Cyber Policy Advisor I spoke with agreed stating, "one thing we pushed back on was the notion that we need to set red lines to respond to any specific cyberattack." "These are all political determinations made by political leadership," he disclosed. "There is no if this happens then we will do that." "We never want there to be," he professed. "We want to preserve flexibility." It "does no good to generalize," he declared. We "always want to look at this situation by situation." This was a key finding applicable to poliheuristic theory. Since poliheuristic theory "promises precision in its predictions (outcome validity) as well as greater accuracy in reflecting the manner in which decisions are made (process validity),"[36] I incorrectly presumed I could generalize to some extent. Thus, I did not conclude with a future decision board. This is another way in which the interviews impacted my research.

Overall, the interviews added some new pieces of information to the proposed decision matrixes. In Chapter 3, I stated that a limitation of poliheuristic theory is that since domestic politics is seen as frequently the most influential dimension in the first stage of

[36] Brulé, "The Poliheuristic Research Program: An Assessment and Suggestions for Further Progress," 273.

decision-making, it would appear that other (first-stage) dimensions are thereby often rendered effectively irrelevant. Although a Senior Cyber Policy Advisor said political determinations are important, I am not sure the political dimension dominated since a lot of the interview content in the decision matrixes corresponded to the military as well as diplomatic dimensions. Of course, there were several military considerations since many of the interviewees had a military background. Thus, for future research, I would like to continue interviewing different professionals in order to further understand the political dimension.

Another core assumption of poliheuristic theory is the noncompensatory strategy– or the idea that an alternative that is unacceptable can be ruled out immediately. When I inquired as to whether anything was ruled out immediately during the decision-making process, a former Remote Operations Center employee said, “nothing was taboo right off the bat but if there was a link to the possibility of loss of life, they would stay away from that.” Thus, perhaps casualties are a noncompensatory option. But, this too is an area for additional research since the interviews did not provide full clarity as to how the decisionmaker moves from the first to the second stage of the decision-making process. Furthermore, I could have labeled more alternatives on the diplomatic dimension noncompensatory and some cases have more in-depth explanations than others. Thus, even though I utilized all of the available information that I gathered, these are some of the ways one could falsify these results.

Poliheuristic theory was useful in addressing the many cyberweapons that were not deployed as well as the few that supposedly were. This is one way in which my research differs from those who have previously utilized poliheuristic theory. Although this study

focused on deployments, there were many non-events in regards to cyberwarfare, so having a theory that addressed both events and non-events was instrumental in understanding the parameters of using these weapons. In Chapter 3, I referenced Karl DeRouen Jr. who said non-events are rarely discussed in foreign policy decision-making scholarship but they should be discussed because they could broaden decision-making theory.[37] I think this dissertation helped broaden the foreign policy decision-making scholarship.

Another advantage of poliheuristic theory is that it can be used to analyze all types of decisions. This is significant because some of the cyberweapons were joint operations whereas others were single decisions, or at least, they were not a joint operation with another country. This study did not account for the decision-making process of other countries that conduct joint offensive cyber operations with the U.S. Thus, this is another area for future research.

One of the novel aspects of this dissertation is the comparison of the nuclear strike process and the cyberweapon deployment process. Now that we know the cyberweapon deployment process is similar to the nuclear strike process, I ask again whether poliheuristic theory was an adequate lens for understanding the decision-making process over deployment. I still believe it was because the nuclear strike process is similar to poliheuristic theory insofar as alternatives and options are weighed and then sent upwards for approval. If I could have continued interviewing people, I would ask what happens if the target package is rejected? Is there likely to be a modified proposal and a second round

[37] Karl DeRouen Jr., "The Decision Not to Use Force At Dien Bien Phu: A Poliheuristic Perspective," in *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making*, ed. Alex Mintz (New York: Palgrave Macmillan, 2002): 11.

of approvals by higher authorities? If so, is this a routinized procedure or only one available in unusual cases—or is generalization simply impossible?

CONCLUSION

At the hearing on "Cybersecurity Threats and Defense Strategy" on May 9, 2017, Admiral Michael Rogers, the commander of U.S. Cyber Command stated,

> Every conflict around the world now has a cyber dimension. 'Cyber war' is not some future concept or cinematic spectacle, it is real and here to stay. The fact that it is not killing people yet, or causing widespread destruction, should be no comfort to us as we survey the threat landscape. Conflict in the cyber domain is not simply a continuation of kinetic operations by digital means, nor is it some Science Fiction clash of robot armies. It is unfolding according to its own logic, which we are continuing to better understand.[38]

This is the best explanation for the purpose as well as significance of my research. At the beginning of this dissertation, I provided a brief overview of the evolution of cyberwarfare in the U.S. Next, I surveyed the major literature about offensive cyberwarfare and U.S. capabilities and related policies. Then, I explained how I was going to approach the problem of understanding the conditions under which the U.S. is likely to deploy a cyberweapon in a first strike. Next, I explained all of the known cases of alleged U.S. cyberweapons that were used against countries. I used a mixed-methods approach to first, empirically test what I classified as 13 cases where the U.S. used or debated about using an offensive cyberweapon from 2001 – 2016. The cases were Stuxnet, Iraq (2007),

---

[38] *Statement of Admiral Michael S. Rogers: Hearing on Cybersecurity Threats and Defense Strategy Before the Senate Committee on Armed Services*, 115th Cong., 4, (May 9, 2017), (statement of Admiral Michael S. Rogers, Commander United States Cyber Command), https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

Shotgiant (2007), Quantum (2008), Turbine (2010), Nitro Zeus, Libya (2011), Pakistan (2011), Syria, North Korea (2014), ISIS (2016), Russia (2016), and Iraq (2003). Second, I employed the poliheuristic theory of decision-making to reconstruct the decision-making process for each case study. Third, I conducted 22 confidential, semi-structured interviews to gather information about these case studies as well as further thoughts about the decision-making process behind deploying a cyberweapon. As a result of these findings, there are several policy implications which will be discussed later. I am certain this three-pronged approach helped construct a fuller picture of what is a very classified subject, although of course there were some limitations.

A limitation of the qualitative methodology was the software. Nvivo for Mac does not allow a researcher to run a compound query, which might have been useful for exploring and visualizing the text within my coding. For instance, I coded some loosely-connected ideas into a decision-making node, but I could have used a compound query to unpack these thoughts instead of doing this manually.

One academic cautioned that I did not have enough data since the U.S. has not admitted to using cyberweapons. However, considering that much of the subject is indeed highly classified, other authors have certainly been venturing to write about it. There have been a number of books that have come out since I started working on this project, most of which have been referenced here. Additionally, in March 2017, *The Journal of Cybersecurity* published a special issue dedicated to offensive cyberwarfare. Some of these articles were referenced in this dissertation.

When I interviewed an academic in February 2017, he insisted that I needed to speak to the "guys at the top." I followed his advice to the extent that I ended up

interviewing key individuals, but I was also careful to talk to persons in a variety of professions relevant to the use of cyberweapons. I succeeded in uncovering a wide set of views about the definitions of central concepts, the range of potential policies, the utility of specific policies in particular situations, and the process(es) involved in making crucial decisions.

Although the authority to deploy a cyberweapon rests with the President, the interviews emphasized that there are almost always others such as USCYBERCOM who are involved. So I verified that the deployment of a cyberweapon is a multi-staged decision process. Thus, a policy implication of this finding is that agencies are forced to cooperate in order to collectively recommend or in some instances actually deploy a cyberweapon. For future research, I would like to interview more individuals from think tanks, T.A.O., R.O.C., U.S. Cyber Command, and the Department of Defense. I wish to better understand the differences between T.A.O. and R.O.C. Finally, I would be eager to interview more persons who were involved with the decision-making in specific cases, as well as relevant policymakers in the current administration.

One aspect of the quantitative analysis that might not have worked so well was that a simple re-ordering of the cases could change everything, thus falsifying the results. For example, although I marked the creation date of Russia as 2016, maybe I should have noted the date as 2015 since one of the Russian hacking groups had been in the D.N.C. systems since then. Furthermore, Iraq (2003) is listed last, but if I listed the cases chronologically, Iraq (2003) should have been first. I did not list Iraq (2003) first because this case would have served as the basis for the rest of the cluster analysis and I wanted Stuxnet to be the

basis since many scholars classify Stuxnet as a cyberweapon and we have considerable information about it.

Additionally, I could have added other variables such as "is the U.S. currently at war with that country?" This might have helped in breaking down the PERCEIVED ADVERSARY category. For instance, I coded Libya "Yes" under PERCEIVED ADVERSARY because the U.S. was about to conduct airstrikes, but the U.S. was not yet at war with Libya, so this could have skewed the PERCEIVED ADVERSARY category. There was also a possibility that the CONVENTIONAL ENABLER variable could have been skewed since I used "force multiplier" and "conventional enabler" interchangeably. The academic term is "force multiplier" but U.S. Cyber Command uses the term "conventional enabler." However, conventional enabler deals with preparing for a conventional military conflict and a force multiplier increases the force of an attack. Perhaps I should have split these two categories instead of lumping them together. For example, the Pakistan case involves a force multiplier but not a conventional enabler as defined here since the U.S. was not gearing up for a conventional war with Pakistan and yet, I coded this variable Yes.

Furthermore, although I used case studies and I think this worked well overall, I am probably missing some case studies. For instance, I cited a Special Operations Forces member from Carr's work who said that the U.S. government was deploying cyberweapons[39] "in combat in Iraq and Afghanistan when they can be employed as part of

[39] Jeffrey Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," *Bulletin of the Atomic Scientists* 69, no. 5 (September 1, 2013): 36, EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

the US rules of engagement."[40] Harris' book discussed some of the cyber operations in Afghanistan and one of the journalists I spoke with mentioned Afghanistan as well. A former R.O.C. employee I spoke with discussed Afghanistan in response to the Five Eyes question. Interestingly, a cybersecurity official I spoke with also mentioned Afghanistan, but he did say that much of what he knows is based on media reports. So for future research, perhaps I could include Afghanistan as a case study even though information is scarce and difficult to access. Moreover, I combined all of the options for Syria into one decision matrix but these were separate events so I could have analyzed them individually. Additionally, perhaps I could move the start date of my timeframe to include the Haiti and Serbia cases as well. Another point to note is that in March 2017, Wikileaks released the largest trove of stolen C.I.A. documents in the agency's history which spoke about their covert cyberweapons.[41] This leak happened after I finished many of the interviews.

Regarding poliheuristic theory, perhaps it could be useful to show the proposed decision matrixes to interviewees in order to gain their feedback and/or it might be a useful experiment to have the participants fill in a decision matrix. Other poliheuristic studies have used computerized decision boards and hypothetical scenarios as experiments. One would need to present a situation and walk the respondents through a menu of options.

---

[40] Carr, "The misunderstood acronym: Why cyber weapons aren't WMD," 35.

[41] Scott Shane, Matthew Rosenberg and Andrew W. Lehren, "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents," *The New York Times,* March 7, 2017, accessed August 12, 2017, https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.; Greg Miller and Ellen Nakashima, "WikiLeaks says it has obtained trove of CIA hacking tools," *The Washington Post,* March 7, 2017, accessed August 12, 2017, https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?utm_term=.cfec5a650b1a.

As for cyberwarfare generally, there are many avenues for future research. Since I only focused on the U.S., my research question could be applied to other countries. Under what conditions will Russia or China deploy a cyberweapon in a first strike? These would be useful studies since countries do appear to view cyberwarfare differently and thus, are likely to have different conditions for deployment. Additionally, as mentioned earlier, another area in need of investigation is the burgeoning cybersecurity insurance market, which would entail looking at the costs associated with insuring critical infrastructure and the private-public cooperation in this arena.

