Technogeopolitics of Militarization and Security in Cyberspace

By

Panayotis Alexander Yannakogeorgos

Graduate School-Newark

Rutgers University, 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. Norman Samuels

and approved by

……..

……..

……..

……..

Newark, New Jersey

May 2009

Abstract

Based on democratic principles that encourage creation and transmission of information and knowledge using information and communication technologies, the Information Society has become the organizing paradigm for a digital age. Humans residing in digital rich regions of the world rely on cyberspace, the Information Society's enabling environment, for their business, commerce, education, socialization. Governments and industry are migrating their critical processes into this domain. These trends will intensify as more people realize cyberspace's utility. However, the promises of the Information Society may never transpire since there is a lack of trust and security in cyberspace. These two concepts are the foundation on which the utility of inter-networked ICTs, such as the Internet, are built. The increasing rate in the occurrence and sophistication of cybercrimes erodes users' trust in subscribing to networked services Further the militarization of cyberspace by states as a new domain through which they conduct their operations also presents challenges to the Information Society. Both crime and conflict in cyberspace erode trust in digital networks.

The development of a comprehensive international law for cyberspace is essential to govern state and non-state actor behavior in this global commonage. The formation of the World Summit on the Information Society (WSIS) in the early twenty-first century marks the first time that state and non-state actors convened to develop plans of action to guide the development of in the digital world. This project examines the negotiating positions of the United States, Russia and China in the area of cybersecurity through the lens of technogeopolitics. It is shown how the political and military interests of each

affect their negotiating positions in the WSIS. The methods of content analyses on material from diplomatic archives, participant-observation at international conferences and interview surveys of participants at these conferences are used to investigate the reasons why decision are made or not made in the field of international cybersecurity cooperation.

Preface/Acknowledgements

This work grew out of a need identified during my year long tenure as an Adviser for Greece at the United Nations Security Council in 2006. Sitting in consultations and listening to briefings, one would think that computer network technology had no impact on international peace and security. Generally, when discussions on the topic did occur, the main concern expressed by several states was focused on the question of how Council action might have affect freedom of speech. On these very rare occasions discussion was brief.

This study would not have been possible without the encouragement, advice and support of many people. I am particularly grateful to my thesis director, Norman Samuels, for his insights on terrorism, and suggestions throughout the course of my research. Professors Yale H. Ferguson, and Richard Langhorne of the Division of Global Affairs have also been extremely helpful providing insight and inspiration on the topic in during our discussions on the topic.

I am also grateful for having had the opportunity to work with the United Nations staff, and thank Greek Ambassadors Adamantios Vassilakis and Alexandros Rallis for entrusting me with the unique privileges rarely given to a scholar. Mr. Alexandros Vidouris, Gregory Delavekouras Dr. George Papadatos. On the U.S. side, I am gracious to the insight provided by Ms. Jade Nester, Rhode Island State Senator Leonidas Raptakis, Rhode Island U.S. Congresman James Langevin and Ms. Kim Casci for their contributions to my research. I am particularly grateful to men and women of whom little

is known, and even less that can be told, who expressed interest in my project and offered invaluable information to guide my research.

The patience and support of Constantine, Evdokia and Ari Yannakogeorgos mean the most.

Without fail, a man harms his foes thus: those things that they most dread he discovers, carefully investigates, then inflicts on them.

+ Thucydides, *The Peloponnesian War*, 6.91.6

Table of Contents

Chapter One- **Introduction**.....1

Part One | **Cyberspace: the Electromagnetic Wilderness**

Chapter Two- **The Environment of Cyberspace**…..26
Chapter Three- **The Militarization of Cyberspace…..**47
Chapter Four- **The Athens Affair: The Limitations of Privatized Cybersecurity**…82
Chapter Five- **Al-Qaida and the Taliban's Misuse of Cyberspace to Circumvent U.N. Counterterrorism Sanctions**…..100

Part Two | **Negotiating Global Cybersecurity**

Chapter Six- **Information Society Stakeholders**…..120
Chapter Seven- **World Summit on the Information Society**….137
Chapter Nine- **Promises and Pitfalls of the U.S. National Strategy to Secure Cyberspace**…..174
Chapter Ten- **Conclusion**…..219
Bibliography….225

APPENDICES

Appendix A**- Relevant United States Policies**….249
Appendix B- **Interview-Survey**….271
Appendix C- **Council of Europe Convention on Cybercrime**…..267

Curriculum vitae

List of Figures

Number of Participants at the WSIS….127
Number of Entities Represented at the WSIS….142
United States Cybersecurity Federal Chain of Command…..195
*United States Federal IT Spending*206

List of Abbreviations

ADAE Authority for the Assurance of Communications Security and Privacy (Greece)
B2B Business-to-Business networks
CALEA Communications Assistance for Law Enforcement Act (United States)
CERT Computer Emergency Response Teams
CTC Counter Terrorism Committee (United Nations)
CTED Counter-Terrorism Executive Directorate (United Nations)
DNS Domain Name System
DOD Department of Defense
ECLAC Economic Commission for Latin America and the Caribbean
FAPSI Russian Federal Agency for Government Communications and Information
FTP File Transfer Protocol
GCA Global Cybersecurity Agenda
GCC Global Culture of Cybersecurity
GIG Global Information Grid
HLEG High Level Experts Group
ICANN Internet Corporation for Assigned Names and Numbers
ICT Information and Communication Technologies
IIIC International Independent Investigation Commission (United Nations)
IMPACT International Multilateral Partnership Against Cyber Threats
IMS Interception Management System
IMS Interception Management System
IP Internet Protocol
IR International Relations
ISO International Standards Organization
ITI IT infrastructures
ITU International Telecommunications Union
JFCC Joint Functional Component Command
LAN Local Area Network
LI Lawful Interception
MAC Media Access Control protocol
NATO North Atlantic Treaty Organization
OSI Open Systems Interconnection
P3 Public-Private Partnerships
RES Remote-control Equipment Subsystem
RMA Revolution in Military Affairs
SFITS Federal Information and Telecommunications System (Russian)
SWIFT Society for Worldwide Interbank Financial Transactions
TCP/IP Transmision Control Protoco/Internet Protocol Suite
UNGA United Nations General Assembly
UNSC United Nations Security Council
VNSA Violent Non-State Actors
VOIP Voice over Internet Protocol
WEOG Western European and Others Group
WGIG Working Group on Internet Governance
WSIS World Summit on the Information Society
WWW World Wide Web

Chapter One
Introduction

Cyberspace is a global commonage that enabling the existence and growth of the digital Information Society that has emerged in the developed world. Information and communication technology (ICT) using the electromagnetic spectrum to network computers are not readily available to all communities. This is considered by the United Nations and national governments as a serious hindrance to development goals. To resolve this, there exists a worldwide movement to see that no society is left on the wrong side of the digital-divide.[1] The establishment of cyberspaces in underdeveloped countries is aided through programs, such as One Laptop Per Child, designed to bridge the digital divide and network the world.[2] The critical issue is not solely how to bridge the digital-divide, but how to create e-commerce, e-learning and e-government programs, all of which are important in assuring the development and expansion of an Information Society. However, in order for any of these programs to achieve their promised potential, cyberspace requires security regulations mandated by national government that are guided by an international law fostering international cooperation to govern global ICT such as the Internet.

Cyberspace is an electromagnetic wilderness. Unlike the other commonages (sea, air and outer space), this environment lacks a comprehensive international treaty

---

[1] John Feather, "Information Rich and Information Poor" in *The Information Society: A Study of Continuity and Change,* 4th Edition (London, UK: Facet Publishing, 2004) 111-136.
[2] U.N. General Assembly, *United Nations Millennium Declaration***,** Resolution **55/2,** 18 September 2000
Also see: Laptop.org
"China To Produce Low-Cost Computers of Its Own"
Xinhua 14March, 2006, NewsEdge Document Number: 200603141477.1_22a40018245f4430.

regulating its use. Forging a secure enabling environment for the Information Society requires more than just installing sophisticated hardware and software to secure information systems. The ability to launch attacks in cyberspace from any point on Earth with a degree of anonymity indicates the global nature of the problem. Advanced cybersecurity measures might fluster a computer cracker trying to penetrate a network to steal valuable private information such as credit card numbers. In the case of a successful attack, a knowledgeable attacker will use the current state of cyberanarchy to his or her advantage to avoid discovery. International cooperation is essential to address the global cybersecurity challenge.

As evidenced in negotiations at the United Nations, World Summit for the Information Society (WSIS) and related conferences and forums, the international community is aware of the need to harmonize domestic laws and create international norms for the governance of cyberspace. However, competing national interests are impeding progress in these efforts. Although much has been written on the need for such a body of law, there are numerous technological and geopolitical challenges to achieving this desired goal.

Misuses of cyberspace by violent non-state actors (VNSA), such as organized criminals and terrorists, and the increasing proliferation of strategic information warfare programs amongst militaries have raised awareness of the need to incorporate cybersecurity strategies as part of foreign and security policies. However, legal and technical complexities present challenges to authorities tasked with responding to acts of cyberwar and preventing, identifying and prosecuting perpetrators of cybercrime and cyberterrorism.

Protecting cyberspace, especially critical information infrastructures, including the Internet and World Wide Web (WWW), is unachievable unless all states cooperate with interested stakeholders to harmonize legislation within the frameworks being negotiated by the international community (e.g. the U.N. General Assembly's "global culture of cyber-security"). Until a law of cyberspace is established, this global commonage will remain an electromagnetic wilderness. Hence, global cooperation based on a body of international law containing the appropriate political and technical elements governing human activity in cyberspace is necessary in order for the Information Society to reach its anticipated potential.

Information Society

Terms such as "Information Revolution," "Information Age," and "Information Society," are new paradigms through which scholars interpret the geo-strategic, economic and social implications of information and communication technologies (ICT) of a truly global character, such as the Internet.[3] The evolution of this critical information infrastructure from a specialized military network to a ubiquitous globe-spanning communications infrastructure is indicative of the potential of digital networks to change society. In the developed world, there has been a shift from a paradigm in which rapid cross-border information flows did not occur rapidly, to one where a migration of all

[3] The use of "information" to define the current era is misleading since information has always been critical for commerce, politics and war. This project does not attempt to contribute to deconstructing definitions association with the "Information Age."

existing human practices has occurred on a global scale via the electromagnetic spectrum. As a result, a digital information society has emerged.[4]

Broadly defined, the Information Age is the historic period during which infinite amounts of information can be transmitted globally and inexpensively over open networks. The advent of technologies that enable low-cost long-distance communication, such as the Internet, have bolstered the Information Age.[5] While states, especially those that have heavily contributed to the development of ICT, are the core operators of the foundation of the Information Age, ICT has "enormously expanded the number and depth of transnational channels of contact."[6] Therefore, the playing field between states and not-state transnational actors appears to have leveled.

Robert Keohane and Joseph Nye define the information revolution as:

> The rapid technological advances in computers, communications and software that have led to dramatic decreases in the cost of processing and transmitting information…the distinguishing mark of the information revolution is the enormous reduction in the cost of transmitting information.[7]

This revolution, they argue, must be understood as the result of post-Second World War policies of the United States and international institutions that laid the framework for the globalization of the world economy.[8]

In his influential work, *The Structure of Scientific Revolutions,* Thomas Kuhn describes how conceptual worldviews are replaced over time.[9] While Kuhn intended to

---

[4] Jachim K Rennstich, *The Making of a Digital World: The Evolution of Technological Change and How it Shaped our World* (New York, New York: Palgrave Macmillan 2008), 78.
[5] Robert O. Keohane and Joseph S. Nye Jr., "Power and Interdependence in the Information Age," in *Foreign Affairs* 77 no. 5 (September/October 1998).
[6] Ibid., 10.
[7] Robert O. Keohane and Joseph S. Nye, "Power and Interdependence in the Information Age" in Democracy.com? Governance in a Networked World (Hollis, NH: Hollis Publishing Company, 1999), 197-214, 200.
[8] Ibid.

describe how philosophy and science progress throughout history, it is also a useful framework through which to understand the lackadaisical reaction of governments to address the challenges posed by ICT. Paradigm shifts occur as a "series of peaceful interludes punctuated by intellectually violent revolutions," which cause "one conceptual world view to be replaced by another view."[10] As a result, the old view is completely abandoned as truth. The revolutionary periods during which paradigm shifts occur are characterized by confusion and alarm.

Evidence for the current confusion in understanding the new paradigm exists in the domain of international relations (IR) and its subfield, security studies. It has been suggested that no security studies theory can adequately address the realities of the Information Age. For example, Johan Eriksson and Giampiero Giacomello argue that although new challenges have emerged as a result of the information revolution, realist, liberal and constructivist approaches to international relations have not successfully addressed the impact of ICT on global security, and therefore do not explain contemporary security relations and policies.[11] While theorists have made efforts to analyze power and security in the information age, they are constrained by the limits of their theories, each of which is deemed incompatible with the other. The authors argue

---

[9] Thomas Kuhn. *The Structure of Scientific Revolutions*, (Chicago, IL: University Of Chicago Press 1996). Also see: Yale H. Ferguson and Richard W. Mansbach, "Technology and Change" in *Remapping Global Politics: History's Revenge and Future Shock* (Cambridge, UK: Cambridge University Press, 2004), 273-311.

[10] Kuhn.

[11] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?," in *International Political Science Review* 27, No. 3 (2006), 221-244, 228.

that a pragmatic approach is needed in which scholars draw from all IR theories as well as policy-oriented literature.[12]

In *Technology and International Transformation: The Railroad, the Atom Bomb and the Politics of Technological Change,* Geoffrey L. Herrera argues that current international relations frameworks do not treat technology, one source of international systemic change, as an integral part of the international system. Instead, IR models factor sources of international change, including technology, as exogenous factors in international relations theory.[13] Herrera isolates the logic of the various IR theories into two categories: technological determinism and technological constructivism.[14] Neorealists hold the technological determinist view while economic liberalists maintain that technologies cause change. Social constructivist views focuses on the emergence of new technologies, rather than on their political implication.[15] Both views, he argues, complement each other, but are misdirected and incomplete alone since "no technology is truly autonomous; they are all partly social."[16] A pragmatic approach, which carefully blends the determinist and constructivist theories of technology and politics, is proposed as a way to resolve this problem in international relations.

Herrera's holistic approach aims to enrich other IR theories by conceptualizing technology as an integral part of the international system in which technology and

---

[12] Absent from their study is the recognition of the concept of noopolitiks, conceptualized in: John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: Toward An American Information Strategy* (Santa Monica, CA: Rand 1999).

[13] Geoffrey L. Herrera, *Technology and International Transformation: The Railroad, the Atom Bomb and the Politics of Technological Change* (Albany, New York: State University of New York Press, 2006), 3. Similar treatment of the subjet is given in: John Gerard Ruggie, "International Responses to Technology: Concepts and Trends" in *International Organization* 29, No. 3, (Summer, 1975), pp. 557-583.

[14] Herrera, 28.

[15] Ibid., 32.

[16] Ibid., 34.

politics have a "fundamental and mutually constitutive" relationship.[17] Not all technologies are pertinent to IR. Thus, the focus of Herrera's work is on systemic technologies, defined as: "those sociotechnical systems - typically communication, transportation or violence systems - that structure interaction among international actors and are global in scope." [18] The Internet is one such sociotechnical system that neatly fits into Herrera's view of "the mix of material and social institutions that cohere around artifacts"[19] Telecommunications systems such as the telegraph and telephone fall into this category. Both have strong social institutions cohering around them that regulate their use. The Internet is a technology of international significance, although it is still in its formative stages. Herrera notes that social institutions are required to regulate such large technological systems.[20] The International Telecommunications Union (ITU) is one social institution that is contributing to the effort to create a global regulatory scheme for the Internet.

Time is identified as an important factor in the politics of sociotechnical systems of international significance:

> Complex sociotechnical systems are likely to have differing political impacts at different points in their life cycle. In the beginning the system does not exist at all. If successfully imagined and built, the sociotechnical system evolves and spreads slowly at first before reaching a "take-off" phase, after which it spreads rapidly and widely. Finally, in its mature phase, the system is widely diffused as its further spread slows and possibly even stops.[21]

---

[17] Herrera, 4.
[18] Ibid., 27.
[19] Ibid., 36.
[20] Ibid., 36.
[21] Ibid., 36.

Through time, technology is imagined. Interested parties invest in its development, and as the sociotechnical system spreads, further investments are injected into the cycle and interested stakeholders further propel the spread of the technology. As new technologies emerge with the potential to replace the old technology, switching to the new may initially be too expensive due to the investments in the old. During this phase, social factors may begin to reshape the old technology before the new technology takes hold.[22]

Technogeopolitics

Currently, theories of international relations do not adequately account for how cyberspace is changing global politics. This is indicative of the paradigm shift from the Industrialized Society to the Information Society. In order to better assess the reasons for cooperation and conflict in cyberspace negotiations, the lens of technogeopolitics is used to demonstrate why a law of cyberspace negotiated on the basis of existing international customs is either facilitated or stalled by current technological development and geopolitical considerations of the negotiating parties.

I have examined the negotiating positions of the United States, European Union (E.U.), Russian Federation and China at international conferences are traced back to 2002, when the WSIS process was formally initiated, until today. Attention is also given to work in meetings and summits held under the auspices of the International Telecommunications Union (ITU), United Nations General Assembly or Security Council. Thus, I will analyze the diplomatic record, in addition to trends in militarizing cyberspace, through the lens of technogeopolitics to understand impediments to international cooperation.

[22] Herrera, 37.

David Butler introduces and develops the concept of technogeopolitics in his article, *Technogeopolitics and the Struggle for Control of World Air Routes.*[23] He suggests that technogeopolitics is a novel lens "through which specific geopolitical insights can be made, in particular, instances where technology was a leading factor."[24] However, it cannot be used as paradigm to understand all geopolitical events: "Instead, it is a specific lens that can be used in particular geopolitical or technological instances to help us understand the diplomatic position of parties involved."[25] Applying this lens to cyberspace negotiations is apt.

After developing the framework for his theory, Butler examines cases of international aviation conferences to determine the extent to which the geopolitical realities and diplomatic positions of each nation were influenced by developments in their own aviation industries. He identifies five general themes that can be used as "powerful" conceptual tools to understand the recursive diplomatic positions of parties involved in negotiations where geopolitics and technology overlap. These five themes are:

- States pursue specific technologies to enhance their geopolitical positions;
- States react to other states' technical developments geopolitically, which in turn affects their own geopolitical position;
- If a state is technologically immature, it will use its power to restrict access by other nations to enable it time to catch up technologically and compete on a level technological field;
- If a state is technologically mature, vis-à-vis its commercial and military rivals, it will push for the most liberal aerial policy allowing a comparative advantage to its aircraft and goods in foreign markets; and
- At any given time technological developments may evolve at such a rate as to potentially wipe out any geopolitical gains or losses for a nation, thus forcing states to reexamine their geopolitical foreign policy and possibly call for a convening of an international conference to address their concerns.

[23] David L. Butler, "Technogeopolitics and the Struggle for Control of World Air Routes," 1910-1928, in *Political Geography* 20 (2001) 635-658.
[24] Ibid, 654.
[25] Ibid, 654.

Butler derives this lens from negotiations regarding airline routes in the early 20th century.[26] The diplomatic record on issues of international cybersecurity cooperation and Internet governance confirm Butler's hypothesis that these five themes are present in negotiations where geopolitics and technology overlap. On the first point, the United States developed the basis of the Internet infrastructure during the 1960s (ARPANET), in part to assure that its nuclear forces could communicate and deliver a second strike. Over time, this technology became global, giving rise to the Information Society. States such as Russia and China have reacted geopolitically to U.S. dominance of cyberspace by militarizing it and domestically developing their own ICT. Both appear to act within the lens of technogeopolitics by attempting to restrict U.S. control of critical information infrastructures as they develop their own networks. The U.S., on the other hand, is urging liberal policies to push for the advantage of its ICT goods in foreign markets. On the final point, technological advances in both Russia and China appear to be in the early phases of wiping out U.S. geopolitical gains. On the basis of an analysis of diplomatic archival material from intergovernmental conferences within the context of the militarization of cyberspace Butler's theory is confirmed as a useful analytical tool for understanding the current political positions of examined states.

[26] The aviation developments in the twentieth century presented challenges to state sovereignty similar to those that cyberspace pose today. As aerospace technology developed, state's traditional sovereignty was challenged since regulations did not exist to protect state sovereignty over their airspace. Similar questions of sovereignty of a state's cyberspace exist today. An important difference between the airline debates in the twentieth century and cyberspace issues today is that ICT, such as the Internet, are global and easily accessible. Furthermore, it is simpler to acquire the skill set required to access and use the Internet than it is to develop and fly a jet plane. Furthermore, it takes significantly less expertise and resources to use ICT and cyberspace as a medium through which to launch a strategic attack against a target than it does to launch a strategic bombing attack using aerospace weapons systems. Thus, the consequences for geopolitics are much greater given that strategic information warfare can be waged at the speed of light against targets located thousands of miles from the attacker.

Conferences relevant to the governance of elements of cyberspace have been ongoing since the 19th century to establish the rules for operating a variety of telecommunications technology. What is lacking, however, is an international regime-governing cyberspace as a whole. Laws and regulations regarding elements of cyberspace, such as the telegraph, are well developed. However, for other domains such as the Internet, there is a significant gap not only in individual nation's regulatory and legal frameworks, but at the international level as well.

Some scholars have observed similar phenomena. Stephen Krasner argues that when it comes to global communications regimes, states may agree that certain outcomes are mutually undesirable, while disagreeing on preferred outcomes. Shifts in power resulting from the development of new technologies create controversy in international negotiations.[27] Further, he argues that if power and technology are distributed symmetrically, regimes will be established to solve the problem of coordinating behavior.

Although cyberspace itself lacks a comprehensive governing treaty, international institutional arrangements regulate some global telecommunications. Krasner examines the reason why various institutional arrangements have emerged to resolve problems and ensure a stable global communications environment.[28] Although written before the strategic conceptualization of cyberspace as the commonage through which global communications flow, his analysis informs the discussion of the politics observed during intenraitonal negotiation in the area of cyberspace governance. Krasner covers four issue areas in global communications governance: radio and television broadcasting, remote

[27] Stephen D. Krasner, "Global Communications and National Power: Life on the Pareto Frontier" *World Politics* 43, No. 3 (April 1991), 336-366.
[28] Ibid, 343.

sensing, allocation of the electromagnetic spectrum, and telecommunications (telephone and telegraph links, including communications satellites.[29] He argues that:

> Information flows and knowledge have been less important than relative power capabilities for international communications regimes or the lack thereof. Where there have been disagreements about basic principles and norms and where the distribution of power has been highly asymmetrical, international regimes have not developed. Stronger states have simply done what they pleased.[30]

Therefore, he argues, institutional arrangements are better explained by "the distribution of national power capabilities than by efforts to solve problems of market failure"[31] Others researchers have argued similarly that any multilateral institution can be used by states (particularly by hegemonic powers), to further their own interests. by deliberately designing political institutions to ensure that their own interests will be served.[32] Hence, stronger and more technologically developed states secure their primary interests through their unilateral or bilateral actions, rather than through multilateral regulatory regimes. Butler's theory of technogeopolitics shares this view.

When actors sat down to negotiate standards aiming to eliminate the undesirable effects of trans-boarder radio interference and incompatible national communications systems, the third world displayed its source of power in influencing the regime allocating use of the electromagnetic spectrum using what technical power it had to influence the allocation of the electromagnetic spectrum. The capability and intent to use technology to interfere with the electromagnetic spectrum, in conjunction with their

---

[29] Krasner 343.
[30] Ibid., 337.
[31] Ibid., 337.
[32] Barbara Koremenos, Charles Lipson and Duncan Snidal, "The Rational Design of International Institutions" *International Organization*, 55 (Autumn 2001) 761-799.
Also see: Lisa L. Martin, "Interests, Power, and Multilateralism" in *International Organization* 46, No. 4 (Autumn 1992 765-792).

voting privileges in the International Telecommunications Union (ITU), the third world proved that it could modify the regime by initiating public threats of defection or unilateral action.[33] While such actions are part of the negotiations process and may lead to cooperative outcomes, it has been noted that global policy issues involving scientific and environmental uncertainty, require the learning of knowledge and processes during negotiations. These processes form the foundation of joint problem solving mechanisms established as a result of political agreements.[34] The process is often hindered by hostilities amongst actors during negotiations. This project documents examples of emerging hostilities between the United States and the rest of the world resulting from the U.S. being the core operator of the Internet and other elements composing cyberspace.

Cyberspace Militarization

Information and communications technologies have been strategic assets since time immemorial.[35] Throughout history, nations, empires and other polities have extended their activities throughout the global commons. Air, land and sea spaces have been used strategically by political entities to project power. The latter half of the 20th century saw technologies allowing for the strategic utilization of space and cyberspace.[36]

---

[33] Krasner 343.

[34] James K. Sebenius, "Challenging Conventional Explanations of International Cooperation: Negotiation Analysis and the Case of Epistemic Communities" *International Organization* 46 (Winter 1992) 323-365, 331.
Also see: Arthur Applebaum, "Knowledge and Negotiation: Learning Under Conflict, Bargaining Under Uncertainty," Ph.D. dissertation, Harvard University, Cambridge, Massachusetts, 1987.

[35] Appendix C offers a more complete account of the historical uses of ICT in the conduct of war and politics in the Classical and Byzantine Greek eras.

Both of these technologies rendered geographic boundaries less relevant. Significant scientific and technological advances made space and cyberspace viable strategic environments that are essentially "up for grabs" by state actors. Threats to and breaches of the peace in cyberspace are becoming increasingly consequential as states continue to militarize cyberspace and exploit it in war.[37] Unlike other strategic military technologies, such as nuclear weapons, rockets and aircraft, the cost and resources required to militarize cyberspace are low, while the effects can be just as consequential as a missile strike.[38] This lowers the threshold for both state and violent non-state actors (VNSA), including terrorist and criminal networks, to militarize cyberspace.[39] Current international efforts coordinating a global response to secure cyberspace are focused on threats posed by VNSA's, the most visible cybersecurity challenge, strategic threats of national significance emanating from cyberspace are largely ignored despite a trend of states militarizing cyberspace. The proliferation of cyberwarfare programs and cooperation between some governments, such as the Russian and Chinese, with cybergangs, to attack critical information infrastructures further complicate global cybersecurity efforts.[40]

---

[36] Alfred Price, *Instruments of Darkness: The History of Electronic Warfare 1939-1945* (London: William Kiner and Co., 2005).
Martin Streetly, *Airborne Electronic Warfare: History, Techniques and Tactics* (London: Janes Publishing Company Limited 1988).

[37] Bruce Berkowitz, "The New Terrain" in *The New Face of War: How War Will be Fought in the 21st Century* (New York, New York: The Free Press 2003, 1-8).
Bill Frezza, "The Militarization Of Cyberspace," *Network Computing* (15 March 1997), 35.

[38] Bobbie Johnson, "NATO says cyber warfare poses as great a threat as a missile attack: Concern follows strikes by 'Titan Rain' hackers. State-sponsored online aggression said to be rising," *The Guardian*, (March 6, 2008, 2).

[39] *Information Operations: Warfare and the Hard Reality of Soft Power: A Textbook Produced in Conjunction with the Joint Forces Staff College and the National Security Agency*, Ed. Leigh Armistead (Washington D.C.: Potomac Books, 2004).
Also see: Richard Hunter, "The N Party System of the Network Army" in *World Without Secret: Business Crime and Privacy in the Age of Ubiquitous Computing* (New York, New York: Gartner Inc. 2002, 69-84).

[40] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic" *The Washington Post* (19 May 2007), p. A1).
Also see: Mark Landler and John Markoff, "After Computer Siege in Estonia, War Fears Turn to Cyberspace" *The Washington Post* (29 May 2007) A1.

Cyberwarfare and was not possible on any level in the past, but now information systems are able to launch attacks without regard for geography at the speed of light. Technologies such as intercontinental ballistic missiles (ICBM) and global telecommunications have made geography appear to be less significant than it was in the past.[41] Colin S. Gray argues that such views are plausible fallacies.[42] Acknowledging that "new weapons technologies can offset distance, terrain, and even climate to an important degree" he identifies three limitations on the strategic value of such technology.[43]

- Technological progress cannot be owned or retained by one security community alone.
- Conflict cannot occur beyond geography; men are needed to control territory.
- Logistical requirements to control territory.[44]

The advent and proliferation of nuclear weapons, and the threat of violent non-state actors gaining access to them is a testament to the first point. Science cannot remain secret forever. The second point assumes that "the exercise of continuous influence or control requires the physical presence of armed people in the area at issue."[45] Geographic distance from an area of operations also determines whether or not all the required men and materiel will be able to get to a conflict zone in time to allow for the offensive actor

---

[41] Harold and Margaret Sprout, "Geography and International Politics in an Era of Revolutionary Change" in *The Journal of Conflict Resolution,* IV, No. 1 (1960), 145-161.
Also see: Yale H. Ferguson and Richard Mansbach, *Remapping Global Politics*
[42] Colin S Gray, "The Continued Primacy of Geography." *Orbis* 40, no. 2 (Spring 1996): 247. *Academic Search Premier*, EBSCO*host* (accessed 22 September 2008), 251.
[43] Ibid.
[44] Ibid.
[45] Ibid, 252. NATO required a U.N. peacekeeping force to maintain the peace in Serbia after its 1999 air war. The U.S. continues to face problems with Al-Qaeda and the Taliban in Afghanistan. Additionally, although unmanned aerial vehicles (UAV) can strike at suspected terrorists, geographic and political barriers bar U.S. troops from overtly entering Pakistani territory to directly control the area where strongholds of Al-Qaida and the Taliban operate.

power to either conquer a territory, or continue its dominance. The third assumption is that a military cannot send the same weight over air as it might by land or sea.

Today, with societies increasingly relying on cyberspace, the militarization of this commonage is changing the nature of conflict. This is natural, as history informs us that technological progress transforms when, where and how wars are fought and won. Globally, a revolution in military affairs (RMA) is underway wherein advances in ICT drive the reorganization of militaries.[46] Increasingly, governments are adjusting their national security policies, procedures and doctrines to include cyberspace as a new realm through which they seek to achieve their strategic interests.[47] The struggle to command these technologies is geopolitical.[48] The consequences of the militarization of cyberspace for the development of an Information Society are magnified since existing international laws do not adequately address cyberwarfare issues. It has been suggested that what is required is "a new legal framework specifically conceived to cyberspace warfare that has

---

[46] Yale Ferguson and Richard Mansbach, *Remapping Global Politics*.

[47] Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, (Santa Monica, CA: RAND 1996).
Recent U.S. publications include: U.S. Joint Chiefs of Staff, *Joint Publication 3-13.1: Electronic Warfare* (25 January 2007). A document to guide the application of military tactics in the electromagnetic environment. Organization, planning and coordination of joint service electronic warfare operations are covered.
Department of Defense, *Information Operations Roadmap* (30 October 2003).
U.S. Army Training and Doctrine Command, *Handbook No. 1.02: Cyber Operations and Cyber Terrorism* (Fort Leavenworth, Kansas, 15 August 2005).
Congressional Research Service, *Information Operation, Electronic Warfare and Cyberwar: Capabilities ad Related Policy Issues* (20 March 2007).

[48] Bruce Berkowitz, "Command of the Nets" in *The New Face of War: How War will be Fought in the 21st Century* (New York, New York: The Free Press 2003, 179-195, 179).
Scholarly debates regarding the most important geographic space in relation to state power. These discussions have traditionally focused either on land or maritime power and their associated geographies.
See for example:
Halford John Mackinder, *Democratic Ideals and Reality: A Study in the Politics of Reconstruction* (New York, New York, Henry Holt and Company, 1919).
Alfred Thayer Mahan: *The Influence of Sea Power Upon History: 1660-1783*. (Boston, Massachusetts: Little Brown and Company, 1898).
Jill Hills. *The Struggle for Control of Global Communications: The Formative Century* (Chicago, Illinois: University of Illinois Press 2002.)

to be based on a set of certain basic legal principles that will allow it not only to be effective but also, and perhaps primarily so, to shut the door to potential abuses on the part of states that find themselves at the unhappy receiving end of cyber-warfare attack."[49] These uncertainties highlight the need to negotiate an international law for conflict in cyberspace.

Comparing strategic information warfare to strategic bombing, David Lonsdale argues that:

> Like strategic bombing, SIW [strategic information warfare] seeks to bypass enemy surface forces to strike directly at the perceived centre of gravity. However, whereas airpower still works through the application of destructive firepower and physical force, SIW primarily operates through such non-violent means as 'malicious software' and electromagnetic pulses. In this sense, SIW does not constitute an act of physical violence, nor does it involve any real degree of physical excretion…the instrumental aim of SIW is more often than not to create strategic effect via disruption rather than destruction.[50]

Strategic information warfare, according to Lonsdale, can have destructive effects, though it typically does not. His classification of it as a non-violent act which does not require much physical exertion when used strategically is questionable, especially considering the recent fusion of kinetic and cyberspace weapons.[51] As Israel demonstrated in its 2007 attack against a Syrian nuclear plant, tactical network attacks are the lynchpin for the successful outcome of military operations.[52] The cyberwar system

---

[49] Dimitrios Delibasis, "Information Warfare Operations Within the Concept of Individual Self Defense" in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni (London, Routledge 2009, 95-111, 96).
[50] Lonsdale, 135.
[51] David A. Fulghum, "Cyber, Kinetic War Collide; Two-seat fighters take on multiple missions as bombing and network-attack combine" in *Aviation Week & Space Technology*, 167, No. 13 (1 October,2007, 27).
[52] David A. Fulghum, Robert Wall and Amy Butler, "Cyber-Combat's First Shot;
Attack on Syria shows Israel is master of the high-tech battle" in *Aviation Week & Space Technology*, 167 No. 21 (November 26, 2007, 28)

used in this attack allowed for the Israeli Air Force "…to invade communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions where approaching aircraft can't be seen."[53]

Jerry Everand suggests that the difference between information warfare and other forms of war is that it focuses on dominance of information systems as a whole. That is, both the information and the systems on which it is stored and distributed.[54] *David J. Lonsdale offers the following elegant definition of information warfare: "the ability to conclude……"*: "the ability to conclude wars by attacking the National Information Infrastructure (NII) of an enemy through cyberspace"[55] In this view, information warfare is strategic if, and only if, a war's end can be brought about solely by attacking national information infrastructures through cyberspace, and not any other domain. Lonsdale also acknowledges that a cyber attack on a NII is not as difficult to achieve as, say, an airstrike on the same target.[56] The system of innovation and training required to conduct a strategic aerial campaign is costlier, as it requires a variety of skill sets ranging from flying the bomber aircraft and controlling air traffic to repairing runways. All a cyber attack requires is a laptop and knowledge of the targeted computer-network's vulnerabilities and how to exploit them. In Lonsdale view: "The proliferation of SIW capabilities is possibly unique, in that the hardware and software required to wage it are readily available, even to individuals….A computer is the epitome of dual-use technology, and the software and techniques required are widely available on the

---

[53] David A. Fulghum and Douglas Barrie, "Off The Radar; Israel used electronic attack in air strike against Syrian mystery target," in *Aviation Week & Space Technology*, 167 No. 14 (October 8, 2007, 28)
[54] Jerry Everard, "The @ of War" In *Virtual States: The Internet and the Boundaries of the Nation-State*, (London, UK: Routledge 2000, 97-118, 117).
[55] David J. Lonsdale, "How Strategic is Strategic Information Warfare?" in *The Nature of War in the Information Age: Clausewitzian Future* (London, UK: Frank Cass 2004, 135-176, 135).
[56] Lonsdale, 11.

Internet…a CD-ROM of hacker tools and information, is a weapon of war."[57] Therefore, the threshold for developing information warfare programs is significantly lower than that for developing an air force. Thus, the focus of this project on the militarization of cyberspace within the context of technogeopolitics provides evidence for why international efforts to forge laws to govern cyberspace are impeded by competing state interests.