One central objective of this dissertation was to investigate the rules of engagement applied during the decision-making process over the deployment of a cyberweapon in a first strike. In the Introduction, I stated, "I could conclude that there are too many conditions and differing situations to make one conclusion but I think we will be able to better understand that the U.S. is covertly deploying these weapons to address a significant threat that cannot be effectively addressed by traditional methods of warfare." Now, I can say yes, this statement seems plausible. Overall, I think my work sheds some light on U.S. policy and practice about cyberweapons and adds to the academic discourse. By quantitatively and qualitatively analyzing 13 alleged U.S. cyberweapons, we discovered that some key conditions affecting deployment were threat, access and collateral damage and that the authorization process is similar to the nuclear strike process. These are the main contributions of this dissertation to the overall literature on cyberwarfare. These findings are useful to both policymakers and military planners as it helps set the parameters for using cyberweapons. As one interviewee told me, "you do not want an adversary setting

the parameters for the kind of targets." Now that there are some known parameters, U.S. policymakers can make some progress towards their desire for an E-Neva Convention.

Although I was wrong about generalizing, I stand by my claim that the two questions to first consider when thinking about deploying a cyberweapon are:

1) Is there a threat?

2) Is the intended target out of the reach of troops, drones or airstrikes?

A former R.O.C. employee said this really is an authority question and thus, my dissertation is "cutting to the heart of this" because "the N.S.A. has the capability but no authority." A practitioner also reassured me that he thought I was asking the right questions.

Previous scholarly work has largely focused on Stuxnet, a few cases, or attacks against the U.S., but my dissertation is distinct partly because it has attempted to discuss the major cases of U.S. cyberweapons that were used against other countries, including newer cases such as the U.S.' response to Russia's actions in the 2016 U.S. presidential election. As I have previously stressed, a mixed methods approach proved highly useful because I was able to analyze the cases both quantitatively and qualitatively and the interviews allowed me to further clarify discrepancies and provided new insights into the decision-making process.

Another main contribution of my dissertation was in regards to poliheuristic theory which "promises precision in its predictions (outcome validity) as well as greater accuracy in reflecting the manner in which decisions are made (process validity.)"[42] Through the use of decision matrixes, we were able to better understand the process behind these decisions.

[42] Brulé, "The Poliheuristic Research Program: An Assessment and Suggestions for Further Progress," 273.

We learned that cyberweapons are "political determinations made by political leadership," and thus, "There is no if this happens then we will do that." Every time the U.S. wants to deploy a cyberweapon, they have to assess each individual situation. This forces decisionmakers and military planners to fully consider all of the conditions involved. This leads to better decision-making as well as more effective use of these weapons. Better decisions can change policy as well as possibly the tide of a war as seen by the Iraq (2007) case. Assessing each individual situation may seem like a simple thought but it is important because there is a new U.S. president in office.

Additionally, each dimension provided different policy implications. For instance, the diplomatic dimension highlighted the international implications of using these weapons, pointing out that using a cyberweapon is a potential violation of state sovereignty. The political dimension highlighted the domestic ramifications of using cyberweapons which was often a delicate balance between the government's desire to do something and the U.S. public not wanting to get bogged down in an intractable conflict. The economic dimension highlighted the costs of using cyberweapons indicating that these weapons could possibly be more useful than other expensive options or better position the U.S. to achieve its desired goals.

In the Introduction, I also stated that this dissertation could create the spectrum of action that Robert Belk and Matthew Noyes called for. The interviewees (and a recent *New York Times* article) suggested covert cyberweapons can be useful for targeting W.M.D. programs, (reinforcing my original claim). This is another contribution and policy implication of this dissertation. Additionally, confidence, escalation and tit-for-tat were

concerns that resurfaced in many deliberations over deployment. Thus, perhaps we could add these ideas to the spectrum of action.

In June 2017, I attended the 2nd annual "State of the Field of Cyber Conflict Studies Workshop" at Columbia University where the discussions raised questions that were directly pertinent to this dissertation.[43] For instance, there was a discussion about terminology. Some participants encouraged the use of "necessary" as opposed to "required" conditions.[44] This dissertation aligns with this recommendation. However, some participants did not like the term "cyber capability" [45] which is interesting, because that was not the consensus from the practitioners I spoke with in this field. Thus, here is a difference between academics and practitioners. Some participants urged that "cyberweapons" or "tools" or "capabilities" does not matter but rather it is the effects or outcome that matters.[46]

Another discussion point was about decision-making. One cyber scholar said a key question for decisionmakers was "is this worth what it's going to cost me?"[47] Another participant claimed that cyber is one domain that is good for decisionmakers because there are computer activity logs so decisionmakers know what to expect.[48] "We have the data," proclaimed one participant.[49] This is interesting though because some of the people who

---

[43] "The State of the Field of Cyber Conflict Studies Workshop," (conference, Columbia University, New York, N.Y., June 8, 2017).

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Ibid.

were at this conference are the same people who declined to be interviewed citing a lack of data or they told me during the interview that there was a lack of data.

Another interesting point raised was that we are producing a set of decisionmakers that would not make a decision until they know everything.[50] I think the 13 cases of this dissertation disproves this point. One participant also claimed that the U.S. goes to war when the American public sustains it.[51] This coincides with the arguments discussed in Chapter 6.

Other questions that emerged were what sustains cyberweapons?[52] One participant raised the question of are there clear distinctions between strategic and tactical cyberwarfare?[53] Another asked how does cyber represent having to face strategic surprise?[54] One attendee said how and to what end do cyber operations integrate with conventional military capabilities?[55] These are all subjects that were touched upon in this dissertation, further adding to the national discussion that these attendees as well as many experts cited in this dissertation are calling for.

Another discussion point was in regards to authorization. One participant questioned how should authorization for cyber operations be structured? [56] The Title 10 vs.

---

[49] "The State of the Field of Cyber Conflict Studies Workshop."

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Ibid.

Title 50 debate emerged. Additionally, one participant asked can the authority to employ cyberweapons be delegated?[57] I will revisit this point later but according to the Trump administration, yes, the authority to deploy cyberweapons can be delegated.

What is the likely future of U.S. offensive (or, for that matter, defensive) use of its ever-increasing cyber capabilities? For all that I believe we have learned from this dissertation, the answers to this question are still extraordinarily difficult to predict. Part of the difficulty, of course, is that we know even less about the cyber strategies and evolving capabilities of other countries (and rogue non-state actors), but that is not all. When I began this project three years ago, I could not imagine how drastically the world would shift in such a relatively short time. Most notably, the Brexit referendum happened, Donald Trump became President of the United States, and Russia interfered in the 2016 U.S. presidential election through cyber means. All of these events impacted my dissertation, I am keenly aware, because I was conducting my research and writing with an implicit assumption of rationality on the part especially of decisionmakers, which has now (to my mind) been seriously eroded or completely upended.

From 2011 - 2014, the Obama administration thought about using a cyberweapon to attack Syria. In 2017, the Trump administration bombed Syria, a radical departure from their statements only a few days prior.[58] Whereas the Obama administration may have agonized over making decisions, this new administration thus far seems inclined to act on

---

[57] "The State of the Field of Cyber Conflict Studies Workshop."

[58] Michael R. Gordon, Helene Cooper and Michael D. Shear, "Dozens of U.S. Missiles Hit Air Base in Syria," *The New York Times,* April 6, 2017, accessed April 10, 2017, https://www.nytimes.com/2017/04/06/world/middleeast/us-said-to-weigh-military-responses-to-syrian-chemical-attack.html.

impulse, public bombast, largely empty promises and threats, and thus a sort of consistent unpredictability. Possibly this partially reflects a strategy of the rationality of irrationality, but it is profoundly destabilizing and dangerous. Moreover, with all the initial chaos emanating from the White House, there is also possibly early indication of a decentralizing trend regarding some military decisions. This is a policy implication of this dissertation. During the Obama administration there were many officials involved in the deliberations, but President Obama often signed off. Additionally, according to the nuclear strike process, there are many committees that review these decisions. Now, that may no longer be the procedure. A Senior Cyber Policy Advisor I spoke with commented that "something to watch in the new administration is their decision-making and authority to delegate will be greater." The controversial Yemen raid of January 29, 2017, appears to have been a case in point. Following that, the media pointed out that the Trump administration "has said that it wants to speed the decision-making when it comes to such strikes, delegating more power to lower-level officials so that the military may respond more quickly."[59] Will the decision process over using offensive cyber capabilities be similarly changed, with the probable effect of making such use all the more likely? A journalist I spoke with said, if the Trump administration decides to use these capabilities today (as they have indicated), then the only thing probably stopping them is legality, not money. Frankly, I wonder if even legality will prove to be much of a deterrent.

[59] Eric Schmitt and David E. Sanger, "Raid in Yemen: Risky from the Start and Costly in the End," *The New York Times,* February 1, 2017, accessed March 1, 2017, https://www.nytimes.com/2017/02/01/world/middleeast/donald-trump-yemen-commando-raid-questions.html.

Bibliography

"2010 SIGINT Development Conference." *Spiegel Online International,* December 29, 2013. Accessed November 2, 2016. http://www.spiegel.de/media/media-35667.pdf.

Adams, James. "Virtual Defense." *Foreign Affairs* 80, no. 3 (May/June, 2001): 98-112. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/20050154.

Albright, David, Paul Brannan, and Christina Walrond*. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*. Institute for Science and Technology, December 22, 2010. Accessed May 27, 2016a. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

———. *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*. Institute for Science and Technology*,* February 15, 2011. Accessed May 27, 2016b. http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8.

Aldenderfer, Mark S. and Roger K. Blashfield. *Cluster Analysis*. Quantitative Applications in the Social Sciences (Book 44). Newbury Park, CA: Sage University Paper, 1984.

Aldridge, Robert C. *First Strike!: The Pentagon's Strategy for Nuclear War*. Boston: South End Press, 1983.

Alexander, David. "Cost of a U.S. Strike against Syria could top Hagel's estimate." *Reuters,* September 5, 2013a. Accessed December 13, 2016. http://www.reuters.com/article/us-syria-crisis-usa-costs-idUSBRE98415K20130905.

———. "Hagel Estimates Cost of Syria Strike at 'Tens of Millions' of Dollars." *Reuters,* September 4, 2013b. Accessed December 13, 2016. http://www.reuters.com/article/us-syria-crisis-usa-cost-idUSBRE98312N20130904.

Allison, Graham. *Essence of Decision: Explaining the Cuban Missile Crisis*. Canada: Little, Brown & Company, 1971.

———. "U.S. National Interests." *Belfer Center for Science and International Affairs*. February 18, 2010. Accessed October 15, 2014. https://dnnpro.outer.jhuapl.edu/media/RethinkingSeminars/021810/Allison_ppt.pdf.

al-Salhy, Suadad and Tim Arango. “Sunni Militants Drive Iraqi Army Out of Mosul.” *The New York Times,* June 10, 2014. Accessed December 12, 2016. https://www.nytimes.com/2014/06/11/world/middleeast/militants-in-mosul.html.

Appelbaum, Jacob, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt, and Michael Sontheimer. “The Digital Arms Race: NSA Preps America for Future Battle.” *Spiegel Online International,* January 17, 2015. Accessed May 26, 2016. http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html.

Appelbaum, Jacob, Judith Horchert, and Christian Stöcker. “Shopping for Spy Gear: Catalog Advertises NSA Toolbox.” *Spiegel Online International,* December 29, 2013. Accessed May 26, 2016. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Arkin, William M. “The Cyber Bomb in Yugoslavia.” *The Washington Post,* October 25, 1999. Accessed November 18, 2016. http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

Arkin, William M., Ken Dilanian, and Robert Windrem. “CIA Prepping for Possible Cyber Strike Against Russia.” *NBC News*. October 14, 2016. Accessed August 12, 2017. http://www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636.

Arquilla, John. “Cyberwar Is Already Upon Us.” *Foreign Policy,* February 27, 2012. Accessed May 25, 2016. http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/.

Arquilla, John and David Ronfeldt. “Cyberwar is Coming!.” *Comparative Strategy* 12, no. 2 (Spring 1993): 23-60. Accessed March 16, 2014. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf.

Baker, Peter and Jonathan Weisman. “Obama Seeks Approval by Congress for Strike in Syria.” *The New York Times,* August 31, 2013. Accessed December 6, 2016. http://www.nytimes.com/2013/09/01/world/middleeast/syria.html.

Baldor, Lolita C. “U.S. to Create the Independent U.S. Cyber Command, Split Off from NSA.” *PBS*. July 17, 2017. Accessed August 1, 2017. http://www.pbs.org/newshour/rundown/u-s-create-independent-u-s-cyber-command-split-off-nsa/.

Bamford, James. “Edward Snowden: The Untold Story.” *Wired,* August 22, 2014. Accessed March 22, 2017. https://www.wired.com/2014/08/edward-snowden/.

Barnes, Brooks and Michael Cieply. “Sony Drops ‘The Interview’ Following Terrorist Threats.” *The New York Times,* December 17, 2014. Accessed November 29, 2016. http://nyti.ms/1GtuCOw.

Barnes, Brooks and Nicole Perlroth. “Sony Films Are Pirated, and Hackers Leak Studio Salaries.” *The New York Times,* December 2, 2014a. Accessed June 14, 2016. http://www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html.

———. “Sony Pictures and F.B.I. Widen Hack Inquiry.” *The New York Times,* December 3, 2014b. Accessed November 29, 2016. http://www.nytimes.com/2014/12/04/business/sony-pictures-and-fbi-investigating-attack-by-hackers.html.

Barry, John. “America’s Secret Libya War.” *The Daily Beast*. August 30, 2011. Accessed December 13, 2016. http://www.thedailybeast.com/articles/2011/08/30/america-s-secret-libya-war-u-s-spent-1-billion-on-covert-ops-helping-nato.html.

Barzashka, Ivanka. “Are Cyber-Weapons Effective?” *The Rusi Journal* 158, no. 2 (April 28, 2013): 48-56. http://www.libraries.rutgers.edu/rul/index.shtml.

Bazeley, Patricia and Kristi Jackson. *Qualitative Data Analysis with Nvivo.* London: Sage Publications, 2013.

Beard, Sterling C. “Marine officer says US using cyberwarfare in Afghanistan.” *The Hill*. August 24, 2012. Accessed August 12, 2017. http://thehill.com/policy/defense/245421-marine-officer-says-us-using-cyberwarfare-in-afghanistan.

Becker, Jo and Scott Shane. “The Libya Game | Part 1 Hillary Clinton, ‘Smart Power’ and a Dictator’s Fall.” *The New York Times*. February 27, 2016. Accessed December 6, 2016. http://www.nytimes.com/2016/02/28/us/politics/hillary-clinton-libya.html.

Belk, Robert and Matthew Noyes. *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*. (Cambridge, MA: Belfer Center for Science and International Affairs, 2012). Accessed October 1, 2014. http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf.

Bendery, Jennifer. "Obama Pleads Again For Congress To Authorize His ISIS War." *Huffington Post,* December 7, 2015. Accessed August 20, 2017. http://www.huffingtonpost.com/entry/obama-war-authorization-isis_us_5661d411e4b08e945fef455c.

Bennett, Brian, David S. Cloud, and W. J. Hennigan. "Pentagon Weighs Cyber Campaign Against Islamic State." *Los Angeles Times*. December 20, 2015. Accessed December 12, 2016. http://www.latimes.com/world/la-fg-cyber-isis-20151220-story.html.

Berman, Russell. "The War Against ISIS Will Go Undeclared." *The Atlantic,* April 15, 2015. Accessed December 6, 2016. http://www.theatlantic.com/politics/archive/2015/04/the-war-against-isis-will-go-undeclared/390618/.

Biddle, Sam. "The NSA Leak is Real, Snowden Documents Confirm." *The Intercept,* August 19, 2016. Accessed November 10, 2016. https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/.

Blechman, Barry M. and Stephen S. Kaplan. *Force without War: U.S. Armed Forces as a Political Instrument*. Washington, D.C.: The Brookings Institution, 1978.

Bohn, Kevin and Brian Todd. "Obama, McCain Campaigns' Computers Hacked for Policy Data." *CNN,* November 6, 2008. Accessed February 28, 2017. http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/.

Boldewin, Frank. "Rootkit.TmpHider." *Wilders Security Forums* (blog). July 14, 2010. Accessed June 18, 2016. http://www.wilderssecurity.com/threads/rootkit-tmphider.276994/#post-1712134.

Bowden, Mark. "The Hunt for 'Geronimo.'" *Vanity Fair*. October 12, 2012. Accessed April 22, 2017. http://www.vanityfair.com/news/politics/2012/11/inside-osama-bin-laden-assassination-plot.

Bradley, Matt. "ISIS Declares New Islamist Caliphate." *The New York Times,* June 29, 2014. Accessed December 12, 2016. http://www.wsj.com/articles/isis-declares-new-islamist-caliphate-1404065263.

Brantly, Aaron Franklin. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Athens, GA: University of Georgia Press, 2016.

Brito, Jerry and Tate Watkins. "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy." *Harvard Law School National Security Journal* 3, no. 1 (2011): 39-84. Accessed May 2, 2016. http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Brito-and-Watkins.pdf.

Broad, William J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *The New York Times,* January 15, 2011. Accessed April 18, 2016. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Brown, Gary D. and Andrew O. Metcalf. "Easier Said Than Done: Legal Reviews of Cyber Weapons." *Journal of National Security Law & Policy* 7, no. 115 (2014): 115-138. http://www.libraries.rutgers.edu/rul/index.shtml.

Brown, Gordon. "Statements By President Obama French President Sarkozy And British Prime Minister Brown On Iranian Nuclear Facility." September 25, 2009. Accessed June 25, 2016. *The White House*. https://www.whitehouse.gov/the-press-office/2009/09/25/statements-president-obama-french-president-sarkozy-and-british-prime-mi.

Brulé, David J. "Explaining and Forecasting Leaders' Decisions: A Poliheuristic Analysis of the Iran Hostage Rescue Decision." *International Studies Perspectives* 6, no. 1 (February 2005): 99-113. EBSCOhost via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

———. "The Poliheuristic Research Program: An Assessment and Suggestions for further Progress." *International Studies Review* 10, no. 2 (June 2008): 266-293. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/25481960.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. New York: Oxford University Press, 2016.

Bumiller, Elisabeth. “Threats and Responses: The Cost; White House Cuts Estimate of Cost of War with Iraq.” *The New York Times,* December 31, 2002. Accessed December 11, 2016. http://www.nytimes.com/2002/12/31/us/threats-responses-cost-white-house-cuts-estimate-cost-war-with-iraq.html.

Bumiller, Elisabeth and David D. Kirkpatrick. “NATO Agrees to Take Command of No-Fly Zone in Libya.” *The New York Times,* March 24, 2011. Accessed December 5, 2016. http://www.nytimes.com/2011/03/25/world/africa/25libya.html?pagewanted=all.

Bumiller, Elisabeth and Thom Shanker. “Panetta Warns of Dire Threat of Cyberattack on U.S.” *The New York Times,* October 11, 2012. Accessed April 16, 2014. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

Bush, George W. “President Bush Addresses Nation on Iraq War.” Speech, Washington, D.C., January 10, 2007. Accessed August 12, 2017. *CQ Transcripts Wire*. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011002208.html.

Bush, George W. “President Bush Addresses the Nation.” Speech, Washington, D.C., March 19, 2003. Accessed December 10, 2016. *The White House*. https://georgewbush-whitehouse.archives.gov/news/releases/2003/03/20030319-17.html.

Callimachi, Rukmini. “3 ISIS Terrorism Planners Killed in Syria Airstrike, Pentagon Says.” *The New York Times,* December 13, 2016. Accessed December 13, 2016. http://www.nytimes.com/2016/12/13/world/middleeast/isis-airstrike-raqqa.html.

———. “The Horror Before the Beheadings.” *The New York Times,* October 25, 2014. Accessed December 12, 2016. https://www.nytimes.com/2014/10/26/world/middleeast/horror-before-the-beheadings-what-isis-hostages-endured-in-syria.html.

Carr, Jeffrey. *Inside Cyber Warfare*. California: O’Reilly Media, 2010.

———. “The misunderstood acronym: Why cyber weapons aren’t WMD.” *Bulletin of the Atomic Scientists* 69, no. 5 (September 1, 2013): 32-37. EBSCOhost via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Carroll, Joseph. *Americans Say Iran Is Their Greatest Enemy*. Gallup. February 23, 2006. Accessed December 10, 2016. http://www.gallup.com/poll/21607/americans-say-iran-their-greatest-enemy.aspx.

Cartwright, James E. *Joint Terminology for Cyberspace Operations*. Washington, D.C.: Department of Defense. 2010. Accessed March 18, 2017. http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

Caudle, Daryl L. "Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers." PhD diss., University of Phoenix, 2010. ProQuest via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Chozick, Amy. "Obama to See if North Korea Should Return to Terror List." *The New York Times,* December 21, 2014. Accessed November 29, 2016. http://nyti.ms/1GJUkhU.

Cirenza, Patrick. "Cyberweapons Aren't Like Nuclear Weapons." *Slate,* March 15, 2016. Accessed May 28, 2016. http://www.slate.com/articles/technology/future_tense/2016/03/cyberweapons_are_not_like_nuclear_weapons.html.

Clapper, James. "Russia's Hacking of U.S. Elections." *C-SPAN* video. January 5, 2017. Accessed March 12, 2017. https://www.c-span.org/video/?c4641807/living-nsa-glass-house.

Clark, David D. and Susan Landau. "Untangling Attribution." *Harvard National Security Journal* 2, no. 2 (2011): 323-352. Hein Online via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins Publishers, 2010.

Clayton, Mark. "From the man who discovered Stuxnet, dire warnings one year later." *The Christian Science Monitor,* September 20, 2011. Accessed July 28, 2016. http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later.

———. “In any US-Syria conflict, cyberweapons could fly in both directions.” *The Christian Science Monitor,* September 6, 2013. Accessed December 6, 2016. http://www.csmonitor.com/USA/Military/2013/0906/In-any-US-Syria-conflict-cyberweapons-could-fly-in-both-directions-video.

“Combined Joint Task Force - Operation Inherent Resolve (CJTF-OIR).” *U.S. Central Command*. Accessed December 13, 2016. http://www.centcom.mil/OPERATIONS-AND-EXERCISES/OPERATION-INHERENT-RESOLVE/.

Cooper, Helene. “Obama Cites Limits of U.S. Role in Libya.” *The New York Times,* March 28, 2011. Accessed December 5, 2016. http://www.nytimes.com/2011/03/29/world/africa/29prexy.html.

Cooper, Helene, Mark Landler, and Alissa J. Rubin. “Obama Allows Limited Airstrikes on ISIS.” *The New York Times,* August 7, 2014. Accessed December 12, 2016. https://www.nytimes.com/2014/08/08/world/middleeast/obama-weighs-military-strikes-to-aid-trapped-iraqis-officials-say.html.

“Cyber Incident Severity Schema.” *The White House*. July 26, 2016. Accessed December 2, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf.