Research Questions and Hypothesis

This research project addresses the following questions:

- Why is an international convention establishing a law of cyberspace necessary?
- What decisions have states made, not made (and why) in the field of global cybersecurity cooperation at conferences held under the auspices of the U.N., such as the World Summit for the Information Society (WSIS).
    - How does U.S. hegemony over critical information infrastructures, such as the Internet, affect diplomatic processes, and what are Russian and Chinese reactions to U.S. dominance?
- Can the theory of technogeopolitics serve as a lens to explain the politics of international cybersecurity cooperation?
- What conditions are necessary for compromise on issues for which decisions cannot be made?

The research hypothesis is that it is possible to negotiate an international convention for the law of cyberspace addressing the concerns of all negotiating parties. There are, however, necessary conditions for this outcome:

- Willingness to host conferences to specifically negotiate a convention for cyberspace under the auspices of the United Nations
- Willingness of all parties to provide open access to critical information resources such as the domain name system

[57] Lonsdale, 140.

Research Design and Methods

The project fits into the philosophical category of realism. It is guided by the rationalist tradition. The theory is constructed on the foundation of both deductive and inductive inference. An overview of the literature of cyberspace and global politics will comprise the deductive component of the theory. Fieldwork, including survey-interviews and participant observation at the U.N. conference comprise the inductive component of the theory.

Units of Analysis and Observation

The major entity being studied in this project is cyberspace within the context of creating institutions of governance to regulate its peaceful uses, and the inevitable conflicts that will arise in this domain. The following is a non-exhaustive list of the units of observation from which data is collected:

- Individuals: Diplomats, Congressmen, Cybersecurity Professionals
- Groups: WSIS Preparatory Committees, High Level Experts Group (HLEG) for the Global Cybersecurity Agenda
- Organizations: World Summit for the Information Society, Institutions of Diplomacy, Militaries, Business Entities, Private Organizations and Civil Society
- Social Artifacts: Records of relevant conferences from Foreign Ministry archives

What Types of Evidence are Needed?

The project required primary data collection abroad, and includes visits to the United Nations (U.N.), International Telecommunications Union (ITU), pertinent Ministries of Foreign Affairs, business entities, epistemic communities, and other stakeholders in the global cybersecurity agenda.

The evidence used to test the hypothesis within the frame of technogeopolitics is drawn from primary source documents from domestic (e.g. Department of Homeland

Security (U.S.)), regional (e.g. European Union), and international conferences (e.g. World Summit on the Information Society (WSIS), Internet Governance Forum (IGF), and International Telecommunications Union (ITU) global cybersecurity agenda working groups), and interested stakeholders (e.g. Internet Corporation for Assigned Names and Numbers (ICANN)).

The documents are substantiated by conducting interviews with government officials and other relevant stakeholders as well as through my participation in relevant conferences organized under the auspices of the United Nations. Additionally, globalization, public international law, information warfare and ICT literatures will provide a context for the study.

Research Methods

Case studies and mini-case studies will be used in this research to help facilitate a better understanding of the issues driving nations to begin negotiations to create global regulations for the use of cyberspace, as well as the implementation of legal solutions in the real world.

The case of data-espionage of the Vodafone cellular network in Greece was selected to demonstrate why a global cybersecurity regime is necessary, and to identify problems with the current tenets of the Global Culture of Cybersecurity (GCC). The focus of the analysis of diplomatic documents is on the intergovernmental preparatory committee meetings leading up to the World Summit on the Information Society (WSIS). The positions of states at this multilateral global summit are well documented in the diplomatic record. The U.S. national security strategy for cyberspace is examined in order to demonstrate the dangers to the core operator of the Internet and other ICTs.

Cases are examined with the analytical tool of process-tracing using detailed narrative. This method has been selected since, as Alexander L George and Andre Bennett suggest, it "… is a methodology well-suited to testing theories in a world marked by multiple interaction effects, where it is difficult to explain outcomes in terms of two or three independent variables."[58] This method is limited by the fact that "even with close observation, it may be difficult to eliminate all potential rival explanations but one, especially when human agents are involved - for they may be doing their best to conceal causal processes. Evidence for the case study will be drawn from content analysis of diplomatic correspondence, treaties, laws and standards as well as survey-interviews and participant observation in international conferences.

Content Analysis

This method is applied to diplomatic communications, conference proceedings, laws and other policies relevant to global and national cybersecurity to answer the question of "who said what to whom, why, how, and with what effect."[59]

Participant Observation and Interview- Survey

Simply analyzing the text of the documents is not enough to understand the dynamic environment in which cybersecurity is being discussed at the international level. My experience working as an Adviser for the Greek U.N. Security Council allowed me access to meetings of the 1267 Sanction Committee, which dealt with terrorist misuse of the Internet. Further, in the summer of 2008 I attended the High Level Experts Group

[58] George and Bennet, 206.
[59] Earl Babbie, *The Practice of Social Research*, 307.

(HLEG) of the International Telecommunications Union (ITU) Global Cybersecurity Agenda (GCA) as a Delegate Expert. I used the method of participant observation to examine the interactions of actors during cybersecurity meetings of a global character held under the auspices of the United Nations and its specialized agencies. Earl Babbie suggests that this sort of "field research can reveal things that would not otherwise be apparent."[60] Hearing the tonality of exchanges during conferences is an example of one element that cannot be captured during content analysis. Thus, participant-observation is used along with content analysis to determine the current state of play in global cooperation in the field of cybersecurity.

My administration of a questionnaire to subjects of interest to the study allows me to ask specific questions in a face-to-face setting, thereby gaining their perspective on issues of global cybersecurity cooperation. The structured questionnaire is included as an appendix to the study.

Overall, this project contributes to the understanding of what obstacles exist to the diplomatic efforts to coordinate a response to cybersecurity issues. Beginning with an overview of the cyberspace environment, the project turns to examples of how cyberspace is militarized, and why security is a problem. The Greek case studies illustrate what can happen when the public-private partnership paradigm meets a sophisticated cyberattack requiring the resources of a state to carry out. The case study on how violent non-state actors, including terrorists, use cyberspace to circumvent sanction regimes mandated by the United Nations Security Council demonstrates how state power is eroded by the misuse of ICT. Identifying these issues, global summits such as the WSIS, are investigated to understand what decisions have been made, not made, and the reasons

[60] Babbie, 281.

why decisions on controversial technical issues related to Internet governance exist. Finally, the U.S. national strategy for securing cyberspace is examined in order to show both the challenges to the Internet hegemon as well as the promise of some elements of the U.S. model.

PART ONE
Cyberspace: The Electromagnetic Wilderness

Chapter Two
The Environment of Cyberspace

Cyberspace is considered by some a global commonage, much like land, sea, air and outer space.[61] Although the basic environment of cyberspace - i.e.: the electromagnetic spectrum - has existed as long as the other commons, recent technological progress in the 20th century has resulted in the harnessing of the spectrum's potential to facilitate social, economic, political and military activities. In order to assure conceptual elegance throughout the work, the concept of cyberspace is refined. Definitions of cyberspace are numerous, and fall into two categories: strategic and metaphorical. Through the eight criteria of conceptual goodness, it is shown that the strategic definition is the one that is the most parsimonious and coherent, and has the greatest field utility. Further, this conceptualization is internally coherent, has a greater contextual range across languages and resonates in ordinary contexts as well as the context of global governance.[62]

Scholars arguing against the assumption that cyberspace is a global commonage claim that it is not rooted in physical reality. Instead, they suggest, it is a highly malleable

---

[61] See, for example: Ahmad Kamal. The *Law of Cyber-Space: An Invitation to the Table of Negotiations* (Geneva, Switzerland: United Nations Institute for Training and Research, 2005). <http://www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf>

[62] Gerring. *Coherence*: How internally coherent and externally differentiated are the attributes of the concepts vis a vis neighboring concepts and entities, operationalization (measurement),
Validity: construct, measurement or cue validity, accuracy truth, reliability. Is the concept valid? Are we measuring what we purport to be measuring?
Field Utility: How useful is the concept within a field of closely related terms?
Resonance: How resonant is the concept in ordinary and or specialized contexts?
Contextual Range: Across how many linguistic contexts is a concept viable? How far can it travel?
Parsimony: How short is the are and its list of defining attributes?
Analytic/Empirical Utility: How useful is the concept with a particular analytic (theoretical context or research design?

social construct to which the laws of physics do not apply.[63] This metaphorical definition focuses on technology such as the Internet or World Wide Web (WWW). This view oversimplifies the natural environment of cyberspace; such a view stems from the complexity of the interaction of the technology harnessing the electromagnetic spectrum, and the invisibility of the information flowing through it. It is easier to understand why the ocean, for example, is more commonly conceived of as a global commonage, since one can swim in it and see ships docking after an intercontinental voyage to deliver goods.

> Technology is obviously an artifact: a physical thing. As such, it confronts its user as a material fact- a natural part of the physical world, but technology is also the creation of humans and thus social in character…[64]

This chapter defends the view that cyberspace is a global commonage To support this view, the physical environment of the electromagnetic spectrum and its convergence with high-technology is introduced.. It is argued that the strategic definition, as coined by the U.S. Department of Defense (DOD), is one that will best serve the world community in international negotiations aiming to govern cyberspace. Metaphorical conceptions of cyberspace are introduced and shown to be inadequate since it is envisioned as merely a social construct. Its physicality is lost in the disorienting metaphor. Any international law for cyberspace must be attentive to geospatial elements so that the Information Society uses cyber resources equitably and efficiently.[65]

---

[63] Martin Libicki, *Conquest in Cyberspace*.
[64] Herrera, 34.
[65] Rob Frieden, "Balancing Equity and Efficiency Issues in the Management of Shared Global Radiocommunication Resources," in *University of Pennsylvania Journal of International Economic Law* 24 (Summer 2003), 289

Strategic Definitions of Cyberspace

The U.S. Joint Chiefs of Staff definition of cyberspace is:

> A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure."

This is the most accurate conceptualization of cyberspace. Overall, this definition has greater analytical utility for the study of how this domain will be governed by a regime of a global character. It is argued that the strategic conceptualization is precise, internally coherent and parsimonious, thereby offering a greater field utility and contextual range for such a study. Deemphasizing or ignoring the physical character of cyberspace, as metaphorical definitions do, does not contribute to the effort of governing this commonage.

It should be noted that there is conflict even within the DOD regarding the constitution of cyberspace. Electronic warfare specialists argue that the broad definition of cyberspace, which includes the electromagnetic spectrum as a defining feature of cyberspace, is not precise.[66] This line of thinking envisions cyberspace as applying only to information technology infrastructures (ITI). Electronic warfare, the argument goes, should be the only domain in which the concept of the electromagnetic spectrum is considered as the defining feature of the environment in which an operation takes place. The proposed solution is for the DOD to create a spectrum warfare commands outside the mandate of a cyberspace command in order to preserve electronic warfare as unique domain of combat. Such views ignore the complex interconnections between electronic warfare and attacks against ITI. Instead, the arguments appear to be part and parcel of the

[66] John Knowles, "Spectrum Warfare" in *The Journal of Electronic Defense* (September 2008), 6.

DOD bureaucracy. Electronic warriors, who have been in existence since the Second World War, are not keen on giving up their domain to cyberspace warriors. This has spurred a reexamination of the DOD's definition of cyberspace.

General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, in late 2008 suggested that a new definition of cyberspace operations should exclude activities which might have effects in cyberspace, such as electronic warfare and psychological operations, but do not make use of cyber capabilities.[67] General Cartwright's suggested refined definition of cyberspace operations is:

> The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[68]

The above suggested definition is confined to operations in cyberspace, such as cyberwar. Cyberspace is still defined as the broader environment in which computer network attacks occur, and in which the Global Information Grid (GIG) exists. Thus, refinements of concepts and definitions of the aims and scope of operations in cyberspace do exist. However, the broader DOD conceptualization of cyberspace is not affected by a rethinking of the definitions of operations within the domain.

Information and Communication Technology

Information

It is useful to discuss the nature of *information* when studying the composition of transmission technologies. Three abstract levels encompassing the term information exist.

---

[67] M. Kunkel, "New Cyber Definition Excludes EW" in *The Journal of Electronic Defense* (November 2008, 26).
[68] Ibid..

These are: data, information and knowledge.[69] Information is present in each level, but its content and level of processing determines how it is distinguished from one level to the next.[70] Data is characterized as the most primitive form of information. Observations, measurements and primitive messages constitute data at this level.[71] Usually, data is useful when it is recorded in some form, be it through human cognitive processes or other electromagnetic means. Information emerges from organized data sets. Sorting, classifying, indexing and linking data are examples of processes for organizing data. For example, if data is organized in such a way that all data elements in set A are distinguishable from data elements in set B, then set A or set B is information.

Knowledge emerges from interpretations of information in data sets A and B. In this way, one can make sense of information for the sake of understanding the information in and of itself, or to identify relationships between data sets. The process of making valid observations based on these data sets can eventually form new content, and thus new *information* or knowledge. True knowledge is the highest form of *information*. Without delving into the epistemological debate on a topic that has bewildered philosophers for at least three millennia, it is roughly in this way that subjective beliefs based on observations of external realities are formed.[72]

---

[69] For the purpose of this study, *information* is the general term "information," whereas information is an abstract concept.

[70] Edward Waltz, *Information Warfare: Principles and Operations*, (Boston, MA: Artech House, 1998), 1-3.

[71] Ibid.

[72] Since in a work of this scope and length it is not possible to engage in an epistemological dialogue on the topic of knowledge, belief and reality, some readings are suggested for the further consideration on this topic:
Plato, "The Allegory of the Cave," in *The Republic of Plato*, trans. Francis MacDonald Cornford (New York: Oxford University Press, 1945), 514a-521b.
Idem., *Gorgias*, in *Plato*: *Complete Works*, eds. John M. Cooper and D. S. Hutchinson (Indianapolis, IN: Hackett Publishing Company, 1997), 454a-456b.
Ibid., *Thaetetus*, 198d-199b.

Open Systems Interconnection (OSI) Reference Model

The electromagnetic spectrum composes only part of cyberspace; the rest of the cyber environment is comprised of internetworked information systems. The suite of protocols standardized by the International Organization of Standards (ISO) for the Open Systems Interconnection (OSI) model form the basis of networking. One should keep in mind that this is an abstract conception of which many parts overlap in the real world. These protocols are built on an open architecture designed on a cross platform client/server model intended to minimize network traffic.[73] Computers connecting over an open network depend on the communications protocol defined in the OSI reference model. Seven layers of internetworking form this basic model, which comprehensively illustrates the standards to which computer networks must adhere to so that they can interconnect and exchange information.[74] The seven layers of internetworking consist of the following:

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Bits of information are received in the aforementioned sequence, and transmitted in the reverse order.

René Descartes, "Meditation Four: Concerning the True and the False," in *Discourse on Method and Meditations on First Philosophy*, Trans. Donald A. Cress (Indianapolis, IN: Hackett Publishing Company, 1998) 81-87.

73 Ibid., 29.

74 Gene White. *Internetworking and Addressing* (New York, McGraw Hill, 1992), 12.

The physical layer is composed of the signals facilitating network communications. This layer includes signals such as light and electricity, mechanical standards and signaling procedures (such as the voltage and frequency of the signal).[75] A terrorist aiming to disrupt the first layer would have to damage the network's hardware components in order to succeed. Such an attack might consist of nothing more than gaining access to a poorly secured wiring closet and cutting connecting wires.

The data link layer is responsible for data movement across networks in the form of packets. This includes protocols for the interconnection of hardware devices such as hubs, bridges, switches and other hardware not connected to the Internet. This equipment functions to move packets across a network.[76] Local area network Ethernet services are an example of a data link layer network. On local area networks (LAN), computers are addressed and identified via the Media Access Control (MAC) protocol, which controls the addressing of devices connected to a specific LAN.

The network layer is a hierarchical addressing mechanism through which data is routed from machine X to machine Y. Internet Protocol (IP) is one element of the network layer. This protocol is responsible for assuring the accurate transmission of packets to their proper destination across networks. The Internet relies on IP.

The Internet, World Wide Web, and other computer networks rely on a suite of military grade protocols commonly referred to as the Transmission Control Protocol/Internet Protocol suite (TCP/IP) to transport packets uncorrupted between across networked devices. While a part of the transport layer, the TCP/IP suite consists of its own four abstract layers, known as the network access, Internet, host-to-host and

75 Molyneux, 39.
76 Ibid., 66.

application layers. These layers, for the most part, overlap with the layers of the OSI Reference Model. The network access layer allows for TCP/IP to work with just about any network and its associated infrastructure. Therefore, it operates on almost any technology equivalent to OSI layers one or two. The main component of the Internet's network layer is the IP header. It is this protocol that facilitates the delivery of service requests across the Internet to the correct machine. The IP header contains critical information pertaining to source and destination addresses. Machines require source and destination addresses to connect with each other through the Internet.[77] All hardware connected to the Internet must have a valid IP address to function.

The session layer controls the establishment, maintenance and termination of connections between applications across a network. Applications such as chat programs, web conferencing or voice over IP (VOIP) software rely on the session layer to synchronize the flow of information. The presentation layer delivers and formats information to the application layer. This is where the computer code is compressed, decompressed, encrypted or decrypted in response to service requests made by the user at the application layer.

The application layer is where application protocols such as File Transfer Protocol (FTP), telnet and email protocols exist. A crucial element of the Internet suite - the Domain Name System (DNS) - is the part of the application layer that makes the Internet user friendly. DNS allows people to use Uniform Resource Locators (URLs) to communicate with other machines on the Internet. Instead of having to type in the IP address of a website, (which might read as 165.230.79.226) a person can type URL

77 Ibid., 85-86.

http://dga.rutgers.edu in a web browser to connect with the desired corresponding IP address. IP addresses reside on DNS databases on root servers that allow for the translation of URLs into IP addresses.[78] The top-level domain names, such as ".com" or ".net," are maintained and updated by the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN). It is the responsibility of this corporation to copy parts of this database through twelve other root servers that communicate with servers maintaining the connections of other machines to the Internet. Country-coded top-level domains, such as .us or .tv, are considered the sovereign territory of the owning state.[79]

Tom Leighton, professor of Mathematics at MIT and co-founder and chief scientist of Akamai Technologies, argues that beyond worms, viruses, and Trojan horses, the fundamental protocols on which the Internet runs are too weak to provide reliable security mechanisms.[80] According to Leighton, the DNS, ports, and IP address systems are plagued by flaws that "…imperil more than individuals and commercial institutions. Secure installations in the government and military can be compromised" as well.[81] The reason for the current flaws in the Internet's network architecture is due to continued reliance on protocols created thirty-five years ago when the Internet was not a global entity, but a closed research network. When the Internet became aaa global phenomenon, there was no shift to create stronger security mechanisms. Thus, many of the issues that global cybersecurity efforts hope to resolve stem from current communications protocols. Therefore, Internet criminal or terrorist misuse is possible, and critical information infrastructures are vulnerable to attack.

---

78 Molyneux, 86.
[79] World Summit for the Information Society, *Tunis Agenda for the Information Society*, II.63.
80 Tom Leighton. "The Net's Real Security Problem." In *Scientific American* (September 2006), 44.
[81] Ibid.

The Internet, which is based on the OSI model, is the most recognizable interconnected computer network. However, not all networks are open systems. Closed global systems, such as the Society for Worldwide Interbank Financial Transactions (SWIFT), Business-to-Business (B2B) networks, and private local area networks (LAN) which are not connected to the Internet also compose parts of cyberspace.

Geospatial Elements of Cyberspace

The geography of cyberspace is the final element composing the Information Societies enabling environment. The geospatial aspects of cyberspace reside in the first layer of the OSI Reference Model: the physical layer. Hardware such as transoceanic fiber-optic cables, radios and satellites are the infrastructure over which global information flows take place. The free flow of this information is bound to the geographic location of the first layer of the OSI model.

Bits of information flow through a complex network of machines, wires and other components. Scholars are aware of the importance of the study of the geography of information flows and its associated technology in order to understand social and political behaviors.[82] Writing in 1993, Ahoron Kellerman explains why the study of the geographical distribution of electronic information flows has been neglected.[83] First, by

---

[82] See, for example:
Eugene Van Cleef, *Trade Centers and Trade Routes* (New York, New York: D. Appleton Century, 1937).
Donald, Q Innis "The Geography of Radio in Canada" in *The Canadian Geographer* (1953 (3) 89-97.
George Kingsley Zipf, "Some Determinants of the Circulation of Information" in *American Journal of Sociology* 1946 (59) 401-421.
Torsten Hägerstrand, "Aspects of the Spatial Structure of Social Communication and the Diffusion of Information," *Papers of the Regional Science Association* (16) 27-42.
R.F. Abler, "The Geography of Communications" in *Transportation Geography: Comments and Readings.* in Michael E. Eliot Hurst (Ed.) (New York, New York: McGraw-Hill Book Company, 1974, 327-346).
[83] Ahoron Kellerman. *Telecommunications and Geography* (New York: Belhaven Press, 1993), 12.

their nature, electronic information flows tend to be "intangible or invisible" when electronic transmissions are compared with the transportation of people and goods over various visible modes of transportation such as via ships or railways.[84] Kellerman identifies a paradox in this notion. Although information flows are not visible, the infrastructure on which bits travel consists of vast terrestrial elements comprising an extensive geography.[85] Examples of each environment and the technologies utilizing it are as follows:

Terrestrial	Transmission media, networks and nodes
Maritime	Transoceanic cables
Outer Space	Satellites
Air (Spectrum)	Electromagnetic waves

Table 1: Elements of the Cyberspace Environment

Geographical aspects of telecommunications include nodes, networks and transmission media.[86] The organization of these components may differ at the national level. The focus of this study is on the international linkages of national telecommunications infrastructure. It is useful to briefly examine the geographical components of the Internet, since its infrastructure is the main conduit for global information flows and the backbone of the Information Society.

Terrestrial

Networks, nodes and computers, are the land-based elements of cyberspace geography.

[84] Kellerman 12-13.
[85] Ibid., 13.
[86] Ibid., 17.

Maritime

Submarine communications cables are the foundation of international telecommunications. Since the laying of the first cables in 1851, they have enabled point-to-point communications between continents.[87] The technology has improved considerably since those days, with the vast majority of communications flowing across fiber optic cables.[88] Each cable is laid by ship in order to establish connections between landing points. The vast majority of these systems are transatlantic, connecting New York/New Jersey in the U.S. with Europe.[89] Each cable system has a domestic, regional and interregional networking function.[90]

Outer Space

The main use of outer space in cyberspace is for the global transmission of data via the electromagnetic spectrum. Satellites have been referred to as "flying

---

[87] R.S. Newall, *Facts and Observations Relating to the Invention of the Submarine Cable and to the Manufacture and Laying of the First Cable Between Dover and Calais in 1851* (London: E & F.N Spon 1882).
H.W. Malcolm, *The Theory of the Submarine Telegraph and Telephone Cable* (London: Benn Bros 1917).
H.A. Affel, et. Al. "The New Key West-Havana Carrier Telephone Cable," in *Bell System Technical Journal* 11(January 1932),197-212
O.E. Buclkey, "The Future of Transoceanic Telephony" *Bell System Technical Journal* (January 1942), 1-19.
Russell T. Nichols *Submarine Telephone Cables and International Communications* (Santa Monica, CA: Rand Corporation 1963).
Louis Solomon, *Voiceway to the Orient: The First U.S.-Japan Telephone Cable* (New York: McGraw Hill 1964).
Robert M. Black, *The History of Electric Wires and Cables*, (London: Peter Peregrinus Ltd. 1983).
[88] United States Patent 4866704, *Fiber optic voice/data network*
[89] For a complete listing of the cables, see, Bill Glover, *Cable Timeline: 2001-* <http://www.atlantic-cable.com/Cables/CableTimeLine/index2001.htm>
Williams, David O. "An Oversimplified Overview of Undersea Cable Systems". European Laboratory for Particle Physics (CERN), Geneva, Switzerland. Last revision March 1999.
< http://nicewww.cern.ch/~davidw/public/SubCables.html>
[90] Howard Kidorf, "Network Architecture for Submarine Systems" in José Chesnoy, Govind Agrawal, Ivan P. Kaminow, Paul Kelley (eds.), *Undersea Fiber Communication Systems* (Academic Press, 2002, 413-415).

computers."[91] It has been suggested that "they represent the ultimate in advanced multiple-use IT systems that can engage in commercial transactions of various forms as well as military actions."[92]

Electromagnetic Spectrum

Electric and magnetic fields are strong physical forces in our universe. The electromagnetic spectrum of wave frequencies emerges when these two physical forces are unified mathematically. Electromagnetic waves, which are invisible to the human eye, form the backbone of the Information Age. Today, humans are able to use new technologies, such as computers, TCP/IP and satellites, that rely on the electromagnetic spectrum to transmit communications globally at light speed.

The force of electricity is characterized by a property in which likes like forces repel, but unlikes unlike energies forces attract.[93] For example, an atoms electrical charge determines what an interaction between a like or an unlike things will be. Atomic interactions produce electromagnetic waves. Wave frequency is determined by oscillation. The human neuro-optical system in the brain has evolved to allow sense electromagnetic waves oscillating between [(5×10^{14}) and (5×10^{15})] on the electromagnetic spectrum. Bits of information are collected by the human eye and are interpreted in the brain to form a picture of reality. Heated discussions concerning whether consciousness affects information or information affects consciousness have

[91] Dr. Daniel Hastings *Issues in Space* Talk to the Federation of American Scientists 20th Feb 2003.
[92] Hall Gardner, "War and the Media Paradox" in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni (London, Routledge 2009, 11-30).
[93] Richard P. Feynman, *Six Easy Pieces: Essentials of Physics Explained by its Most Brilliant Teacher*, (California Institute of Technology 1995), 28.

been ongoing throughout history and continue today, however it is not within the scope of this dissertation to resolve such neuro-philosophical problems. It is assumed here that, *ceteris paribus,* the conscious brain receives bits of information which form an understanding of the environment and the subject's reaction to it.

Richard Feynman suggests that "the fact that we can see in a particular frequency range makes that part of the electromagnetic spectrum no more impressive than the other parts from a physicist's standpoint, but from a human standpoint, of course, it *is* more interesting."[94] The contributions of Benjamin Franklin, Michael Faraday, John Maxwell Clerk and Heinrich Hertz to the study of electromagnetic fields have laid the foundation for the global communications systems in place today. Faraday observed the reciprocal relationship between electricity and magnetism described above.[95] However, his work lacked a sophisticated mathematical explanation, and thus his contemporaries did not see merit in his findings. It was not until Clerk's mathematical refinement of Faraday's work, published in the *Treaties on Electricity* in 1873, that other physicists, who had until then ignored Faradays work, began to seriously consider possible the applications of electromagnetism.[96] Benjamin Franklin contributed to "the electric branch of natural philosophy."[97] His famous kite experiment demonstrated not only that lighting and

---

[94] Feynman, 32.
[95] Robert H. March, *Physics for Poets*, Fifth Edition (New York: McGraw Hill,2003), 66.
[96] Ibid., 64.
Also see: L. Larmor, "The Origins of Clerk Maxwell's Electric Ideas, as Described in Familiar Letter to W Thomson," in *Proceedings of the Cambridge Philosophical Society*, 32:695-750 (1936).
H. Poincare and Frederick K. Vreeland. *Maxwell's Theory and Wireless Telegraphy* (New York McGraw Hill, 1904).
G.W. de Tunzelmann "Hertz Reserces on Electrical Oscillations" *Annual Report of the Board of Regents of the Smithsonian Institute* (1889).
Oliver J. Lodge, Space Without Wires: Being a Description of the Work of Hertz and His Successors (Arno Press 1974).
[97] Benjamin Franklin, *The Autobiography of Benjamin Franklin* (Philadelphia, PA: University of Pennsylvania Press, 2005), 43.

electricity were the same, but also that electricity could be harnessed from lighting in order to perform electric experiments.[98]

Figure 1: *The Electromagnetic Spectrum.*[99]

Hertz's experiments with electromagnetic waves demonstrated that Faraday and Clerks' predictions that electromagnetic waves travel over distance were correct by developing a device that emitted electromagnetic waves. These scientific discoveries inspired inventors such as Nikola Tesla and Guglielmo Marconi to develop devices capable of transmitting information on the spectrum's radio frequency wirelessly to a device designed to receive and reproduce radioed information.[100] These technologies formed the basis of global communications networks.[101]

Metaphorical Definitions of Cyberspace

Some attention must be given to the metaphorical definitions of cyberspace. The defining characteristic of this conceptualization is the reluctance to identify cyberspace as something real that is part of the Earth's environment. Kellerman ascertains that the popular perception that global telecommunication will eliminate distance and turn the world into a global village is a metaphorical conceptualization. Such definitions attempt

---

[98] Benjamin Franklin, "The Kite Experiment," in *The Papers of Benjamin Franklin, 4: July 1, 1750 through June 30, 1753*, Ed. Leonard W. Labaree, (New Haven, CT: Yale University Press 1961).
[99] http://www.centennialofflight.gov/essay/Dictionary/ELECTROSPECTRUM/DI159G1.htm
[100] Guglielmo Marconi,"On Methods Whereby the Radiation of Electric Waves May be Mainly Confined to Certain Directions," *Proceedings of the Royal Society*, A. 77 No. A518 (April 20, 1906), 413-421.
[101] A more complete history may be found in the following works:
Hugh G.J. Aitken *Syntony and Spark: The Origins of Radio* (New York: Wiley Interscience,1976).
Edmund T. Whittaker, *A History of the Theories of Aether ad Electricity* (London: Longmans Green, 1910).

to explain geography by suggesting that no regional or national differentiations exist that impact the organization of physical infrastructures.

William Gibson first introduced the term "cyberspace" in his science fiction novel *Neuromancer.*[102] He describes cyberspace as a:

> Consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.[103]

This view of cyberspace is global and permeates all levels of society as a complex and non-physical cognitive abstraction of the interlinking of data via computers. In his book, *Cybercultural Theorists: Manuel Castells and Donna Haraway,* David Bell states that Gibson's conceptualization of cyberspace, or Gibsonian Cyberspace, "had a profound influence on its development and its representation - an influence Gibson admits he did not foresee when he cobbled the word together."[104] This is apparent in Gibson's essay, *Academy Leader*, which describes how his coining of the term "cyberspace" was more of an effort in poetics than a contribution to science. Explaining that the term cyberspace was conceived as he:

> Assembled the word cyberspace from small and readily available components of language [which]… Preceded any concept whatever. Slick and hollow-awaiting received meaning. All I did: folded words as taught. Now other words accrete in the interstices.[105]

---

[102] William Gibson, *Neuromancer. (*Ace Books 1984)
[103] Ibid.
[104] David Bell, "Moments in Cyberculture" in *Cybercultural Theorists: Manuel Castells and Donna Haraway* (New York, New York: Routledge 2007, 2-3).
[105] William Gibson "Academy Leader" in *Cyberspace: First Steps (ed)* (Cambridge, MA: MIT Press, 1991).

Gibson thus did not have any particular conceptualization for cyberspace in mind when he first coined the term, and acknowledges that it has come to mean various things. His account influenced many conceptualizations of cyberspace, which emphasize the non-physicality of this domain.

Scholars studying the national security and international legal aspects of cyberspace are not immune to having some elements of Gibsonian cyberspace present in their analysis. For example, Thomas C. Wingfield in *The Law of Information Conflict* defines cyberspace as a non-physical place which:

> …defies measurement in any physical dimension or time-space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems and telecommunication infrastructures commonly referred to as the Internet and World Wide Web. Information is the valued commodity of cyberspace, but nothing actually exists in cyberspace.[106]

Similarly, Martin Libicki's early assessment of cyberspace defined the domain as "the sum of the globe's communications links and computational nodes."[107]

Some have argued that states are places, while the Internet is:

> A collection of places, a multiplicity of spaces, The people that use the Internet inhabit a physical space, as do the machines, the computer and cables that provide the technical infrastructure that underlies the Internet. Before they log on and while they are logged on, the same people are subject to the 'laws of the land', the State, where they happen to be located…once they are logged on, they are also in 'Cyberspace' which is not a tangible territory but which is a vase space nevertheless, a space (or possibly a

[106] Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace (*Falls Church, Virginia: Aegis Research Corporation, 2000), 17.
[107] Martin Libicki, "The Emerging Primacy of Information," *Orbis* 40, Issue 2 (Spring 1996), 261-274.

> collection of spaces) that was promoted as having no national boundaries.[108]

Additionally, Robert Keohane and Joseph Nye suggest that:

> The contemporary information revolution, however, is inherently global since 'cyberspace' is divided on a nongeographical basis. The addresses 'edu,' 'org,' and 'com' are not geographical."[109]

Such conceptualizations define cyberspace as a social construct outside of the realm of the physical environment. Keohane and Nye's analysis in particular is invalid since the domain names they mention do have geographical coordinates. This is a serious oversight, since the ICANN - a U.S.-based corporation whose servers are located in the U.S. and operated under agreement with the Department of Commerce - is responsible for the administration of top-level domains such as .com, .org. Currently, the U.S. is resisting a worldwide effort to internationalize the domain-name system. Since the servers are based in the U.S., there is little the global community can do other than condemn, criticize and complain at international conferences. I will discuss this situation in greater detail in a later chapter. However, it is one example of how scholars overlook the geospatial elements of cyberspace.

Martin Libicki, an influential information warfare theoretician, argues in *Conquest in Cyberspace* that cyberspace cannot be considered a global commonage in the same way as seas, air and outer space, since cyberspace and its rules are social constructs. He emphasizes that "what can and cannot be done in cyberspace need not follow the laws

---

[108] Jeanne Pia Mifsud Bonnici. *Self Regulation in Cyberspace* (The Hague, Netherlands: TMC Asser Press, 2008), 1.

[109] Robert O. Keohane and Joseph S. Nye, "Power and Interdependence in the Information Age" in Democracy.com? Governance in a Networked World (Hollis, NH: Hollis Publishing Company, 1999), 197-214, 199.

of physics or the laws of man."[110] Therefore, cyberspace is not a global commonage in the same way as other commons. The rules that exist do so because they are persistently used. These rules and conventions, such as networking protocols and computer code, are "constructs in which people have invested value."[111] That is, they are persistent as long as these rules and conventions are deemed valuable to those establishing them.[112] Libicki acknowledges that cyberspace is composed of physical (wires), syntactic (protocols such as TCP/IP) and semantic (information meaningful to humans and computers) layers. This is concordant with the International Standards Organization model of internetworking. Relying on metaphorical conceptualizations of cyberspace in an investigation of types of conflict in cyberspace, as Libicki does, is useful for understanding his concept of friendly conquest in cyberspace. Libicki deemphasizes the physical environment of cyberspace as a defining feature of it. Instead, socially constructed elements such as code and protocols, rather than electromagnetism, determine his conceptualization.

It might be suggested that since Libicki's focuses on friendly conquest in cyberspace he is dealing with different mechanisms from hostile conquest, and as such does not need to rely on the strategic definition. This assumes that friendly and hostile conquest have characteristics making the one unique from the other. As is described Chapter Three, Russian and Chinese cyberwarfare programs do not distinguish between hostile and friendly conquest. Both are forms of strategic threats to their national security.

---

[110] Idem., *Conquest in Cyberspace*, 6.
[111] Ibid., 7.
[112] This view is not unique to Libicki. See also: Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999). Johnathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, Connecticut: Yale University Press, 2008).

Therefore, Libicki's definition is not parsimonious in the way that the DOD definition is. There is a limited contextual range for the term, since cyberspace is used in many languages as a popular metaphor for the Internet, something that Libicki correctly disagrees with but does not resolve with his definition. It is therefore not a valid conceptualization that can be used in negotiations aiming to govern cyberspace. Hence, such definitions cannot accurately account for various uses of cyberspace, such as electronic warfare, which rely on the physical sciences.

As noted above, Libicki is redefining a concept for which a satisfactory conceptualization already exists (i.e.: the DOD definition mentioned above). In contrast to Libicki's definition, the DOD designates cyberspace as a physical environment composed of electronic hardware and software powered by and inter-networked via the electromagnetic spectrum to communicate and store information. It is more than just a social construct. Cyberspace is a part of the Earth's environment whose global potential have only recently been harnessed.

Using metaphorical definitions of cyberspace in global negotiations would prohibit the chartering of any law governing it. Metaphorical definitions envision cyberspace as something different from other elements in Earth's environment. Consequentially, it might be argued that cyberspace is not a global commonage and does not require institutions of global governance since it is not a physical resource.