“Cyberspace & Information Operations Study Center.” *Air University*. Accessed March 8, 2017. http://www.au.af.mil/info-ops/influence.htm#top.

“Cyberwar: The Threat from the Internet.” *The Economist*. July 1, 2010. Accessed May 4, 2016. http://www.economist.com/node/16481504.

Daalder, Ivo H. and James G. Stavridis. “NATO’s Victory in Libya.” *Foreign Affairs* 91, no. 2 (March/April, 2012). JSTOR via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Debeck, Charles. “The Correlates of Cyber Warfare: A Database for the Modern Era.” Master’s thesis, Iowa State University, 2011. Accessed November 8, 2014. http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3066&context=etd.

Deibert, Ronald. “Tracking the Emerging Arms Race in Cyberspace.” *Bulletin of the Atomic Scientists* 67, no. 1 (January 1, 2011): 1-8. EBSCOhost via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1 (Spring, 2011): 32-61. ProQuest via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Dempsey, General Martin E. "General Dempsey's Letter to Senator Levin on the U.S. Military and the Syrian Conflict, July 2013." *Council on Foreign Relations*. July 19, 2013. Accessed December 13, 2016. http://www.cfr.org/syria/general-dempseys-letter-senator-levin-us-military-syrian-conflict-july-2013/p31198.

Denning, Dorothy E. "Stuxnet: What Has Changed?" *Future Internet* 4, (2012): 672-687. Accessed March 12, 2016. http://www.mdpi.com/1999-5903/4/3/672.

Denning, Dorothy E. and Bradley J. Strawser. "Moral Cyber Weapons," *Naval Postgraduate School.* 1-20. Accessed June 5, 2016. http://faculty.nps.edu/dedennin/publications/Moral%20Cyber%20Weapons%20-%20Part-II-CH-6%20-%2024Oct2013%20(3).pdf.

"The Department of Defense Cyber Strategy." *Department of Defense*. Accessed April 2, 2017. https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

DeRouen Jr., Karl. "The Decision Not to Use Force at Dien Bien Phu: A Poliheuristic Perspective." In *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making*. Edited by Alex Mintz, 11-28. New York: Palgrave Macmillan, 2002.

———. "Presidents and the Diversionary Use of Force: A Research Note." *International Studies Quarterly* 44, (2000): 317-328. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Dictionary of Military and Associated Terms. February 15, 2016. Accessed September 19, 2016. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4 (2010): 384-410. EBSCOhost via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Dixon, Paul. "'Hearts and Minds'? British Counter-Insurgency from Malaya to Iraq." *Journal of Strategic Studies* 32, no. 3 (2009): 353-381. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

DOD Dictionary of Military and Associated Terms. March 2017. Accessed April 1, 2017. http://www.dtic.mil/doctrine/dod_dictionary/.

DOD Dictionary of Military Terms. Accessed April 2, 2014. http://www.dtic.mil/doctrine/dod_dictionary/.

Dugan, Andrew. *In U.S., Syria Emerges as a Top Problem, but Trails Economy*. Gallup, September 11, 2013a. Accessed August 20, 2017. http://www.gallup.com/poll/164348/syria-emerges-top-problem-trails-economy.aspx.

———. *U.S. Support for Action in Syria Is Low Vs. Past Conflicts*. Gallup. September 6, 2013b. Accessed December 6, 2016. http://www.gallup.com/poll/164282/support-syria-action-lower-past-conflicts.aspx.

Dunn, Ashley. "Battle Spilling Over Onto the Internet." *Los Angeles Times,* April 3, 1999, Accessed November 29, 2016. http://articles.latimes.com/1999/apr/03/news/mn-23851.

Employee of The New York Times and Hubbard, Ben. "Life in a Jihadist Capital: Order with a Darker Side." *The New York Times,* July 23, 2014. Accessed December 12, 2016. https://www.nytimes.com/2014/07/24/world/middleeast/islamic-state-controls-raqqa-syria.html.

"FACT SHEET: Presidential Policy Directive on United States Cyber Incident Coordination." *The White House*. July 26, 2016. Accessed December 2, 2016. https://www.whitehouse.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1.

Falliere, Nicolas, Liam O'Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Symantec, February 2011. Accessed March 3, 2016. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Farwell, James P. and Rafal Rohozinski. "The New Reality of Cyber War." *Survival* 54, no. 4 (August 2012): 107-120. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

———. "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1 (February - March 2011): 23-40. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Fearon, James D. “Iraq’s Civil War.” *Foreign Affairs* 86, no. 2 (March - April 2007): 2-15. JSTOR via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Feldmann, Linda. “The Impact of Bush Linking 9/11 and Iraq.” *The Christian Science Monitor,* March 14, 2003. Accessed December 11, 2016. http://www.csmonitor.com/2003/0314/p02s01-woiq.html.

Fink, Lt. Cmdr. Kallie D., Maj. John D. Jordan, and Maj. James E. Wells. “Considerations for Offensive Cyberspace Operations.” *Military Review* (May-June 2014): 4-11. Accessed November 29, 2016. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20140630_art005.pdf.

Fulghum, David A. “Kosovo Conflict Spurred New Airborne Technology Use.” *Aviation Week & Technology* 151, no. 9 (1999): 30-34. http://www.libraries.rutgers.edu/rul/index.shtml.

“Full Text: Bush’s Speech.” *The Guardian*. March 17, 2003. Accessed December 10, 2016. https://www.theguardian.com/world/2003/mar/18/usa.iraq.

Gady, Franz-Stefan. “The US Military Wants to Train More Cyber Warriors.” *The Diplomat,* February 6, 2015. Accessed June 1, 2016. http://thediplomat.com/2015/02/the-us-military-wants-to-train-more-cyber-warriors/.

Gallagher, Ryan and Glenn Greenwald. “How the NSA Plans to Infect ‘Millions’ of Computers with Malware.” *The Intercept,* March 12, 2014. Accessed May 13, 2016. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.

Gauss: Abnormal Distribution. Kaspersky Lab, August 9, 2012. Accessed June 11, 2016. https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (Fall, 2013): 41-73. EBSCOhost via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Geers, Kenneth. "Cyber Weapons Convention." *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 5 (2010): 547-551. Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Gellman, Barton and Ellen Nakashima. “U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show.” *The Washington Post*. August 30, 2013. Accessed March 22, 2016. https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

Gilbert, David. “Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog.” *International Business Times,* February 6, 2014. Accessed December 13, 2016. http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.

Glendinning, Lee. “Obama, McCain computers ‘hacked’ during election campaign.” *The Guardian,* November 7, 2008. Accessed February 28, 2017. https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa.

Gordon, Michael R., Helene Cooper, and Michael D. Shear. “Dozens of U.S. Missiles Hit Air Base in Syria.” *The New York Times,* April 6, 2017. Accessed April 10, 2017. https://www.nytimes.com/2017/04/06/world/middleeast/us-said-to-weigh-military-responses-to-syrian-chemical-attack.html.

Gordon, Michael R. and David E. Sanger. “Deal Reached on Iran Nuclear Program; Limits on Fuel Would Lessen with Time." *The New York Times,* July 14, 2015. Accessed August 12, 2017. https://www.nytimes.com/2015/07/15/world/middleeast/iran-nuclear-deal-is-reached-after-long-negotiations.html.

Gostev, Alexander. “Kaspersky Security Bulletin 2012. Cyber Weapons.” *Securelist*. December 18, 2012. Accessed January 28, 2015. http://securelist.com/analysis/kaspersky-security-bulletin/36762/kaspersky-security-bulletin-2012-cyber-weapons/.

“Government Assessment of the Syrian Government’s Use of Chemical Weapons on August 21, 2013.” August 30, 2013. Accessed December 6, 2016. *The White House.* https://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21.

Greenberg, Andy. “No One Wants to Buy Those Stolen NSA-Linked ‘Cyberweapons.’” *Wired*. August 16, 2016. Accessed November 1, 2016. https://www.wired.com/2016/08/no-one-wants-buy-stolen-nsa-linked-cyberweapons/.

———. “Shopping for Zero-Days: A Price List for Hacker’s Secret Software Exploits.” *Forbes,* March 23, 2013. Accessed October 30, 2014. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Greenwald, Glenn. “XKeyscore: NSA tool collects 'nearly everything a user does on the internet.’” *The Guardian,* July 31, 2013a. Accessed August 12, 2017. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Greenwald, Glenn and Ewen MacAskill. “Obama orders US to draw up overseas target list for cyber-attacks.” *The Guardian,* June 7, 2013b. Accessed November 1, 2014. http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Gross, Michael Joseph. “A Declaration of Cyber-War.” *Vanity Fair,* March 2, 2011. Accessed May 20, 2014. http://www.vanityfair.com/news/2011/03/stuxnet-201104.

Guccifer 2.0 (@GUCCIFER_2). “@wikileaks published #DNCHack docs I'd given them!!! #HillaryClinton #DonaldTrump #BernieSanders #Guccifer2.” Twitter. July 22, 2016. 9:44 a.m. Accessed August 12, 2017. https://twitter.com/GUCCIFER_2/status/756530278982684672.

Haberman, Maggie and David E. Sanger. “Transcript: Donald Trump Expounds on His Foreign Policy Views.” *The New York Times,* March 26, 2016. Accessed March 30, 2016. http://www.nytimes.com/2016/03/27/us/politics/donald-trump-transcript.html.

Hagel, Chuck. “As Delivered Remarks by Secretary of Defense Chuck Hagel at the Retirement Ceremony for General Keith Alexander.” Speech, Fort Meade, M.D., March 28, 2014. Accessed May 1, 2016. *Office of the Director of National Intelligence IC on the Record*. https://icontherecord.tumblr.com/post/81297943300/as-delivered-remarks-by-secretary-of-defense-chuck.

Harris, Shane. *@War: The Rise of the Military-Internet Complex*. New York: Houghton Mifflin Harcourt Publishing Company, 2014.

Harrison, Todd, John Stillion, Eric Lindsey, and Jacob Cohn. *Estimating the Cost of Operations Against ISIL*. Center for Strategic and Budgetary Assessments. September 2014. Accessed December 13, 2016. http://csbaonline.org/uploads/documents/Estimating-the-Costs-of-Operations-against-ISIL.pdf.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986-2012*. Virginia: Cyber Conflict Studies Association, 2013a.

———. "Why the U.S. Should Use Cyber Weapons Against Syria." *Defense One*. August 30, 2013b. Accessed December 6, 2016. http://www.defenseone.com/technology/2013/08/why-us-should-use-cyber-weapons-against-syria/69776/.

Hendren, John. "'Sunni Awakening': Insurgents Are Now Allies." *ABCNews,* December 23, 2007. Accessed August 12, 2017. http://abcnews.go.com/International/story?id=4045471.

Hersh, Seymour M. "The Online Threat." *The New Yorker*. November 1, 2010. Accessed May 15, 2014. http://www.newyorker.com/magazine/2010/11/01/the-online-threat.

Hilsenrath, Jon, Serena Ng, and Damian Paletta. "Worst Crisis Since '30s, With No End Yet in Sight." *The Wall Street Journal,* September 18, 2008. Accessed December 10, 2016. http://www.wsj.com/articles/SB122169431617549947.

"Himes, Westmoreland, Members of Cybersecurity Subcommittee Call for Cyberwarfare Rules." November 5, 2015. Accessed May 10, 2016. https://himes.house.gov/press-release/himes-westmoreland-members-cybersecurity-subcommittee-call-cyberwarfare-rules.

Hirschfeld, Julie and David E. Sanger. "Obama and Xi Jinping of China Agree to Steps on Cybertheft." *The New York Times,* September 25, 2015. Accessed March 10, 2017. https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

Hubbard, Ben. "Qaeda Branch in Syria Pursues its Own Agenda." *The New York Times*. October 1, 2013. Accessed December 12, 2016. http://www.nytimes.com/2013/10/02/world/middleeast/in-pushing-its-own-agenda-for-syria-a-qaeda-franchise-turns-rebels-into-enemies.html.

———. "Al Qaeda Breaks with Jihadist Group in Syria Involved in Rebel Fighting." *The New York Times,* February 3, 2014. Accessed December 12, 2016. https://www.nytimes.com/2014/02/04/world/middleeast/syria.html.

Iasiello, Emilio. "Are Cyber Weapons Effective Military Tools?." *Military and Strategic Affairs* 7, no. 1 (March, 2015): 23-40. Accessed June 18, 2016. http://www.inss.org.il/uploadImages/systemFiles/2_Iasiello.pdf.

Iran. (Gallup). Accessed December 10, 2016. http://www.gallup.com/poll/116236/iran.aspx.

Jaffe, Greg and Thomas Gibbons-Neff. "Obama Seeks to Intensify Operations in Syria with Special Ops Troops." *The Washington Post,* October 30, 2015. Accessed December 10, 2016. https://www.washingtonpost.com/politics/obame-decides-on-small-special-operations-force-for-syria/2015/10/30/a8f69c0e-7f13-11e5-afce-2afd1d3eb896_story.html?utm_term=.562b8fd2582d.

Jervis, Robert. "Deterrence Theory Revisited." *World Politics* 31, no. 2 (January 1979): 289-324. JSTOR via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

———. *Perception and Misperception in International Politics*. Princeton, N.J: Princeton University Press, 1976.

Joint Publication 3-05 Special Operations. Department of Defense*,* July 16, 2014. Accessed March 15, 2017. http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf.

Joint Publication 3-12 (R) Cyberspace Operations. Department of Defense, February 5, 2013. Accessed March 15, 2017. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Joint Publication 5-0 Joint Operation Planning. Department of Defense, August 11, 2011. Accessed March 15, 2017. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

Jones, Jeffrey M. *Americans Shift to More Negative View of Libya Military Action*. Gallup. June 24, 2011a. Accessed December 10, 2016. http://www.gallup.com/poll/148196/americans-shift-negative-view-libya-military-action.aspx.

———. *Obama Approval Rallies Six Points to 52% After Bin Laden Death*. Gallup. May 5, 2011b. Accessed June 2, 2017. http://www.gallup.com/poll/147437/obama-approval-rallies-six-points-bin-laden-death.aspx.

Junio, Timothy J. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies* 36, no. 1 (February 6, 2013a): 125-133. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

———. “The Politics and Strategy of Cyber Conflict.” PhD diss., University of Pennsylvania, 2013b.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016a.

———. “The First Drone Strike.” *Slate,* September 14, 2016b. Accessed August 12, 2017. http://www.slate.com/articles/news_and_politics/the_next_20/2016/09/a_history_of_the_armed_drone.html.

Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” 38, no. 2 (Fall 2013): 7-40. Project Muse via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

———. “The Virtual Weapon: Dilemmas and Future Scenarios.” *Politique Étrangère* 79, no. 4 (Winter 2014-2015): 1-12. Accessed November 29, 2016. https://www.ifri.org/sites/default/files/atoms/files/kello_vanglaise_0.pdf.

“Key Players in Operation Buckshot Yankee.” *The Washington Post,* December 8, 2011. Accessed August 12, 2017. https://www.washingtonpost.com/world/national-security/key-players-in-operation-buckshot-yankee/2011/12/08/gIQASJaSgO_story.html?utm_term=.5280e6e02a7d.

Kirkpatrick, David D., Steven Erlanger, and Elisabeth Bumiller. “Allies Open Air Assault on Qaddafi’s Forces in Libya.” *The New York Times,* March 19, 2011a. Accessed December 5, 2016. http://www.nytimes.com/2011/03/20/world/africa/20libya.html?pagewanted=all.

Kirkpatrick, David D. and Kareem Fahim. “Qaddafi Warns of Assault on Benghazi as U.N. Vote Nears.” *The New York Times,* March 17, 2011b. Accessed December 5, 2016. http://www.nytimes.com/2011/03/18/world/africa/18libya.html?pagewanted=all.

Kristensen, Hans M. *Obama and the Nuclear War Plan*. Washington, D.C. Federation of American Scientists. February 2010. Accessed April 1, 2017. https://fas.org/programs/ssp/nukes/publications1/WarPlanIssueBrief2010.pdf.

———. “White House Guidance Led to New Nuclear Strike Plans Against Proliferators, Document Shows.” *Federation of American Scientists* (blog). November 5, 2007. Accessed April 1, 2017. https://fas.org/blogs/security/2007/11/white_house_guidance_led_to_ne/#more.

Landler, Mark. “Obama Threatens Force Against Syria.” *The New York Times,* August 20, 2012. Accessed December 6, 2016. http://www.nytimes.com/2012/08/21/world/middleeast/obama-threatens-force-against-syria.html.

Landy, Heather. “With Bannon Out, Here’s Trump’s New National Security Council.” *Defense One*, April 6, 2017. Accessed August 11, 2017. http://www.defenseone.com/politics/2017/04/bannon-out-heres-trumps-new-national-security-council/136805/.

Langner, Ralph. “Stuxnet logbook, Sep 16 2010, 1200 hours MESZ.” *Langner* (blog). September 16, 2010. Accessed June 12, 2016. http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/#more-217.

———. “Stuxnet’s Secret Twin.” *Foreign Policy,* November 19, 2013. Accessed June 18, 2016. http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

Lawson, Sean. “DOD’s ‘First’ Cyber Strategy is Neither First, Nor a Strategy.” *Forbes,* August 1, 2011. Accessed April 15, 2016. http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/#5ebcfbd133a8.

Lee, David. “Flame: Massive Cyber-Attack Discovered, Researchers Say.” *BBC,* May 28, 2012. Accessed April 8, 2014. www.bbc.com/news/technology-18238326.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, California: RAND Corporation, 2009. Accessed June 10, 2014. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

———. *Cyberspace in Peace and War*. Maryland: Naval Institute Press, 2016.

———. “What is Information Warfare?.” Washington, D.C.: Institute for National Strategic Studies. August 1995. Accessed June 10, 2014. www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662.

Library of Congress, Congressional Research Service, *Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*. By Clay Wilson, RL32114, (January 29, 2008). Accessed April 2, 2014. fas.org/sgp/crs/terror/RL32114.pdf.

———. Congressional Research Service, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*. By Clay Wilson, RL32114 (October 17, 2003). Accessed April 2, 2014. fas.org/irp/crs/RL32114.pdf.

———. Congressional Research Service, *Information Operations and Cyberwar: Capabilities and Related Policy Issues*. By Clay Wilson, RL31787 (September 14, 2006). Accessed April 2, 2014. http://fas.org/irp/crs/RL31787.pdf.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (June 2012): 401-428. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml;

———. "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio." *Journal of Strategic Studies* 36, no. 1 (February 12, 2013): 134-138. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4, no. 1 (2010): 63-86. Hein Online via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (August, 2013): 365-404. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Lindsay, Jon R. and Lucas Kello. "Correspondence: A Cyber Disagreement." *International Security* 39, no. 2 (Fall 2014): 181-192. Project Muse via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Lipton, Eric, David E. Sanger, and Shane Scott. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." *The New York Times,* December 13, 2016. Accessed December 14, 2016. http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?hp=undefined&action=click&pgtype=Homepage&clickSource=story-

heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&_r=0.

Long, Austin. "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." *SRRN,* (June 15, 2016): 1-24. Accessed March 25, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836204.

Lubold, Gordon. "Obama's Favorite General Stripped of His Security Clearance." *Foreign Policy,* September 24, 2013. Accessed July 1, 2016. http://foreignpolicy.com/2013/09/24/obamas-favorite-general-stripped-of-his-security-clearance/.

Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (September/October, 2010): 97-108. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/20788647.

MacAskill, Ewen. "Stuxnet Cyberworm Heads Off US Strike on Iran." *The Guardian,* January 16, 2011. Accessed August 12, 2017. https://www.theguardian.com/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran.

MacFarquhar, Neil and Eric Schmitt. "Syria Threatens Chemical Attack on Foreign Force." *The New York Times,* July 23, 2012. Accessed December 6, 2016. http://www.nytimes.com/2012/07/24/world/middleeast/chemical-weapons-wont-be-used-in-rebellion-syria-says.html.

Madrigal, Alexis C. "The Stuxnet Worm? More Than 30 People Built It." *The Atlantic*, November 4, 2010. Accessed June 11, 2016. http://www.theatlantic.com/technology/archive/2010/11/the-stuxnet-worm-more-than-30-people-built-it/66156/.

Maillard, Laurent. "Iran's Nuclear Agency Hit by Computer Worm." *The Sydney Morning Herald,* September 27, 2010. Accessed July 2, 2016. http://www.smh.com.au/technology/iran-denies-nuclear-plant-computers-hit-by-worm-20100926-15sam.html.

"Malware from the Five Eyes." *Der Spiegel,* January 17, 2015. Accessed November 19, 2016. http://www.spiegel.de/media/media-35668.pdf.

"Man-in-the-middle attack." *Symantec Glossary,* accessed November 29, 2016. https://www.symantec.com/security_response/glossary/define.jsp?letter=m&word=man-in-the-middle-attack.

Markoff, John. "Malware Aimed at Iran Hit Five Sites, Report Says." *The New York Times,* February 11, 2011. Accessed May 21, 2016. http://www.nytimes.com/2011/02/13/science/13stuxnet.html.

Markoff, John and Thom Shanker. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *The New York Times,* August 1, 2009. Accessed July 5, 2016. http://www.nytimes.com/2009/08/02/us/politics/02cyber.html.

Marquis-Boire, Morgan, Claudio Guarnieri, and Ryan Gallagher. "Secret Malware in European Union Attack Linked to U.S. and British Intelligence." *The Intercept,* November 24, 2014. Accessed November 19, 2016. https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/.

Mazzetti, Mark and Eric Lichtblau. "C.I.A. Judgment on Russia Built on Swell of Evidence." *The New York Times,* December 11, 2016. Accessed December 12, 2016. http://www.nytimes.com/2016/12/11/us/politics/cia-judgment-intelligence-russia-hacking-evidence.html?ref=politics.

McGraw, Gary. "Cyber War is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36, no. 1 (2013): 109-119. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Medetsky, Anatoly. "KGB Veteran Denies CIA Caused '82 Blast." *The Moscow Times,* March 18, 2004. Accessed November 28, 2016. http://infoweb.newsbank.com.proxy.libraries.rutgers.edu/resources/doc/nb/news/1016B69A2902F371?p=AWNB.

Mele, Stefano. "Cyber-Weapons: Legal and Strategic Aspects Version 2.0." *Italian Institute of Strategic Studies Niccolo Machiavelli* (June 2013): 1-22. Accessed June 2, 2016. http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf.

Melzer, Nils. "Cyberwarfare and International Law," *United Nations Institute for Disarmament Research*, 2011. Accessed April 12, 2016. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Menn, Joseph. “Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed – sources." *Reuters,* May 29, 2015. Accessed April 9, 2017. http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529.

Miller, Greg and Ellen Nakashima. “WikiLeaks says it has obtained trove of CIA hacking tools.” *The Washington Post,* March 7, 2017. Accessed August 12, 2017. https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?utm_term=.cfec5a650b1a.