Conclusion

As with other global commons, cyberspace is a part of Earth's environment and is rooted in the physical sciences. It requires governance as a result of technological advancements making human activity in the commons possible.

Metaphorical conceptualizations of cyberspace do not adequately cover the environmental aspects of cyberspace however, strategic definitions that treat this domain as another part of Earth's physical environment. Technology harnessing frequencies on the spectrum transmit and receive information across international borders at light speed. Cyberspace is a global commons created by widespread geospatial distribution of terrestrial, maritime, outer space and electromagnetic spectrum technologies. The Internet in particular has caused a information revolution. The Information Society continues to grow and expand across the digital-divide. On the digitial side of the divide, society has come to depend on ICT due to the rapid migration of critical infrastructures, financial service and commerce into cyberspace. The misuses of ICT become more consequential as all aspects of human behavior become reliant on, and are influenced by, what is seen and done in cyberspace.

Chapter Three
The Militarization of Cyberspace

This chapter begins with an overview of the toolkits that anyone with a rudimentary knowledge of computers and networking can draw from to attack information systems using information. It is noted from the outset that although each

method alone requires basic knowledge, complex attacks require an understanding of how to converge all of the tools to exploit information systems. I will discuss the militarization of cyberspace from the point of view of the U.S.. Russian and Chinese reactions and countermeasures will also be discussed. Furthermore, the misuse of digital information and communications technologies (ICT) violent non-state actors will be covered. Overall, I will show that cyberspace has become a new domain in which the use of organized violence for the purposes of the state, and the empowerment of violent non-state actors occurs. This chapter sets the background for the next two chapters on the Greek data espionage and United Nations sanctions case studies.

A Toolkit of Tactics and Payloads for Misusing Cyberspace

Tools and Tactics

The changing nature and variety of the network vulnerabilities, tools and tactics available to cyber criminals and terrorists makes it impossible to document the full range of threats in cyberspace. Dorothy Denning's classification of tools and tactics that computer criminals, terrorists and information warriors might use in their information warfare campaigns is still relevant eleven years after its publication. The tools and tactics developed since the article was published fit neatly into Denning's following classifications:

- Eavesdropping and Packet Sniffing
- Tampering or Data Diddling
- Snooping and Downloading
- Spoofing
- Jamming or Flooding
- Injecting Malicious Code
- Exploiting Flaws in Design, Implementation or Operation

- Cracking Passwords, Codes and Keys[113]

These archetypical types of cyber attacks have become enhanced and more widespread in the past eleven years in that the cyberattacks are more complex. A sophisticated attack today may use all of the above attack methods to penetrate an information system. This complexity is due to overlap between categories, and will be noted below. The Greek case study discussed in Chapter Four, will further demonstrate that when a group of highly sophisticated hackers, possibly using state resources, are involved in a highly complex attack, all of the basic elements converge.

Eavesdropping and Packet Sniffing

These techniques refer to the capturing of data packets en route to their destinations without altering information. They are typically used to capture user IDs and passwords. Technological changes that have occurred since Denning's first writing have made such attacks more consequential. Whereas in the past data was transmitted over copper wire, the mass adoption of wireless technologies such as WiFi and Bluetooth enable hackers to sniff out data from the electromagnetic ether rather than having to find a way to have direct access to a data source.

Tampering or Data Diddling

Denning defines tampering or data diddling as "making unauthorized modifications to software stored on a system, including file deletions."[114]

[113] Dorothy E. Denning, "Cyberspace Attacks and Countermeasures" in *Internet Besieged: Countering Cyberspace Scofflaws (*Eds) Dorothy E. Denning and Peter J. Denning (New York, New York: ACM Press 1998, 29-55).

[114] Denning, 33-34

Snooping and Downloading

Snooping and downloading does not involve capturing information that is in transmission. Rather, attackers obtain access to files and folders on a given computer and are able to browse without restriction. Files of interest may then be downloaded to the attacker's data storage device, such as a flash drive.[115] To conduct such an attack, physical access to the information system is required. Indeed, outright theft of an information system constitutes such an attack. The consequences of snooping and downloading are not light. In 1996 "United Nations officials reported that four computers containing data on human rights violations in Croatia were stolen from their New York offices, dealing a heavy blow to efforts to prosecute war crimes."[116] Thus, in at least one case, evidence critical to the reconciliation process of populations in post-conflict zones suffered setbacks after such an attack.

Key loggers are tools that can be used by unauthorized persons to gain access to information on a computer. Software and hardware key loggers exist, and both types record all keystrokes made on a computer. They are used to capture passwords and other information required for login. A criminal can glean other sensitive information so that he or she might access a computer network. Software key loggers are installed directly on a computer, and therefore may be identified and removed by a suspicious skilled person, or by anti-malware software, which most users rely upon to detect malicious code. However, hardware key-loggers are undetectable by such software since they are physically attached to the cable that connects the keyboard to the computer. This data can

---

[115] Ibid., 33.

[116] *The risk: The usual hazards of not having a good data backup plan?, Wall Street Journal, January 17, 1996; [Brian_Mulvaney@intersolv.com via risks-digest 17, Issue 65]*. See Also, Denning, 33.

be read if the device is retrieved and the captured keystroke data is output to a computer. The only way to discover hardware key loggers is by physically examining the keyboard-to-computer connection.

Spoofing

Spoofing attacks strike at the root of trust in identity and security in cyberspace. An individual may manipulate various layers of the OSI in order to create the false appearance of a user, device or website. Given the global nature of the Internet, it is possible for a hackers can exploit software vulnerabilities, spoofing their location an making the attack to appear to have originated anywhere in the world. This technique permits skilled computer criminals to thwart cybercrime investigations. Denning aptly points out that in order to "trace an intruder, the investigator must get the cooperation of very system administrator and network service provider on the path."[117] This time- and patience-consuming task is complicated by weak domestic legislation and regulation. Attackers bouncing their attacks through a maze of servers in different countries increase their chance of getting away with a crime due to the lack of international cooperation for political and technical reasons.

Jamming or Flooding

This method is used to disable or tie up system resources. Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks are the primary examples of these sorts of attacks. Hackers targeting information systems with DOS or DDOS have been able to prevent legitimate consumers from accessing e-commerce websites, slowed down the domain name server system (DNS) and even shut down the country of Estonia during a

[117] Denning, 35.

massive cyberattack in May 2007. What is notable about the Estonian incident is that the Kremlin-backed youth group that claimed responsibility for the attack asserts that they did not use any software programs to conduct their operations.[118] Instead, they claim, they used the Internet to organize thousands of dispersed youth to make legitimate requests on specific Estonian information systems. The high volume of legitimate requests precipitated the outage of the information systems.

Injecting Malicious Code

A computer virus is one form of software that contains malicious code. These functions can range from simple annoyances to the user, such as resetting the computer's clock, to completely erasing all the data on the drive. Viruses can replicate, and have the ability to spread to other computers. Worms are similar to viruses, however, they spread by scanning networks and replicate themselves on networks that have specific security holes. Trojan horses are malicious codes disguised as legitimate programs. When run, they perform some malicious task instead of the task that a user was expecting the program to perform. In all instances, compromised computers are known as bots or zombie computers.

While a single malicious program (or malware) installed on a single computer can compromise data on that computer, cyber-criminals are now using malware to potentially take over thousands of computers infected with malware. In doing so, the criminals create expansive networks of computers, called botnets, from which cyberattacks can potentially

---

[118] Ian Grant, "Kids Responsible for Estonia Attack" *Computer Weekly* (13 March 2009) http://www.computerweekly.com/Articles/2009/03/13/235262/kids-responsible-for-estonia-attack.htm

be launched.[119] A botnet containing a large number of bots can be used to send spam, commit click-fraud, and steal information via computers the attackers do not own, unbeknownst to the legal user, granting them distributed computing power dispersed geographically allowing diligent attackers time to cover their tracks.[120]

A rootkit is a stealthy software program that conceals its presence from security and other software by modifying parts of the target computer's operating system and/or computers kernel (core), thereby preventing the system owner from discovering, managing or getting rid of the rootkit.[121]

Exploiting Flaws in Design, Implementation or Operation

Poor programming of computer software and operating systems creates flaws which hackers exploit "to gain access to systems, files, accounts, or root privileges, or to sabotage the system or its files."[122] The danger of not identifying these errors, or making the errors public, can make information systems insecure, unbeknownst to trusting users. Since most users lack the knowledge to discover bugs on their own, they rely on patches and updates from software manufacturers. They then have to have to know how to fix the problem themselves, and vigilantly keep tabs on whether or not their information systems are running software with the latest security patches installed.

Cracking Passwords, Codes and Keys

---

[119] John Markoff, "Attack of the Zombie Computers is a Growing Threat Experts Say," *The New York Times*, (7 January 2007) Section 1; column 5.
[120] Nicholas Ianelli and Aaron Hackworth, *Botnets as a Vehicle for Online Crime*, CERT Coordination Center, 1 December 2005.
[121] Stephen Cass, "Antipiracy Software Opens Door to Electronic Intruders: Sony BMG shoots itself—and its customers—in the foot" in *IEEE Spectrum* (January 2006) 12-13.
[122] Denning, 38.

These methods entail either a brute force or guess and check method of guessing a user's password, or the use of sophisticated software designed to decrypt password files and keys. Denning notes that: "It is often possible to crack a key much faster than would be expected by exploiting a hole in the implementation of the encryption algorithm or key management function."[123]

Examples of Computer Network Attacks

Although the Greek case study offers below deeper insight as to what a highly sophisticated attack against a secure and complex digital cellular phone network looks like, a non-exhaustive explanation of how the OSI layers may be attacked within Denning's classification schema of cyberattacks is provided below.

Attacks Targeting TCP/IP Network Architectures

Various malicious programs (malware) exploit the session layer to allow unauthorized access to a computer. A variety of software exists on the market that aims to protect information on a computer from malicious code. Encrypting and compressing (packing) malware are two popular methods that terrorist programmers use to conceal malware from security software and/or computer network security analysts. Packers and cryptors disguise malware code by compressing or encrypting the program or file in which malicious code has been inserted. This transforms the code into random byte sequences, and has the effect of making the malicious code appear harmless to malware detection programs. Approximately ninety percent of malicious code is delivered in

[123] Denning, 40.

packed or encrypted form, and the level of sophistication increases each year, posing new challenges to computer security officers.[124]

The application layer is where application protocols such as FTP, telnet and email protocols exist. A crucial element of the Internet suite, Domain Name Servers (DNS) are the part of the application layer that make the Internet user friendly. DNS allows people to use Uniform Resource Locators (URLs) to communicate with other machines on the Internet. Instead of having to type in the IP address of a website, which might appear as 64.236.91.22, a person can type the URL http://www.cnn.com in a web browser to connect with the desired corresponding IP address. IP addresses reside on DNS databases on root servers that allow for the translation of URLs into IP addresses.[125] The top-level domain names, such as .com or .net are maintained and updated by the Internet Corporation for Assigned Names and Numbers (ICANN). It is the responsibility of this corporation to copy parts of this database through twelve other root servers that communicate with servers maintaining the connections of other machines to the Internet. Country-coded top-level domains, such as .us or .tv, are considered the sovereign territory of the owning state.[126]

Vital computer networks that are part of the domain name system are open to electronic attacks. In some cases, computer security officers do not take the necessary steps to safeguard the domain name system.[127] Common exploits include Denial of Service (DOS) and Distributed Denial of Service (DDOS). The consequences of such

---

[124] Robert Lyda and James Hamrock, "Using Entropy Analysis to Find Encrypted and Packed Malware," in *IEEE Security and Privacy* 5, no. 2 (March/April 2007): 41-45.

125 Molyneux, 86.

[126] World Summit for the Information Society, *Tunis Agenda for the Information Society*, II.63.

127 Erik Sherman, "DNS: Definitely Not Safe, New Attacks on the Internet's Domain Name Systems Keep CISOs Guessing," in *CSO* (February 2007) 38-41.

attacks were observed in February 2007 when attackers from the Asia-Pacific region launched a DDOS attack on the Internet's thirteen DNS servers.[128] Six root servers were affected including the DOD's "g-root" and the ICANN "I-root" DNS servers were severely crippled during the attack. Neither of these critical infrastructures were outfitted with new security technology that had already been implemented on the unaffected servers.[129] This demonstrates the importance installing software updates meant to fix security holes in software. Further root servers, which host a company's DNS, are vulnerable to complicated attacks known as "pharming."[130] Pharming occurs when an attacker replaces the IP address of a company's server with the address of a machine he or she has set up, thus hijacking the companies' website traffic. When pharming occurs, users access their bank's website IP address and unwittingly send their personal information to hackers, rather than to the intended online banking site Thus, DNS has much potential for misuse by a variety of actors with differing objectives. Some might want to bring down the Internet, while others might want to preserve the Internet in order to carry out the equivalent of high-robbery in cyberspace.

While attackers can exploit DNS, they face enormous redundancy by design. The DNS is composed of tens of thousands of systems through which information can be routed. [131] However, although it might be difficult to bring down the Internet, insecurities in network infrastructure lead to a reduction in people's trust of the technology.

---

128 Internet Corporation for Assigned Names and Numbers, *Factsheet: Root Server Attack on February 7, 2007* <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>, cited on 27 April 2007.
129 Ibid., 2.
130 Sherman, 41.

131 James A. Lewis. "Cybersecurity and Critical Infrastructure Protection," In *Homeland Security*: *Protecting America's Targets*. III: Critical Infrastructure. ed. James J.F. Forest (Praeger Security International: Westport, CT, 2006), 324-338, 332.

Countermeasures

A variety of countermeasures to the aforementioned types of attacks are offered below:

- Encryption (secrecy)
- Authentication Access Control and Monitoring
- Auditing (Logging) and Intrusion Detection
- Virus Scanner and Disinfectors
- Backup
- Secure Design, Implementation and Operation[132]

A variety of software exists on the market that aims to protect information from malicious code. Encrypting and compressing (packing) malware are two popular methods that a programmer might use to conceal a malicious program from security software or computer network security analysts. Approximately ninety percent of malware is delivered in a packed or encrypted form.[133] Packers and cryptors disguise the code of a malicious program by compressing or encrypting the program or file in which malicious code has been inserted. This transforms the code into random byte sequences, and has the effect of making the malicious code appear harmless to the program tasked with detecting the sequence of the code of particular malware. These programs remain a menace, and it is forecast that they will increase in sophistication in the years to come.

The greatest threat to information systems comes from the insecure design, implementation and operation of software. Programmers may not realize that they have overlooked flaws that allow hackers to remotely take over a system. A company or individual might not have the awareness or know-how to change, default software

[132] Dorothy E. Denning, "Cyberspace Attacks and Countermeasures" in *Internet Besieged: Countering Cyberspace Scofflaws (*Eds.) Dorothy E. Denning and Peter J. Denning (New York, New York: ACM Press 1998, 29-55).
[133] Robert Lyda and James Hamrock, "Using Entropy Analysis to Find Encrypted and Packed Malware," in IEEE Security and Privacy (March/April 2007 5 No. 2), 41-45.

configurations to prevent hackers from having easy access to their systems. Insecure practices, such as not updating software with the latest patch to fix programming flaws, also gives hackers the opportunity to break into networks.

To resolve these issues, the Common Weakness Enumeration (CWE) initiative was recently sponsored by the U.S multi-stakeholder National Security Agency. This initiative has led efforts resulting in the identification and publication of twenty-five common critical programming errors that have the potential to weaken the security of the national cyberinfrastructure. Releasing the parameters of these programming errors raises user awareness and promises to improve the standards of computer software development.[134]

The CWE will achieve its goal when:

- Software buyers will be able to buy much safer software.
- Programmers will have tools that consistently measure the security of the software they are writing.
- Colleges will be able to teach secure coding more confidently.
- Employers will be able to ensure that they have programmers who can write more secure code.[135]

[134] Thomas Claburn, "25 Most Dangerous Programming Errors Exposed," in *InformationWeek* (January 12, 2009). <http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=212701491&subSection=News>

[135] "Experts Announce Agreement on the 25 Most Dangerous Programming Errors - And How to Fix Them.Agreement Will Change How Organizations Buy Software." <http://www.sans.org/top25errors/>.

One should keep in mind that there are ongoing efforts to develop next-generation network services, such as Internet2. This new Internet is in an advanced deployment phase at the research and academic levels. However, since the Internet will continue to be the global element of cyberspace, the increased security offered by Internet2 will not benefit users at large. In addition, other efforts to secure the Internet's protocols exist. Among these is IPv6, which has been deployed on a very small number of networks.

National Critical Information Infrastructure

Cyberattacks targeting essential services, such as power stations or air traffic control, may use the same tactics and payloads that attackers utilize in small-scale attacks on individual or enterprise computer systems. In early 2008, the U.S. CIA disclosed that hackers had successfully launched cyberattacks against foreign utilities.[136] These attacks are the outgrowth of a trend that has been building over the past decade in which hackers install computer systems that allow them to remotely control critical infrastructures, such as power, water and transportation, through the Internet. Recent years have seen the advent of wireless networks.

Supervisory Control and Data Acquisition (SCADA) is an ubiquitous information system used worldwide to remotely control industrial and critical infrastructure. SCADA is comprised of distributed remote access points that allow users to remotely connect to an infrastructure linked to a particular SCADA network. The system's direct or indirect connections to the Internet allow for the remote monitoring of industrial and critical

[136] Ellen Nakashima and Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *Washington Post* (19 January, 2008) Page A04.

infrastructure.[137] Since nations and industries rely on these computer networks to efficiently maintain crucial machinery, SCADA itself is a critical system that enables countries and companies to function.[138] Thus, attacks on such networks pose significant threats to human and national security.

SCADA is made up of numerous components that include instruments, operating equipment, local processors, short-range communications, host computers and long-range communications. Instruments sense and report on the condition of critical infrastructures. For instance, instruments in an oil pipeline will sense at what rate oil flows through a section of the pipe. The operating equipment, such as oil pumps, can control this rate of flow by energizing actuators to bring the flow to a desired level.[139] Local processors include Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Intelligent Electronic Devices (IED) and Process Automation Controllers (PAC). These These processors communicate with instruments and operating equipment to either collect data or control equipment remotely. These instructions can be programmed internally on the PLC, administered remotely by a human operator accessing the system from a RTU, or automated computer commands input by IED or PAC.

Communication between the instruments, operating equipment and local processors is short-range; short cables or wireless connections are used to "carry analog and discreet signals using electrical characteristics such as voltage and current, or using

---

[137] Aaron Mannes. 'The Terrorist Threat to the Internet," In *Homeland Security*: *Protecting America's Targets*. III: Critical Infrastructure, ed. James J.F. Forest (Westport, CT: Praeger Security International, 2006), 339-353.

[138] Andrew Hildick-Smith, *Security for Critical Infrastructure SCADA Systems*, <http://www.sans.org/reading_room/whitepapers/warfare/1644.php>, 1 (cited on 27 April 2009).

[139] Ibid.

other established communications protocols."[140] The local processors facilitate communications by translating the different protocols used by the controller, instrument and equipment. The host computer, or Master Terminal Unit (MTU), is often a standard PC. It contains the Human Machine Interface (HMI) software, which allows for the human supervision of the SCADA system. It is through the MTU that long-range communications take place between the local processors and the MTU.

Bruce Berkowitz notes, "Security in the information age depends heavily on who has 'command of the nets' that is, who has greater control over the design, manufacture and operation of information technology."[141] The United States has been, and is currently, commanding the infrastructure of cyberspace, including the Internet. It is therefore in the best position for offensive and defensive computer network operation. U.S. command of the nets is not guaranteed in the long term, especially given that great strides are being made by states in the global community to wean themselves off of ICT developed by U.S.-based entities.

The United States' Militarization of Cyberspace

Organizing violent action in cyberspace for the purposes of the state is an increasing threat to global security. U.S. military information, warfare doctrine and concepts of information war are limited to planning and preparations for hostile operations in times of conflict. This differs from Russian and Chinese threat perceptions,

---

[140] Ibid., 3.

[141] Bruce Berkowitz, "Command of the Nets" in *The New Face of War: How War will be Fought in the 21st Century* (New York, New York: The Free Press 2003, 179-195).

which see the information war occurring in peacetime as well as during wartime. Additionally, both countries are using asymmetric methods to attack information systems, that is, non-state entities guided by elements of the state.[142]

In his book, *Conquest in Cyberspace*, Martin Libicki offers a U.S. view that closely matches the Russian and Chinese perception. He differentiates between conquest *in* cyberspace and conquest *of* cyberspace. An example of conquest in cyberspace is an attack against a power generator. Conquest of cyberspace, in Libicki's view, would mean taking out cyberspace as a whole. He defends this distinction by arguing "while something akin to conquest can be defined for cyberspace, cyberspace itself cannot be conquered in any conventional sense."[143] Instead, he argues that there are two types of conquest that can occur: hostile and friendly. The focus of these types of conquest is on how information and information systems are used to destroy or confuse decision-makers through the manipulation of bits. Thus, for Libicki, conquest in cyberspace is seen more as an attack against the decision-making cycle relying on computer systems in times of war, but occurs in peacetime as well.

Environmental mechanisms operate in Libicki's discussions of information in cyberspace. The information infrastructures within which actors of friendly and hostile conquest in cyberspace operate influence the conditions within which these actors take action. Using the analogy of castles and agoras, Libicki explores two general structures of information environments that information warriors may encounter. Castles "protect

---

[142] Reports have emerged of U.S. programmers serving in the military reserve and being stationed in cyberwarfare units. See: John Lasker "Air Force Draws Weekend Cyberwarriors From Microsoft, Cisco" in *Wired* (08.07.07). <http://www.wired.com/politics/security/news/2007/08/262nd>

[143] Libicki, 4.

noise intolerant environments; agoras are noise-tolerant, indeed noisy environments."[144] Both these environments have consequences for how hostile conquest might take place. In a castle there are bridges, moats and walls which information must penetrate before gaining access to the targeted information system. In the agora, there are more direct routes to the information source, however, the information is redundant in a noisy environment. Therefore, in a poorly secured agora, a hostile actor seeking to either disrupt the information flow or to inject false information meant to confuse decision makers, will deal with the complexities of the information environment.

In the agora, data is redundant (i.e., backed up on other systems which are not attacked or known by the attacker), and thus even a successful attack on that system might not be ultimately crippling to the victim, since data can be restored from the backup. In the castle data is not redundant, however, the attacker faces many obstacles that offer the defender numerous opportunities to detect the attack and take precautions to secure the information. Thus, Libicki uses the analogy of castles and agoras to describe the environmental mechanisms independent of the attackers and defenders in cyberspace.[145]

Libicki describes cognitive mechanisms in his discussion of how humans decide whether information received is credible since information warfare can lead to doubt in

---

[144] Libicki 62.

[145] It should be noted that the scope of this project does not allow for the coverage of all of the environmental mechanisms Libicki uses to explain information warfare and friendly conquest. In the context of the environmental mechanisms, he acknowledges that noise exists in all information systems, and uses the analogy of the human immune system to describe the mechanism of how the information environment deals with noise in a similar way to how the human body identifies, differentiates, and attacks foreign cells which might cause disease. (See Libicki, 60). Further, it should also be noted that the environmental mechanism Libicki uses to describe friendly conquests, the environmental mechanism is the powerful information system whose functions are either appealing or not to an actor.

the credibility of information and excessive deception.[146] In his explanation of the how evidence (information) is converted into judgment, Libicki uses an example of Bayesian games to highlight this mechanism. Briefly, the mechanism of deception rests on an individual's evaluation of new information. This evaluation is based on his *a priori* assumptions. An individual will not alter his previous judgments "unless and until the volume of [contrary] evidence is high."[147] Libicki uses the historical episode of the Allies in World War II deceiving Hitler prior to the invasion of Normandy.[148] The cognitive mechanism of hostile conquest is based on injecting false information into a decision making cycle. Hence, the manipulation of a decision-maker's perception is largely based on his or her *a priori* assumptions that can be shaped by information injections over time.

Hostile Conquest

Hostile conquest is the use of information to attack information. The U.S. military's recent efforts to increase its cyberwar capabilities have turned to hostile conquest. Increases in research and development expenditures in the field of Dominant Cyber Offensive Engagement and Supporting Technology (DCOE&ST) are noted as going from $3 million in FY2008 to $8 million in FY2OO9.[149] This funding is intended for projects including:

> High-risk, high-payoff capabilities for gaining access to any remotely located open or closed computer information systems, those systems enabling full control of a network for the purposes of information-gathering and effects-based

[146] Libicki, 52.
[147] Libicki, 53
[148] Hitler, being convinced as a result of allied misinformation campaigns that the brunt of the allied attack would not occur at Normandy, but rather in Calais, did not change his judgment even when Allied troops were landing in Normandy in great numbers.
[149] "Offensive Cyber Capabilities Sought" in *The Journal of Electronic Defense* (July 2008, 20).

> operations… [including] the capability to provide a variety of techniques and technologies to be able to affect computer information systems through Deceive, Deny, Disrupt, Degrade, Destroy (D5) effects."[150]

An increase in D5 capabilities indicates the U.S.'s intention to expand its offensive cyber capabilities. It is in a better position than any other state or non-state actor to bring together its private and government sector research and development communities in order to innovate cyberwar tools and tactics. Such collaboration between scientists and the state has empowered the U.S. in the past.[151] With U.S.-based business entities controlling much of the global cyberinfrastructure, the U.S. has succeeded for the time being in the friendly conquest of cyberspace. The only way that other nations can counteract is either through investing resources in the research, development and deployment of information systems not dependent on U.S. technology, or by exploiting their knowledge of U.S. backed information systems to mount offensive operations against them.

Friendly Conquest

Martin Libicki's differentiation between hostile and friendly conquest in cyberspace is useful to understanding that conflict in cyberspace is more than just the threat of malicious code destroying data on an information system. Conquest occurs when the core operator of an information system provides legitimate system access to third parties. This access can potentially lead to the reliance of the third-party on that

---

[150] Ibid.

[151] See for example: Chandra Mukerji, *A Fragile Power: Scientists and the State* (Princeton, New Jersey: Princeton University Press, 1989).
Herbert N. Foerstel, *Secret Science: Federal Control of American Science and Technology* (Westport, Connecticut: Praeger 1993).

system. If a third-party comes to rely on said information system to function then friendly conquest has occurred. This does not assume the core operator has designs to use its position to conduct hostile operations in cyberspace, although this is many cases the reality which fuels controversy in international negotiations.

An exploration of this type of conquest is important to understanding the scope of conflict in cyberspace. As described further below in this chapter the world has come to rely on products designed and operated by U.S. based entities including the DNS, ICANN, Microsoft and Cisco products. Confirming Libicki's hypothesis, the world is dependent to a large extent on the U.S. for its access to the Internet. As described in Part Two, U.S. hegemony of DNS and ICANN is a serious point of contention in political processes. The world cannot walk away from the Internet or build another Internet independent of the United States overnight. As described below, Russia and China developing national networks inaccessible via the Internet. However, these do not provide the same services that are designed for the Internet, and thus cannot serve as an alternative for a bitter global community.

Libicki uses relational mechanisms to explain how coalitions leading to friendly conquest occur. Friendly conquest in cyberspace can be interpreted as the willing participation of X in Y's information system. X willingly enters into a coalition with Y in cyberspace. Y's friendly conquest of X occurs when X depends on Y's system. This is not to say that X merely entering the coalition will cause the conquest. X's perceived need for access to (or inability to construct its own) Y's cyberspace causes it to willingly enter a coalition with Y. X adopts to Y's standards and protocols, making up the information system architecture of Y's cyberspace in a way that allows it to interoperate

with X's cyberspace. X's adoption of Y's cyberspace architecture is thus the necessary condition for Y's friendly conquest, and it is a facilitating condition for X's hostile conquest. X might begin to use the standards and protocols of Y's cyberspace as a model for its own cyberspace. Since Y is expert in its own standards and protocols, X's modeling of these standards in its own systems is another cause that can facilitate X's hostile conquest of Y's cyberspace. X does not have to be a friend. It can be a neutral, or a possible future enemy of Y. There is utility in Y opening its cyberspace to X only if Y sees some benefit to itself if X has access to shared cyberspace Once friendly conquest is accomplished, Libicki argues it can facilitate hostile conquest in cyberspace. Friendly conquest of X by Y may facilitate hostile conquest in cyberspace conducted by Y against X.

Although most of the discussion in the open sources are not concerned with friendly conquest in cyberspace, as will be shown below, military officials in other countries such as Russia treat this type of conquest as a serious threat and incorporate it into their doctrines on information warfare.

Russian Militarization of Cyberspace

Russian military operations in cyberspace have been the most visible in the recent past, with much global media attention paid to Russian operations in this domain. Although the Kremlin-backed Estonian plot is one example of how Russia uses its ICT resources in a

decentralized manner, the Russia-Georgia War in 2007 is perhaps the best indicator of how the Russian's include attacks in cyberspace as part of their military doctrine.[152]

Threat Perceptions

America controls nearly eighty percent of the global information grid. The Russians do not, and therefore perceive themselves to be more vulnerable to information warfare.[153] This is one explanation why the Russians vociferously insisted on the creation of a treaty for cyberspace, and on the inclusion of language pertaining to military uses of cyberspace during the WSIS and related conferences. James Adams describes his interviews with Russian military officials and their perceptions of the U.S.:

> These men all wanted to transmit a common message, that Russia is a nation at war. It is in an information war that the country is losing both at home and abroad, and that the current technology gap is comparable to the perceived missile gap of the 1950's that did so much to fuel the Cold War. This time, the race is not for space, but cyberspace. And the Russians are angry and frustrated that the Americans appear to be winning the war and that victory appears more assured every day.[154]

The theory of technogeopolitics predicts that when the technology gap between two states is so vast, the state behind the curve will press for international negotiations, whereas the other will avoid them since its position of technical superiority does not require it to form laws to protect itself. The information war that the Russians see themselves fighting, and their technological gap in terms of ICT with the U.S., confirms this view. The Russians believe that negotiating an arms control agreement with the U.S.

---

[152] John Markoff, "Web becomes a battleground in Russia-Georgia conflict" International Herald Tribune (August 12, 2008) <http://www.iht.com/articles/2008/08/12/technology/webcyber.php>.
[153] James Adams, "The New Arms Race" in *The Next World War: Computers are the Weapons and the Frontline is Everywhere* (London, IK: Hutchinson 1998, 233-244, 233).
[154] Ibid., 234.

is one option to help secure their cyberspace. Washington sees this "as a ploy to allow the Russians to buy time while they attempt to narrow the technological gap between them" and the U.S.[155] If the theory of technogeopolitics is to serve as a guide, this is a rational suspicion on the part of the U.S. However, the U.S. position in international conferences, such as the WSIS, discourages the inclusion of language legalizing information warfare or the military uses of cyberspace.

Timothy L. Thomas describes the recklessness of such U.S. positions, arguing that if the U.S. continues this stance it will lead to yet another weapons race. This new weapons race "will be centered on how to attack information systems through the electromagnetic spectrum, (via third generation nuclear weapons) or to destroy software (via sophisticated computer viruses)."[156] While it is too early to tell what will happen, technogeopolitical theories predict that when the Russians acquire a position of technological hegemony within their sphere of influence, the U.S. will be compelled to sit at the negotiating table to create a law of to regulate conflict in cyberspace, if not a more comprehensive cyberspace treaty.

A debate within Russian military circles as to what cyberspace is, the Russian concept of cyberspace, is geo-strategic in much the same way as the U.S. conception is, albeit with a different name. Russians organize their thinking on the topic of information warfare with the term radio-electronic warfare.[157] Radio-electronic warfare includes intelligence and reconnaissance, psychological, electronic and psychic or paranormal

---

[155] Adams, 244.

[156] Timothy L. Thomas, "Russian View on Information Based Warfare" Originally Appeared in *Airpower Journal*, Special Edition (1996), 25-35, 26.

[157] James Adams, "The New Arms Race" in *The Next World War: Computers are the Weapons and the Frontline is Everywhere* (London, IK: Hutchinson 1998, 233-244, 235).

operations.[158] This is a blend of American information warfare and cyberwarfare concepts of operations with the addition of a paranormal element.[159]

Although the Russians acknowledge the American advantage in cyberspace, they have been described as psychologically more likely to "win a cyberwar if the technological playing field is level," since their radio-electronic war fighters have a more devious organizational culture.[160] While the U.S. presently maintains control of a large percentage of the Internet and other elements of cyberspace, evolving Internet patterns indicate an incremental decrease in traffic passing through the U.S..[161] It is important to consider the advanced level of Russian radio-electronic warfare capabilities as a challenge to U.S. national security when assessing the U.S.'s stance at international conferences, where they object to discussions on the use of cyberspace for military or espionage purposes.

Friendly Conquest

[158] Ibid.

[159] It should be noted that the U.S. Air Force has documented its interest in telepathy and other paranormal phenomena, however, it does not include this in its conceptual paradigm for cyber conflict as the Russian's do. See, for example: Eric W. Davis, *Teleportation Physics Study* (Edwards Air Force Base, CA: AIR FORCE RESEARCH LABORATORY 2004).

[160] James Adams, "The New Arms Race" in *The Next World War: Computers are the Weapons and the Frontline is Everywhere* (London, IK: Hutchinson 1998, 233-244, 235).

[161] John Markoff, "Internet traffic begins to bypass the U.S." *New York Times,* (August 31, 2008).

Onekey area of Russian concern is within the domain of friendly conquest in cyberspace, although they refer to it as "peacetime information warfare."[162] They conceive friendly conquest as a secret information operation conducted through the means of intelligence, politics and psychological actions using specially designed hardware and software techniques against enemy information assets. They perceive a threat from the dominance of U.S. ICT companies, such as Microsoft and Cisco, upon which many government and non-government organizations rely on for their operations.[163] These threats are not merely Russian paranoia, since the U.S. does use its technological superiority and control of the networks to further its hostile information operations. As has been noted:

> Both the CIA and NSA continue to use the importation of computers into Russia for espionage purposes. In some cases, this is done with the cooperation of the companies concerned and in other cases the CIA simply intercepts shipments and inserts the devices that have been perfected by its own scientists. The extent of this program is huge and the most successful of the post-Cold War intelligence environment.[164]

In one case, U.S. intelligence infected IBM and Siemens mainframe computers with logic bombs, viruses and backdoors to allow for the destruction, disruption or data espionage targeting the Russian-owned (but U.S.-built) information systems. Thus, the Russians are aware of U.S. efforts aiming towards the friendly conquest of cyberspace through the use of U.S.-based business entities operating in Russia.

Hostile Conquest

---

[162] Timothy L. Thomas, "Dialectical Versus Empirical Thinking: Ten Key Elements of Russian Understanding of Information Operation" in *The Journal of Slavic Military Studies* 11, No. 1 (March 1998) 40-62, 48.
[163] "Microsoft Identified As the Enemy -- Fire!" *Gazeta.ru* (5 February, 2008) FBIS translation.
[164] Adams, 238.

The Russians are not standing idly by hoping for the U.S. to cease its own use of cyberspace as a medium for projecting its strategic interests. Encouraging academic research and development in information technology and having an educated urban workforce, along with the necessary organizational cultures, gives Russia a comparative advantage against the U.S. in the long-term.[165] A testament to this potential is the development by the Russian Federal Agency for Government Communications and Information (FAPSI) of a Federal Information and Telecommunications System (SFITS) based on Russian-developed hardware and software that is not connected to the Internet.[166] With this system, Russia considers itself the "only country which is capable of providing 100 percent security for consumers at the very first stage of the mass introduction of SFITS in daily life."[167] Thus, the Russians plan on using the SFITS system as the basis for the creation of their own Internet, believing that it will be less vulnerable to friendly and hostile conquest since it will be based on different engineering than the U.S. Internet.

The Russians have been developing federal-level technologies for over a decade, including: multiprocessor parallel structure computers; a computer system based on neuronet computers, transputers, and optical computers; artificial intelligence and virtual reality systems; super large integrated circuits; and nanoelectronics and other information systems.[168] Evidence for the militarization of the electromagnetic spectrum can be found

---

[165] *Information Technology in Russia Analysis: IT Strengths and Weaknesses* <http://www.american.edu/initeb/nb2224a/analysis1.html>.

[166] Timothy L. Thomas, *Russian View on Information Based Warfare* in *Airpower Journal* X, EE, Special Edition 1996 25-35, 26.

[167] Ibid.

[168] Timothy L. Thomas, "Dialectical Versus Empirical Thinking: Ten Key Elements of Russian Understanding of Information Operation" in *The Journal of Slavic Military Studies*, 11, No. 1 (March 1998) 40-62, 50.

in the publications of scientists researching areas such as electromagnetic pulse weaponry.[169]

Chinese Militarization of Cyberspace

As with Russia, U.S. cyberwarfare capabilities are the main cause of worry for the Chinese. Unlike the Russians, the Chinese are late arrivals on the scene of national systems of innovation in the field of ICT. Some analysts argue that the Chinese have unique attributes in the field of ICT which gives them advantages that the Russians lack, making China a more serious competitor against the U.S. in cyberspace than Russia. China's advantages include:

- U.S. ICT companies relying on Chinese manufacturing for the assembly of ICT products
- The Great Firewall of China
- Multi-organizational network collaboration between the Chinese military and civilian hackers

These attributes have led some analysts in the open sources to conclude that the Chinese are in the best position to win a cyberwar against the U.S.[170] Well organized attacks of Chinese origin, such as Titan Rain and Byzantine Foothold, have compromised information systems worldwide with impunity, and have given the U.S. reason to consider China as its greatest cybersecurity threat.[171]

---

[169] Yury Lazarev, Peter Petrov, Generation of an intense, directed, ultrashort electromagnetic pulse. *SPIE* 2557, 512-515.

[170] James Adams, "A Mole in the Oval Office" in *The Next World War: Computers are the Weapons and the Frontline is Everywhere* (London, IK: Hutchinson 1998), 233-244.

[171] Rogin, Josh. "Cyber Officials: Chinese hackers attack 'anything and everything.". http://www.fcw.com/article97658-02-13-07-Web (13 February 2007).
Espiner, Tom. "Security Experts Lift Lid on Chinese Hack Attacks." ZdNet http://news.zdnet.com/2100-1009_22-5969516.html. (23 November 2005).

Threat Perceptions

The Chinese perception of information warfare (IW) differs from U.S. military doctrine in that "most American military experts consider IW as a way of fighting, hence the term warfare, where Chinese experts look at IW as the fight itself."[172] Like the Russians, the Chinese limit their conceptualization to planning for open conflict, but consider this to be a peacetime activity, as well. The Chinese government maintains tight control over Internet activity within China. The so-called Great Firewall of China (GFC) is a technological filter which censors Internet content deemed indecent by the Chinese government.[173] Backed by laws and enforcement mechanisms to punish those bypassing the GFC, it is the response of an authoritarian regime that relies on the control of information flows to maintain its power and avoid outside influences. This places the Chinese government in an excellent position against the U.S. in the event of a cyberwar.

Friendly Conquest

U.S. reliance on China as a manufacturer of computer chips and other ICT hardware puts China in an excellent position to implant viruses and backdoors in equipment used by U.S.-based entities, including the military. It has also been noted that extraordinarily low priced Chinese-made computer hardware are lucrative buys in Asia and the developing world.[174]

---

[172] Barrington M Barrett Jr., 'Information Warfare: China's Response to U.S. Technological Advantages,' *International Journal of Intelligence and CounterIntelligence*, 18:4, .(2005) 682 -706.
[173] John G. Palfrey, Jr, "Local Nets: Filtering and the Internet Governance Problem," in *The Global Flow of Information* (XXXXX 2005)
[174] Lieutenant Commander A. Anand, "Threats to India's Information Environment" *Information Technology: The Future Warfare Weapon* (New Delhi, India: Ocean Books Pvt. Ltd 2000, 56-62).

An example of how U.S. efforts at friendly conquest can backfire and make the U.S. vulnerable to cyberattack demonstrated in Microsoft's experience with China. In 2003, China received access to the source code for Microsoft Windows in a partnership between Microsoft and China to cooperate on the discovery and resolution of Windows security issues. China Information Technology Security Certification Center (CNITSEC) Source Code Review Lab, described as "the only national certification center in China to adopt the international GB/T 18336 idt ISO 15408 standard to test, evaluate and certify information security products, systems and Web services," was the focal point of this collaboration. [175] Unanticipated by ISO standards, Chinese computer scientists reverse-engineered the code. This allowed them to develop malicious code, including viruses, Trojan horses and backdoors, that exploited vulnerabilities in the operating system. These efforts resulted in the shutting down of the U.S. Pacific Command Headquarters after a Chinese-based attack.[176]

Hostile Conquest

The Chinese stratagem of attacking information systems "with a borrowed sword" is perhaps the most difficult to contend with.[177] This stratagem rests on the People's Liberation Army (PLA) interfacing with patriotic Chinese hackers such as the Network Crack Program Hacker" (NCPH). The groups are identified by the PLA through

---

[175] *China Information Technology Security Certification Center Source Code Review Lab Opened* (September 26, 2003) <http://www.microsoft.com/presspass/press/2003/sep03/09-26gspchpr.mspx>.
[176] Barrington M. Barrett Jr., 'Information Warfare: China's Response to U.S. Technological Advantages,' *International Journal of Intelligence and CounterIntelligence* 18 No. 4. (2005) 682 -706.
[177] Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance" *Military Review*, (November-December 2008) 47-54.

competitions in which the winners are awarded with a monthly stipend from the PLA.[178] The NCPH in particular was used by the PLA to teach its cadets tactics and tools for conducing cyberwar.

Other than filtering Internet content, the GFC provides the Chinese government to shut-off access to Internet traffic from abroad, while allowing for Chinese communications to exit China.[179] Thus, in a cyberwar it would be extremely difficult, if not impossible, for the U.S. to launch cyberattacks over the Internet against Chinese targets, although other alternatives exist. The Chinese could still target U.S.-based systems and control malicious botnets established by the military or their patriotic citizen affiliates around the globe.

VNSA's and the Emergent Netwar Paradigm

Today, most violent non-state actors, including terrorist organizations, organize themselves and conduct their operations differently than their predecessors. Whereas in the past terrorist organizations had a more hierarchical, vertical structure, today the use of ICT by terrorists allows them to organize as horizontal networks with decentralized leadership.[180] This has allowed for the emergence of a form of conflict called "netwar."[181] Scholars have identified the impact of advanced ICT on small organizations prior to the

[178] Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance" *Military Review*, (November-December 2008), 47-54.
[179] Jack Linchuan Qiu, "Virtual Censorship in China: Keeping the Gate Between the Cyberspaces," *International Journal of Communications Law and Policy*, Issue 4, (Winter 1999/2000), 1-25.
[180] Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age." In, Networks and Netwars, eds. John Arquilla and David Ronfeldt (RAND, Santa Monica, CA, 2001), 29-60.
[181] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996).

coining of the term netwar.[182] Although various manifestations of netwar exist, its underlying pattern is described as:

> An emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organizations and related doctrines strategies and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command.[183]

For over a decade, terrorists groups, including Al-Qaida, have emerged as netwar actors.[184] The emergence of sophisticated communications technology, such as the Internet, has facilitated this phenomenon. While it is not within the scope of this paper to untangle the dynamics of the netwar concept, it is useful to identify this emerging paradigm of conflict in order to understand the challenges faced by current international counterterrorist efforts in the information age.

While thoughts of devastating cyberattacks using basic tools against critical infrastructure might make for sensationalistic headlines, it has been suggested that such attacks do not pose an immediate threat to national security since "infrastructures are robust and resilient, capable of absorbing damage without interrupting operations, and accustomed to doing so after natural disasters, floods, or other extreme weather

---

[182] See, for example: R.F. Abler, "The Geography of Communications" in *Transportation Geography: Comments and Readings*. Michael E. Eliot Hurst (Ed.) (New York, New York: McGraw-Hill Book Company, 1974, 327-346). In which the author predicts advanced ICT will "make it possible for special interest groups to gather together in distinct places and intensify human and landscape differences, while at the same time maintaining whatever contacts they must or which to have with other specialized groups vial telecommunications (341).

[183] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar and Information Age Terrorism." In *Countering the New Terrorism* (Santa Monica, CA: RAND, 1999).
Also see Arquilla and Ronfeldt, 1996, 5.

[184] Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age" in *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001) 29-60.

conditions."[185] Hence, even if a terrorist organization managed to take down a power station, the effects of such an attack may not be deemed as putting the national security of the United States at grave stake.

The Naval Postgraduate School white paper *Cyberterror Prospects and Implications* outlines three levels of cyberterrorist organizational development: "simple-unstructured," "advanced-structured" and "complex-coordinated." A simple-unstructured organization will be able to conduct operations against individual systems using basic hacking skills. They do not have the skills to create their own programs, and therefore must rely on technology created by others. As a result, the organization has limited command and control capabilities, as well as limited abilities to analyze targets and learn from its experiences. A advanced-structured organization possesses the skills to conduct attacks against multiple systems that are more sophisticated than the simple-unstructured, and also has the ability to program new hacking tools or tailor existing programs to suit its needs. However, the command and control and target analyses capabilities of the advanced-unstructured organization are elementary. If VNSAs reach the complex-coordinated stage, they will be as capable as state militaries with developed cyberwar divisions. This means that, like states, they will have the ability to launch cyberattacks capable of "causing mass-disruption against integrated, heterogeneous defenses (including cryptography)." Further, they can create sophisticated hacking tools and exhibit a high capability for target analysis, command and control as well as learning at the organizational level.

[185] Lewis, 325.

For terrorists to use such devices against targets that have active countermeasures, terrorists must have the knowledge and training to mount a counter counter-offensive utilizing the electromagnetic spectrum to accomplish their goal. They need the right equipment and training in order to achieve success. Therefore, they must be very professional. Such terrorists do exist. They continue to conduct their attacks against their targets using equipment that is either easily available in the global market, supplied by States or obtained on criminal black market networks.

Overall, the shift to the information age brings both opportunities and danger. In the past, it seems that government efforts to combat terrorist use of new technologies, such as airplanes, fit snuggly into their perceptions of security threats. ICT does not. Hence, there exists a great challenge in reforming policymakers' understanding that the threat from the terrorist misuse of cyberspace goes beyond the catastrophic scenarios depicting mass power outages. Terrorists use ICT in all aspects of their operations, however governments do not act against terrorist misuse of ICT for a variety of reasons. When states have acted against other misuses of technology, new dangers were understood since they fit into the framework of conventional dangers. The problem today is that policymakers do not see new technologies, such as the Internet, as a tool for terrorism, but as another means through which attacks can be carried out.[186] Despite the migration of terrorist activities into cyberspace, there has been no equivalent to the firm global response which dealt with the hijacking of airliners. This results in terrorists using cyberspace to efficiently recruit, radicalize, and incite individuals to action; command, control, communicate; gather intelligence, and raise funds on a global scale. These issues

[186] Evan Kohlmann. "The Real Online Terrorist Threat." In *Foreign Affairs* 58 issue 5 (Sep/Oct 2006) p. 115-124.

are dealt in greater detail in Chapter Five, where it is shown that U.N. counterterrorist efforts are being circumvented by terrorists using the Internet.

Conclusion

Focusing on on the information warfare programs of the most active cyberwarfare nations, the United States, Russia and China because indicates that cyberspace is militarized. The actions and reactions to hostile and friendly conquest by all three states are good indicators of the trends that will surely come with the proliferation of cyberwarfare programs. This trend that will only increase as more national governments around the world begin to understand that cyberspace is not a metaphorical construct, but a strategic realm through which national power is projected.

The American, Russian and Chinese cyber warfare programs are interlinked in the following ways. The United States currently commands and controls the Internet infrastructure through its friendly conquest. U.S. government and private entities control the vast majority of the hardware and software on which the Internet, and the rest of cyberspace, functions. Russian military theoreticians and professionals have felt the brunt of U.S. information dominance during the Cold War and after, some directly linking U.S. information warfare campaigns as a major contributing factor to the collapse of the Soviet Union. The U.S. followed its national interest bringing all elements of national power to bear on the Soviet Union, including its ICT resources. As Russia resurges and continues to develop its advanced strategic information warfare capabilities, technical superiority as core operator of the Internet and other ICT resources, U.S. advantages in a cyberwar may decrease. Russian offensive uses of cyberspace were officially

demonstrated during the Russian-Georgian war of 2008, notably against NATO ICT and training protocols. Furthermore, the FAPSI's development of a secure telecommunications network in Russia independent of the Internet and based on Russian technical design and communications protocols is an indicator of Russia's capability to build its own private Internet-like information infrastructure. This could be indicative of a future trend in which the nations prefer to filter the bulk of their communications via domestic private networks.[187] This could be sparked in part by U.S. policies regarding ICANN and DNS (described further in Chapter Seven in conjunction with fears over U.S. military and intelligence programs exploiting U.S. information systems purchased by foreign entities.

China's threat to the U.S. critical information infrastructure is credible, though some might argue over-hyped. The global economy led many U.S.-based entities involved in the manufacture of technology to build factories in China. China took advantage of this by tampering with the supply of hardware and software that is shipped all over the world from these foreign-owned factories. By building malicious code into the supply of ICT, the Chinese effectively wage a form of friendly conquest against the U.S. This may give it an advantage in a cyberwar. Additionally, the Great Firewall of China allows the Chinese to shut off information flowing into China. Thus, in a cyberwar with the U.S., China would be a strong competitor.

It has been suggested in that media attention on Chinese cyber capabilities is the result of Chinese clumsiness in their methods of attacks. Some information security professionals argue that the Russians have superior cyberwarfare capabilities compared to

[187] BR staff writer, "ITU head foresees internet Balkanization" http://www.cbronline.com/news/itu_head_foresees_internet_balkanization <Last accessed on 15 April 2009).

those Chinese posses. One could argue that the Russians have been involved in the field for decades, whereas the Chinese are still testing the waters, having found the front door unlocked and eager to learn how to conduct information operations, albeit in many cases in an amateurish manner. On the other hand, Russian threats are characterized has running silent and deep within information systems. The dynamic nature cyberspace creates an environment in which cyberweapons designed to exploit flaws in the design and implementation of software or hardware remain classified. Military capabilities are kept under close guard so as not to alert adversaries of holes in our systems or the existence of security flaws in their own. Thus, it is more difficult to provide an accurate assessment of national cyber warfare capabilities without being a cleared information warrior.

U.S. friendly conquest and hostile information operations programs, along with the U.S. control of the networks, may give it a distinct advantage. However, if history is to be an indicator, this situation will not continue indefinitely. As I will prove, the U.S.'s reluctance to open access to DNS and ICANN at global cybersecurity negotiations might work for the short term, however, there is a distinct threat that countries around the world might use the Russian or Chinese model of countering U.S. dominance. Overall, the militarization of cyberspace along with public cases of cyberattacks and cyberespionage linked to either U.S., Russian or Chinese interests will continue their upward trend. As more and more people gain access to advanced ICT and join the digital Information Society the consequences of how states direct or and response to cyberattacks targeting their national critical information infrastructures and other systems are unclear due to the lack of an international law regulating information warfare in cyberspace.

Chapter Four
The Athens Affair: The Limitations of Privatized Cybersecurity

Global information flows through cyberspace and is regulated to some extent by national and regional bodies coordinating their policies internationally. Standards that have been created for elements of cyberspace have required lengthy diplomatic processes in order to assure sufficient technical and political cooperation among nation-states. Ongoing efforts are being undertaken under the auspices of the United Nations to promote what the United Nations General Assembly UNGA refers to in numerous resolutions as the "global culture of cybersecurity" (GCA). This is based on a public-private partnership (P3) model of cybersecurity in which the private sector takes the lead in providing security. It is accepted by the UNGA as the organizing principle around which the global efforts to secure cyberspace should occur. An overview of what this cybersecurity culture entails is offered below. It is shown that policies, placing the burden of securing cyberspace on private industry and individuals are flawed.

The focus of this chapter is on the basic tenets of the GCC. While these efforts are indicative of a declared will of the international community to secure cyberspace, the emphasis on private-public partnerships is identified as the Achilles heal of these efforts. The case of the strategic information attack against Vodaphone's cellular telephone network in Greece demonstrates why the P3 model cannot work. On the basis of a review of the technical aspects of this attack, and a review of the Greek information security legal code, it is shown that the standards and practices of P3 advocated by the GCC are perilous. It is argued that proponents of the current P3 cybersecurity model must take the

lessons of the Greek case into account so as to modify their policies to assure that the Information Society is founded on the principles of trust, security and justice, rather than giving the lion's share of responsibility for cybersecurity to private entities more concerned with concealing the full extent of an attack.[188]

Establishment of the Global Culture of Cybersecurity

The establishment of a "global culture of cybersecurity" (GCC) is the main emphasis of UNGA resolution 57/239.[189] Beginning with the fifth preliminary paragraph, the UNGA declared its awareness that "effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society."[190] Further, the UNGA indicates a global awareness "that technology alone cannot ensure cybersecurity and that priority must be given to cybersecurity planning and management throughout society."[191] The first part of this assertion is a valid observation. However, the second part does not identify the main actor responsible for managing and planning society-wide cybersecurity. Not having clearly identified government's role becomes problematic in the resolution's next paragraph, where the UNGA recognizes "that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and

[188] It the norm for providers of digital services to not report all security incidents to their customers and law enforcement authorities.
[189] United Nations General Assembly, "Creation of a Global Culture of Cybersecurity." A/RES/57/239. 31 January 2003.
[190] United Nations General Assembly, "Creation of a Global Culture of Cybersecurity." A/RES/57/239. 31 January 2003, Preliminary Paragraph 5.
[191] Ibid., Preliminary Paragraph 6

must assume responsibility for and take steps to enhance the security of these information technologies."[192] Therefore, the trend of a large number of actors (including governments), all of whom are responsible for securing ICT and preventing its misuse, is established in a manner which relieves government of the primary responsibility of national security in the cyber domain. Thus, in the sequence and wording of these elements, the UNGA manages to shed its responsibility to act as the primary mover in cybersecurity efforts. Instead, the UNGA encourages a trend of emphasizing the role of private actors in providing cybersecurity to society, rather than signifying their importance in *supporting* government and law enforcement efforts.

A significant component of resolution 57/239 is its annex, which establishes nine elements forming the foundational tenets of the global culture of cybersecurity.[193] These are:

- Awareness
- Responsibility
- Response
- Ethics
- Democracy
- Risk assessment
- Security design and implementation
- Security management
- Reassessment.[194]

A brief summation of these nine elements follows. All participants in the global culture of cybersecurity should sustain a level of awareness regarding the importance of having secure information systems.[195] Each participant is responsible for securing their own

[192] Ibid., Preliminary Paragraph 7.
[193] United Nations General Assembly, "Creation of a Global Culture of Cybersecurity." A/RES/57/239. 31 January 2003, Operational Paragraph 3.
[194] Ibid, annex.

information systems, and reviewing the policies, practices, measures and procedures pertaining to their own cyberspace. Timely and cooperative response is achieved with Information Society members sharing information about threats, vulnerabilities and security incidents in order to facilitate the detection of and response to the misuse of information systems.

The UNGA recognizes that cross-border information sharing may be required. The ethical basis of the GCC is founded on utilitarian grounds in that each participant is expected to respect the interests of others and to avoid inaction that will harm others. Cybersecurity regimes are guided by democratic principles, identified as the freedom of thoughts and ideas, free flow of information, confidentiality of information and communication, protection of personal information, openness and transparency. Periodic broad-based risk assessments of the security implications of technological, physical and human factors, policies and services should be conducted to determine appropriate levels of cybersecurity risk are. Security should be incorporated during the planning, design, development, operation and use of an information system. It is on the basis of dynamic risk assessment that security management occurs. Finally, in order to assure that all the above elements remain relevant, periodic reassessment is required.

As with the preliminary paragraphs,of UNGA resolutions do not clearly define government's role in cybersecurity. It appears that members of the GCC are responsible for the protection of their own information systems and developing cybersecurity policies in a way that assures that vulnerabilities in one information system do not affect other systems. Moreover, not all information systems are equal since some information is considered more valuable than other information. It will be argued below that this

[195] Ibid.

approach is incorrect and does not take into account the underlying reasons pertaining to states, organizations and individuals using ICT.

The global culture of cybersecurity grew from previous UNGA resolutions dealing with ICT and security issues. UNGA resolution 56/19 entitled "Developments in the Field of Information and Telecommunications in the Context of International Security" highlights several key issues pertaining to the Information Society and the provisioning its cybersecurity. The UNGA recognizes the global characteristics of ICT, such as the Internet and World Wide Web (WWW), as the basis for the Information Society, and determines that international cooperation is required to assure the peaceful use of ICT.[196]

In resolution 56/19, the UNGA acknowledges the potential misuse of ICT in ways that will "adversely affect the security of states in both civil and military fields."[197] Member States are encouraged to prevent the use of information technology for criminal or terrorist use while concurrently promoting its peaceful use, though guidelines for how to do so are not offered. In the operational paragraphs of resolution 56/19, the GA calls on Member States to support and contribute multilateral efforts to identify present and future threats to international security resulting from the misuse of information technology, and to develop countermeasures to these threats. Cybersecurity solutions must be "consistent with the need to preserve the free flow of information."[198]

Preserving the free flow of information is a challenging objective, since countermeasures to misuse cyberspace tend to prevent the flow of information in on way or another. For example, when one installs a firewall on a computer network and sets it to

---

[196] U.N. General Assembly. "Developments in the field of information and telecommunications in the context of international security." A/RES/56/19, PP7. 7 January 2002.
[197] U.N. General Assembly. "Developments in the field of information and telecommunications in the context of international security." A/RES/56/19, PP7. 7 January 2002, PP8.
[198] Ibid, OP1.

the most secure setting, the firewall makes the use of Internet applications more of a hassle than before the firewall was installed. Free-flow of information is preserved when the firewall is tweaked to fit the patterns of an individual's usage. Analogous problems exist on a when implementing cybersecurity solutions on a larger scale. A corporate firewall may block certain applications that are useful for some users, but which present a security risk for most users. However, if one cannot afford firewalls and anti-virus software, an attacker can exploit the lack of security and likewise prevent the free flow of information, among other things. Both of these examples indicate the pitfalls of holding the private sector and individuals responsible for cybersecurity.

In resolution 56/121, "Combating the Criminal Misuse of Information Technologies," the UNGA strengthens the language of resolution 56/19.[199] It is recognized in the preliminary paragraphs of the resolution that the "misuse of information technologies may have a grave impact on all States" as a result of the utilization of ICT to enhance international cooperation and coordination.[200] Furthermore, "gaps in the access to and use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technologies."[201] The best way forward is "for cooperation between States and the private sector in combating the criminal misuse of information technologies… [and] the need for effective law enforcement."[202] Thus, in order to preserve the utility of ICT for enhancing international cooperation and coordination, all States must have access to and use ICT,

[199] United Nations, General Assembly, Resolution 56/121 (2002), preliminary paragraph 5.
[200].Ibid.
[201] Ibid., preliminary paragraph 6.
[202] Ibid., preliminary paragraphs 8, 11.

and establish P3s and law enforcement mechanisms to deter the criminal misuse of telecommunications technologies.

As the UNGA suggests in resolution 56/121, transferring information technology to developing countries and training local personnel to use it could enhance global efforts to combat misuse. It follows that if one State is unable to thwart the use of ICT by terrorists on its territory, then that state is a weak link in the chain countering the criminal misuse of cyberspace.

In 2004, the UNGA addressed cyber threats to critical information infrastructures.[203] Critical infrastructures are identified as "those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health – and the critical information infrastructures that increasingly interconnect and affect their operations."[204] In this resolution, the role of the government in dealing with the critical information infrastructure is clearer than in previous resolutions. The following are the tenets that are agreed upon by the UNGA as requirements for the protection of critical information infrastructures:[205]

- It is urged that emergency warning networks should be established to identify and warn of cyber-vulnerabilities, threats and incidents.
- General awareness should be raised in order to facilitate comprehension of the role that stakeholders play in understanding the function of critical infrastructures, as well as the role that the stakeholder has in protecting the infrastructure.
- Encourages the formation of partnerships between private and public stakeholders to better prevent, investigate and respond to threats on critical information infrastructures.
- Communications networks should be in place and regularly tested to assure their effective operation during a crisis situation.

---

[203] UNGA. "Creation of a global culture of cybersecurity and the protection of critical information infrastructures." A/RES/59/199. 30 January 2003.
[204] Ibid, PP3.
in the annex of this resolution

- Urges States to develop adequate domestic laws and policies that will allow for the investigation and prosecution of cybercrime, as well as the trained personnel that enable the investigation and prosecution of such misuses.
- Moreover, States are held responsible for identifying the perpetrators of an attack against critical information infrastructure, and sharing of this information with affected states.
- In this regard, appropriate international cooperation should take place in accord with properly crafted domestic laws to assure that critical information infrastructures are secure.

Constant testing of the protection systems and education of personnel are deemed essential for the success of such measures.

The Athens Affair and the Perils of P3 Cybersecurity: Network-Effects, Trust and Community Harm

As discussed above, the Information Society depends on the free flow of information over computer networks. The utility of computer networks rests within the concept of network-effects or network-utility. That is, the greater the size of a network, the greater the benefits of the network to its users.[206] A networked community benefits each time a new user joins that network. People tend to join networks if they can trust that they will benefit from their membership.

In *The Dark Side of Private Ordering: The Network/Community Harm of Crime,* Neal K. Katyal identifies identifies the main reason that current cybersecurity strategies are taking the wrong approach in addressing cyber injustice. This, he argues, is due in part to the focus of criminal justice on the individual impact of a crime, rather than on the harm a crime inflicts upon the community at large.[207] In his view, the focus on the harm

[206] Ibid.

done to the community rather than the crime's individual impact is especially important in cyberspace some each instance of a cybercrime, no matter how trivial it is, leads to the eroding of a user's trust in a network users to not trust the network.[208] With each intrusion, mistrust increases, and the number of users using the intruded network decreases. As a result, the utility of that network to the remaining users decreases.[209]

Katyal argues against the common global perception dominating cybersecurity dialogue that "the strong arm of law enforcement has no business when the only harm to a victim is remote and intangible."[210] This view is fallacious, since it focuses only on the individual harmed rather than the harm done to the computer-network. Katyal argues that even breaches of computer networks motivated by curiosity seriously damage a community's trust in the network, thereby decreasing the principle of network-effect. It follows that justice in the Information Society can be achieved only if the injustice to the community is considered in addition to the injustice to the individual. In order for the Information Society to reach its full potential, all cybercriminals should be tracked and punished to the fullest extent possible under the law, so as to prevent the loss of trust and increase network usage.

Even if laws exist, this does not mean that the crime will be prevented, since law enforcement authorities must have the capabilities and procedures to prevent, investigate and prosecute cybercrime.[211] Contrary to the views of the UNGA, WSIS, IGF and NSSC, Katyal argues that is the responsibility of law enforcement organizations, and not private

---

[207] Neal K. Katyal, "The Dark Side of Private Ordering: The Network/Community Harm of Crime" in *The Law and Economics of Cyberspace* Mark Grady and Francesco Parisi (eds.) (Cambridge, Enlgland: CUP, 2006, 193-217).
[208] Ibid, 197.
[209] Ibid.
[210] Ibid 196.
[211] Ibid., 194.

individuals or corporations, to enforce cyber-law and prosecute all infringements. Private ordering efforts, such as proprietary anti-virus or firewall software, will not prevent computer crime simply because this software or hardware is purchased and installed by a user, and the interests of private industry is to:

> Promote sales of anti-virus software, intrusion systems and the like. Yet, the ability to afford and the knowledge to use such technologies will not be distributed equally. Those with fewer resources will not be able to adopt them in the same way that richer individuals and institutions can. Further, because these technologies are often complicated, there will be some who have the resources to purchase them but lack the skills necessary to use them effectively.[212]

Thus, since not all computer users will be able to afford or know how to use protection software, their computers will be prey to attackers. This gap will result in those without protective measures to use the network less because they lack the trust in the network to allow for more migration of human activity into cyberspace.[213] These constraints indicate that private efforts cannot protect every user. Hence, governments must steer clear from the current approach and bear greater responsibility for network protection in order to assure that the Information Society is a secure environment in which information flows freely.

A further consequence of private industry being given the responsibility of securing cyberspace is that in their effort to assure they meet benchmarks set by the government, connectivity to their networks may be diminished.[214] Put otherwise, if ISPs are burdened with the responsibility of assuring that their services are not being used for

---

[212] Katyal, 199.
[213] Ibid, 194.
[214] Ibid, 214

criminal acts, then they might react to any suspicious activity (no matter how minor) by purging users for such actions. This also harms open networks overall.

One could argue that Katyal is being overly pessimistic in his view that the private ordering of cybersecurity harms the network and prevents the equal distribution of justice. An examination of the so-called "Athens Affair" is indicative of the consequences of relying on the private sector to provide security in cyberspace and follow the best practices and standards set by the international community for the Information Society.

The Case of Cyberespionage in Greece

The "Athens Affair," is, to date, the most successful and sophisticated recorded intrusion of a digital network. An examination of this case reveals an elaborate account of cyberespionage, where hackers stealthily accessed the legal interception function programmed into Vodafone's cellular network, using it to capture the voice-data streams of three hundred Greek officials, including the Prime Minister, and transmitting conversations back to the perpetrators.[215] It is a telling example of how a small group of skilled individuals can breach network security with impunity as a result of private-sector negligence in its provisioning of cybersecurity. As a result of the criminally negligent handling of the case by Vodafone, the perpetrators of this attack remain at large.

Anatomy of the Attack

Since the perpetrators exploited the lawful interception (LI) software installed on Vodafone's network, it is necessary to briefly outline how LI works. LI allows law

[215] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair: How Some Extremely Smart Hackers Pulled off the Most Audacious Cell-Network Break-In Ever" in *IEEE Spectrum* (July 2007) 25-33.

enforcement and intelligence authorities to eavesdrop on suspected criminals and terrorists' cell phone conversations after a court issues a warrant authorizing the remote interception of a suspect's communications devices remotely from a central office.[216] The LI consists of two components: the Remote-control Equipment Subsystem (RES) and the Interception Management System (IMS), both provided to Vodafone by Ericsson. The RES is installed on the exchange of a cellular network, and gives law enforcement officials the capability to remotely tap into a target phone by monitoring the voice-data streams of phones listed in the RES. During a LI, a copy of the monitored voice-data stream is made. This second voice data-stream is relayed back to law enforcement officials.[217] The IMS is software which provides law enforcement with an operator interface through which they initiate and manage the LI.[218] If a tap is initiated in the RES, and there is no corresponding request for a tap in the IMS, it is indicative of the possibility that an unauthorized tap is taking place. In the Greek case, Vodafone technicians had implemented the RES on the cellular exchanges via a software upgrade. Although the RES computer-code existed on the servers, it remained inactive and lacked the IMS option; thereby giving the perpetrators an opportunity to initiate their historic attack.[219] Their attack was successful since the attackers had:

[216] Prevelakis and Spinellis, 29. The Greek procedures for issuing such warrants are nearly identical to American and European standards. Therefore, they do not require further elaboration.
[217] Ibid.
[218] Ibid.
[219] Ibid.

- An esoteric knowledge of the LI method outlined above and Ericsson's special-purpose AXE telephone switch system (which is programmed in the secret FLEX computer language.)[220]
- The ability to use this knowledge to gain access to the cellular telephone switch and create a root super-user account, [221]
- A detailed knowledge of the Vodafone network demonstrated in their abilities to handle network-security alarms and place the illegal software on specific switches providing cellular coverage to Attica, the Cycladic and Dodecanese island groups, the Peloponnesian peninsula, etc.[222]

The perpetrators commenced their attack in June 2004 when the first five of fourteen shadow-phones (serving as the equivalent of the RES and IMS for the hackers) were activated. On August 9, 2004, the other nine phones were activated, and the next day the installation of a rootkit occurred on four of Vodafone's switches.[223] According to an investigatory report of the Authority for the Assurance of Communications Security and Privacy (ADAE), there were eighty-two phones subscribed on four different cellular networks that were known to have communicated with the shadow-handsets, thirty-three Vodafone employees that had access to compromised switches, and two Vodafone and Ericsson employees that accessed one of the tapped switches without permission in February 2005.[224] Furthermore, ADAE findings indicated that the shadow-phones were "calibrated via messages and calls from the United States, United Kingdom, Sweden, Australia, India and satellite phones subscribed to the Inmarsat network."[225] The presence of the rootkit allowing for the illegal interception of communications remained undetected until it gave a faint sign of its existence on January 24, 2005. On that day that,

---

[220] Ibid, 31.
[221] Unknown Author. "Τα Μυστήρια της Παιανιίας, ο Eric ο Listener και η Ericsson" (Paianias' Mysteries, Eric, the Listener and Ericsson) in *Kathimerini* (30 June 2006).
[222] Unknown Author, "Η «Εισβολή» της 10ης Αυγούστου του 2004" (The "Invasion" of the 10th of August 2004.) In *Kathimerini* (30 June 2006).
[223] A switch is "a computer controlled component of a phone network that connects two telephone lines to complete a telephone call" (Prevelakis and Spinellis, 27)
[224] Report as cited in Bouyatsou.
[225] Bouyatsou. Translation is mine.

Vodafone technicians were alerted by Q-Telecom of the delivery failure of several text messages resulting from errors at Vodafone switches.[226] We now know that the perpetrators of the attack had attempted to update their rootkit, resulting in a glitch in Vodafone's software and causing the failure of text message delivery.[227] To diagnose these errors, Vodafone called in Ericsson technicians who discovered the existence of the rootkit utilizing the LI functions of that switch and another four switches. Vodafone was not alerted to the actual existence of the rootkits, including two in switches at Vodafone's central offices, until March 4, 2005, when Vodafone technicians located the stealth software.

The response of Vodafone's leadership to its technicians' discovery demonstrates the pitfalls in having privately ordered cybersecurity. The existence of the rootkit was revealed to Vodafone-Hellas' CEO, George Koronias March 7, 2005. After consulting with Vodafone's legal department and London headquarters, Koronias ordered its removal on March 8, 2005.[228] Furthermore, between March 5-8, 2005 Ericsson and Vodafone technicians in Stockholm and London were monitoring the rootkit's activity via the LI's remote management protocol.[229] On March 9, 2005 a Vodafone technician who had access to the compromised switches, Kostas Tsakilidis, was found dead in his apartment from an apparent suicide. The Greek government was unaware of this serious breach of national security until March 10, 2005, when it was notified via political channels. Koronias did not follow procedures to (belatedly) alert the Authority for the

---

[226] Aristeas Bouyatsou "Ακτινογραφία του Μηχανισμού Υποκλοπων" (X-Ray of the Tapping Mechanism) in *Kathimerini* (30, June 2006). Translation is mine. See also: Prevelakis and Spinellis.
[227] Prevelakis and Spinellis, 24.
[228] Aristeas Bouyatsou, «Η «Άλωση» Vodafone από το λογισμικό των Υποκλοπών" (The Fall of Vodafone from Eavesdropping Software) in *Kathimerini* 3 February 2006.
[229] Aristeas Bouyatsou, "Δεκατέσσερα Ερωτήματα που Ζητούν Απάντηση" (Fourteen Questions Without Answers) in *Kathimerini* 2 February 2006.

Assurance of Communications Security and Privacy (ADAE), which was established under Greek law to assure information security on public and private networks.[230] Moreover, Vodafone destroyed or never collected key data such as the transaction logbooks at the exchanges and sign-in books for the switch facilities. The result of Vodafone's action was the loss or destruction of data critical to identifying the perpetrators who "not only received a warning that their scheme had been discovered, but also had sufficient time to disappear."[231] Thus, at the very least, Vodafone's actions are indicative of the criminal act of breach of duty on the part of its leadership.

While Vassilis Prevelakis and Diomidis Spinellis focus on the technical aspects of the hacking of Vodafone's cellular telephone network, their account does not examine the policies of the Hellenic government, and how Vodafone neglected to follow the P3 existing in Greece on the basis of the regulatory framework created to ensure the confidentiality of private information.[232] This is precisely what makes the Athens Affair a stark warning against giving the private sector prime responsibility for cybersecurity.