Miller, Zeke J. “U.S. Sanctions North Korea Over Sony Hack.” *Time,* January 2, 2015. Accessed December 13, 2016. http://time.com/3652479/sony-hack-north-korea-the-interview-obama-sanctions/.

Mintz, Alex. “Applied Decision Analysis: Utilizing Poliheuristic Theory to Explain and Predict Foreign Policy and National Security Decisions.” *International Studies Perspectives* 6, (February 2005): 94-98. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

———. “The Decision to Attack Iraq: A Noncompensatory Theory of Decision Making.” *The Journal of Conflict Resolution* 37, no. 4 (December 1993): 595-618. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/174541.

———. “How Do Leaders Make Decisions?: A Poliheuristic Perspective.” *The Journal of Conflict Resolution* 48, no. 1 (February 2004): 3-13. JSTOR via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Mintz, Alex and Nehemia Geva. “The Poliheuristic Theory of Foreign Policy Decisionmaking.” In *Decisionmaking on War and Peace: The Cognitive-Rational Debate*. Edited by Nehemia Geva and Alex Mintz. 81-101. Boulder, Colorado: Lynne Rienner Publishers, Inc., 1997a.

Mintz, Alex, Nehemia Geva, Steven B. Redd, and Amy Carnes. “The Effect of Dynamic and Static Choice Sets on Political Decision Making: An Analysis Using the Decision Board Platform.” *The American Political Science Review* 91, no. 3 (September 1997b): 553-566. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/2952074.

Morgan, Steven. “Cybersecurity Market Reaches $75 Billion in 2015; Expected to Reach $170 Billion by 2020.” *Forbes,* December 20, 2015. Accessed May 12, 2016. http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#4f9c9e421916.

Mueller, John E. “Presidential Popularity from Truman to Johnson.” *The American Political Science Review* 64, no. 1 (March, 1970): 18-34. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/1955610.

Myers, Steven Lee and David D. Kirkpatrick. “Allies Are Split on Goal and Exit Strategy in Libya.” *The New York Times,* March 24, 2011. Accessed December 5, 2016. http://www.nytimes.com/2011/03/25/world/africa/25policy.html?pagewanted=all.

Nakashima, Ellen. “List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare.” *The Washington Post,* May 31, 2011. Accessed May 15, 2014. http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html.

———. “National intelligence director: Hackers have targeted 2016 presidential campaigns.” *The Washington Post,* May 18, 2016a. Accessed August 20, 2017. https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html?utm_term=.ebd6e7b293ed.

———. “Obama Moves to Split Cyberwarfare Command from the NSA.” *The Washington Post,* December 23, 2016b. Accessed May 25, 2017. https://www.washingtonpost.com/world/national-security/obama-moves-to-split-cyberwarfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html?utm_term=.74a3793bc045.

———. “Russian government hackers penetrated DNC, stole opposition research on Trump.” *The Washington Post,* June 14, 2016c. Accessed August 11, 2017. http://wapo.st/1tuiAUt?tid=ss_tw&utm_term=.664687e10d33.

———. “U.S. accelerating cyberweapon research.” *The Washington Post,* March 18, 2012. Accessed November 29, 2016. https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html?utm_term=.a7280c3b0778.

———. “U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies.” *The Washington Post,* May 9, 2017. Accessed May 10, 2017. https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.b4d7df09ba88.

“Newly Released GCHQ Files: UKUSA Agreement.” *The National Archives*, June 2010. Accessed November 19, 2016. http://www.nationalarchives.gov.uk/ukusa/.

Newport, Frank. *Americans Back Bin Laden Mission; Credit Military, CIA Most*. Gallup, May 3, 2011. Accessed August 8, 2017. http://www.gallup.com/poll/147395/americans-back-bin-laden-mission-credit-military-cia.aspx.

Newport, Frank, Jeffrey M. Jones, Lydia Saad, and Joseph Carroll. *Gallup Poll Review: 10 Key Points about Public Opinion on Iraq*. Gallup, April 27, 2007. Accessed August 12, 2017. http://www.gallup.com/poll/27391/gallup-poll-review-key-points-about-public-opinion-iraq.aspx.

Norman, Jim. *Four Nations Top U.S.’s Greatest Enemy List*. Gallup, February 22, 2016. Accessed December 10, 2016. http://www.gallup.com/poll/189503/four-nations-top-greatest-enemy-list.aspx.

Nossiter, Adam, Aurelien Breeden, and Katrin Bennhold. “Three Teams of Coordinated Attackers Carried Out Assault on Paris, Officials Say; Hollande Blames ISIS.” *The New York Times,* November 14, 2015. Accessed December 12, 2016. http://www.nytimes.com/2015/11/15/world/europe/paris-terrorist-attacks.html.

“The NSA and GCHQ’s QUANTUMTHEORY Hacking Tactics.” *The Intercept,* March 12, 2014. Accessed May 13, 2016. https://theintercept.com/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/.

“NSA Phishing Tactics and Man in the Middle Attacks.” *The Intercept,* March 12, 2014a. Accessed May 13, 2016. https://theintercept.com/document/2014/03/12/nsa-phishing-tactics-man-middle-attacks/.

“NSA Technology Directorate Analysis of Converged Data.” *The Intercept,* March 12, 2014b. Accessed May 13, 2016, https://theintercept.com/document/2014/03/12/nsa-technology-directorate-analysis-converged-data/.

"The NSA's Spy Catalog." *Der Spiegel,* December 30, 2013. Accessed November 2, 2016. http://www.spiegel.de/international/world/a-941262.html.

Nvivo for Mac. "About comparison diagrams." *QSR International*. Accessed March 22, 2017. http://help-nv11mac.qsrinternational.com/desktop/concepts/About_comparison_diagrams.htm.

———. "About hierarchy charts." *QSR International*. Accessed March 22, 2017. http://help-nv11mac.qsrinternational.com/desktop/concepts/about_hierarchy_charts.htm.

———. "Nvivo for Mac Help." *QSR International*. Accessed March 14, 2017. http://help-nv11mac.qsrinternational.com/desktop/welcome/welcome.htm.

Nye, Jr., Joseph S. "From bombs to bytes: Can our nuclear history inform our cyber future?" *Bulletin of the Atomic Scientists* 69, no. 5 (2013): 8-14. EBSCOhost via, Rutgers Universities Libraries, http://www.libraries.rutgers.edu/rul/index.shtml.

———. "Cyber Power." *Belfer Center for Science and International Affairs*, (May 2010): 1-24 Accessed May 1, 2016. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

———. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 18-38. ProQuest via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Obama, Barack. "Letter from the President -- Authorization for the Use of United States Armed Forces in Connection with the Conflict in Syria." August 31, 2013a. Accessed August 8, 2017. *The White House*. https://obamawhitehouse.archives.gov/sites/default/files/docs/aumfresolutiontext.pdf .

———. "Letter from the President – Authorization for the Use of United States Armed Forces in connection with the Islamic State of Iraq and the Levant." February 11, 2015. Accessed December 12, 2016. *The White House*. https://www.whitehouse.gov/the-press-office/2015/02/11/letter-president-authorization-use-united-states-armed-forces-connection.

———. “Letter from the President regarding the commencement of operations in Libya.” March 21, 2011. Accessed December 5, 2016. *The White House*. https://www.whitehouse.gov/the-press-office/2011/03/21/letter-president-regarding-commencement-operations-libya.

———. “Remarks by the President in Address to the Nation on Syria.” Speech, Washington, D.C., September 10, 2013b. Accessed December 6, 2016. *The White House*. https://www.whitehouse.gov/the-press-office/2013/09/10/remarks-president-address-nation-syria.

———. “Remarks by the President on Securing our Nation's Cyber Infrastructure.” Speech, Washington, D.C., May 29, 2009. Accessed February 4, 2016. *The White House*. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

———. “Statement by the President on Progress in the Fight Against ISIL.” April 13, 2016. Accessed December 10, 2016. *The White House*. https://www.whitehouse.gov/the-press-office/2016/04/13/statement-president-progress-fight-against-isil.

———. “Statement by the President on Syria.” August 31, 2013c. Accessed December 6, 2016. *The White House*. https://www.whitehouse.gov/the-press-office/2013/08/31/statement-president-syria.

Office of the Director of National Intelligence. *Background to ‘Assessing Russian Activities and Intentions in Recent US Elections,’: The Analytic Process and Cyber Incident Attribution*. National Intelligence Council, January 6, 2017. Accessed February 18, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer. *Defense Budget Overview: United States Department of Defense Fiscal Year 2017 Budget Request*. February 2016. Accessed March 1, 2016. http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_Budget_Request_Overview_Book.pdf.

Oleg, Kupreev and Ulasen Sergey. *Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.Gen.2 Review*. VirusBlokAda, June 17, 2010. Accessed March 20, 2014. ftp://antivirus.by/pub/docs/english/Rootkit.TmpHider_en.pdf.

O'Murchu, Liam. "Countdown to Zero Day—Did Stuxnet escape from Natanz?." *Symantec* (blog). November 11, 2014. Accessed, July 5, 2016. http://www.symantec.com/connect/blogs/countdown-zero-day-did-stuxnet-escape-natanz.

"Operation Inherent Resolve." *Department of Defense*. Accessed December 13, 2016. http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve.

Ostrom, Charles W. and Brian L. Job. "The President and the Political Use of Force." *The American Political Science Review* 80, no. 2 (June, 1986): 541- 566. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/1958273.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, D.C.: The National Academy of Sciences, 2009. Accessed March 7, 2017. http://www3.nd.edu/~cpence/eewt/Owens2009.pdf.

Paletta, Damian. "NSA Chief Says U.S. at 'Tipping Point' on Cyberweapons." *The Wall Street Journal,* January 21, 2016. Accessed June 17, 2016. http://www.wsj.com/articles/nsa-chief-says-u-s-at-tipping-point-on-cyberweapons-1453404976.

Panetta, Leon E. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City." Speech, New York City, N.Y., October 11, 2012. Accessed April 10, 2016. *U.S. Department of Defense*. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Perlroth, Nicole. "Hacking Group Claims N.S.A. Infiltrated Mideast Banking System." *The New York Times,* April 15, 2017. Accessed August 12, 2017. https://www.nytimes.com/2017/04/15/us/shadow-brokers-nsa-hack-middle-east.html.

———. "Researchers Find Clues in Malware." *The New York Times,* May 30, 2012. Accessed November 12, 2016. http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

Perlroth, Nicole and David E. Sanger. "North Korea Loses its Link to the Internet." *The New York Times,* December 22, 2014. Accessed January 28, 2015. http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

Peterson, Andrea. "Wikileaks posts nearly 20,000 hacked DNC emails online." *The Washington Post,* July 22, 2016. Accessed August 12, 2017. https://www.washingtonpost.com/news/the-switch/wp/2016/07/22/wikileaks-posts-nearly-20000-hacked-dnc-emails-online/?utm_term=.5b46ca985699.

Peterson, Dale. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies* 36, no. 1 (February 7, 2013): 120-124. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

"Plan X." *Defense Advanced Research Projects*. Accessed April 23, 2016. http://www.darpa.mil/program/plan- x.

Presidential Approval Ratings -- George W. Bush. (Gallup). Accessed December 10, 2016. http://www.gallup.com/poll/116500/presidential-approval-ratings-george-bush.aspx.

Presidential Approval Ratings – Barack Obama. (Gallup). Accessed December 10, 2016. http://www.gallup.com/poll/116479/barack-obama-presidential-job-approval.aspx.

"President Obama on U.S. Strategy Against ISIS." *C-SPAN* video. December 14, 2015. Accessed November 13, 2016. https://www.c-span.org/video/?402051-1/president-obama-statement-us-strategy-isis.