Since November 7, 2003, Greece has updated its regulatory framework for the security of private information and communications.[233] What the Greek government can be faulted with is failure to properly equip and staff the ADAE, something which did not

---

[230] Hellenic Government. Law No. 3115 "Σύσταση Αρχής Διασφάλισης του Απορρήτου των Επικκοινονίων" (Recommendation of the Committee on the Security and Confidentiality of Communications) 27 February 2003. See also, Hellenic Government, Regulations for the Internal Management of the Authority for the Assurance of Communications Security and Privacy (7 November 2003).

[231] Prevelakis and Spinellis, 33.

[232] They do note Vodafone's bad practices, however, not in the context of the legal code at the time. This is understandable since their paper's aim is to notify readers of the technicalities of the breach, and the general bungling of the cybercrime investigation.

[233] Hellenic Government. Law No. 3115 "Σύσταση Αρχής Διασφάλισης του Απορρήτου των Επικκοινονίων" (Recommendation of the Committee on the Security and Confidentiality of Communications) 27 February 2003. See also, Hellenic Government, Regulations for the Internal Management of the Authority for the Assurance of Communications Security and Privacy (7 November 2003).

begin in earnest until the New Democracy party came to power in March 2004.[234] This does not absolve Vodafone from its responsibility under Greek law 3115/2003 to notify ADAE from the moment it discovered the breach in its security, nor to abide by its own company policy in assuring all necessary information was collected and stored in order to aid the ADAE investigation. What was expected of Vodafone was for it to follow best practices in keeping with ISO and ITU standards.

Greek Law 3115/2003 is based on the international regulatory standards BS 779-2:2002, ISO/IEC 17799:2000 and ITU-T X.1051.[235] It establishes the ADAE as an independent autonomous administrative authority "with the aim to protect the confidentiality of communications, and in this regard, to confirm compliance with the appropriate terms and procedures…"[236] To fulfill its mission, the Authority is invested with the power to "conduct regular or emergency audits, under its own initiative or by court order of facilities, technical equipment, archives and documentation…including those of private corporations which provide postal or telecommunications services, and other services responsible for communications."[237] ADAE therefore was established as a regulatory authority with investigatory powers for government and private sector services. During investigations, committees may be formed in which people who are not members of the ADAE may participate.[238] Further, Law 3115/2003 lays out the minimal

---

[234] Under leadership of the socialist party PASOK, the ADAE had a total of five personnel which convened meetings at the ADAE president's home until the conservative New Democracy government gained power in March 2004. See: Sotiris Hadjiyakis, Ομιλία του Υπουργού Δικαιοσύνης στη Βουλή για τις Τηλεφωνικές Υποκλοπές (Statement of the Minister of Justice on the Eavesdropping of Cellular Phones). 3 March 2008.

[235] Georgia Bafoutsou, Nikolaos Antoniadis, Eugenia Nikolouzou, Athanassios Panagopoulos, *Regulatory Framework for Communications Security and Privacy in Greece* Presentation at the ETSI Security Workshop: Future Security (16-17 January 2007, Sophia-Antipolis, France), 4.

[236] Law 3115/2003, Articles 1.1 & 1.2. Translation is mine.

[237] Ibid. Article 6.1.a. Translation is mine.

[238] Ibid. Article 6.3.

punishment for compromising the confidentiality of communications or procedures for assuring the confidentiality with fines ranging from €15,000- €60,000 and a minimum prison sentence of one year, unless further punishment is required if other laws were broken, or if the indicted person is a member of the organization or service provider.[239] Notably, in the Vodafone case substantial multi-million Euro fines were given to both Vodafone and Ericsson, however, no one was imprisoned, and the fines each company received amounted to no more than a slap on the wrist.

In accordance with its mission and responsibilities under Greek Law 3115/2003, ADAE developed regulations for the protection of confidential information. These regulations are firmly within the P3 trend, with the brunt of cybersecurity responsibility being given to the private sector. Pertinent to the Athens Affair is ADAE's *Regulation for the Security of Confidential Information on Cellular Telecommunications Networks*.[240] Under these regulations, the cellular service provider is deemed responsible for developing its own security policy under the guidelines set by ADAE (which are concordant with the relevant international standards), and must inform ADAE what these policies are.[241] Specifically, ADAE calls for service providers to inform its users, through specific procedures established as part of the company policy, of any emergency threats to the confidentiality of information on the provider's network.[242] Further, records of all security incidents must be kept, and safeguards aiming to prevent insider security threats must be part of company policy.[243] Vodafone had all of these policies in place, but those

---

[239] Ibid. Article 10.1-10.2.
"Κανονισμός Για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπερεσιών" in *Εφημερίς της Κυβερνυσεώς* (No. 629a, 26 January 2005) 1013-1020.
[241] Ibid. Article 4.1α-ζ.
[242] Ibid. Article 5.3.
[243] Ibid. Article 12.3

conducting the internal corporate investigation of the network intrusion chose to disregard the law, international standards and best practices, in addition to ignoring company policy by deleting log files in which traffic data was stored.[244]

A consequence of this event for Vodafone, beyond the harm to its network from the rootkit, was the reduced network-effect. This is best encapsulated in the words of M.P. Miltiadis Evert, who, in a letter to Vodafone that he made public, wrote "…I am a subscriber to your services with telephone number 6944337552. As a result of all the revelations related to the eavesdropping of your company's services, I am requesting the immediate termination of my phone service since I can no longer trust your company with assuring the confidentiality of my conversations."[245] This confirms Katyal's argument that the private ordering of security decreases trust thereby causing people to leave a network.

The Athens Affair demonstrates the perils in entrusting service providers with the responsibility of securing cyberspace. Adequate framework of enforceable domestic and international laws drafted to protect information systems and deter malicious actors are necessary for the GCC to exist. Only national governments and regional and international organizations have the resources to coordinate and manage the security of complex critical information infrastructures. [246]

---

[244] Prevelakis and Spinellis, 35.
[245] Miltiadis Evert, "Εβερτ: 'Δεν Μπορώ να έχω εμπιστοσύνη στη Vodafone'" (Evert: "I Cannot Trust Vodafone at All.") In Kathimerini (02 February 2006). Translation is mine.
[246] Bill Hancock, "How to Stop Talking About – and Start Fixing – Cyber Security Problems. In *Cutter IT Journal* (May 2006) 6-11, 10.

Chapter Five
Al-Qaida and the Taliban's Misuse of Cyberspace to Circumvent U.N. Counterterrorist Sanctions

INTRODUCTION

On the basis of a review of relevant U.N. Security Council resolutions pertaining to counterterrorism, I will argue that the misuse of elements of cyberspace, including the Internet, by terrorists nullifies the international community's efforts to counter the terrorist threat.

United Nations Security Council Responses to Terrorism

Sanctions Targeting Al-Qaida and the Taliban: UNSC Resolution 1267

The U.N. Security Council has addressed the issue of terrorism and set a precedent of targeting State sponsors of terrorism with sanctions in the past.[247] Today, the Council has focused its counterterrorist options on imposing sanctions on individuals and their State sponsors, and assisting in the investigation and prosecution of those responsible for certain terrorist attacks. It has also directed all States to harmonize their domestic laws relevant to counterterrorism. This represents a shift in the Council's strategy from solely targeting State sponsors of terrorism to globalizing, militarizing and setting a precedent for investigating and prosecuting transnational terrorism.

This section will demonstrate that while the Security Council is aware of the changing nature of terrorist threats, as well as the misuse of elements of cyberspace by

[247] See, for example, Security Council resolutions, 731 (1992), 1970 (1996).

terrorists, its commitments to addressing this issue are rhetorical. Plugging the cyber-gap in its resolutions as it has done in the past when terrorism and technology overlap should be a main priority of the UNSC. Addressing and offering solutions for problems arising from the overlap of terrorism and technology is not without precedent in Council.[248]

The Security Council is the main U.N. body responsible for determining if there exists "any threat to the peace, breach of the peace or act of aggression, and if there is such a threat, to assure that the Council carries out its duties of maintaining international peace and security."[249] Recognizing the Al-Qaida terrorist organization as constituting a threat to international peace and security, the Security Council established, pursuant to resolution 1267, the Al-Qaida/Taliban Sanctions Committee (1267 Committee) in 1999. In 2001, the Counter-Terrorist Committee (CTC) was established to monitor the implementation of the elements of resolution 1373. While the mandates of the CTC differ from that of the 1267 Committee, their missions do overlap in some areas.

1267 Committee

The 1267 Committee was established in 1999 with the adoption of Security Council resolution 1267 under Chapter VII of the U.N. Charter. Resolution 1267 sought to compel the Taliban into denying Al-Qaida use of its territory by imposing sanctions on the regime so that it would "cease the provision of and training for international terrorists and their organizations, take effective measures to ensure that the territory under its control is not used for terrorist acts against other States or their citizens, and cooperate

[248] United Nations Security Council, "Marking of Plastic or Sheet Explosives for the Purpose of Detection," Resolution 635 (1989).
[249] United Nations, *Charter of the United Nations*, VII.39.

with efforts to bring indicted terrorists to justice."[250] Sanctions included travel restrictions, the freezing of funds and other financial resources, and called on other States to cooperate with these efforts.[251]

In December 2000, the Security Council adopted resolution 1333. This resolution modified the 1267 mandate by requesting it to "establish and maintain updated lists based on information provided by States, regional, and international organizations" of aircraft belonging to the Taliban, and another list "of individuals and entities designated as being associated with Usama bin Laden, including those in the Al-Qaida organization.[252] These lists are known today as the Consolidated List.[253] The contents of these lists were intended to assist other U.N. member states in identifying members of and financial resources associated with Al-Qaida in their territories.

With the adoption of resolution 1390, the Security Council decided that *all* States should:

> "freeze without delay the funds and other financial assets or economic resources…prevent the entry into or the transit through their territories…prevent the direct or indirect supply, sale and transfer…of arms and related materiel of all types including weapons and ammunitions, military vehicles and equipment, paramilitary equipment, and spare parts for the aforementioned and technical advice…to any member of the Taliban and the Al-Qaida organization, and any individuals, groups, undertakings and entities…who have participated in the financing, planning, facilitating and preparation or perpetration of terrorist acts or in supporting terrorist acts."[254]

---

[250] U.N. Security Council, *Resolution 1267*, OP1.
[251] Ibid., OP 4a-b, 5, 6a-e, 7, 8.
[252] U.N. Security Council, *Resolution 1333,* OP 8c, 16a-b.
[253] U.N. Security Council 1267 Sanctions Committee, *The Consolidated List established and maintained by the 1267 Committee with respect to Al-Qaida, Usama Bin Laden, and the Taliban and other individuals, groups, undertakings and entities associated with them* <http://www.un.org/sc/committees/1267/consoltablelist.shtml> Updated on 17 October 2007.
[254] U.N. Security Council, *Resolution 1390*, OP 2 a-c, 4

Resolution 1390 also required all States to submit reports to the 1267 Committee on their efforts to implement the sanctions listed above, and urged them to draft, enact and enforce domestic legislation aimed at preventing and punishing those who acted in violation of these sanctions in their territory.[255] As I will demonstrate in the next section, it is possible for individuals on the Consolidated List to evade these sanctions in cyberspace. All the information flowing into the 1267 Committee requires the assistance of a Monitoring Group. The creation of the Monitoring Group was first called on in resolution 1363, as an expansion of the original Committee of Experts.[256] Resolution 1526 requested the Secretary-General, in consultation with the 1267 Committee, to appoint members to the Monitoring Group who are experts in the fields of arms embargoes, travel bans, counterterrorism and the financing of terrorism.[257] The group prepares reports to guide the 1267 Committee in its work, and organizes visits by members of the Committee to monitor the implementation of sanctions in countries of interest.

Resolution 1617 contains elements encouraging cooperation between States and Interpol, including the use of Interpol databases of stolen and lost travel documents, in order to assist in the implementation of sanctions against Al-Qaida, the Taliban and associated individuals. This cooperation was expanded in resolution 1699 to include use of Interpol's I-24/7 global police communication system, which facilitates information exchange and communication between national police forces of Interpol member countries, thereby allowing them to better deal with the transnational nature of criminal

[255] U.N. Security Council, *Resolution 1390*, OP 6, 8.
[256] U.N. Security Council, *Resolution 1363*, OP 3a-c.
[257] U.N. Security Council, *Resolution 1526*, OP 7.

and terrorist networks.[258] Resolution 1699 also encourages Interpol to provide access to and develop better tools to help Member States implement Security Council counterterrorist resolutions.[259]

The Council's concern regarding the use of various media, including the Internet, by Al-Qaida, Usama bin Laden, the Taliban, and their associates for purposes including terrorist propaganda and inciting terrorist violence is first mentioned in resolution 1617. Resolution 1624 calls on States to "act cooperatively to prevent terrorists from exploiting sophisticated technology, communications and resources to incite support for criminal acts."[260]

The Security Council's most comprehensive effort to date in dealing with the misuse of the Internet by Al-Qaida and the Taliban is read in resolution 1735. This is not to say that the resolution focuses on the criminal and terrorist misuse of the Internet, however, its elements indicate that the Council's members are taking into account the Monitoring Group's suggestions on dealing with the terrorist misuse of cyberspace of identifying and informing the Council of the use of the Internet by Al-Qaida to circumvent sanctions.[261] While expressing its "deep concern" about the misuse of the Internet, it notes "the changing ways in which terrorist ideologies are promoted" and stresses the importance of "meeting all aspects" of the threat from Al-Qaida." The operational paragraphs of the resolution note that financial sanctions now "include but are not limited to those used for the provision of Internet hosting or related services used for

---

[258] Interpol, *Connecting Police: I-24/7* <http://www.interpol.int/Public/ICPO/FactSheets/GI03.pdf> cited on 4 October 2008.
[259] U.N. Security Council, *Resolution 1699* OP1-3.
[260] U.N. Security Council, *Resolution 1624*, pp 14.
[261] U.N. Security Council, Resolution 1267 Monitoring Group, *Fifth Report of the Monitoring Team* (20 September 2006) <http://daccessdds.un.org/doc/UNDOC/GEN/N06/529/76/PDF/N0652976.pdf?OpenElement> cited on 4 October 2008.

the support of Al-Qaida."[262] Furthermore, the Security Council encourages an increase in cooperation between the U.N. and relevant international and regional organizations "including Interpol, ICAO, IATA and WCO."[263] Notably, it does not urge for cooperation with computer emergency response teams (CERTs), ICAAN, and other important Internet bodies. This is indicative of the Council's rhetorical, rather than practical, commitment to addressing the misuse of sophisticated communications technologies. Moreover, the resolution, as understood from its second annex, does not go far enough coordinating the international community's response to the misuse of ICT by terrorists, since its focus is on preventing terrorists from misusing the Internet for their financial transactions.

While the Monitoring Group has offered several useful suggestions, most were not included in resolution 1735. Some members of the Council did not endorse the suggestions for a variety reasons.[264] It has been over a year-and-a-half since the fourth report of the monitoring team recommended measures to strengthen the 1267 sanctions regime by addressing the terrorist misuse of ICT. In that time, the Committee stalled time and time again on this issue, taking nine months for the inclusion of some of the monitoring team's proposals. Suggestions left out of resolution 1735 include the "creation of a register of entities (or use of an existing registry of entities) that create websites promoting terrorism in any form," the introduction of "know your customer" rules for hosting companies and internet service provider and having U.N. Member States oblige "hosting companies and Internet service providers under their jurisdiction to

[262] U.N. Security Council, *Resolution 1735*, OP 20.
[263] U.N. Security Council, *Resolution 1735*, OP 23.
[264] Author's observation in the Council's Informal-Informal meetings of the 1267 Committee.

provide relevant information to the national authorities charged with combating terrorism."[265]

CTC and CTED: Harmonizing States' Response to Terrorism

Resolution 1373, adopted by the Security Council two weeks after the terrorist attacks against the United States on September 11, 2001, urges States to take specific actions preventing and suppressing acts supporting terrorism. Importantly, it established the Counter Terrorism Committee CTC, pursuant to operational paragraph six, with a mandate to monitor States' progress in implementing the resolution, and reporting its findings to the Council. Resolution 1373, adopted under chapter seven of the U.N. Charter, requires States to undertake a series of actions to criminalize terrorism and prevent terrorist fundraising by freezing funds, transfers of funds and other financial assets, economic resources or related services identified as belonging to persons and entities that are in any way associated with terrorist acts. Frozen funds include those "generated from property owned or controlled directly or indirectly" by terrorists and their associates, who are also to be prevented from using a State's territory for their activities. [266] Further, States are called on to prevent the support of terrorist organizations within their boundaries by suppressing recruitment and "eliminating the supply of weapons to terrorists."[267] Information exchanges between States are encouraged to provide early warning of possible terrorist attacks. Cooperation with criminal investigations or proceedings is also encouraged in cases related to the financing or

---

[265] 1267 Monitoring Group, *Fourth Report of the Monitoring Team* (20 September 2006) <http://daccessdds.un.org/doc/UNDOC/GEN/N06/230/45/PDF/N0623045.pdf?OpenElement>, 39, cited on 4 October 2007.
[266] U.N. Security Council, *Resolution 1373*, OP 1 a-d, 2c-d
[267] Ibid., OP 2a.

support of terrorism.[268] States are to prevent terrorist movement by having effective border controls in place, and measures aimed at "preventing the counterfeiting, forgery or fraudulent use of identity papers and travel documents."[269] The exchange of operational information relevant to the possible use of forged identity papers, the movements of persons or networks associated with terrorist acts, trafficking in arms, explosives, sensitive materials, or the use of communication technology is also required under resolution 1373. States are further encouraged to cooperate with each other through bilateral and multilateral arrangements and to implement and attend international conventions relating to terrorism in order to increase international cooperation.[270] The Council also links international terrorism and transnational organized crime, illicit drugs, money laundering, illegal arms trafficking and the proliferation of weapons of mass destruction, and the strengthening of the global response to terrorism by coordinating State actions directed against terrorism at the national, sub-regional, regional and international levels.[271] While the CTC made an effort to monitor and assist States in implementing resolution 1373, a need to revitalize the resolution was recognized. The Counter-Terrorism Executive Directorate (CTED) was established pursuant to 1535.[272] CTC/CTED and the 1267 Sanctions Committee have a close working relationship.

One might argue that all of the above resolutions can be interpreted as implicitly applying to the misuse of cyberspace by terrorists. However, implicit rhetoric does not contribute to raising international awareness and coordinating the fight against terrorists in cyberspace. This cooperation is of utmost importance, as demonstrated by the findings

[268] U.N. Security Council, *Resolution 1373*, OP 2f.
[269] Ibid., OP g.
[270] Ibid., OP 3c-e.
[271] Ibid. OP 4.
[272] U.N. Security Council, *Resolution* 1535.

of the International Independent Investigation Commission (IIIC) mandated by the Council to offer its technical assistance to the investigation of the assassination of Rafik Hariri and others in Lebanon.[273] The IIIC investigation "has researched over 200 gigabytes of electronic data…analyzed a number of mobile telephones and the records contained therein and examined large volumes of communications traffic."[274] Challenges to the investigation include encrypted electronic data and the synthesis of all the electronic data collected. Since the IIIC has experience in collecting electronic evidence with the intention of prosecuting those responsible for terrorist attacks in a hybrid international criminal court, the UNSC should consider examining the IIIC investigation of electronic evidence as a model for gathering digital evidence.

Misusing Cyberspace in Practice to Get Past U.N. Counterterrorist Sanctions

In its reports, the Monitoring Group of the 1267 Sanctions Committee identified the fight against Internet terrorism as a primary issue for the Security Council, since it

> "offers Al-Qaida and its associates instant communication with little or no regulation or traceability; it allows the Al-Qaida message to reach all parts of the globe, regardless of its existing influence; provides Al-Qaida operatives with anonymity; offers the opportunity for Al-Qaida to abuse sophisticated, multi-media messaging to glorify terrorist acts; enables Al-Qaida to influence traditional mass media through its websites; serves as a medium for the conduct of misleading theological debate; helps link local terrorist cells into a global Al-Qaida campaign; allows small but effective Al-Qaida groups to gain wide influence; and helps

[273] U.N. Security Council resolutions: 1595, 1636, 1644, 1664.
[274] Independent International Investigation Commission, *Sixth Report of the International Independent Investigation Commission* <http://daccessdds.un.org/doc/UNDOC/GEN/N06/654/33/PDF/N0665433.pdf?OpenElement>, 18. cited on 4 October 2007.

> isolate potential recruits from the counter-balancing influences of family and friends."[275]

While a paper of this length cannot comprehensively address all these possible methods of misusing cyberspace, a mention of some techniques is useful to highlight the fact that, with minimal effort, those on the 1267 Consolidated List can circumvent sanctions and other actions taken by the Council to combat terrorism.

Cyberplanning

Terrorists use cyberspace as a tool to plan their operations. Known as "cyberplanning," this activity is defined as "the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed."[276]

An outline of how cyberplanning occurs is useful. Members of a terrorist cell can communicate via email, instant messenger software, or Internet phone services with others in their network, regardless of their location.[277] Furthermore, terrorists can set up websites that have content aimed at a specific target population that serves "as a recruiter of talent for a terrorist cause."[278]

Voice over Internet Protocol (VOIP) is one technology used by terrorists to communicate security. It poses challenges to law enforcement and intelligence efforts. VoIP is a technology used to make telephone calls from computer to computer using a

---

[275] 1267 Monitoring Group, *Fourth Report of the Monitoring Team* (20 September 2006) <http://daccessdds.un.org/doc/UNDOC/GEN/N06/230/45/PDF/N0623045.pdf?OpenElement>, 39, cited on 4 October 2007.
[276] Timothy L. Thomas. "Al Qaida and the Internet: The Danger of 'Cyberplanning.' In *Parameters* (*Spring 2003, XXXIII, No. 1).* US Army War College, Carlisle, PA, 112-123, 113.
[277] Ibid., 115.
[278] Ibid., 118.

VoIP application, or to a traditional phone line.[279] Although counterterrorism investigators can conduct surveillance on calls that are placed from VoIP services to traditional phone services by monitoring a suspected telephone line, a computer-to-computer VoIP communication can be encrypted using features embedded in VoIP software such as Skype, AOL Instant Messenger, or Microsoft's Instant Messenger. Thus, if law enforcement personnel intercept the data stream containing voice data packets, they will not be able to instantly listen in on such encrypted conversations. Hence, VoIP gives terrorists the secure communications capabilities that can thwart sophisticated law enforcement efforts.

While domestic laws, such as the United State's Communications Assistance for Law Enforcement Act (CALEA), require U.S. companies to allow for legal interception of suspects information it is not binding across borders. The global nature of the Internet and the fact that many VoIP companies are not located in the U.S, makes international cooperation a necessity. For example, Skype, a German VOIP company, does not have to act in accord with CALEA and is not required to provide mechanisms that allow the FBI or other law enforcement agencies to eavesdrop on VoIP communications.

It is often assumed that the only way one can use VoIP technology is by subscribing to a commercial carrier that offers VoIP services. This view ignores the emergence of illegal Internet networks. The abundance of illegal Internet service providers in the developing world presents an opportunity for terrorists to bypass government monitoring. Joshua Gordon argues this point in his paper, *Illegal Internet*

279 Federal Communications Commission, *Voice Over Internet Protocol: Frequently Asked Questions*, <http://www.fcc.gov/voip/> (Cited on 27 April 2007).

Networks in the Developing World.[280] Illegal Internet access is provided by unlicensed operators of international telecommunications networks. Since these networks are clandestine due to their illegal nature, the exact number of these networks is unknown. These networks are established when operators illegally obtain bandwidth by tapping into commercial satellite networks such as StarBand. On this stolen bandwidth, they set up illegal ISPs and sell Internet access to others. However, another use of these networks is for VoIP communication.[281] This "compromises the ability of local or international telecom authorities to monitor voice conversations."[282]

To illustrate the importance of bridging the digital divide to enhance cyber-security, it is useful to briefly examine illegal Internet service providers in Africa. Such networks present opportunities for criminal and terrorist organizations to bypass law enforcement efforts.[283] Illegal Internet services are established when network operators obtain bandwidth needed to create an Internet Service Provider (ISP) without abiding by national regulations or paying for access to Internet backbone services. This is possible after bandwidth is diverted by the operators of an illicit ISP from a commercial Internet backbone network to the illicit network. The illicit ISP is then in a position to sell Internet access to interested parties at a significantly reduced cost compared to licit ISP. The low cost is a result of the illegal ISP not paying the necessary access and regulatory fees, which are typically high in less developed countries since there is high demand and low supply of available bandwidth.[284] Another factor in the high cost of legal ISPs is the fact

---

[280] Joshua Gordon. *Illegal Internet Networks in the Developing World*. (The Berkman Center for Internet and Society at Harvard Law School: Research Publication No.2004-03 2/2004).
[281] Ibid., 5.
[282] Ibid., 8.
[283] Ibid.. *Illegal Internet Networks in the Developing World*. (The Berkman Center for Internet and Society at Harvard Law School: Research Publication No.2004-03 2/2004).

that telecommunications monopolies are typical in these regions. Thus, illegal ISPs have great appeal, since they offer the same service as legal ISPs for a fraction of the cost.[285]

Some have suggested that illegal ISPs are a good thing, since in some cases, such as South Africa, they have helped de-monopolize the Internet industry by competing directly with the legal telecommunications provider.[286] However, law enforcement issues arise when illegal ISP service is combined with VoIP. When this occurs, the result is the negation of legal communication interceptions methods used by law enforcement.[287] Thus, bridging the technological gaps in developing countries is a crucial element in assuring that the P^3 and law enforcement efforts outlined by the UNGA's global cybersecurity strategy are not undermined.

Anonymity

The Internet, World Wide Web, intranets and other computer networks rely on a suite of military grade protocols called Transmission Control Protocol and Internet Protocols (commonly referred to as TCP/IP). These protocols are used to transmit packets of data over networks in a standardized format. The IP protocol header contains essential information identifying the source and destination of a data-packet. Machines require these strings of numbers to deliver data-packets requested across the Internet to the correct machine. All internetworked machines must have valid IP headers to communicate.

---

[284] Ibid.
[285] Ibid.
[286] Personal communication with Daniel Aghion during the United Nations Institute of Training and Research, Web Seminar Series on ICT Policy Issues for Development, *Broadband Wireless to Bridge the Digital Divide* (New York, New York: United Nations Headquarters, 17 May 2006).
[287] Ibid., 5.

One might argue that intelligence and law enforcement agencies have resources that can locate a terrorist through his or her IP address, thereby negating the usefulness of ICT to terrorists. Law enforcement can trace the origin of terrorist communications if they are sent without any attempts to conceal the identity of the sender. The assumption in this paper is that all terrorists have undergone training that emphasized the importance of maintaining anonymity both online and offline. Thus, although the technology exists to track the movements of suspected terrorists online, a terrorist can bypass law enforcement efforts by establishing an anonymous presence in cyberspace.

Using spoofing techniques, a terrorist can manipulate the IP protocol in a way that can conceals his or her true location. Anonymity can be achieved through the proper use of technology. One such technology is known as "the Onion Router" (TOR), which was first developed by the U.S. Naval Research Laboratory to protect data packets on open networks. TOR is a distributed anonymous network of proxy servers connected by virtual encrypted tunnels. A computer linked to a TOR network transmits data through a series of proxy servers which strip the IP identification information, replace it with new IP information, and send it off to another proxy server before connecting to the final server. The ultimate outcome is that if someone is observing the network traffic on any of the proxy servers, the observer will not be able to discern the true location of point A, nor will the observer be able to tell what the destination of the data is unless he or she is observing the final transmission point. An observer at point B will not know where the data is really coming from, as he will only be able to detect the location of the proxy server from the point in which the data arrived at point B. In this manner, a network address is masked.

It has been suggested that in experimental small network tests, TOR is vulnerable to traffic-analysis attacks. However, this research was not done on large-scale open networks such as the Internet. Webprinting is another method that can be used to trace the authors of online content.[288] A webprint is the use of sophisticated artificial intelligence programs, databases, and mathematical algorithms to identify anonymous authors through patterns in his or her writings. This useful technique should be made available to the 1267 Sanctions Committee to assist in the identification of possible pseudonyms of individuals on the 1267 Consolidated List. These pseudonyms should then be registered on the Consolidated List.

Radicalization, Recruitment and Incitement

It has been suggested that the Internet serves as an incubator for radicalizing otherwise ordinary Muslims residing in the West.[289] The NYPD has identified four phases of radicalization in which there is a direct correlation with an individual's Internet activity. These are the pre-radicalization, self-identification, indoctrination and jihadization phases. In the pre-radicalization phase, the user has no motivation to conduct acts of terrorism. During the self-identification phase, a person seeking information about Islam on the Internet is exposed to the numerous sites promoting extremist ideologies that misrepresent Islamic theology. Indoctrination occurs when the individual begins to devote time to exploring terrorist websites, and forming online relationships with individuals who promote extreme ideologies. This leads to the jihadization phase, in

[288] Jiexun Li, Rong Zheng and Hsinchun Chen, "From Fingerprint to Wireprint," in *Communications of the ACM* (April 2006 Vol 49. No. 4).
[289] Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat* (New York Police Department, New York, 2007)
< http://home2.nyc.gov/html/nypd/html/nypd/pdf/dcpi/NYPD_Report-Radicalization_in_the_West.pdf> cited on 17 August 2007.

which the online relationship between individuals serves to incite terrorist actions by encouraging violent action, and providing the technical material required for this action. Thus, despite the sanctions targeting terrorist networks, the Internet can be used to recruit and incite people residing in the West to commit terrorist acts.

Funding

One way that is used by terrorists bypass to sanctions is to gain a new identity. Those wishing to buy a new identity can use the Internet to connect to sites that allow one to illegally obtain personal information to commit credit card fraud and identity theft. However, the assumption is that the VNSA in question already has access to some monetary assets that can then be used to buy the new identity. Further, law enforcement efforts are succeeding in shutting down such sites, but their existence is indicative of the opportunities available to terrorists on the Internet. Thus, allowing terrorists access to the Internet negates law enforcement efforts, since it possibly allows a terrorist to function properly in the real world by gaining a new identity.

Assume that terrorist A is an individual listed on the 1267's Consolidated List, and cannot gain access to his bank account. Furthermore, consider that the charities which used to contribute to terrorist financing have been shut down by the government, and all other government efforts to assure that no money gets into the terrorists hands have succeeded. The terrorist cannot rely on his old financial network, and is forced to gain a new identity by diving into a dumpster, finding credit card and bank account information belonging to individuals he has never met, and establishing a new financial identities based on these. The first might be an operational identity that it is not used for quick money making, but rather for monetary storage. The second is used to gain the

initial funds for an operation by making a quick heap of money, but also alerting the individual whose identity is stolen to whom the identity belongs to that his accounts have been compromised. After gaining the initial funds through the second identity, the cash is withdrawn, and for operational security the terrorist goes to a new geographic area (within the State which he wishes to conduct his operation), and opens up a bank account using the operational identity to store the cash. The question arises, how can a terrorist raise cash if he is isolated from his or her organizations fund raising apparatus? The answer: click-fraud.

Google AdSense is a program that allows a publisher of a website to monetize the site by displaying advertisements provided by Google on the website. Every time someone clicks on an advertisement, money is posted to the publishers AdSense account. At the end of the month, if a publisher has earned over $100.00 USD, he is then eligible to receive payment in the form of a check or electronic money transfer straight into the publishers account within thirty days. It is conceivable that a terrorist can exploit this program in order to raise funds. It is further conceivable that a terrorist organization can set up a series of websites that feature Google AdSense ads, which will provide them with an elaborate network of people who click on the ads.

Online digital payment services, such as Pay Pal, have existed for some time.[290] Such services allow one to send, receive and withdraw funds after providing some personal information to the company so that he or she can withdraw funds to a local bank account, or request a check. Non-anonymous online digital payment services, such as Pay Pal, can conceivably be misused by terrorists on the Consolidated List to transfer funds by using middlemen who are not on the Consolidated List to facilitate the transaction.

[290] See: http://www.paypal.com

However, it has been suggested that non-U.S.-based digital payment services, such as Web Money or E-Gold,[291] assure greater anonymity than Pay Pal and present greater challenges to law enforcement and intelligence professionals seeking to proactively track illicit digital fund transfers in real time, since terrorists can exploit the anonymity of the Internet to disguise their illicit financial transaction.[292]

The focus on terrorist misuse of cyberspace has highlighted the use of the Internet and WWW to facilitate terrorist networking and communications, fundraising, incitement and radicalizations. In this way, terrorists elude relevant international sanctions. The Internet and other elements of cyberspace are utilized by terrorists to conduct their attacks. While the UNSC places sanctions and compels the international community to fight terrorism at home, terrorists bypass these precautions by migrating their actions into cyberspace. Would it be appropriate to replace this sentence with: Terrorists skillfully take advantage of the fact that information security is universally weak, and have myriad opportunities to conduct network attacks undetected. However, many State arsenals include cyberweapons of mass destruction, such as the electromagnetic bomb (e-bomb) and microwave, x-ray laser and other electromagnetic beam weapons.[293] The Council's program of work should include such issues as the militarization of cyberspace and terrorist misuse of ICT and cyberspace. In this way, it will address the militarization of

---

[291] See: http://www.wmtransfer.com *and* http://www.e-gold.com

[292] Thomas Winston, "Intelligence Challenges in Tracking Terrorist Internet Fund Transfer Activities." In *International Journal of Intelligence and Counterintelligence* (20:2, 2007) 327-343, 330.

[293] Carlo Kopp, "The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction," (1996) available at: *http://www.qsl.net/n9zia/pdf/apjemp.pdf* .
Also see: Jeff Hecht, "Beam Weapons and Strategic Arms Control" in *Beam Weapons: The Next Arms Race*, (New York, New York: Plenum Press 1984, 325-334).

cyberspace in a more comprehensive manner and help guide the global culture of cybersecurity.

PART TWO | NEGOTIATING GLOBAL CYBERSECURITY

Chapter Six
Information Society Stakeholders

As the global community identifies areas of common concern, new rules of conduct and practices are established in order to address the problem through cooperation, given the absence of a global sovereign entity.[294] The aim of this project is to document and analyze the evolution and structure of current international cybersecurity cooperation efforts. It is beyond the scope of this dissertation to test theories of institutional design within the context of global cyberspace governance and reflect on the best way for a cyberspace regime to move forward based on such theories.[295] Instead my focus remains on answering the question of why states take the positions they do in global cybersecurity negotiations. Technogeopolitics is identified as the best paradigm for this. It is a useful lens through which the global politics of securing cyberspace may be understood, and may predict how cyberspace will evolve.

Global Governance

Efforts to govern global communications include the establishment of regimes that aim to regulate the behavior of all concerned parties. Regimes governing commonages, such as the U.N. Convention on the Law of the Sea (UNCLOS), are useful in that they "lay the groundwork for transnational economic, cultural and social networks,

---

[294] Robert Jervis, "Cooperation Under the Security Dilemma" *World Politics*, 30, Issue 2 (Jan 1978) 167-214.
Kenneth A. Oye, "Explaining Cooperation Under Anarchy: Hypothesis and Strategies, *World Politics* 38, No. 1 (October 1985) 1-24.

[295] Alexander Wendt, "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organizations* Vol 46, No. 2 (Spring 1992), 391-425.
Alexander Wendt, "Driving with the Rearview Mirror: On the Rational Science of Institutional Design. *International Organization*, Vo. 55, No. 4 (Autumn 2001 (1019-1049).

thereby setting the terms of international practice."[296] In order to govern effectively, regimes must account for the multitude of actors involved in global politics. For the U.N, global governance is a "process through which conflicting or diverse interests may be accommodated and cooperative action taken," including formal institutions or regimes that have the authority to enforce compliance, or other actions agreed on by people as being in their interest.[297] As Frank Biermann suggests, these notions appear to encompass all human relations, and therefore, differ from traditional concepts of world politics. Hence, the key difference between theories of global governance and regime theory is that global governance takes into account the multitude of transnational actors affecting global political processes.[298]

Two notions of global governance dominate the field: the normative and phenomenological views.[299] Phenomenological notions of global governance either "see global governance as the combined efforts of international and transnational regimes," or they could suggest that global governance is an extension of a national government's domestic responsibilities into the international realm in order to govern transnational relations without individual sovereignty.[300] Normative notions of global governance aim to identify the causes and effects of globalization, and offer solutions to address the consequences of globalization.[301] Normative scholars argue that states are no longer the only legitimate constituents in an international society, and call for a redefinition of

---

[296] Wapner, 74.
[297] Frank Biermann, "Global Governance and the Enviroment," in *International Enviromental Politics*, Michele M. Betsil, Kathryn Hochstetler and Dimitris Sevidis (eds), (New York: Palgrave Macmillan, 2006), 237-261.
[298] Stokke, 58.
[299].Biermann, 240.
[300] Biermann suggests that narrow phenomenological definitions are problematic since they are do not clearly distinguished themselves from traditional political science fields such as international relations or world politics, and therefore might be considered redundant.(Biermann, 239).
[301] Biermann, 240.

international society that includes certain transnational actors as legitimate constituents. Their proposed solutions include creating new governance mechanisms, or reforming existing international organizations, to replace state-centric efforts to resolve issues emerging from the interdependence between states and non-state actors that is characteristic of globalization. Thus, normative theorists argue for transnational governance of global politics.