"Presidential Policy Directive." Accessed November 1, 2014. http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Presidential Ratings -- Issues Approval. (Gallup). Accessed December 10, 2016. http://www.gallup.com/poll/1726/presidential-ratings-issues-approval.aspx.

Poitras, Laura, Marcel Rosenbach, Fidelius Schmid, and Holger Stark. "Attacks from America: NSA Spied on European Union Offices." *Der Spiegel,* June 29, 2013. Accessed November 29, 2016. http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html.

Poulsen, Kevin. "Surprise! America Already has a Manhattan Project for Developing Cyber Attacks." *Wired,* February 18, 2015. Accessed June 1, 2016. https://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/.

Powell, Robert. “Bargaining Theory and International Conflict.” *Annual Review of Political Science* 5, no. 1 (2002): 1-30. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Redd, Steven B. “The Influence of Advisers and Decision Strategies on Foreign Policy Choices: President Clinton's Decision to Use Force in Kosovo.” *International Studies Perspectives* 6, no. 1 (Feb 2005): 129-150. http://www.libraries.rutgers.edu/rul/index.shtml.

———. “The Influence of Advisers on Foreign Policy Decision Making: An Experimental Study.” *The Journal of Conflict Resolution* 46, no. 3 (June 2002): 335-364. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/3176230.

Reiger, Frank. “Stuxnet: targeting the Iranian enrichment centrifuges in Natanz?.” *Knowledge Brings Fear* (blog), September 22, 2010. Accessed June 18, 2016. http://frank.geekheim.de/?p=1189.

“Remarks by the President on the Situation in Libya.” *The New York Times*. March 18, 2011. Accessed December 5, 2016. https://www.whitehouse.gov/the-press-office/2011/03/18/remarks-president-situation-libya.

Remler, Dahlia K. and Gregg G. Van Ryzin. *Research Methods in Practice: Strategies for Description and Causation*. Thousand Oaks, California: SAGE Publications, 2011.

Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected. (Kaspersky Lab, June 11, 2012). Accessed November 29, 2016. http://www.kaspersky.com/au/about/news/virus/2012/resource_207_kaspersky_lab_research_proves_that_stuxnet_and_flame_developers_are_connected.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington: Georgetown University Press, 2012.

Revision 03 Periodic Update. (United States Strategic Command, November 5, 2007). Accessed April 1, 2017. https://fas.org/wp-content/uploads/2007/11/revision03.pdf.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (February 2012a): 5-32. Journal of Strategic Studies via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Rid, Thomas and John Arquilla. “Think Again: Cyberwar.” *Foreign Policy* (March/April, 2012b): 80-84. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/23237859.

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1-2 (December 23, 2014): 4-37. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Rid, Thomas and Peter McBurney. “Cyber-Weapons.” *The Rusi Journal* 157, no. 1 (February 29, 2012c): 6-13. http://www.libraries.rutgers.edu/rul/index.shtml.

Riffkin, Rebecca. *Americans Name Terrorism as No. 1 U.S. Problem*. Gallup, December 14, 2015. Accessed December 12, 2016. http://www.gallup.com/poll/187655/americans-name-terrorism-no-problem.aspx.

Roberts, Dan and Spencer Ackerman. “Barack Obama authorises air strikes against Isis militants in Syria.” *The Guardian,* September 11, 2014. Accessed June 1, 2017. https://www.theguardian.com/world/2014/sep/10/obama-speech-authorise-air-strikes-against-isis-syria.

Rootkits. (Symantec Security Response). Accessed May 28, 2016. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/rootkits.pdf.

Rosenbach, Marcel, Hilmar Schmundt, and Christian Stöcker. “Experts Unmask ‘Regin’ Trojan as NSA Tool.” *Der Spiegel,* January 27, 2015. Accessed November 19, 2016. http://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html.

Rothkopf, David. “The Cool War.” *Foreign Policy,* February 20, 2013. Accessed April 18, 2016. http://foreignpolicy.com/2013/02/20/the-cool-war/.

Rouse, Margaret. “Back Door.” *Search Security*. Accessed November 19, 2016. http://searchsecurity.techtarget.com/definition/back-door.

———. “RAT (Remote Access Trojan).” *Search Security*. Accessed November 19, 2016. http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan.

Rustici, Ross M. “Cyberweapons: Leveling the International Playing Field.” *Parameters* 41, no. 3 (Autumn, 2011): 32-42. ProQuest via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Saad, Lydia. *Americans Resist a Major U.S. Role in Libya*. Gallup, March 29, 2011a. Accessed December 10, 2016. http://www.gallup.com/poll/146840/americans-resist-major-role-libya.aspx.

———. *Majority in U.S. Say Bin Laden's Death Makes America Safer.* Gallup, May 4, 2011b. Accessed August 8, 2017. http://www.gallup.com/poll/147413/majority-say-bin-laden-death-makes-america-safer.aspx.

Safire, William. “The Farewell Dossier.” *The New York Times,* February 2, 2004. Accessed June 4, 2016. http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html.

Sagan, Scott D. “SIOP-62: The Nuclear War Plan Briefing to President Kennedy.” *International Security* 12, no. 1 (Summer, 1987): 22-51. Accessed March 16, 2017. http://www.belfercenter.org/sites/default/files/legacy/files/CMC50/ScottSaganSIOP62TheNuclearWarPlanBriefingtoPresidentKennedyInternationalSecurity.pdf.

Sanger, David E. *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power*. New York: Crown Publishers, 2012a.

———. “Countering Cyberattacks Without a Playbook.” *The New York Times,* December 23, 2014a. Accessed November 29, 2016. http://www.nytimes.com/2014/12/24/world/asia/countering-cyberattacks-without-a-playbook.html.

———. “*Zero Days* Screening.” Discussion, Harvard University, Cambridge, Massachusetts, April 29, 2016a.

———. “Obama Order Sped Up Wave of Cyberattacks Against Iran.” *The New York Times,* June 1, 2012b. Accessed March 17, 2014. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

———. “Obama Strikes Back at Russia for Election Hacking.” *The New York Times,* December 29, 2016b. Accessed January 13, 2017.

https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=0.

———. "Pentagon Announces New Strategy for Cyberwarfare." *The New York Times,* April 23, 2015a. Accessed December 1, 2016. http://nyti.ms/1ProCKP.

———. "Syria War Stirs New U.S. Debate on Cyberattacks." *The New York Times,* February 24, 2014b. Accessed December 10, 2016. http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?ref=davidesanger.

———. "U.S. Cyberattacks Target ISIS in a New Line of Combat." *The New York Times,* April 24, 2016c. Accessed August 20, 2017. http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

———. "U.S. Decides to Retaliate Against China's Hacking." *The New York Times,* July 31, 2015b. Accessed November 29, 2016. http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0.

———. "U.S. Says Russia Directed Hacks to Influence Elections." *The New York Times,* October 7, 2016d. Accessed December 1, 2016. http://nyti.ms/2dLddLS.

———. "Under the Din of the Presidential Race Lies a Once and Future Threat: Cyberwarfare." *The New York Times,* November 6, 2016e. Accessed November 30, 2016. http://nyti.ms/2etAn66.

Sanger, David E., David Barboza, and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *The New York Times,* February 18, 2013. Accessed June 19, 2016. http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

Sanger, David E. and William J. Broad. "Trump Inherits a Secret Cyberwar Against North Korean Missiles." *The New York Times,* March 4, 2017. Accessed March 5, 2017. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

Sanger, David E. and Martin Fackler. "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say." *The New York Times,* January 18, 2015c. Accessed

January 28, 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0.

Sanger, David E. and Mark Mazzetti. "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict." *The New York Times*, February 16, 2016e. Accessed May 10, 2016. http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Sanger, David E. and Nicole Perlroth. "N.S.A. Breached Chinese Servers Seen as Security Threat." *The New York Times,* March 22, 2014c. Accessed January 28, 2015. http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

———. "U.S. Said to Find North Korea Ordered Cyberattack on Sony." *The New York Times,* December 17, 2014d. Accessed June 14, 2016. https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

Sanger, David E. and Michael S. Schmidt. "More Sanctions on North Korea After Sony Case." *The New York Times,* January 2, 2015d. Accessed December 1, 2016. http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

Sanger, David E., Michael S. Schmidt, and Nicole Perlroth. "Obama Vows a Response to Cyberattack on Sony." *The New York Times,* December 19, 2014e. Accessed November 29, 2016. http://nyti.ms/1Gz1GF9.

Sanger, David E. and Eric Schmitt. "Russian Ships Near Data Cables Are Too Close for U.S. Comfort." *The New York Times,* October 25, 2015e. Accessed May 10, 2016. http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

———. "Spy Agency Consensus Grows That Russia Hacked D.N.C." *The New York Times,* July 26, 2016f. Accessed August 12, 2017. https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.

Sanger, David E. and Scott Shane. "Russian Hackers Acted to Aid Trump in Election, U.S. Says." *The New York Times,* December 9, 2016g. Accessed December 10, 2016. http://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html.

Sanger, David E. and Thom Shanker. "N.S.A. Devises Radio Pathway Into Computers." *The New York Times,* January 14, 2014f. Accessed January 28, 2015. http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html.

Sanger, David E. and with John F. Burns. "Bush Orders Start of War on Iraq; Missiles Said to be Aimed at Hussein." *The New York Times,* March 19, 2003. Accessed December 11, 2016. http://www.nytimes.com/2003/03/19/international/bush-orders-start-of-war-on-iraq-missiles-said-to-be-aimed-at.html.

Sang-Hun, Choe. "North Korea Warns U.S. Over Film Mocking its Leader." *The New York Times,* June 25, 2014. Accessed June 14, 2016. http://nyti.ms/TvMzsx.

Sathasivam, Kanishkan. "'No Other Choice': Pakistan's Decision to Test the Bomb." In *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making*. Edited by Alex Mintz, 55 – 76. New York: Palgrave Macmillan, 2002.

Savage, Charlie. "Obama Pardons James Cartwright, General Who Lied to F.B.I. in Leak Case." *The New York Times,* January 17, 2017. Accessed August 12, 2017. https://www.nytimes.com/2017/01/17/us/politics/obama-pardons-james-cartwright-general-who-lied-to-fbi-in-leak-case.html.

Schmidt, Michael S. and Richard Pérez-Peña. "F.B.I. Treating San Bernardino Attack as Terrorism Case." *The New York Times,* December 4, 2015. Accessed December 12, 2016. http://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

Schmitt, Eric and David E. Sanger. "Raid in Yemen: Risky from the Start and Costly in the End." *The New York Times,* February 1, 2017. Accessed March 1, 2017. https://www.nytimes.com/2017/02/01/world/middleeast/donald-trump-yemen-commando-raid-questions.html.

Schmitt, Eric and Thom Shanker. "U.S. Debated Cyberwarfare in Attack Plan on Libya." *The New York Times,* October 17, 2011. Accessed July 5, 2016. http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2009. Accessed February 27, 2016. https://ccdcoe.org/tallinn-manual.html.

Schneier, Bruce. “Cyberweapons Have No Allegiance.” *Motherboard,* January 25, 2015. Accessed June 27, 2016. http://motherboard.vice.com/read/cyberweapons-have-no-allegiance.

“Search the DNC email database.” *Wikileaks*. July 22, 2016. Accessed August 12, 2017. https://wikileaks.com/dnc-emails/.

Security Council. “Security Council Approves ‘No-Fly Zone’ Over Libya, Authorizing ‘All Necessary Measures’ to Protect Civilians, by Vote of 10 in Favour with 5 Abstentions.” *The United Nations,* March 17, 2011. Accessed December 5, 2016. http://www.un.org.proxy.libraries.rutgers.edu/press/en/2011/sc10200.doc.htm.