While both the phenomenological and normative definitions of global governance have their merits within certain contexts, Biermann recognizes a need for an empirical definition of global governance that restricts the term to current developments in world politics. This notion has three characteristics. The first is the assumption that the reality of global politics today is different from that of the 1950s, because states are no longer the sole actors in international relations. Multiple actors such as multi-national corporations (MNCs), non-governmental organizations (NGOs), and international governance organizations (IGOs), among other non-state actors, have been empowered by advancements in ICT. Business entities participate in global conferences representing their interests. Therefore, States are no longer the sole actors in global politics. They do have a say, since decisions made at international conferences are still based on the results of State voting. At times non-state actors will impact and contribute to international negotiations.[302] Vertical and horizontal fragments are interdependent. It is this interdependence that requires the state to give up *some* of its traditional monopoly over decision-making to institutions that conform to the new transnational reality.

---

[302] Additionally, Biermann's idea of global governance is characterized by the vertical and horizontal segmentation of rule-making and rule-implementing clusters.

[302] Vertical segments of global governance include supranational, international, national and sub-national layers of authority. These tend to be state-centric constructions. Horizontal fragmentation occurs "between different parallel rule-making systems maintained by different groups of actors" such as NGOs. Ibid.

Typically, NGOs that have taken direct actions to reform and redefine global politics have had little success.[303] They recognize that the international treaties and conventions that make up the laws that regulate State behavior, including those establishing international organizations and financial regimes, are contracts between States. However, the normative lens suggests that since global politics have changed, States and current international regimes that depend on the just leadership of national governments are not the only course of collective action.[304]

The assumptions of rationalist regime theory is that when states are the ultimate authorities in a regime, a regime is more likely to modify actors.'[305] However, this is not always the case, since transnational cooperation on the standardization of policies is not new or unique to telecommunications.[306] Global cyberspace politics is being organized through efforts to establish networks between public and private entities will regulate cyberspace based on cooperation on a P3 model. Scholars note that institutions of global governance, such as the U.N., allow for transnational actors such as international NGOS, to actively engage in international politics.[307] This is increasingly the case for negotiations related to cyberspace and the Information Society. The practice of the International Telecommunications Union (ITU) of permitting business entities and other telecommunications sector members to participate in the meetings of ITU working and

---

[303] Oran R. Young, "Global Governance: Toward a Theory of Decentralized World Order," in *Global Governance: Drawing Insights from the Environmental Experience*, Oran R. Young (ed), (MIT Press, 1997), 274-299, 294.
See also: Biermann, 242.
[304] Biermann, 240.
[305] Stokke, 43.
Stephen Haggard and Beth A. Simmons, "Theories of International Regimes" *International Organization* 41, No. 3 (Summer 1987) 491-517.
B. Peter Rosendorff and Helen V. Milner, "The Optimal Design of International Trade Institutions: Uncertainty and Escape" *International Organization*, 55, No. 4 (Autumn 2001) 829-857.
[306] R. Lipschutz, The National Origins of International Environmental Policies and Practices: My Country is in the World, in *Global Environmental Politics – Power, Perspectives, Practice* CQ Press, 177-222.
[307] Betsill, 187.

study groups gave them the power to influence regulatory regimes. This practice of including non-state actors in ITU meetings was adopted by WSIS, which expanded it beyond business entities to allow for civil society participation as well.

A review of ongoing efforts to address global cybersecurity confirms the trend of networked-minimalism.[308] That is, "a set of practices for governance that improve coordination and create safety valves for political and social pressures consistent with the maintenance of nation-states as the fundamental form of political organization"[309] Keohane and Nye identify the most efficient form of governance in a global world as "networked-minimalism." Such governance mechanisms are networked because globalism is composed of increasingly complex global networks, thereby requiring less hierarchical governance and more "extensive networked cooperation."[310] However, this networked cooperation must be *minimal,* since there is a need to preserve the autonomy of states, which is done by justifying networked action in terms of cooperative results.[311] Although this view signifies a shift from the traditional international system in which nation-states were the only actors to a global system in which nation-states cooperate with other actors, the nation-state remains, in principal, the sole legitimate source of power.

James Rosenau suggests that the mobius-web model of global governance is the trend towards which current modes of global governance, such as Keohane and Nye's networked-minimalism, are evolving.[312] Mobius-web governance is characterized as a structure of governance in which different dynamics of governance overlap in their

[308] Keohane and Nye, 204
[309] Keohane and Nye, 204.
[310] Ibid., 208.
[311] Ibid., 204.
[312] Rosenau, 396.

response to a particular issue that needs to be subjected to governance. While laws and compliance to laws are a part of mobius-webs, they are supplemented by others norms and regulations as well. International cybersecurity cooperation efforts appear to fit within this paradigm.[313] Establishing an international convention for cyberspace presents significant challenges for international cooperation, however, as it will be argued, current efforts to establish a global culture of cybersecurity appear to fit comfortably with networked-minimalist, or mobius-web, models of global governance with the state in a leading role.[314]

The establishment of the GCA's International Multilateral Partnership Against Cyber Threats (IMPACT) in March 2009 as the world's first global public-private initiative against cyber-threats demonstrates the decentralized multi-lateral framework that serve as bodies of international cybersecurity cooperation.[315] In an interview with a U.S. diplomat, this effort was not categorized as holding any legal authority from the U.S. perspective, since there is no specific agreement mandating its creation other than a

---

[313] Rosenau 398.
"Mobius-web governance is rooted in the impetus to employ rule systems that steer issues through both hierarchical and networked interactions across levels of aggregation that may encompass all the diverse collectivities and individuals who participate in the processes of governance. Hybrid structure in which the dynamics of governance are so intricate and overlapping among the several levels as to form a singular weblike process that like a mobius neither begins nor culminates at any level or at any point in time. Does not culminate with the passage of a law or compliance with its regulations. Rather, it is operative as long as the issues subjected to governance continue to be of concern."

[314] It appears to be the case that the conflict between regime theory and global governance are being bridged since regime theorists are beginning to incorporate insights from the study of domestic governance and civil society to the transnational level (Biermann, 240). Some scholars of regimes are beginning to view states not as prime movers in solving collective actions problems, but as "learners who are exploring a range of possibilities in a permissive international environment" (Stokke, 59). Regime theory is taking a more process-oriented approach in which "the origin and transformation of preferences or identities; the role of perception and how cognition is shaped by features of the situation and the behavior of others; and in the case of environmental regimes, the role of interactive generation of scientific knowledge in international management" are discussed (Stokke, 61). Thus, regime theory is in flux as it adapts to notions of global governance and a transnational worldview.

[315] Notes from authors interview with a member of the International Telecommunications Union High Level Exert Group (HLEG) of the Global Cybersecurity Agenda.

note verbale.[316] Therefore, while it is an example of an entity where mobius-networks can be formed and nurtured to deal with the terrorist misuse of cyberspace, the IMPACT is not a law enforcement or judiciary authority.

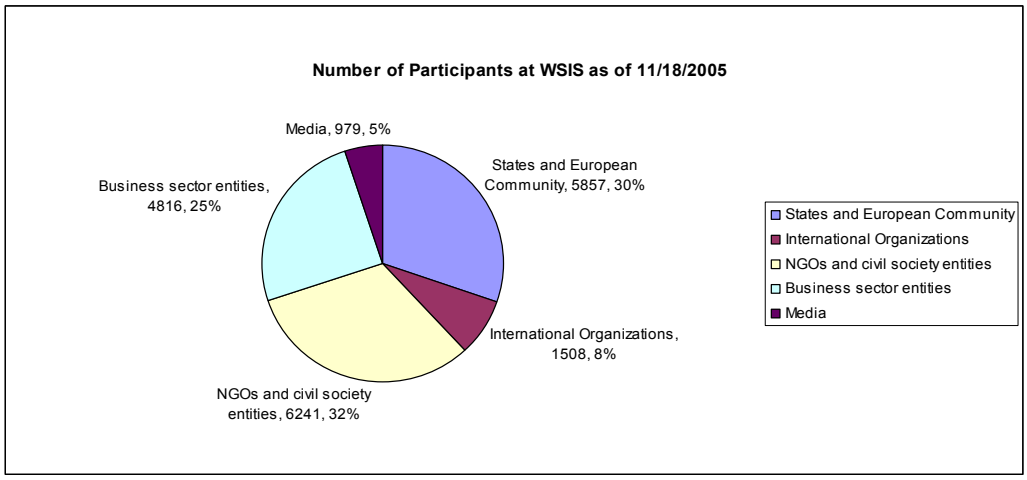
Information Society Cybersecurity Stakeholders

The Information Society is a political partnership being forged among a multitude of global actors in response to the organizational changes occurring as a result of the information revolution. As noted in relevant United Nations General Assembly Resolutions, as well as the declarations and outcomes of the World Summit for the Information Society (WSIS) and the Internet Governance Forum (IGF), this society must be regulated through international standards and norms.[317] The importance of organizing and expanding the Information Society was recognized by the United Nations General Assembly (UNGA). Prior to the World Summit for the Information Society, states were the sole actors responsible for creating and operating regimes.[318] The ITU model of resolving issues in the field of spectrum allocation and telecommunication regulation and standardization via a multi-stakeholder process was adopted by the U.N. as the framework for the WSIS. All relevant stakeholders, including business entities, other private organizations and global civil society are invited to lay the groundwork for the Information Society. In the field of telecommunications, business entities and academia

[316] Notes from authors interview with a member of the International Telecommunications Union High Level Exert Group (HLEG) of the Global Cybersecurity Agenda.
[317] This project focuses on developments in the field of security within this context.
[318] Regime analysis has a tradition of studying "global governance through statist lenses, focusing on the creation and operation of rules in international affairs. Olav Schram Stokke, "Regimes as Governance Systems," in *Global Governance: Drawing Insights from the Environmental Experience*, Oran R. Young (ed), (MIT Press, Cambridge, Massachusetts, 1997), 28-63, 28. According to most regime theories, states are "unitary, rational actors," that interact with each other while taking into account civil society. Traditional regime theory holds "that opening the black box of domestic politics in an interactive rather than an additive manner is not likely to be worth the costs involved" (Stokke, 29).

have taken part in the ITU's work in standard setting. Some non-state actors play a significant role in influencing decision-making and contribute to the development of the information society. An examination of the state system, business entities and global civil society and their interrelation is important.

As displayed in the table below, states compose thirty percent of the total participation at the WSIS. Non-state actors (not including the media and international organizations) make up fifty-seven percent of the participation at the conference.



States remain the most influential actors, as they are the entities that reserve decision making authority and voting privileges, including on issues relating to the accreditation and participation of private actors.[319] Business and civil society entities do affect state decision making to a varying degree. [320] Thus, it is important to understand the interaction between states and non-state actors in creating a global culture of cybersecurity.

Nation-States

[319] WSIS Executive Secretariat, Accreditation of NGOs, Civil Society and Business Sector Entities to the World Summit on the Information Society, (9 June 2004) <WSIS-II/PC-1/DOC/3-E>
[320] Wapner, 79-81.

The nation-state is a relatively new political organization built on centuries old foundations formalized by series of treaties comprising the Peace of Westphalia (1648).[321] This entity was initially confined to a handful of Imperial West European states.[322] The process of decolonialization, starting at the end of the eighteenth century through the nineteenth century, and concluding in the mid twentieth century, saw the territorial holdings of these trading empires replaced by the nation-states. The result was "the division of the globe's surface into mutually exclusive, geographically defined jurisdictions enclosed by discrete and meaningful borders."[323]

State sovereignty is a key principle in international relations. The assumption, in theory, is that within a state, there is no authority other than that of the legitimate government exercising internal and external sovereignty over the territory. Sovereignty gives states independent control over their policy preferences. In having autonomy, a State can expect not to have its policies constrained by outside actors.[324] The dynamics of global politics today rule out the possibility of every state having formal sovereignty and autonomy. This is in part due to the rise of international institutions, such as the U.N., which on the one hand guarantees state sovereignty, while on the other requires states to give up some of their jurisdiction to international laws, regimes and norms.[325] Thus,

---

[321] Gregory Jusdanis, *The Necessary Nation,* (Princeton, NJ: Princeton University Press, 2001).
[322] Andre Liebich, Nationalizing the Globe, Globalizing the Nation, 105.
[323] Stephen J. Kobrin, "Sovereignty @ Bay: Globalization, Multinational Enterprise and the International Political System," 184.
[324] Kobrin,185.
[325] See, for example: Judith Goldstein, Miles Kahler, Robert O. Keohane, and Anne-Marie Slaughter, "Introduction: Legalization and World Politics" *International Organization,* 54, No. 3 (Summer 2000) 385-399.
Ann-Marie Slaughter Burley, "International Law and International Relations Theory:A Dual Agenda" *The American Journal of International Law,* 87, No. 2 (April 1993) 205-239.
Kenneth W. Abbot and Duncan Snidal, "Hard and Soft Law in International Governance" *Internat*ional Organization*,* 54, No. 3. (Summer 2000) 421-456.

complexities arise in the area where the jurisdiction of the state ends and the jurisdiction of international institutions overlaps or begins. [326]

In *National Policies and Domestic Politics,* Deborah Spar argues that if trade is a political activity, then firms are political actors.[327] In this way, states can utilize firms to distribute or reward power in order to meet their own political objectives.[328] Since states and firms both cause effects on the behavior of the other, a dynamic bidirectional interaction exists between the state and the MNC. One area where this is apparent is in the formation of strategic trade policies.

Important policy tools that affect the behavior of MNCs include export controls, protectionism and strategic trade policy. Export controls tend to have a political purpose, since "they are designed to prevent rival states from gaining access to key resources and technologies," or to punish a state.[329] Firms manufacturing strategic goods rely on governments to adopt strategic trade policies that will support the firm's competitive stance in the global market.[330] States do place restrictions on what may be exported, even if it is to the detriment of a firm's competitiveness in foreign markets.[331] In the U.S., the

---

[326]The crux of the argument made by those holding the opinion that state's sovereignty is at bay is that "the multinational corporation has broken free from its home economy and has become a powerful independent force determining both international and political affairs. [While] others reject this argument that the multinational corporation remains a creature of its home economy."[326] It follows that by breaking free from its home economy, the sovereignty and autonomy of a state is compromised. Those that disagree with the above claim argue that the MNC has not become fully independent from the home country, but remains "a creature of the home country." (Gilpin 278)

[327] Deborah L. Spar, "National Policies and Domestic Politics", 207.

[328] Spar, "National Policies and Domestic Politics", 207.

[329] Spar, 209.

[330] Spar, 212.

[331] Standard export restrictions are meant to prevent access, whereas sanctions or embargoes aim to act as punitive measures. Sanctions appear to have the greatest effects on firms. For example, firms in state I which import from state A will be at a loss if state A subjects state I to a sanctions regime. However, firms that export from state A to state I will also be at a loss, since they will suffer from a decline in sales and face the possibility of ties being severed with state I in the long-term. Thus, as Spar notes, MNCs must remain aware of political developments within the countries in which they operate so as to not find

federal government lost the so-called "encryption wars" of the 1990s when private industry protested policies prohibiting the export of strong encryption software for strategic reasons.[332] In an effort to prevent criminals from communicating using unbreakable codes, some U.S. firms implement backdoors so that national security agencies can monitor criminal and terrorist communications.[333] U.S. firms such as Cisco and Microsoft, which developed and maintain core elements of cyberspace, are stigmatized by such revelations, thereby decreasing consumer trust. Thus, the close relationship between governments and firms in the area of strategic trade policy affects both how firms operate and how governments counteract the misuse of cyberspace.[334]

Elements of Multinational Corporations

Business entities, such as multinational corporations, contribute to the formation of international policies regulating international communications within the ITU. The trend of forming public-private partnerships to secure cyberspace rests on the cooperation of private companies, including MNCs, in order to strengthen the critical information

---

themselves prohibited from accessing a market due to sanctions. Export controls are one mechanism that can affect the behavior of firms and economies.

[332] Richard C. Barth and Clint N. Smith, "International Regulation of Encryption: Technology Will Drive Policy" in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, (Eds.) Brian Kahin, Charles Nesson (Cambridge, Massachusetts, MIT Press 1998, 283-299).

[333] Claude Crepeau, Alain Slakmon, "Simple backdoors for RSA key generation" (Lecture Notes in Computer Science, 2003 – Springer)
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69.1878&rep=rep1&type=pdf.
Benjamin J. Romano "Microsoft device helps police pluck evidence from cyberscene of crime"
The Seattle Times (April 29, 2008)
<http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html>

[334] The crux of the argument made by those holding the opinion that state's sovereignty is at bay is that "the multinational corporation has broken free from its home economy and has become a powerful independent force determining both international and political affairs. [While] others reject this argument that the multinational corporation remains a creature of its home economy."[334] It follows that by breaking free from its home economy, the sovereignty and autonomy of states is compromised. Those that disagree with the above claim argue that the MNC has not become fully independent from the home country, but remains "a creature of the home country." (Gilpin 278)

infrastructure. Thus, at first glance it seems that the most influential actors in any global cyberspace regime would be relevant MNCs, such as AT&T, CISCO and Microsoft.

In international telecommunications negotiations, a state and its ICT firms have a symbiotic relationship. This is confirmed by observed and documented behaviors of the state-MNC relationship in telecommunications meetings at the ITU.[335] This has been the case ever since the International Telegraph Union, the predecessor of the International Telecommunications Union, began meeting in the mid-nineteenth century to regulate telegraphy policies.[336]

Elements of Civil Society

Global civil society operates within the global economy, including the information economy. This system is "primarily animated by market relations based on private property."[337] Private property is owned, exchanged and consumed by individuals, the most basic units of global civil society. Consumers and corporations freely interact within the global marketplace. In experiencing free transnational associations, allegiances, solidarities and codes of conduct arise from this transnational sector. It is important to recall that such interactions arise "partially because the state system supports them."[338]

A new phenomenon in international negotiations, begun at the WSIS, is the emergence of global civil society as active participants invited by the United Nations to

[335] Author's notes taken at the HLEG meeting on 26 June 2008. *See also:* Edward A. Comor "Communication Technology and International Capitalism: The Case of DBS and US Foreign Policy" in *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy*. Ed. Edward A. Comor (New York, NY: St Martins Press, 1994, 83-102)
[336] Jill Hills. *The Struggle for Control of Global Communications: The Formative Century* (Chicago, Illinois: University of Illinois Press 2002.)
[337] Wapner, 75.
[338] Wapner, 72.

contribute to the drafting of political statements (such as the outcome documents from WSIS). While some members of global civil society are supported by the state, global civil society in general is independent of states, and can generate and define societal norms[339] While the role of states in global governance is not diminished by elements of global civil society, regime theory must take global civil society into account when considering how to address the issues of governing cyberspace.[340]

Michele Betsill broadly identifies transnational actors, which include grassroots organizations, scientific associations and special interest groups.[341] All of these transnational actors can respectively fit into one of three primary units of analysis: (1) non-governmental organizations (NGOs); (2) transnational networks; and (3) multinational corporations.[342] These units are transnational communities that exhibit an extraordinary diversity within their individual domains.[343]

NGOs are organizations that differ amongst themselves in that they might operate in geographic areas and have different interests that they pursue through various types of activities. International NGOs and national NGOs both exist, however, in order to be contribute to global governance efforts they must be recognized as legitimate actors. Such legitimacy can be bestowed on an NGO by an international organization, such as the United Nations, which offers

---

[339] Wapner, 72.
[340] Wapner, 67.
[341] National and international, academics, businesses, trade associations, environmentalists, individuals, the media, churches and religious organizations, independence movements, sub-national governments, political parties, foundations and consumer groups, are all broadly identified as transnational actors) See:
Michele M. Betsill, "Transnational Actors in International Environmental Politics," in *International Environmental Politics*, Michele M. Betsill, Kathryn Hochstetler and Dimitris Sevidis (eds), (Palgrave Macmillan: New York, 2006), 173-202, 174.
[342] Ibid., 175.
[343] Ibid., 186.

accreditations according to U.N. guidelines. In the WSIS process, the U.N. invited members of global civil society to contribute to the work of the WSIS.

In the WSIS process, legitimacy is conferred on civil society actors through the accreditation of NGOs not registered in accordance with the rules and procedures agreed on by states. Furthermore, to facilitate the participation of national, regional, and international civil society in the WSIS process, the WSIS created the Civil Society Facility Fund.[344]

Some transnational communities are more influential than others. Therefore, tensions arise, and these tensions "raise questions about the legitimacy, representation and accountability of transnational actors."[345] Some actors have had positive effects on international relations, and scholars tend to focus on such cases.[346] Thus, it might seem as if transnational actors always matter. However, the importance of transnational communities is relative. Not all have a broad impact on international relations. This is especially true in the context of global environmental politics, since transnational actors tend to engage and shape "particular types of issue areas, at particular stages of the policy process and/or in distinct realms of activity." [347] Hence, transnational actors can prod international action; however, states are still the central actors in the policy process, whose constituents must nudge them towards taking positive domestic or international action on global environmental governance.

Civil society actors are considered to be independent variables that affect global politics in different ways, and Betsill notes that it is important to understand how and

---

[344] World Summit on the Information Society. *Civil Society Facility Fund to participate in the World Summit on the Information Society (WSIS).*
[345] Betsill 188.
[346] Ibid., 192.
[347] Ibid., 193.

why they act. In the context of cyberspace governance, action taken by relevant members of global civil society are identifying the impact of ICT on society and culture, and the need for democratic accountability in the Information Society.[348]

[348] International Telecommunications Union, *The Different Actors in the Information Society*, http://www.itu.int/wsis/basic/actors.html

Chapter Seven
World Summit on the Information Society

The World Summit on the Information Society (WSIS), and its successor, the Internet Governance Forum (IGF), are the main venues where governments and all interested stakeholders debate issues and determine the objectives and principles surrounding the structure of the global Information Society. These diplomatic processes are unique in that they include state and non-state actors. Academic assessments of these conferences are largely absent in cyberspace studies literature. The few studies that do exist are either self-assessments by the WSIS, or focus on civil society.[349] This does not mean that scholars are unaware of the existence of these conferences, as there are passing references to ongoing diplomatic processes in the literature.

Outcome documents of intergovernmental preparatory committee meetings leading up to the Summits two phases are significant primary sources of information providing insight on the political efforts to create a secure cyberspace and regulate the Internet. These conferences and consultations are the main political efforts that determine the standards of the Information Society and how cyberspace resources will be utilized and governed.

The main political documents finalized during the Geneva phase of the summit were the *Declaration of Principles* and the *Plan of Action*. The *Tunis Commitment* and the *Tunis Agenda* reaffirmed the world's will to stimulate a worldwide Information Society based on political agreements. Cybersecurity is recognized as being crucial the

[349] See: Marc Raboy & Normand Landry, *Civil Society Communication and Global Governance: Issues from the World Summit on the Information Society* (New York, New York: Peter Lang, 2005).

creation of a stable Information Society in which e-commerce, e-governance and e-learning can take place in a regulated manner. Thus, governing the Internet is a critical aspect of creating a safe and secure Information Society.

Throughout the WSIS intergovernmental process, the security of computer-networks, information systems and other information and communications technologies (ICTs) is discussed with concern. These discussions continued at the Internet Governance Forum (IGF), which succeeded the WSIS at the 2006 inaugural meeting in Athens, Greece.

During the lead-up preparatory phase of the WSIS, the United Nations Economic Commission for Europe reported on the challenges to the WSIS process. It noted that complexities and controversies arising from the process were due not only to technological development issues, but also to political questions, including the issue of security.[350] Furthermore, it was noted that "there is a growing sense of fatigue with global conferences and processes, and that there is no global architecture for international dialogue on knowledge of information technologies."[351] As of 2009, the appropriate forum for such a global architecture for international dialogue is a hotly contested item, and conference fatigue is still a key concern.[352]

The extant literature on these processes relies either on official WSIS documents, focuses on civil society or assumes the WSIS process is an unimportant event.[353] There is

---

[350] United Nations Economic Commission for Europe, *The Information Society in Europe and North America: Contributions from the UNECE to the WSIS Prep Com 2* (December 2002), 3.
[351] United Nations Economic Commission for Europe, *The Information Society in Europe and North America: Contributions from the UNECE to the WSIS Prep Com 2* (December 2002), 3.
[352] Notes taken during the HLEG meeting on 26 June 2008 by Panayotis Yannakogeorgos. Also, the U.S. position on the IMPACT center for the Global Cybersecurity agenda is described as being an institution which might attract media attention with its catchy name, but is redundant. (Interview with U.S. Department of State official).

a lack of content analysis of the diplomatic positions of states. This project fills the gap. By conducting a content analysis of the diplomatic record, this project identifies what decisions in the field of global cybersecurity are made or not made, and why. The focus is on the positions of the:

- United States (Internet hegemon)
- Russia (perceives greatest threat from U.S. cyberspace dominance)
- China (emerging cyber power)
- European Union (main party catalyzing efforts to harmonize national cyberlaws).

It is argued that cyberspace governance involves more than simply having a technical capacity in place that effectively regulates the Internet and other ICTs.

Efforts hindering cooperation between states have been identified within the scope of how states relate to global civil society and not on how national interests on the topic of cybersecurity affect state's positions in negotiations.[354] This project examines the intergovernmental process through content-analysis of pertinent diplomatic sources. The main areas of contention revolve around U.S.-based entities' dominance of critical information infrastructures such as the Domain Name System (DNS) and Internet Corporation for Assigned Names and Numbers (ICANN). Observations of interactions between states, as recorded by the author during his participation in intergovernmental and multilateral meetings, supplement the textual analysis. This research contributes to the understanding of what decisions states did or did not make (and why) at these conferences.

---

[353] Johnathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, Connecticut: Yale University Press 2008), Giampiero Giacomello, *National Governments and Control of the Internet: A Digital Challenge* (New York: Routledge, 2005, 16-17).
[354] Raboy and Landry, 4.

A Concise Introduction to the WSIS

Organizational Structure of the WSIS

Prior to delving into the internal dynamics of the WSIS process, a broad review of its structure and procedures is necessary. In their book, *Civil Society Communication and Global Governance: Issues from the World Summit on the Information Society,* Marc Raboy and Normand Landry provide a comprehensive account of the WSIS process from the perspective of global civil society. Noting that the global media did not give the Summits prime coverage, they emphasize the importance of the WSIS, since it:

> …has placed the governance of global communication on the world agenda, sparking a long overdue discussion that has, in turn, become the spearhead of a larger reconceptualization of the manner in which global decisions are made.[355]

Although their work does detail the structure of the Summit, it focuses on the participation of global civil society and its interaction with the United Nations (U.N.) system, nation-states, and amongst the multitude of actors that constitute it. Acknowledging that states are the predominant actors in the negotiations taking place during the preparatory phase leading to the actual WSIS summits, their study focuses on civil society: the segment which had the least overall access and impact on the outcomes of the WSIS process.[356] It is noted that this was the first summit in which the United Nations invited civil society to contribute and advise the negotiations process as Summit participants. The authors describe the reluctance of states to allow civil society into the intergovernmental panels and to give them voting privileges at the summit.

---

[355] Raboy and Landry, 1.
[356] Raboy and Landry, 17.

Although the WSIS Summits in Geneva and Tunis received limited media attention, the foundational work occurring in the preparatory committees and other conferences related to the WSIS received even less attention. These conferences were where the foundation for the political understanding of the information society at the WSIS was laid out.[357] The preparatory phases (herein PrepCom) were the most important, since this is where states voted on items on the Summit's agenda, the processes and procedures of the Summit, and the wording of the final outcome documents presented and finalized at the actual Summit. It is also where states interacted with global civil society actors. Regional meetings were held to supplement the work during the PrepCom phases, and assure that each region could design and define its own needs and expectations regarding the information society.[358]

Organizational Structure

The ITU is the main entity tasked with organizing the WSIS. The High-Level Summit Organizing Committee was formed to "coordinate the efforts of the United Nations family in the preparation, organization and holding of WSIS."[359] This committee included a representative of the U.N. Secretary-General and the executive heads of relevant U.N. specialized agencies. Delegates from other U.N. entities were included as observers.[360] The ITU Secretary-General served as the committee chairman. The WSIS

[357] Raboy and Landry, 19.
[358] Raboy and Landry, 20.
[359] World Summit on the Information Society, *Roles of HLSOC, WSIS-ES, host country Executive Secretariats, and ITU* <http://www.itu.int/wsis/basic/roles.html>
[360] Executive Heads of the FAO, IAEA, ICAO, ILO, IMO, ITU, U.N. Regional Economic Commissions, UNCTAD, UNDP, UNEP, UNESCO, UNFPA, UNHCHR, UNHCR, UNIDO, UNU, UPU, WFP, WHO, WIPO, WMO, World Bank, WTO, it also included IADB, IOM, OECD, UNFIP, UNITAR, UNV as observers.

Executive Secretariat – ITU was led by Charles Geiger and other senior ITU officials. One of its important functions was to

> Ensure that the contributions of the actors participating in the various conferences were comprehensively merged with the contributions from PrepComs and regional meetings in consensus document that would serve as the basis for the *Declaration of Principles* and *Plan of Action* of the WSIS.[361]

The Host Countries Executive Secretariats (HCES) of Switzerland, and later Tunisia, were set up to ensure that the host countries met the logistical requirements for preparing and organizing the WSIS.

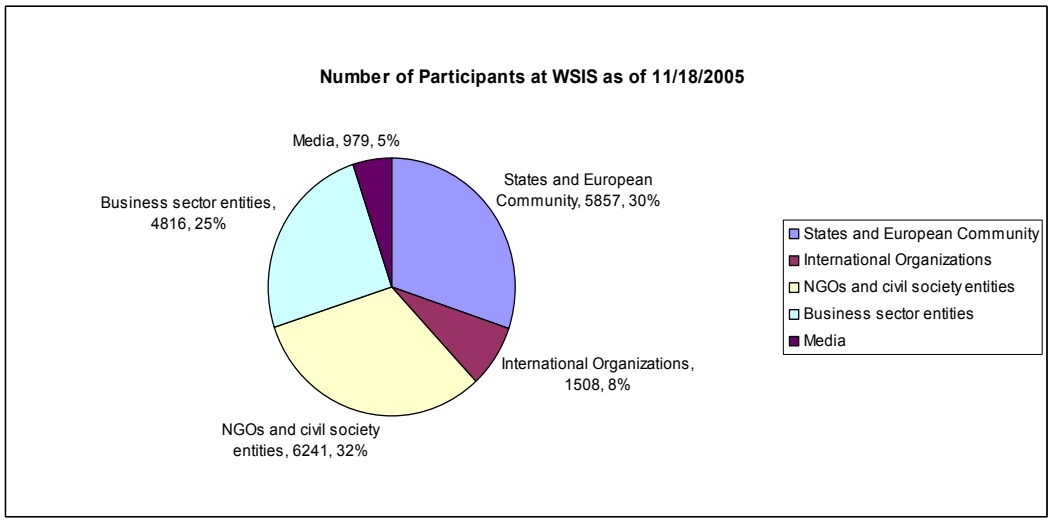
Structure of Participation

Participation in the WSIS was limited to the following entities: states and the European Community, International Organizations, NGOs and other Civil Society entities, and Business Sector entities. States were the sole entities granted voting privileges, though all entities were encouraged to contribute to the discussions. As Raboy and Landry have stated, the WSIS represents the first time "a U.N. summit has been given an organizational structure consisting of a number of components which bring together representatives of member States, the private sector, civil society and various U.N. agencies."[362] It is further noted that "the clearly expressed desire of the Summit organizer to include these actors from the beginning of the preparatory process is something new at the United Nations."[363]

Raboy and Landry note that the role of civil societies during the preparatory committees and regional conferences was minimal due to the predominance of national

[361] Raboy and Landry, 21.
[362] Raboy and Landry, 30.
[363] Raboy and Landry, 30.

government's control of these processes. It appears from the chart above that NGOs and civil society had the greater number of participants, but the least amount of power. The composition of the WSIS is as follows:

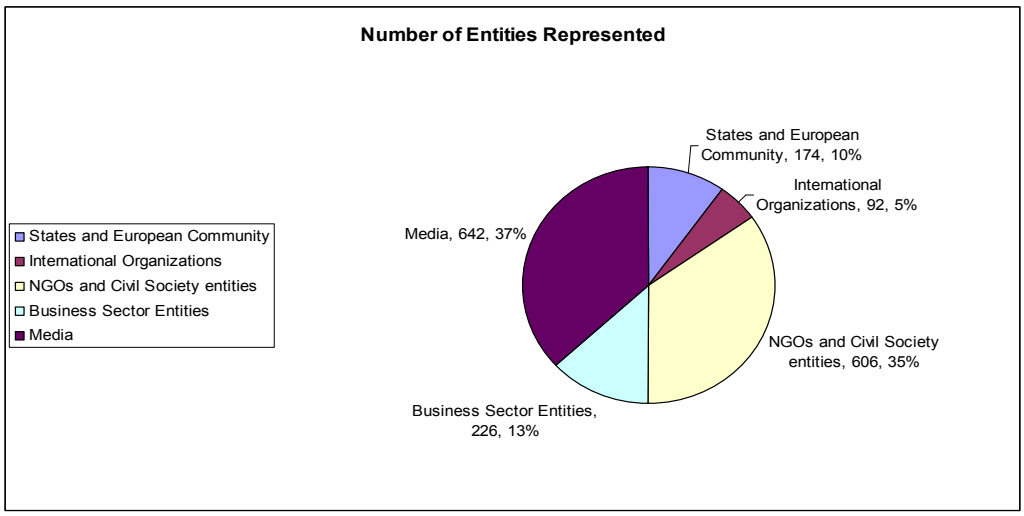


[364]

Closed and informal-informal intergovernmental consultations during the preparatory phase leading to the WSIS Geneva and Tunis phases occurred without non-governmental actors taking part in the decision-making process, even though they constituted the majority of total participants. Some participants who were either members of civil society or business entities acted as advisers to the national governments during the process.[365] Some ICT corporations, having earned trust of the ITU over time as a result of their ownership of the physical telecommunications infrastructure and their proactive contributions to the ITU's program of work, were viewed as more legitimate actors than civil society.[366] This can be attributed to the practice of the ITU in including business entities, such as CISCO or Ros Telecom, in its program of work. Although business

[364] Statistics from: Number of participants recorded by the World Summit for the Information Society, *About WSIS*, <http://www.itu.int/wsis/tunis/newsroom/index.html>.
[365] Raboy and Landry, 17.
[366] Raboy and Landry, 26.

entities did not have voting rights at the WSIS, it will be suggested below that some states may have served as the mouthpiece of the businesses headquartered within their borders.



[367]

Despite the willingness to include civil society in the process, States relegated the participation of non-state entities to the sidelines. In doing so, they effectively monopolized all authoritative decision making through their voting rights on key decisions and texts during the Summit. Thus, the value of prior studies on the WSIS for understanding what transpires in cyberspace negotiations is limited by the focus on the least influential actor in the efforts to govern cyberspace. The crux of the Raboy and Landry argument is that civil society has a lot to contribute and deserves a greater role in the Internet governance debate, however, it is recognized that civil society is not considered an actor that can be trusted with voting privileges. Raboy and Landry offer solutions as to how civil society may overcome its own limitations in an effort to

[367] Number of entities represented as recorded by the World Summit for the Information Society, *About WSIS*, <http://www.itu.int/wsis/tunis/newsroom/index.html>.

remarket themselves as legitimate actors in this and other international conferences where global decision-making occurs.