Segal, Adam. “After Attributing a Cyberattack to Russia, the Most Likely Response Is Non Cyber.” *Council on Foreign Relations* (blog), October 10, 2016a. Accessed December 13, 2016. http://blogs.cfr.org/cyber/2016/10/10/after-attributing-a-cyberattack-to-russia-the-most-likely-response-is-non-cyber/.

———. *Cyber Conflict After Stuxnet: Essays from the Other Bank of the Rubicon*. Edited by Hannah Pitts and Karl Grindal. Vienna, VA: Cyber Conflict Studies Association, 2016b.

———. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: Public Affairs, 2016c.

Shakarian, Paulo. “Stuxnet: Cyberwar Revolution in Military Affairs.” *Small Wars Journal*, (April 15, 2011): 1-10, Accessed May 2, 2016. http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s_eng.pdf.

Shalal-Esa, Andrea. “Six US Air Force Cyber Capabilities Designated ‘Weapons.’” *Reuters,* April 8, 2013. Accessed November 16, 2016. http://www.reuters.com/article/net-us-cyber-airforce-weapons-idUSBRE93801B20130409.

Shamah, David. “Latest Viruses could mean ‘end of world as we know it,’ says man who discovered Flame.” *The Times of Israel,* June 6, 2012. Accessed March 20, 2016. http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/.

Shane, Scott and Jo Becker. “The Libya Gamble | Part 2, A New Libya, with ‘Very Little Time Left.’” *The New York Times,* February 27, 2016. Accessed August 20, 2017. https://www.nytimes.com/2016/02/28/us/politics/libya-isis-hillary-clinton.html.

Shane, Scott, Matthew Rosenberg, and Andrew W. Lehren. “WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents.” *The New York Times,* March 7, 2017. Accessed August 12, 2017. https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.

Shanker, Thom. “U.S. Weighs Options, on Air and Sea.” *The New York Times,* March 6, 2011. Accessed December 9, 2016. http://www.nytimes.com/2011/03/07/world/middleeast/07military.html.

Shanker, Thom, C. J. Chivers, and Michael R. Gordon. “Obama Weighs ‘Limited’ Strikes Against Syrian Forces.” *The New York Times,* August 27, 2013. Accessed December 6, 2016. http://www.nytimes.com/2013/08/28/world/middleeast/obama-syria-strike.html.

Sheldon, John B. “Toward a Theory of Cyber Power.” In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Edited by Derek S. Reveron, 207 – 224. Washington, D.C.: Georgetown University Press, 2012.

Singer, P. W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Snowden, Edward. (@Snowden). “Circumstantial evidence and conventional wisdom indicates Russian responsibility. Here's why that is significant:.” Twitter. August 16, 2016. Accessed November 29, 2016. https://twitter.com/Snowden/status/765514891813945344.

Snyder, Richard C., H. W. Bruck, and Burton Sapin. *Foreign Policy Decision-Making: An Approach to the Study of International Politics*. New York: The Free Press of Glencoe, 1962.

Sorkin, Andrew Ross. “Lehman Files for Bankruptcy; Merrill is Sold.” *The New York Times,* September 14, 2008. Accessed December 10, 2016. www.nytimes.com/2008/09/15/business/15lehman.html.

Spiegel Staff. “Inside T.A.O: Documents Reveal Top NSA Hacking Unit.” *Spiegel Online International,* December 29, 2013. Accessed November 2, 2016.

http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html.

STATA Multivariate Statistics Reference Manual Release 13 (College Station, TX: STATA Press, 1985-2013). Accessed October 25, 2016. http://www.stata.com/manuals13/mv.pdf.

Stern, Eric. "Contextualizing and Critiquing the Poliheuristic Theory." *The Journal of Conflict Resolution* 48, no. 1 (February, 2004): 105-126. Worldwide Political Science Abstracts via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (April 13, 2012): 148-170. http://www.libraries.rutgers.edu/rul/index.shtml.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (November 29, 2012): 101-108. Journal of Strategic Studies via, Rutgers Universities Libraries. http://www.libraries.rutgers.edu/rul/index.shtml.

Sweeney, Patrick. *A Primer for: The Joint Strategic Planning System (JSPS), Guidance for Employment of the Force (GEF), Joint Strategic Capabilities Plan (JSCP), the Adaptive Planning and Execution (APEX) System, and Global Force Management (GFM)*. The United States Naval War College Joint Military Operations Department, January 22, 2016. Accessed April 2, 2017. https://wss.apan.org/s/JSOFUN/Shared%20Documents/GuidingDocuments/Guidance_for_Employment_for_the_Force_GEF_2016.pdf.

Swisher, Kara. "White House. Red Chair. Obama Meets Swisher." *Recode,* February 15, 2015. Accessed August 12, 2017. https://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher.

"Symantec Code Signing Certificates." *Symantec*. Accessed May 28, 2016. https://www.symantec.com/code-signing/.

Symantec Security Response. "Regin: Top-tier espionage tool enables stealthy surveillance." *Symantec* (blog). November 23, 2014. Accessed November 19, 2016. http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance.

Symantec Security Response. *Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance*. Symantec, August 27, 2015. Accessed November 19, 2016. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf.

"Syrian opposition: 1,300 killed in chemical attack on Ghouta region." *Al Arabiya*. August 21, 2013. Accessed December 6, 2016. http://english.alarabiya.net/en/News/middle-east/2013/08/21/Syrian-activists-at-least-500-killed-in-chemical-attack-on-Eastern-Ghouta.html.

Taylor-Robinson, Michelle M. and Steven B. Redd. "Framing and the Poliheuristic Theory of Decision: The United Fruit Company and the 1954 U.S.-Led Coup in Guatemala." In *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making*. Edited by Alex Mintz, 77 – 100. New York: Palgrave Macmillan, 2002.

"The State of the Field of Cyber Conflict Studies Workshop." Conference, Columbia University, New York, N.Y., June 8, 2017.

The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. (2011). Accessed March 14, 2016. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. "Osama Bin Laden Dead." May 2, 2011. Accessed August 8, 2017. https://obamawhitehouse.archives.gov/blog/2011/05/02/osama-bin-laden-dead.

———. "Presidential Memorandum Organization of the National Security Council and the Homeland Security Council." January 28, 2017. Accessed February 2, 2017. https://www.whitehouse.gov/the-press-office/2017/01/28/presidential-memorandum-organization-national-security-council-and.

Thompson, Mark. "Former U.S. Commanders Take Increasingly Dim View of War on ISIS." *Time,* August 31, 2016. Accessed December 13, 2016. http://time.com/4474910/isis-retired-generals/.

Todd, Chuck. "MTP Exclusive: VP Biden Promises Response to Russian Hacking." *Meet the Press,* October 14, 2016. Accessed December 2, 2016. http://www.nbcnews.com/meet-the-press/video/vp-biden-on-russia-and-cyber-warfare-786308675872.

Tumulty, Karen. "Pressure Building on Obama to Specify Scope, Goals of U.S. Action in Libya." *The Washington Post,* March 24, 2011. Accessed December 10, 2016. https://www.washingtonpost.com/politics/pressure-building-on-obama-to-specify-scope-goals-of-us-action-in-libya/2011/03/24/ABE9G6RB_story.html?utm_term=.2603ee22b176.

"UN chief announces independent probe into allegations of chemical attack in Syria." *The United Nations,* March 21, 2013. Accessed December 6, 2016. http://www.un.org/apps/news/story.asp?NewsID=44450.

"U.S. Cyber Policy and Innovation." Discussion, EastWest Institute, New York, N.Y., November 3, 2016.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. (July 2011). Accessed March 1, 2016. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

U.S. Department of Defense. *The DoD Cyber Strategy*. (April 2015). Accessed March 27, 2016. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

"Use of chemical weapons in Syria would be 'crime against humanity' – Ban." *The United Nations*. August 23, 2013. December 9, 2016. http://www.un.org/apps/news/story.asp?NewsID=45684.

Valeriano, Brandon and Ryan Maness. "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype." *Foreign Affairs,* November 21 2012. Accessed April 4, 2016. https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar.

Valeriano, Brandon and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015.

von Clausewitz, Carl. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, New Jersey: Princeton University Press, 1976.

W32.Duqu The precursor to the next Stuxnet. Symantec, November 23, 2011. Accessed May 20, 2014. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf.

Wall, Andru E. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action.” *Harvard National Security Journal* 3, (2011): 85-142. Accessed March 18, 2017. http://www.soc.mil/528th/PDFs/Title10Title50.pdf.

Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press, 1959.

Walzer, Michael. “The Moral Standing of States: A Response to Four Critics.” *Philosophy & Public Affairs* 9, no. 3 (Spring, 1980): 209-229. http://www.jstor.org.proxy.libraries.rutgers.edu/stable/2265115.

Warner, Margaret. “The 5 countries that don’t spy on each other.” *PBS,* October 25, 2013. Accessed November 19, 2016. http://www.pbs.org/newshour/rundown/an-exclusive-club-the-five-countries-that-dont-spy-on-each-other/.

Warner, Michael. “Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014.” *Cyber Defense Review*, August 27, 2015. Accessed August 12, 2017. http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/.

Watt, Nicholas and Nick Hopkins. “Cameron Forced to Rule Out British Attack on Syria After MPs Reject Motion.” *The Guardian,* August 29, 2013. Accessed December 6, 2016. https://www.theguardian.com/world/2013/aug/29/cameron-british-attack-syria-mps.

“What is a PLC?.” *Advanced Micro Controls Inc.* Accessed May 28, 2016. https://www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/.

“What is a Zero-Day Vulnerability?.” *Security News*. Accessed April 20, 2016. http://www.pctools.com/security-news/zero-day-vulnerability/.

“Where the Future Becomes Now.” *Defense Advanced Research Projects*. Accessed April 23, 2016. http://www.darpa.mil/about-us/timeline/where-the-future-becomes-now.

WikiLeaks (@wikileaks). “We had already obtained the archive of NSA cyber weapons released earlier today and will release our own pristine copy in due course.” Twitter. August 15, 2016. 5:20 p.m. Accessed November 29, 2016. https://twitter.com/wikileaks/status/765342384821534722.

Worley, Will. “Russia warns US of ‘painful’ response if it toughens existing sanctions over Syria.” *Independent,* October 20, 2016. Accessed December 13, 2016. http://www.independent.co.uk/news/world/europe/russia-us-sanctions-aleppo-syria-putin-obama-sergey-ryabkov-hollande-merkel-a7371096.html.

Yourish, Karen, Derek Watkins, Tom Giratikanon, and Jasmine C. Lee. “How Many People Have Been Killed in ISIS Attacks Around the World.” *The New York Times,* July 16, 2016. Accessed December 12, 2016. http://www.nytimes.com/interactive/2016/03/25/world/map-isis-attacks-around-the-world.html.

Zarroli, Jim. “The 2007 Economy in Review.” *NPR,* December 31, 2007. Accessed August 12, 2017. http://www.npr.org/templates/story/story.php?storyId=17716248.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York, NY: Crown Publishers, 2014a.

———. “Hacker Lexicon: What is an Air Gap?.” *Wired,* December 8, 2014b. Accessed February 2, 2016. https://www.wired.com/2014/12/hacker-lexicon-air-gap/.

———. “NSA Hacker Chief Explains How to Keep Him Out of Your System.” *Wired,* January 28, 2016. Accessed February 20, 2017. https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/.

Zero Days. 2016. Screening, Harvard University, Cambridge, Massachusetts, April 29, 2016. Magnolia Pictures. 2016.

Zero Days. 2016. Amazon Video, Magnolia Pictures, 2017. Accessed February 6, 2017. https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2EKYTC.