The Geneva Summit Phase

The Geneva Summit of the WSIS, held from 10-12 December 2003, allowed all relevant parties the chance to formally begin the process of developing the Information Society based on trust and security. The priorities established by GA resolutions, notably 56/121 and 57/239, were discussed. The meeting resulted in the drafting and adoption of the *Declaration of Principles* and *Plan of Action* by "the representatives of the peoples of the world."[368] The *Declaration of Principles* decrees that the Information Society should be organized around a:

> Common desire and commitment to build a people-centered, inclusive and development oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.[369]

The Information Society is therefore based on democratic principles in which individuals are guaranteed the right to freely create and transmit information and knowledge, as long as their objectives are not against the principles of the *U.N. Charter* and the *Universal Declaration of Human Rights*.

Security is the cornerstone of the Information Society. Paragraph five of the Geneva *Declaration* states that users must have confidence in the Information Society. A

[368] World Summit on the Information Technology. *Declaration of Principles*, para 1.
[369] Ibid.

framework of trust that includes "information security and network security, authentication, privacy and consumer protection" must be established to assure that data, privacy, access and trade are protected.[370] Additionally, the WSIS recognizes that ICT has the potential to create devastation and recommends that appropriate actions at the national and international levels should be taken to secure cyberspace so that ICT is not used "for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within States.[371] In this regard, the *Declaration of Principles* calls for all interested stakeholders to have a strong commitment to the concept of "digital solidarity" with governments at the national and international level, and recognizes that new forms of partnership will be required in order to meet the goals set out in the *Declaration*.

In addition to the *Declaration of Principles*, participants in the first phase of the WSIS in Geneva negotiated and agreed upon a *Plan of Action* for achieving the goals set therein. In section C5.12, the WSIS defines what actions must be taken to fulfill the objectives contained in paragraph five of the *Declaration of Principles*.[372] Reiterating the importance of security and its role in developing user confidence in ICT, the *Plan of Action* recommends private-public partnerships for the prevention, detection and response to cyber-crime and ICT misuse. For its role, governments are mandated with the task of developing guidelines taking into account the ongoing efforts in these areas.

The main outcome of the second WSIS summit on the Information Society was the adoption of the *Tunis Commitment* and the *Tunis Agenda for the Information Society*. Significantly, the *Tunis Agenda* calls on the Information Society to "requisite legitimacy

---

[370] Ibid., para 5.35.
[371] Ibid, para 5.36.
[372] World Summit on the Information Society, *Plan of Action*, section C5.12.

of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities."[373] Internet governance is defined as "the development and application by government, the private sector and civil society, in their respective roles, of shared principles, norms, rule, decision-making procedures, and programs that shape the evolution and use of the Internet."[374] It does not clearly define the role of each stakeholder (the government in particular) in Internet Governance. However, the statement clearly indicates that actors other than national governments have a strong role in governing the Internet. Recalling the Aristotelian perspective, the risk in allowing non-governmental authorities to develop legislation or decrees lies in the possibility that these parties may seek to further their own interests rather than those of the community as a whole.

Furthermore, the *Tunis Agenda* states that "the existing arrangements for Internet governance have worked effectively to make the Internet the highly robust, dynamic and geographically diverse medium that it is today, with the private sector taking the lead in day-to-day operations, and with innovation and value creation at the edges."[375] It is further stressed that there is a

> "need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues."[376]

Hence, the private sector's role is clearly defined by the *Tunis Agenda* as being responsible for the day-to-day operations of the Internet, and governments should play no

---

[373] *Tunis Agenda*, 31.
[374] Ibid.
[375] Ibid., para. 55.
[376] Ibid., para. 69.

role in these technical and operational trivialities. The government's role remains unclear, other than that it should have a significant role in international public policy making. As will be shown in the diplomatic dispatches, the language relating to Internet governance was shaped by the U.S.'s insistence that the Internet Corporation for Assigned Names and Numbers (ICANN) was, and continues to be, a good mechanism regulating the day-to-day operations of the Internet. The rest of the world disagrees with this stance, and maintains that Internet governance mechanisms should be internationalized.

Intergovernmental Preparatory Committee One

The WSIS Intergovernmental Preparatory Committees (PrepComs) laid the groundwork for the drafting of the *Declaration of Principles* and the *Plan of Action*.

Although the WSIS deals with many important elements of the Information Society, it is not within the scope of this project to trace State's negotiating positions on topics such as whether or not private entities should participate in the WSIS, or bridging the digital divide. Overlaps between the other issue areas and cybersecurity are examined when relevant. However, the focus of this project is on States positions in the field of cybersecurity.[377]

Intergovernmental Subcommittees

Two intergovernmental subcommittees themes were chosen by the WSIS Bureau to set the agenda for the WSIS. Studying the behavior of states in their negotiations during this phase of the WSIS provides insight allowing for the identification of:

[377] It should be noted that in an interview with one official who took part in this phase described Pakistan as being obstructive during negotiations. It's continuous procedural obstructions resulted in the stalling of the PrepCom's program of work.

- What areas there is cooperation and disagreement in
- What conflicts are sustained
- Which conflicts are resolved, and why?

Subcommittee One established the rules and procedures of the PrepComs and for the Summits in Geneva and Tunisia. The inclusion of NGO, civil society and business entity participation as an item on the agenda led to loss of momentum on the more substantive security issues stemming from north-south differences. The second subcommittee focused on WSIS's content and themes identifying "information network security" as foundational to the information society's enabling environment.[378]

Universal Recognition of the Importance of Cybersecurity

The United States did not have specific recommendations on cybersecurity. Instead, it emphasized bridging the digital divide and promoting public-private partnerships, market liberalization and the creation of independent regulatory agencies." [379] The U.S. position on the freedom of information flows was apparent in its suggestions that issues such as content regulation not be discussed since content regulation "…infringes on the right of all to freedom of expression as set forth in Article 19 of the Universal Declaration of Human Rights."[380] The focus of the European Union was on clusters of e-government, e-learning and e-inclusion, and that within each cluster it was "implied that security, privacy protection, and general trust are underlying conditions in order to build people's

[378] See: *DRAFT REPORT OF THE CHAIRMAN OF SUB-COMMITTEE* 2, <http://www.itu.int/dms_pub/itu-s/md/02/wsispc1/doc/S02-WSISPC1-DOC-0010!!PDF-E.pdf>. *Report of the First Meeting of the Preparatory Committee*, 26.

[379] United States Contribution document WSIS/PC-1/CONTR/9-E < http://www.itu.int/dms_pub/itu-s/md/02/wsispc1/c/S02-WSISPC1-C-0009!!MSW-E.doc>, 2.

[380] United States Contribution document WSIS/PC-1/CONTR/9-E < http://www.itu.int/dms_pub/itu-s/md/02/wsispc1/c/S02-WSISPC1-C-0009!!MSW-E.doc>, 2.

confidence on the information society."[381] Russia discussed challenges of the information society it found important, such as "national sovereignty and security in the information space, non-interference in internal affairs and freedom of information, and the safeguarding of human rights in global telecommunication." [382] China identified security as the key to information and communications networks, arguing that:

> Communications security is directly related to the risks and losses in communications. Security guarantees may improve consumer confidence and further promote the applications of infocom technologies and networks. Security of infocom networks involves technologies as well as laws and regulations and requires international cooperation.[383]

The Chinese suggested that fighting cybercrime was of utmost importance in ensuring the security of communications networks, and that international organizations and mechanisms were necessary in order to do so. Research and development initiatives to develop security technologies and the "strengthening control of network security and protection of communications networks through application of laws and regulations" were all identified as areas the Summit should consider.[384] However, one Council of Europe transmission note to heads of missions to the COE describes China's views as "being inclined to show understanding for views expressed by developing countries"[385]

---

[381] Denmark, speech on behalf of the European Union, http://www.itu.int/wsis/docs/pc1/statements_general/denmark.doc.
See also Denmark, speech on behalf of the European Union Content and Themes for the World Summit on the Information Society (WSIS) < http://www.itu.int/wsis/docs/pc1/statements_content/denmark.doc>.

[382] First Deputy Minister of the Russian Federation for Communications and Informatization of the Preparatory Committee for the World Summit on the Information Society.

[383] Statement by Chinese Ambassador Sha Zukang at the First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society, <http://www.itu.int/wsis/docs/pc1/statements_general/china.doc>.

[384] Statement by Chinese Ambassador Sha Zukang at the First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society, <http://www.itu.int/wsis/docs/pc1/statements_general/china.doc>.

The positions of all nations during PrepCom-1 are indicative of the universal understanding that there is a need to secure cyberspace however, competing state interests often obstruct action. As the WSIS process progressed, the preliminary remarks on the importance of securing cyberspace and governing the Internet would soon be supplanted by U.S. resistance to the internationalization of the ICANN, thereby giving up part of its command of the network and allowing its control of day-to-day operations of the domain name system to land in the hands of a more diverse group of actors that might not have U.S. interests in mind. As will become clearer below through content analysis, technogeopolitics is a good predictor of an involved state's actions .

WSIS Intergovernmental Preparatory Committee Two

Regional Conferences Lead up to PrepCom Two

The time period between PrepCom-1 and PrepCom-2 was marked with various formal and informal conferences and meetings at which states continued their negotiations on the content and themes of the declarations and plan of action presented in Geneva and Tunis during the main WSIS summit.[386] Significant outcomes of conference taking place prior to PrepCom-2 including the Bamako, Bucharest, Tokyo, and Bavaro declarations. These declarations were the outcome of regional meeting hosted to provide "major inputs to the WSIS process."[387] These conferences, conducted at the ministerial level, indicate the importance of the direct involvement of ministers to maintain the

---

[385] Council of the European Union General Secretariat, "Main Items Raised at the Working Lunch at Ambassador Level between the Troika and China (Geneva, 5 December 2002 (TGN.1205.02), 3.

[386] The focus of this project is on the issue of cybersecurity and the information society. It should be noted that several side-events took place covering issues that are not related to cybersecurity. It is not the scope of the dissertation to delve into the substance and content of these nonetheless important endeavors. For a comprehensive listing of all such meetings and events.

[387] United Nations Economic Commission for Europe, *The Information Society in Europe and North America: Contributions from the UNECE to the WSIS Prep Com 2* (December 2002), 3.

WSIS preparatory process' momentum, since it gave ministers "a specific competence" and indicated their "direct political interest in the process."[388] Focused insight into which inputs remained on the agenda and which were abandoned during the PrepComs leading up to the Geneva *Declaration of Principles*, *the Tunis Commitment,* and *the Tunis Agenda* are good indicators to identify the interest of each state.

Pan-European Regional Ministerial Conference

The Pan European Regional conference was hosted by Romania on 7-9 November 2002 in order to help the Western European and Others Group (including the United States and Russia) coordinate Member States participation in the WSIS. Preparatory meetings took place in the lead-up to the November meeting. Although other regional conferences took place prior to the second PrepCom, the Pan-European conference included the most diverse number of participants from fifty-five countries.[389]

The main outcome of the Pan-European conference was the *Final Declaration of the Pan European Regional Conference.*[390] Discussions on the final text of this document took place at three levels:

- Between the United States, Russia and Canada
- Between the fifteen members of the European Union
- Between the Danish Presidency of the E.U. and the United States, the latter representing the views of Russia and Canada.[391]

---

[388] United Nations Economic Commission for Europe, *The Information Society in Europe and North America: Contributions from the UNECE to the WSIS Prep Com 2* (December 2002), 3.
[389] Other regional conferences held in preparation of the second PrepCom were held in Bamako for Africa (28-30 May 2002), Tokyo for Asia (13-15 January 2002), Santo Domingo for Latin America and Caribbean countries (29-31 January 2003) and Cairo for Middle Eastern countries (June 2003).
[390] Final Declaration of the Pan European Regional Conference <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-E.pdf>.
[391] Diplomatic Dispatch.

The positions of the United States, European Union and Russian Federation on security are outlined below, after introducing principle six, which reads:

> To realise fully the benefits of ICTs, networks and information systems should be sufficiently robust to prevent, detect and to respond appropriately to security incidents. However, effective security of information systems is not merely a matter of government and law enforcement practices, nor of technology. A global culture of cyber-security needs to be developed - security must be addressed through prevention and supported throughout society, and be consistent with the need to preserve free flow of information. ICTs can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security in both civil and military fields, as well as in relation to the functioning of their economies. It is also necessary to prevent the use of information resources or technologies for criminal or terrorist purposes. In order to build confidence and security in the use of ICTs, Governments should promote awareness in their societies of cyber security risks and seek to strengthen international co-operation, including with the private sector.

These positions echoed the UNGA resolutions on the establishment of a global culture of cybersecurity, and did not stray too far from preexisting diplomatic language. The text of principle six is straightforward enough. Effective security of information systems is not merely the responsibility of government and law enforcement practices.[392] However, the militarization of cyberspace is not included as an item of concern. Comparing the final version of principle six to the revisions suggested by the U.S., E.U. and Russia indicates that the United States preferred not to include mention of this. To safeguard their

[392] *Final Declaration of the Pan European Regional Conference*<http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-E.pdf>.

position, the U.S. led a coalition against the Russians, who were concerned with the issue of cyberspace being militarized. The Russians proposed the following for principle six:

> Development of ICTs should take into account new challenges and threats in the field of security. There is concern that ICTs [they] can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of states in both civil and military fields…It is also considered necessary to prevent the use of information resources or technologies for criminal or terrorist purposes…This suggests the need for a greater awareness and understanding of security issues and the need to develop a "culture of security"…One key element of protection of ICTs against illegal use is the strengthening of information and communication networks security"[393]

The U.S., disagreed with some of the Russians' language, and offered the following revisions:

> "Development of ICTs should take into account **the need to defend against the wide variety and increasing number of threats to information systems and networks** ~~**offer new challenges and threats in the field of security. There is concern that**~~ ICTs can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the **infrastructure of states to the detriment of their security in** ~~**security of states in**~~ both civil and military fields…It is also considered necessary to prevent the use of information resources or technologies for criminal or terrorist purposes…This suggests the need for a greater awareness and understanding of security issues and the need to develop a "culture of security"…One key element of protection of ICTs against **unauthorized** ~~**illegal**~~ use is the strengthening of information and communication networks security"[394]

[393] Russian Federation proposal for the for the text of Principle VI.
[394] United States Revision to the Russian Proposal. Markings duplicated here as they appear on the original document.

The U.S. revisions were guided by the context set in the UNGA resolution on the *Global Culture of Cybersecurity*, which the U.S. also wanted reflected in the E.U.'s declaration on the sixth principle.[395] Furthermore, the U.S. argued that the language the Russians used was "too narrow" and not inclusive of the wide variety of threats to computer systems.[396] The focus was on the security of civil and military cyber *infrastructures* of states. This language more precisely reflects the true nature of the threat indicating that the U.S., as a core operator of many elements of cyberspace, understands the nature of the problem. The removal of the word *illegal*, and replacement with the word *unauthorized* may be an attempt to avoid language that would identify certain U.S. intelligence or military activity in cyberspace as illegal. Using the word *unauthorized* does not indicate that the U.S. is doing anything illegal, rather, it implies that they are just taking actions without the authority of an information operator. As introduced in an earlier chapter, much evidence exists in open sources that documents the U.S.'s successful use of cyberspace as a medium for espionage, targeting several countries, but Russia in particular. Branding such activity as illegal would put both the U.S. government and business entities cooperating with U.S. intelligence in such operations at risk. Thus, one factor motivating the U.S.'s refusal of language constraining state behavior in cyberspace is its ability to collect information traveling through U.S. controlled cyberspace.

The European Union's position, as stated by the Danish Presidency during an E.U. coordination meeting for the Bucharest summit, was that governments should not be singled out as the only actors responsible for cybersecurity. Ole Neustrop offered the

[395] U.S. comments on the Russian text for Principle 6, received October 29.
[396] Ibid.

following revision for principle six: "It is necessary for all instances responsible for information systems and networks, including government, to act at various levels, in order to prevent the illegal use of information resources or technologies"[397] Thus, the E.U. position promotes public-private partnership, but also indirectly addresses the question of cyberspace militarization.

WSIS Bureau Meeting

During the meeting of the group of experts ("wise men") in Montreux, December 13-16, 2002, it was proposed that an orientation document be drafted to aid the work of PrepCom-2. The WSIS Bureau President's *Orientation Document for PrepCom-2* highlighted the key principles and action items for the development of the Information Society. [398] Although they are listed tenth in the Orientation Document, issues pertaining to cyber confidence and security were deemed essential to the "full functioning of the information society."[399] Related to this principle, action items five and six noted the need for a "transparent, competitive and trustworthy" enabling environment for the information society. The development of international and regional legal and regulatory frameworks were considered as one action that could be taken to promote this effort. Action item six focused on the actions that would contribute to "building confidence and security in the use of ICT if they are to be more widely used and with greater reliability."[400] Data protection, trust in cyberspace transactions and e-commerce,

---

[397] Email from Ole Neutrup, Mission of Denmark to Ambassador Fillp 10/29/2002 *Bucharest Declaration E.U. Reaction*.
[398] President of the Preparatory Committee, *Proposal of an Orientation Document for PrepCom-2*, *
[399] President of the Preparatory Committee, *Proposal of an Orientation Document for PrepCom-2*, * , Key Principle 10.

international cooperation against cybercrime, global technical standards fostering deployment and use of ICT, quality of interconnections and interoperability of ICT systems, and issues related to the convergence of ICT and broadcast media were noted as areas where action was needed.[401]

The proposed *Orientation Document* was not accepted by all states at the WSIS Bureau Meeting.[402] Despite the insistence of the Bureau President, Mr. Adama Samassekou, that "the paper was for information only to the Bureau members who were not supposed to start discussing it in substance," countries such as Tunisia, Pakistan and Brazil, suggested additions to the document.[403] This reduced the momentum of the meeting, and is further indication of the obstructive attitude of these countries in WSIS meetings. In its meeting of January 14, 2003, the Western European and Others Group (WEOG) group agreed with the orientation document, as a basis for continuing discussion, although the U.S., Canada and Norway expressed that they had several reservations with the substance of the document. During an E.U. Commission meeting that took place at the Ambassadorial level, it was noted that although differences between the Orientation Document and the E.U. position exist, it was "a major step forward in comparison to the confused situation that emerged from Subcommittee 2 of PrepCom-1."[404] The E.U., realizing that other regions were skeptical of their approach, agreed that

---

[400] President of the Preparatory Committee, *Proposal of an Orientation Document for PrepCom-2*, *, Action Line 6.
[401] President of the Preparatory Committee, *Proposal of an Orientation Document for PrepCom-2*, *
[402] *Summary of the WSIS Bureau meeting held on Wednesday 8 January 2003*.
[403] *Summary of the WSIS Bureau meeting held on Wednesday 8 January 2003*, 2.
[404] Transcript of the First Meeting at the Ambassadorial level of the European Commission Regarding the World Summit on the Information Society (27 January 2003), 3.

there was a need to continue and intensify its outreach efforts towards the Asian and the African groups.[405]

As became clear during this phase of the meeting, E.U. member states were not unified in their own positions. In one diplomatic note it was noted that the United Kingdom and the Netherlands were not particularly concerned with the WSIS process, whereas Germany was interested, but did not provide much positive input to the process. The position of other E.U. countries was described as being characterized by either silence or questions seeking explanation.[406]

Asia-Pacific Regional Meeting

The Asia-Pacific regional perspective was declared during the WSIS Asia-Pacific Regional Conference, which took place in Tokyo, Japan from the 13-15 January 2003. The Tokyo Declaration contains elements pertaining to security in the information society.[407] Preliminary paragraphs eight and nine note that in order for confidence and trust to be built in the information society, "secure and reliable information and communication networks" are required, but need to be secured in such a way that does not place "vulnerable groups" at risk.[408] Preliminary paragraph ten notes that the private sector has an important role to play in building partnerships that facilitate and promote trust and confidence in ICTs, since "ICTs can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security, and

[405] Transcript of the First Meeting at the Ambassadorial level of the European Commission Regarding the World Summit on the Information Society (27 January 2003), 3.
[406] Diplomatic Note 27 January 2003
[407] World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration-The Asia-Pacific Perspective to the WSIS*.
[408] World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration-The Asia-Pacific Perspective to the WSIS*. PP 8, 9.

may adversely affect the integrity of the infrastructure within states, to the detriment of their security…in both civil and military field.[409] Challenges to securing the cyber environment included:

- General lack of awareness of information security issues
- Rapid evolution, complexity, capacity and reach of ICT
- Anonymity offered by ICT
- Transnational nature of communication frameworks[410]

To address these issues, a multidimensional approach was recognized as necessary, "with emphasis on preventive approaches, national guidelines and regional and international cooperation," and focused on education, training, policy and law, and international cooperation as necessary to reach a common international understanding. [411] Overall, the *Tokyo Declaration* provides further points on which the international community generally agrees on the importance of securing the information society's enabling environment: cyberspace.

Regional Ministerial Preparatory Conference for Latin America and the Caribbean

While noting the importance of private enterprises and civil society to the transition to the information society, the Economic Commission for Latin America and the Caribbean (ECLAC) countries indicated that government should lead the process.[412] Furthermore, strengthening of international cooperation in all aspects of the information

[409] World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration-The Asia-Pacific Perspective to the WSIS*. PP 10, and 3.f
[410] World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration-The Asia-Pacific Perspective to the WSIS*. 3.f
[411] Ibid.
[412] *Bavaro Declaration*, 1.h <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0007!!PDF-E.pdf>.

society was deemed as important, given the global nature of this society.[413] In the field of cybersecurity, the *Bavaro Declaration* notes the importance of the priority issues of:

> Establishing appropriate national legislative frameworks that safeguard the public and general interest and intellectual property and that foster electronic communications and transactions. Protection from civil and criminal offences ("cybercrime"), settlement and clearance issues, network security and assurance of the confidentiality of personal information are essential in order to build trust in information networks. Multilateral, transparent and democratic Internet governance should form part of this effort, taking into account the needs of the public and private sectors, as well as those of civil society.[414]

The remarks appear to follow the general framework of the other declarations. However, Latin America, led by Brazil, took an indirect strike at the U.S. dominance of ICANN with the inclusion of language emphasizing the importance of making Internet governance mechanisms transparent and open to more actors as a critical part of securing cyberspace. Throughout the rest of the WSIS process, and continuing in other forums discussing Internet governance and global cybersecurity, Brazil has continued to be a vocal proponent against the U.S. position in ICANN.

PrepCom 2 Geneva, February 17-28

In the days immediately prior it was suggested that during the Tunis phase of the WSIS a legally binding *Charter for the Information Society* was suggested by the WSIS President. Representatives were interested in the idea, however, it was made clear that "a

---

[413] World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration-The Asia-Pacific Perspective to the WSIS*, 1.i, 3.p

[414] *Bavaro Declaration*, 2.g <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0007!!PDF-E.pdf>.

legally binding document would be a non-starter."[415] This is reflective of a hesitancy on the part of the international community to adopt a formal body of international law governing the information society and cyberspace.

The main objective of PrepCom-2 was for the participants to agree on the substance of the text of the Geneva *Declaration* and *Plan of Action*. While disagreement prevailed, participants did compile a draft declaration of principles and plan of action based on input from the regional conferences.

> "Recognizing that confidence, trust and security are essential to the full functioning of the Information Society, guarantees should be provided to users of media, communication and information networks against cybercrime and child pornography as well as protection of privacy and confidentiality."[416]

Paris Intercessional Meeting

As a result of slow momentum during PrepCom-2, the WSIS called for an intersessional meeting, which was held in Paris from 15-18 July 2003. The meeting was called to discuss the *Plan of Action* in order to align it with the text of the draft *Declaration of Principles*.[417] It was noted that in deliberations of the ad hoc group dealing with confidence and security issues of the Information Society there was complete agreement on the part of draft text prepared by the E.U. on the part of the U.S., Brazil, Iran and India. Russia, however, insisted on the inclusion of the security of civil and military cyber infrastructures, and on the inclusion of clauses on cybercrime and

[415] Transcript of Ambassadorial meeting in Geneva regarding latest developments on the WSIS process.
[416] *Report of the Second Meeting of the Preparatory Committee* <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0012!R1!PDF-E.pdf> b.20.
[417] WSIS, Note by the President, (18 July 2003).

terrorism. These clauses were not accepted by the others.[418] Further areas of controversy arose during ad hoc committee discussions on Internet governance. Although there was general agreement on the role of the private sector (mainly ICANN) in governing the Internet, some countries, which now included China, argued for the transformation of this Internet governance mechanism from a private entity to an international governance mechanism.[419] The U.S. and the E.U. opposed this view.

In the lead-up to the intercessional panel, disagreements emerged within the E.U. regarding how the Internet should be governed. France in particular diverged from the common E.U. stance, arguing that the issues of management of Internet governance "notably, those concerning the integrity and the coherence of the system (standardization and subsidiarity), as well as the sovereignty of states in their management of national domain names, must be entrusted to an inter-governmental organization."[420] This supports the rest of the world's position that the U.S. must open up ICANN. However, the dispute between France and other E.U. members was resolved prior to the intersessional mechanism during negotiations at the Deputy Representative level in the Committee of Permanent Representatives (COREPER-1).[421]

WSIS Intergovernmental Preparatory Committee Three (15-26 September 2003)

[418] Diplomatic note on the theme of the Paris intersessional meeting.
[419] Diplomatic note on the theme of the Paris intersessional meeting.
[420] Draft Declaration of Principles refined in April 22/23, Paragraph 18.
[421] Diplomatic dispatch dated 16 May 2003 on the results of the E.U. Commissions meeting at the level of delegate-expert.

Confidence and Security in ICT

Russia and the U.S. continued their disagreement over the language of the *Draft Declaration of Principles* in the area of building confidence, trust and security in the use of ICTs.[422] Although Russia had been isolated in meetings prior to PrepCom-3 in its insistence on the use of language "in both civil and military fields" when referring to cybersecurity threats, China supported Russia on the inclusion of this language in exchange for Russian support on the following two items: "consistent with the need to preserve the free flow of information" and "in accordance with the legal system of each country" in reference to cybersecurity.[423] The language of this item remained unchanged in other drafts prepared during PrepCom-3.[424]

Internet Governance

The issue of Internet governance proved to be one of the most contentious issues during the PrepCom-3. The U.S.'s insistence that language referring to the coordination of the international management of the Internet be removed from the draft was the main sticking point on this issue. In paragraph 40, the U.S. disagreed with language referring to a "technical level" of private sector involvement in the Internet:

> The management of the Internet encompasses both technical and policy issues. The private sector has had and

[422] World Summit for the Information Society, *Draft Declaration of Principles* (19 September 2003 <WSIS/PC-3/DT/1-E>.
[423] World Summit for the Information Society, *Draft Declaration of Principles* (19 September 2003 <WSIS/PC-3/DT/1-E>. Para. 28.
[424] World Summit for the Information Society, *Draft Declaration of Principles* (26 September 2003 <WSIS/PC-3/DT/1(rev.2B)-E>. Para. 28.

> will continue to have an important role in the development of the Internet at the technical level.[425]

The U.S. agreed to the addition of a new paragraph (42) in which "Internet issues of an international nature related to public policies should be coordinated between government and other interested parties."[426] However, less developed countries preferred alternative language referring to coordination "through/by appropriate intergovernmental organization under the U.N. framework" or "as appropriate on an intergovernmental basis."[427] Thus, it is clear that the U.S. is hesitant to relinquish its informal control over ICANN, and the Europeans reluctantly support this. The rest of the world appears determined to see that ICANN be transferred to an intergovernmental organization, preferably within the U.N. framework. In a second draft prepared during PrepCom-3, an alternative paragraph 40 was introduced which included language regarding the important role the private sector should play at "the technical and commercial levels.[428]

PrepCom-3 concluded on terrible note. Instead of focusing on the future of the Information Society, the committee battled over which issues between the North and South were debated. Thus, with only a few months until the WSIS's main event in Geneva, the international community continued to wrangle over the text of the document

---

[425] World Summit for the Information Society, *Draft Declaration of Principles* (19 September 2003 <WSIS/PC-3/DT/1-E>. Para. 40.
[426] World Summit for the Information Society, *Draft Declaration of Principles* (19 September 2003 <WSIS/PC-3/DT/1-E>. Para. 42.
[427] World Summit for the Information Society, *Draft Declaration of Principles* (19 September 2003 <WSIS/PC-3/DT/1-E>. Para. 42, alternatives b & c.
[428] World Summit for the Information Society, *Draft Declaration of Principles* (26 September 2003 <WSIS/PC-3/DT/1(rev.2B)-E>. Alternative Para. 40.

in an effort to bridge the North-South divide including on the issue of U.S. dominance over ICANN.[429]

The topic of Internet governance appears in paragraph thirteen of the Geneva *Plan of Action*, under the subheading "enabling environment." Following a preamble on the importance of information security, the issue of Internet governance is introduced as an important component to achieve this objective, which sets the parameters and terms of reference for the Working Group on Internet Governance (WGIG) as follows:

> i. develop a working definition of Internet governance
> ii. identify the public policy issues that are relevant to Internet governance
> iii. develop a common understanding of the respective roles and responsibilities of governments, existing intergovernmental and international organisations and other forums as well as the private sector and civil society from both developing and developed countries
> iv. prepare a report on the results of this activity to be presented for consideration and appropriate action for the second phase of WSIS in Tunis in 2005[430]

An area of contention in the field of Internet governance was, and continues to be, the organization and administration of the ICANN and the internationalization of Internet governance structures. This field also included security issues, including the impact of spam.[431]

---

[429] The main issues of contention were not related to cybersecurity, but rather to human security and human rights. In an effort to bridge this divide the Office of the United Nations High Commissioner for Human Rights prepared a "Background Note on the Information Society and Human Rights" (October 2003) in order to assuage Southern concerns.

[430] Paragraph 13 of POA on Internet Governance.

[431] European Commission Working Party on Telecommunications and Information Society, *Preparation of the Transport/Telecommunications and Energy Council of 1/10 December 2004* (6423/04 TELECOM 30 DEVGEN 37 CONUN 6), 7.

Tunis Phase of the WSIS

The second phase of the WSIS focused on the practical issues of implementing the *Geneva Plan of Action*, addressing two significant open questions that remained unanswered after the Geneva phase the Geneva phase of the WSIS. These questions centered on how the Internet is to be governed, and how the *Plan of Action* would be financed.[432] Both of these were serious areas of contention between North and South. To resolve them, the U.N. Secretary General established two working groups to address these issues. In an effort to avoid the pitfalls of intergovernmental negotiations, these working groups included multiple stakeholders under the independent auspices of the United Nations. This project focuses on the WGIG. The working definition of and scope of Internet governance, was generally agreed to be:

> …the global coordination of the Internet's Domain Name System, consisting of the technical management of core resources of the Internet, namely domain names and IP addresses, and the root server system. The WGIG should firstly concentrate on these issues. A second focal point of WGIG's work should be issues with direct impact on the Internet's stability, dependability and robustness, in particular spam.[433]

WGIG deliberations sought to resolve political issues prior the main Summit meeting in Tunisia. These deliberations contributed largely to the Internet governance section of the *Tunis Commitment* and *Tunis Agenda for the Information Society*.

---

[432] European Commission Working Party on Telecommunications and Information Society, *Preparation of the Transport/Telecommunications and Energy Council of 1/10 December 2004* (6423/04 TELECOM 30 DEVGEN 37 CONUN 6).

[433] Council of the European Union Working Party on Telecommunication and Information Society World Summit on Information Society (WSIS): Internet Governance-Guidelines for Discussions in the WSIS Framework (7 October 2004) 4.2.

Global Forum on Internet Governance

Prior to the commencement of the WGIG's program of work, the United Nations Information and Communication Technologies (ICT) Task Force hosted a Global Forum on Internet Governance from 25-26 March 2004.[434] During the forum, the clashes from the first phase of the WSIS appeared to continue. Marc Furrer, Director of the Swiss Federal Office of Communications representing Switzerland at the meeting, noted that the issue of adjusting or replacing ICANN, a system that is working and improving, deflected from more important issues related to cybersecurity which were of greater concern to the Information Society. [435] In contrast, Brazilian and South African delegates voiced opposition to this argument. Brazilian delegate Maria Luiza Viotti claimed that Internet governance needed reform since it is not inclusive of developing countries, and instead appears to be under the ownership of one group of countries or stakeholders.[436] Lyndall Shope-Mafole, Chairperson of South Africa's National Commission, spoke along similar lines, arguing that the legitimacy of ICANN's processes, rather than its functions, was of most concern for developing countries.[437] Thus, after rigorous talks, it was concluded on the basis of concerns from the developing world that ICANN required further reform.

---

[434] U.N. ICT Task Force Global Forum on Internet Governance to be Held in March http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html.

[435] United Nations Press Release, "Global Internet Governance System is Working But Needs to Be More Inclusive, U.N. Forum on Internet Governance Told" (26 march 2004) PI/1568. http://www.un.org/News/Press/docs/2004/pi1568.doc.htm

[436] United Nations Press Release, "Global Internet Governance System is Working But Needs to Be More Inclusive, U.N. Forum on Internet Governance Told" (26 March 2004) PI/1568. http://www.un.org/News/Press/docs/2004/pi1568.doc.htm.

[437] Ibid.

An assessment of the WSIS process following the first phase of the WSIS was presented at a meeting between ITU Secretary General Yoshio Utsumi and E.U. Heads of Mission.[438] Utsumi stressed the importance of making the current Internet governance structure more democratic, adding that this was more of a technical problem which had been transformed into a politicized issue during the Geneva phase of the Summit.[439] His expectation was that all problems of Internet governance, especially top-level domain names, would not be resolved in Tunisia, and that discussions there should be viewed as part of a longer process. This process continues in the form of the Internet Governance Forum (IGF), discussed further below.

Although the outcome documents of the Geneva phase of the WSIS called for the creation of the WGIG, the *Plan of Action* did not call for intergovernmental negotiations on the subject of establishing the two groups.[440] However, the office of the U.N. Secretary General, through informal contacts with the E.U. Presidency, indicated that E.U. ideas on the composition and organization of the WGIG would be appreciated.[441]

The European Union hoped that phase two of the WSIS would yield the creation of a political document issued by Heads of State and Government that would include a political preamble and focus on operational elements relevant to implementing the

---

[438] Transmission Note for the Attention of E.U. Heads of Mission. *WSIS: Information Exchange of Views Between E.U. Heads of Mission and the ITU Secretary General, Mr. Utsumi* (Geneva, 17 November 2004). See also: Letter from Yoshio Utsumi, "World Summit on the Information Society, Tunis Phase, Tunis, 16-18 November 2008" (2 June 2004). (DM-1138)

[439] Transmission Note for the Attention of E.U. Heads of Mission. *WSIS: Information Exchange of Views Between E.U. Heads of Mission and the ITU Secretary General, Mr. Utsumi* (Geneva, 17 November 2004), 3.

[440] Markus Kummer *Report by Mr. Markus Kummer, Head of the Secretariat of the Working Group on Internet Governance,* <http://www.itu.int/wsis/docs2/pc1/wgig/kummer.pdf>.

[441] E.U. Presidency Non-Paper "The Composition of the U.N. Task Force on Financial Mechanism and the U.N. Working Group on Internet Governance" (9 March 2004), 1.

Geneva *Declaration of Principles* and *Plan of* Action. The E.U. was against the idea of a political charter.[442]

In addition, the E.U. identified security as an area where horizontal cooperation would be useful in addressing the issues of cybersecurity).[443] It advocated for close global cooperation, while understanding that many initiatives would require fine-tuning at the local level. The role of the WSIS, as envisioned by the E.U., is one where awareness is raised on the need for effective legislation, international cooperation on enforcement and the need for best technical practices by industry, and user-level awareness of security issues.[444] Finally, Europe suggests that ICANN could improve its performance and structure through a process of internationalizing itself by opening participation to non-American companies and stakeholders.[445]

Latin American countries led by Brazil were only interested in the issue of Internet Governance. One diplomat observed that during informal consultations, the strategy of this small group was "to flood the first Prepcom with numerous concerns regarding the creation, modalities and functioning of the WG with the ultimate objective of establishing a mechanism of 'disguised guidance of the WG via a process of interactive consultations."[446] It was feared that this tactic of introducing a process of interactive consultations leading to a consensus document would reverse any progress

---

[442] Council of the European Union, Ad Hoc Working Party on Preparation of International Conference for Development- World Summit on Information Society (WSIS), "I/A Item Note: SU Strategy Paper on WSIS (7 June 2004), 3.

[443] Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions, "Toward a Global Partnership in the Information Society: Translation the Geneva Principles into Actions: Commission Proposals for the Second Phase of the World Summit on Information Society (WSIS)" (13 July 2004) [Com 2004 480 Final].

[444] Ibid. Toward a Global Partnership in the Information Society.

[445] Council of the European Union Working Party on Telecommunication and Information Society World Summit on Information Society (WSIS): Internet Governance- Guidelines for Discussions in the WSIS Framework (7 October 2004) 4.4.

[446] Greek Delegation, Preliminary Thoughts on the State of Play Regarding the Preparatory Process of Phase Two (22 June 2004) 1.

made by the WGIG experts by reintroducing tensions that surfaced in the intergovernmental talks.[447]

Intergovernmental Preparatory Conference-One

PrepCom-1 took place on 24-26 June 2004 in Hammamet, Tunisia. This meeting's outcome was the agreement on the outline of the preparatory process. This served as a roadmap for the Tunis phase of the Summit designed to allow participants to focus on drafting the relevant document for the Tunis phase, and not to reexamine the agreements negotiated during the Geneva phase.[448] Therefore, much of the work conducted here focused on the structure and thematic issues that the working groups, including the WGIG would focus on in the lead-up to PrepCom-2.

The contributions of the United States to PrepCom-1 are indicative of its strategy to deal with the ICANN issue. In its published comments, the U.S. focused on its efforts to bridge the digital divide, an issue far more important to the developing world than Internet governance.[449] Cybersecurity was mentioned, however not within the context of Internet governance. This is in stark contrast with the position of the E.U., which noted its intention to actively contribute to the dialogue on Internet governance as well as issues aiming to bridge the digital divide during the Tunis phase of the WSIS.[450] Thus, the fact that the U.S. refrained from mentioning Internet governance in its position paper is

---

[447] Ibid.
[448] World Summit for the Information Society, *Note by the President of PrepCom* (WSIS-II/PC-1/DOC/5-E), http://www.itu.int/wsis/docs2/pc1/doc5.pdf.
World Summit on the Information Society, Final Report of the Preparatory Meeting: PrepCom-1 of the Tunis phase (WSIS-II/PC-1/DOC/6-E) <http://www.itu.int/wsis/docs2/pc1/doc6.pdf>.
[449] *United States Position on Phase II of the World Summit on the Information Society*, http://www.itu.int/wsis/docs2/pc1/contributions/us.pdf.
[450] *Preliminary E.U. Views on the Preparatory Process for the Tunis Phase of the Summit, http://www.itu.int/wsis/docs2/pc1/contributions/eutext.pdf.*

indicative of its attitude toward this issue throughout this and other international processes.

Second Intergovernmental Preparatory Conference

PrepCom-2 took place from 17-25 February 2005 in Geneva, Switzerland.

The PrepCom Chair informed E.U. heads of mission that he preferred that substantive discussion of Internet governance be avoided during PrepCom-2, which should instead focus on creating a general framework for discussion during PrepCom-3 and the Summit based on an interim report of the WGIG.[451]

A Clash Between European and U.S. Views on Internet Governance Between PrepComs

In between the two PrepComs, Europe continued its trend of working on issues of Internet governance in order to better inform the WGIG. Internal debates included a suggestion by France that:

> The new cooperation model should be based on a combination of the current bottom-up public-private partnership, with a light, fast-reacting and flexible oversight entity. This entity would provide a platform for policy dialogue in the interest of all governments.[452]

The suggestion that a formal entity should be established (and by extension replace ICANN), went beyond the E.U.'s language which stuck to the WSIS position of creating a transparent multi-stakeholder framework based on democratic principles. In its final report, the E.U. argued that existing mechanisms and institutions should not be replaced,

---

[451] Council of the European Union, *Transmission Note: Principal Results of the Regular Meeting of Heads of Mission)(Geneva 15 December 2004),* 3.

[452] Presidency of the Council of the European Union, *World Summit for the Information Society- Guidelines for the Exchange of Views at the Council* (Brussels 20 June 2005: 10144/05).

but built on existing structures of Internet governance where public-policy issues of Internet governance could be dealt with in multilateral environment.[453]

After the above declaration, the U.S. National Telecommunications and Information Administration, a bureau of the U.S. Department of Commerce, issued a statement affirming its position that U.S. command and control of ICANN and the DNS system would not be relinquished. While recognizing that country-level domain names should be controlled at the national level, the U.S. reiterated the principle that:

> ICANN is the appropriate technical manager of the Internet DNS. The United States continues to support the ongoing work of ICANN as the technical manager of the DNS and related technical operations and recognizes the progress it has made to date. The United States will continue to provide oversight so that ICANN maintains its focus and meets its core technical mission.[454]

The statement concluded by emphasizing that the "United States will continue to support market-based approaches and private sector leadership in Internet development broadly."[455] Thus, the U.S. then, as today, refuses to let go of its control of ICANN, and as part of its negotiating tactic, has shifted its attention to the issue of bridging the digital divide.

Post-WSIS: Continuing Conflict in the Fields of Cybersecurity and Internet Governance in the Global Cybersecurity Agenda

---

[453] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS *Towards a Global Partnership in the Information Society: The Contribution of the European Union to the Second Phase of the World Summit on the Information Society (WSIS)* Brussels, 02.6.2005 COM(2005) 234 final.

[454] National Telecommunications and Information Administration, Domain Names: U.S. Principles on the Internet's Domain Name and Addressing System (30 June 2005). <http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm>.

[455] Ibid.

On 26 June 2008, the High Level Experts Group (HLEG) for the Global Cybersecurity Agenda (GCA) met at ITU headquarters in Geneva to discuss its recommendations for the ITU Secretary General in the group's five work areas. The GCA is important, since the ITU has institutionalized and operationalized this concept at the International Multilateral Partnership Against Cyber Threats (IMPACT) hosted in Cyberjaya, Malaysia. As of March 2009, all ITU Member States have joined this effort.

The objections of the United States and Canada on the inclusion of the term "data-espionage" in working group on legal issues recommendations. Their view was that they were unclear as to what "data-espionage" refers to, and they required further clarification. Greece might have contributed to this section of the report mentioning the Vodafone phone-tapping case, known to cybersecurity experts as "The Athens Affair," as a good case of data-espionage that could be used as a model to help clarify the definition.

The working group on legal issues could not reach an agreement on the main issue of the Domain Name Server (DNS), an area that continues to be contentious. The United States, Canada, and corporations based in those countries (i.e. Cisco Systems, AT&T, and Microsoft) held the view that the ITU is not mandated to regulate and manage systems such as DNS. They argued that the recommendation, which included language specific to DNS and identity management, should be left out of the recommendations to the ITU Secretary General. Syria, Saudi Arabia, and Brazil held an opposing view. They felt that their country-level top-level domain names (ccTLD, e.g. *.gr*) were not guaranteed protection, since at any time ICANN, which is under U.S. control, could delete the ccTLD. Syria specifically stated that it could compromise on language stating "identity

management, including DNS…"[456] Despite interventions by the ITU Secretary General advising meetings participants that they were there in a personal capacity, and not as representatives of their respective nation-states, no compromise could be found. In the end, the members agreed to submit their recommendations to the Secretary General via the HLEG Chairman in the form of a Chairman's report. This report would highlight the two opposing positions, and describe the positions of each party.

A second major area of contention, primarily raised by Brazil, was on the use of the Council of Europe's Convention on Cybercrime as a model document which the ITU Secretary General should recommend to Member States to ratify and use as a model in their legislation. Brazil argued that because it was not a member of the Council of Europe it and other could be scared away from efforts that highlight this document. Saudi Arabia countered that it is a useful regime, and language of compromise was offered in which "relevant members" would have to ratify the convention.

The rest of the points were mainly centered on representatives of the United States and U.S. corporations objecting on the grounds that certain elements of the recommendations were not part of the ITU's mandate. These elements include the ITU conducting a study of the structure of the Internet, including DNS, and organizing international conferences on cyber security. The main response, voiced mainly by Saudi Arabia and Syria, was that if the ITU's mandate was conservatively interpreted, there should be no HLEG or other cyber security talk within ITU, since it is primarily a telecommunications organization. The United States and Canada were constantly reminded that it is the job of Member States, and not HLEG, to review the ITU mandate.

[456] Author's notes from the 26 June 2008 HLEG meeting.

Agreement was made on a number of other important issues, mainly regarding the awareness of cybersecurity risks, and the need to educate the end-user on the issues of cybersecurity. Experts agreed that there must be a reduction in the number of issues presented, since many overlapped as they stood. This was offered as a way to help focus on recommendations regarding essential elements.

In Work Area-5 (International Cooperation), the primary strategic recommendation was to endorse a framework for dialogue in which all countries could respond to cyber-attacks efficiently and effectively, and each country would have authorities to work domestically and internationally. The three levels of cooperation identified are:

- International-Intergovernmental
- Regional- Intergovernmental
- Private-Public Partnerships

The ITU is mandated with a leading role in these fields under ITU-Telecom and ITU-Development divisions. Thus, it was suggested that a focal point for all ITU cybersecurity activities be created. This focal point would permit contribution of HLEG's work, and would focus its functions on:

- Cooperation improvement
- Take the lead in coordinating others and avoid the duplication of other activities
- Secretary General should moderate the study for line C.5 (WSIS)

During informational discussions with HLEG members, the Estonian delegate told me that Estonia welcomed the May 2007 cyberattacks, since it allowed them to produce a model for themselves and the international community on how to better fend off future attacks. A Canadian expert informed me that the best way to move forward on cybersecurity was to levy fines and penalties against end-users who do not take adequate

measures to protect their information systems. These fines, he argued, should be structured in a similar way to those existing for drivers that do not wear safety belts.

The analysis of the cybersecurity and Internet governance discussions at WSIS Intergovernmental meetings provides insight to what decisions states have made or not made. Decisions have been made on the importance of raising awareness of the cybersecurity policy issue, the need to harmonize domestic laws, and the need for the cooperation between private industry and government to secure information infrastructures. The main areas of disagreement are between the U.S. and most of the rest of the world on the issue of Internet governance, specifically as it pertains to the opening up DNS and ICANN to a group of international stakeholders. The U.S. objects to this on the grounds that the system is working just fine in its current configuration. Furthermore, the U.S. objects to the inclusion of legalistic language to describe some actions, as well as to the idea of drafting an international convention for cyberspace. The Russians, on the other hand, are eager to bring the world to the negotiating table. Overall, the areas of disagreement cannot be resolved without the U.S. shifting its position. Since the U.S. controls the Internet infrastructure, it is unlikely that this position will change in the near future.

Chapter Eight
Promises and Pitfalls of the U.S. National Strategy to Secure Cyberspace[457]

It seems paradoxical that entities other than national governments working under the auspices of international institutions of diplomacy would be tasked with governing any domain, since governance is the responsibility of governments. As Aristotle correctly suggested, the political system exists to eliminate the bias of individuals to the best extent possible. This is not to say that the private sector is guilty of taking advantage of its position as the driving force developing the technology upon which the information society is based. It is quite the contrary. One must keep in mind that national governments were the chief negotiators of the *Declaration of Principles*, *Tunis Agenda* and *Tunis Commitment*. Therefore, it appears that governments are shying away from their responsibilities to provide security in hopes that the private sector and individuals will do the job for them with some legislative guidance. This becomes apparent when reviewing the United States' *National Security Strategy to Secure Cyberspace* (NSSC). This document is important, since the U.S. founded the Internet and thus "has important knowledge and experience" in cybersecurity.[458] In the field of the private-public partnership, the NSSC dictates that:

[457] This chapter was originally a case-study written for the Project for National Security Reform (PNSR), a program funded by Congress to examine how U.S. interagency cooperation in the National Security Council should be reformed to address 21st century threats.

[458] International Telecommunications Union. Research on Legislation in Data Privacy, Security and the Prevention of Cybercrime.

> The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector. The federal government should likewise not intrude into homes and small businesses, into universities, or state and local agencies and departments to create secure computer networks. Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible.[459]

It is therefore apparent that national governments are placing the burden of cybersecurity on the private sector, which has gladly taken up the task. This has been described as a "wonk" approach to cybersecurity.[460]

In the United States, the picture continues to be bleak with regard to the public-ordering of cybersecurity. On the one hand, the Department of Homeland Security has announced a "Manhattan Project" for cybersecurity. Disappointingly, its aim and scope is solely "to protect the federal domain and ensure the security, resiliency and reliability of the nation's information, technology and communications infrastructure.[461] The view of the private sector and individuals being responsible for their own cybersecurity continues to permeate government thinking. According to Secretary Michael Chertoff:

---

[459] President George W. Bush. *National Security Strategy to Secure Cyberspace* (Washington, D.C.: The White House, 2003) 11.

[460] Greg Garcia, "Forging a Private-Public Partnership: The Wonk-Free Approach to Cybersecurity" in *Cutter IT Journal* (19 No. 5, 2006) 21-35.

[461] Michael Chertoff, "Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference," 8 April 2008, < http://www.dhs.gov/xnews/speeches/sp_1208285512376.shtm> cited on 9 April 2008.

> The federal government does not own the Internet, thank God, and it doesn't own the nation's cyber networks. You own the Internet and the nation's cyber networks. The federal government cannot be everywhere at once over the Internet or in cyberspace. There is a network that operates within that domain. And as a consequence, the federal government cannot promise to protect every system, let alone every home computer from an attack.[462]

This logic, which is tantamount to saying that everyone is responsible for protecting their own home from attack since the police force cannot be everywhere, continuously. Until public law enforcement takes the lead in securing cyberspace, with the private sector playing an important but secondary role, the Information Society will not maximize the utility of network.

Human activity is increasingly being transferred to, and becoming reliant on, cyberspace. Governments, militaries, critical infrastructures, businesses, and societies now depend on information and communications technology (ICT) to function. The reliance of the United States on such systems, the possible misuse of the cyber-domain by violent non-state actors (VNSAs) such as terrorists, and the proliferation of nation-state strategic information warfare programs has raised awareness of the need to incorporate cybersecurity strategies into U.S. foreign and national security policies.

Recall that the strategic definition of cyberspace is "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure."[463] Contrary to the popular metaphor, this definition indicates that cyberspace is a physical domain composed of electronic hardware and software internetworked through and powered by the

---

[462] Ibid.

[463] *The National Military Strategy for Cyberspace Operations,* 2006. As read in: Sgt. C. Todd Lopez, "Fighting in Cyberspace Means Cyber Domain Dominance," in *Air Force Print News* (28 February 2007) <http://www.af.mil/news/story.asp?id=123042670> (cited on 6 July 2008).

electromagnetic spectrum to communicate and store information. Thus, cyberspace constitutes more than the Internet or World Wide Web (WWW), although both comprise its most recognizable elements. In the modern era, cyberspace is an extension of earth's environment just as sea, air, and outer space are. Like these other spaces, it is considered a global commonage.[464]

To date, there has been no (unclassified) large scale, nationally significant event from which to judge the costs of an attack on ICT critical to U.S. national security. Other nations have not been as fortunate. Russian hacker networks indirectly linked to the Kremlin opened a devastating cyber-front against Estonia in 2007 as part of a political protest. During the recent war against Georgia, Russian hackers instigated a front in cyberspace the night before conventional forces began their operations. Over the years, China-based hacker networks have managed to extract forty terabytes of information critical to U.S. national security from cyberspace.[465] Such incidents demonstrate that cyberattacks are not limited to the realm of imagination. Challenges to securing cyberspace go beyond preventing the corruption of information system's distributed denial-of-service (DDOS): espionage is an additional challenge.[466] These recent events point to the importance of federalizing cybersecurity. Many military analysts believe cyber defense and attack will be vital to future military efforts. Indeed, according to Lani Kass, director of the Air Force's Cyber Task Force, "We are already at war in

---

[464] David J. Bederman, *Globalization and International Law (*New York: Palgrave-Macmillan, 2008) pp. 36-49.

[465] *Report to Congress of the U.S.-China Economic and Security Review Community* (November 2007). I thank Josh Lampen for providing the exact number of terabytes and for other insights on cybersecurity that informed this paper.

[466] Martin Libicki, Conquest in Cyberspace: National Security and Information Warfare (Cambridge: CUP, 2007) pp. 74-84.

cyberspace," as countries and terrorists are currently carrying out cyber attacks on U.S. interests. Kass points out that "Chinese attacks on DOD [Department of Defense] networks are on the upswing, and China is now the United States' peer competitor in cyberspace."[467] Any reorganization of the U.S. government will have to take into account this new form of warfare, as it is decentralized and transnational and transcends traditional conceptions of national security.

The *National Strategy to Secure Cyberspace* (NSSC) is to date the leading relevant executive branch directive on cybersecurity. The NSSC mandates the Department of Homeland Security (DHS) as the lead agency for cyberspace response within which federal, state, and local agencies coordinate and react to cyber-attacks. The *Cyber Incident Annex* of the *National Response Framework*, which defines standard operating procedures for the interagency response to a cyber incident, and the first *Cyber Storm Exercise Report,*[468] are additional government reports that provide insight into the current cybersecurity strategy.

There is a surfeit of analysis from experts on which to base an assessment of the current U.S. cybersecurity strategy. Current strategy calls for the formation of private-public partnerships (P3) in which the private sector is asked to secure its own networks. Dan Verton, in *Black Ice: The Invisible Threat of Cyber-Terrorism*, and Neal K. Katyal, in *The Dark Side of Private Ordering: the Network/Community Harm of Crime*, both analyze the flaws of the P3 approach. Levon Anderson, in *Countering State-Sponsored*

---

[467] Levon Anderson, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" in *Information as Power: An Anthology of Selected United States Army War College Student Papers*, (Eds.) Jeffrey L. Groh, David J. Smith, Cynthia E. Ayers, William O. Waddell (Carlisle Barracks, Pennsylvania: U.S. Army War College) pp. 105-122, 106.

[468] These exercises have been organized by DHS and conducted across the interagency and include the private sector as well as select international partners.

Cyber Attacks: Who Should Lead?, identifies an overlap between DHS's responsibilities and those of the DOD. This redundancy, according to some analysts, can be attributed to policymakers not adjusting to the realities of transnational security threats, such as netwar, a form of conflict John Arquilla and David Ronfeldt conceptualize in their monograph *The Advent of Netwar*. Arquilla and Ronfeldt argue that vertical (hierarchical) organizations cannot efficiently or effectively fend off horizontally (networked) organized adversaries. Only networks can fight networks, they argue. Thus, the U.S. bureaucracy and most nation-state bureaucracies as they are currently formed are ill equipped to counter netwar. This does not mean that hierarchies should be done away with, and they identify interagency mechanisms as the natural setting for networked responses to security threats.

These and other sources reviewed for this case suggest the following answers to PNSR's guiding questions:

1. *Strategy: Did the U.S. Government generally act in an ad hoc manner or did it develop effective strategies to integrate its national security resources?*

The NSSC is the codification of earlier Presidential Directives and laws into a coherent national strategy. As per NSSC mandate, DHS is assigned as the lead agency to serve as a federal focal point for the coordination of government and industry cybersecurity efforts. As noted in the *Cyber Incident Annex* of the *National Response Framework,* during a cyber-attack, the Interagency Advisory Council (IAC)[469] and National Cyber Response Coordination Group (NCRCG) are the main mechanisms activated to coordinate the interagency response within the National Cyber Security Division (NCSD)

[469] The Interagency Incident Management Group (IIMG) was renamed IAC in 2006.

at DHS. Upon the detection of an attack, the Director of Homeland Security activates the IAC, which is comprised of senior representatives from 13 Federal agencies. The NCRCG provides expertise to the IAC and facilitates a harmonized response to a cyber-attack. To date, these mechanisms have only been activated during crisis management exercises. Additionally, the NSSC grants private industry significant responsibility to secure cyberspace. This element of strategy has drawn criticism from experts. Furthermore, modifications to the NSSC were made with the issuance of the classified Presidential Directive 54/Homeland Security and Presidential Directive 23 in 2008, which detailed a Comprehensive National Cybersecurity Initiative (CNSI). Part of this initiative is the creation of the National Cyber Security Center (NCSC) within DHS to secure cyberspace vital to national security.

2. <u>*Integration:*</u> *How well did the agencies/departments work together to implement these ad hoc or integrated strategies?*

The implementation of the NSSC strategy for responding to and preparing for cyber-attacks among agencies and departments has proceeded well in most key areas. The DHS/NCRCG/IAC have demonstrated through crisis management exercises their utility in coordinating a response to a cyber incident of national significance. However, there is a significant lapse in implementing the cybersecurity strategy within individual agencies/departments. To address this, the NCSC is tasked with securing all federal information systems. Another point of concern brought up in the secondary literature with regard to cooperation involves information sharing limitations between DHS and the private sector, since the private sector tends to withhold information on the threats to and vulnerabilities of their systems out of fear that their customers will discontinue their

patronage after discovering a networks' weakness.

3. *Evaluation: What variables explain the strengths and weaknesses of the strategy?*

Following the guidelines of the NSSC, DHS has produced an interagency mechanism to secure cyberspace. However, DHS exercises indicate that limitations exist in implementing the strategy due to the technological complexity of the subject and lack of private-sector understanding of federal security postures after activation of the IAC and NCRCG. In addition, competing priorities and limited resources make it difficult to implement the strategy. Within individual departments and agencies there is a lack of personnel trained in cybersecurity. Additionally, the private sector and intelligence community's unwillingness to share information with non-members contributes to the weakness of current cybersecurity efforts. This, combined with similar secrecy concerns within DOD, obstructs cybersecurity information sharing. Overlapping responsibilities with various DHS units, limited available resources to deal with the multitude of competing priorities, redundant capabilities in various government departments and agencies, and the lack of an integrated mechanism for coordinating response are additional variables contributing to the weaknesses in the strategy. While the current structure allows the Federal government to respond in a somewhat networked manner to networked threats, the above-mentioned flaws and the strength of hierarchical structures hinder such efforts. Moreover, the current strategy relies on a private sector led effort to secure non-government computer networks while focusing on the impact of crimes against individuals and hostile conquest. These emphases overlook the community effect of cyber threats and the potential harm that may result from friendly competitors developing technology upon which the U.S. becomes dependent. Finally, the inherent

insecurity of Internet communication protocol (TCP/IP), domain name-server (DNS) and other technical variables makes pinpointing the origin of an attack difficult, thereby complicating the response to a security breach.

4. *Assessment: What diplomatic, financial, and other achievements and costs resulted from these successes and failures?*

The United States continues to face significant risk from cyber-attacks. Although DHS leads the interagency response to such threats, and DOD is also organized and equipped to respond to cyber-attacks, failure to plug holes in federal and private critical information systems leaves U.S. cyberspace interests vulnerable to both amateur and professional attackers. Thus far, cyber-assaults of particular note have been Chinese efforts (such as Titan Rain and Byzantine Foothold) indirectly linked to the People's Liberation Army (PLA). These attacks are best described as cyber-espionage, since their scope is geared more towards gathering information rather than destroying ICT. Yet, it has been noted that the full extent of such attacks cannot be known, and it is possible that the hacker networks responsible for carrying them out have left computer programs that may allow for future access to the U.S.'s critical information infrastructure.

Strategy: The U.S. Government Approach to Securing Cyberspace

Conceptualizing Cyberspace

Computer networks are dependent on the positive use of internationally standardized communications protocols, such as the Transmission Control Protocol and Internet Protocol (TCP/IP), to send and receive data packets and information. TCP/IP allows for the flow of data-packets and information across computer networks, including the Internet. TCP/IP is standardized by the International Organization of Standards (ISO)

for the Open Systems Interconnection (OSI) model as the basis of Internet networking. To better understand the significance of TCP/IP, a brief description of how information is sent across networks is necessary. Data-packets are the basic units of network traffic. They are the standard way of dividing information into smaller units when sending information over a network. A significant component of the computer networks is the IP header, which contains information pertaining to the source and destination addresses. Machines require these strings of numbers to connect with other computers on the Internet or other networks.[470] All networked hardware must have a valid IP address to function on a network. Data-packets are recreated by the receiving machine based on information within a header of each packet that tells the receiving computer how to recreate the information from the packet data. Without international standards, such as TCP/IP, there would be no assurance that packets could be read by a receiving machine.[471]

The Domain Name System (DNS) allows people to use Uniform Resource Locators (URLs) to communicate with other machines on the Internet. Instead of entering the IP address of a website, which might look like 67.192.169.178, a person can type the URL http://www.pnsr.org into a web browser to connect with the desired corresponding IP address. This makes the WWW user friendly. IP addresses reside on DNS databases on root servers that allow for the translation of URLs into IP addresses.[472] The top-level domain names, such as .com or .org, are maintained and updated by the Internet Corporation for Assigned Names and Numbers (ICANN), which was once under

---

[470] Robert E. Molyneux, The Internet Under the Hood: An Introduction to Network Technologies for Information Professionals (Westport, CT: Libraries Unlimited, 2003) pp. 85-86.

[471] Molyneux, 27.
[472] Molyneux, 86.

the auspices of the Department of Commerce (DOC). Now operating under a memorandum of understanding with the DOC, ICANN is a private entity responsible for governing and maintaining the DNS database's thirteen root servers that enable global Internet communications.[473]

Vital computer networks that are part of the domain name system are open to electronic attacks. As will become apparent, the trend with computer security officers is to not take the necessary steps to safeguard the domain name system.[474] Common exploits include Denial-of-Service (DOS) and Distributed-Denial-of-Service (DDOS). In both types of attacks, an enormous amount of useless data is sent to a server in an attempt to overload the system and render it inoperable. DDOS attacks are more sophisticated in that thousands of computers controlled by malicious software around the world allow an attacker to mount DOS attacks on a grand scale. technology, combined with the speed, skills and experience learnt by root server operators over the years."[475] Even so, the tangible consequence of a successful attack against the DNS system would mean that the Internet would not be operational until computer programmers could recover from the attack. However, there is a low probability that this could occur given the redundancy of the DNS.

Internet protocols, such as the Internet Protocol version 4 (IPv4), DNS, and the Border Gateway Protocol (BGP) are identified by the NSSC as being prone to security problems.[476] This is significant since critical infrastructures are networked via this

---

[473]ICANN, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority" March 1, 2000, http://www.icann.org/en/general/ietf-icann-mou-01mar00.htm.
[474]Erik Sherman, "DNS: Definitely Not Safe, New Attacks on the Internet's Domain Name Systems Keep CISOs Guessing," in CSO (February 2007) 38-41.
[475] ICANN, Factsheet: Root Server Attack on February 7, 2007, 2.
[476] White House, National Strategy to Secure Cyberspace, February 2003. http://www.whitehouse.gov/pcipbcyberspace_strategy.pdf, 30.

protocol so that key functions may be accessed remotely. University-led efforts to develop next-generation network services exist, such as the Internet2. This new Internet is in an advanced deployment phase at the research and academic levels. However, since the Internet will continue to exist as the global element of cyberspace, the increased security offered by the communication protocols of Internet2 will not benefit users at large in the near-term.[477] The development of Internet protocol version six (IPv6) by the Internet Engineering Task Force is another next-generation effort led by the private sector. This protocol is considered more secure than IPv4 since, among other reasons, it makes available more address space, thereby establishing a system more resistant to DOS and DDOS and other malicious attacks. Recognizing the security benefits of IPv6, the NSSC calls for the DOC to examine and promote its deployment, a call echoed by the National Institute of Standards (NIST). NIST, however, notes that:

> Some key IPv6 design issues remain unresolved. As the USG [U.S. government] begins to undertake significant operational deployments and investments in IPv6 technology, additional efforts are warranted to ensure that the eventual resolution of these design issues remains consistent with USG requirements and investments.[478]

The challenge of securing cyberspace rests in the technical complexities described above. Cyberspace is a dynamic environment where no defense will be perfect, and attackers will have a variety of means available to deny a network's services to users. In addition, if targeting a specific network proves too difficult, taking out its supporting subsystem might prove just as effective.

---

[477] For more information on the Internet2 see: William Jackson, "A Faster Internet Lane" in *Government Computer News (29 September 2008)* < http://www.gcn.com/print/27_24/47246-1.html?page=1>.

[478] Stephen Nightingale, Doug Montgomery, Sheila Frankel and Mark Carson, "A Profile for IPv6 in the U.S. Government – Version 1.0" (National Institute of Standards) <http://www.antd.nist.gov/usgv6-v1-draft.pdf>, 2.

National Strategy to Secure Cyberspace

The NSSC is the main strategy establishing the U.S. government's priorities and response framework for cyber threats. Issued in February 2003, it codified a single coherent approach based on a multifaceted framework established by previous Executive Orders, Presidential Directives, and Congressional Acts addressing threats to and breaches of the security of U.S. ICT.[479] Five critical national cyberspace security priorities are identified in the strategy, including the creation of:

- A national cyberspace security response system
- A national cyberspace security threat and vulnerability program
- A national cyberspace security awareness and training program
- Secure government cyberspace
- Mechanisms for national security and international cyberspace security cooperation[480]

Under the NSSC, DHS is the lead agency tasked with coordinating the State Department, Department of Justice (DOJ), and other Federal, State, and local authorities' responses to a cybersecurity incident. The Office of Cybersecurity and Communications (CS&C) of the National Protection and Programs Directorate, led by the DHS Assistant Secretary for Cybersecurity and Telecommunications, is charged with preparing for and responding to a nationally significant cyber attack. The National Cybersecurity Division (NCSD) has been established within the CS&C to be specifically responsible for efforts to secure U.S. cyber assets.[481]

The concept of operations in the *Cyber Incident Annex* of the *National Response Framework* (hereafter referred to as "Cyber Annex") follows the NSSC's organizing

[479] See Appendix A for a comprehensive list of relevant policy and legislative initiatives.
[480] White House, 3-4.
[481] Organizational details available at http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm

principles. The document provides insight into the conceptualization of any interagency response to a cyber incident of national significance.[482] The Cyber Annex may be supported with DHS's *Emergency Support Function #2 – Communications Annex*.[483] The Cyber Annex coordinates the Federal response, including the following functions:

- Providing indications and warning of potential threats, incidents, and attacks
- Information-sharing both inside and outside the government, including best practices
- Coordination of investigations
- Incident response, and incident mitigation
- Analyses of cyber vulnerabilities, exploits, and attack methodologies
- Conducting investigations, forensics analysis, and prosecution
- Attributing the source of cyber attacks
- Defending against the attack, and
- Leading national-level recovery efforts[484]

The first line of defense against a cyber-attack is DHS's U.S. Computer Emergency Readiness Team (U.S.-CERT), which tracks all cyber-incidents. The principal interagency mechanism for cybersecurity incidents, the National Cyber Response Coordination Group (NCRCG), is informed of any incident via the national cyberspace response system, which relies on U.S.-CERT to identify and analyze incidents. In the event of a cyberattack targeting the nation's critical information infrastructure, DHS/NCRCG is responsible for assisting the Interagency Advisory Council (IAC) on technical matters to facilitate and coordinate the response of thirteen federal agencies, including the intelligence community (IC). The Homeland Security Operation Center (HSOC) is then notified by the NCRCG, which in coordination with the IAC recommends to the Secretary of Homeland Security whether or not he or she should

---

[482] Federal Emergency Management Agency, *National Response Framework, Cyber Incident Annex,* December 2004, < http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf>, 1.

[483] Federal Emergency Management Agency, *Emergency Support Function #2 – Communications Annex,* January 2003, http://www.fema.gov/pdf/emergency/nrf/nrf-esf-02.pdf

[484] Federal Emergency Management Agency, National Response Framework, Cyber Incident Annex, 2.

declare a cyber-incident as an attack of national significance.[485] After such a declaration, interagency responses outlined in the Cyber Annex are implemented to identify the source of an attack, respond to it and assure that those responsible for an attack are held accountable.

Prior to 2008, the NSSC required all Federal agencies to secure their own unclassified information technology (IT) systems.[486] Agencies were required to implement a three step process consisting of: "identifying and documenting enterprise architectures; continuously assessing threats and vulnerabilities, and understanding the risk they pose to agency operations and assets; and implementing security controls and remediation efforts to reduce and manage those risks."[487] The implementation of agency-wide controlling system configurations was encouraged to help facilitate the use of commercially available software in securing an agency's cyberspace. It is implied in the NSSC that the agencies should adopt a policy similar to the one at DOD when selecting commercial ICT software from those evaluated and authorized for use on DOD systems by Pentagon experts.

In recognition of the challenges DHS faces in fulfilling its cybersecurity responsibilities for securing government networks, President George W. Bush signed a classified joint Presidential Directive 54/Homeland Security Presidential Directive 23 in January 2008 detailing a Comprehensive National Cybersecurity Initiative (CNSI).[488] While the fine points of the directive remain classified, key elements include:

---

[485] Ibid, 4.
[486] White House, 44.
[487] White House, 45.
[488] Ellen Nakashima, "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions," *Washington Post,* January 26, 2008 p. A03.

- Limiting connections between government networks and the Internet by cutting the number of portals from 4,000 to about one hundred
- A passive intrusion prevention plan to identify instances of unauthorized access to computer networks
- An active intrusion prevention program to identify the source country and person responsible for any intrusion
- A counterintelligence strategy to deter security breaches on networks
- A program to create counterintelligence tools for cyber forensic analysis
- Training programs to develop skills required to improve security
- Fusing the operations of network operations centers of an unknown number of agencies
- Cyber R&D for offensive and defensive purposes, including leap-ahead technologies to win a cyber arms race
- Private-public partnerships for critical infrastructure protection
- A project analogous to President Eisenhower's Solarium in which multiple teams develop and debate national strategies to deter cyber war
- Improve federal acquisitions to assure ICT used is secure[489]

The CNSI reiterates many of the points found in NSSC and Cyber Annex, although it adjusts the mission of the IC, assigning it further cybersecurity responsibilities. An IC task force headed by the Office of the Director of National Intelligence (ODNI) now coordinates passive and active intrusion prevention efforts.[490] This represents a shift from the role of the IC envisioned in the NSSC, since the IC is now tasked with monitoring and securing federal unclassified computer systems within the .gov domain, whereas in the NSSC, the IC was responsible only for classified systems. Furthermore, the directive called for a new National Cyber Security Center (NCSC) under DHS's hierarchy to protect unclassified government computer networks by limiting the number of non-secure external Internet connections. This directive therefore gives the intelligence community a clearer role in protecting U.S. cyberspace, and indicates flexibility in revising the role of other agencies and departments when their mandates under the NSSC

[489] Brian Grow, Keith Epstein, and Chi-Chu Tschang, "The New E-Spionage Threat: A Business Week probe of rising attacks on America's most sensitive computer networks uncovers startling security gaps." In Business Week (April 21, 2008).
[490] Ibid.

are deemed insufficient.

Emphasis on P3

Partnerships between the government and private industry are identified as essential components of effective implementation of the NSSC. Specifically, the NSSC states that:

> The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector. The federal government should likewise not intrude into homes and small businesses, into universities, or state and local agencies and departments to create secure computer networks. Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible.[491]

Thus, the strategy discourages the use of federal regulations as a means to secure cyberspace, and instead advocates for the market "to provide the major impetus to improve cybersecurity."[492] Government involvement is "limited to those cases when the benefits of intervention outweigh the direct and indirect costs." [493] These cases include scenarios in which critical infrastructures, such as water-treatment facilities, are threatened by sophisticated hackers. In *Black Ice: The Invisible Threat of Cyber-Terrorism,* Dan Verton quotes National Security Council (NSC) officials working in the field of cybersecurity as saying, "the concept of allowing market forces to dictate security requirements remains the centerpiece of the [G.W. Bush] administration's policy on national cybersecurity… government regulation of Internet and software security

---

[491] White House, 11.
[492] White House, 15.
[493] White House, 14.

requirements is out of the question."[494] However, Verton suggests that by pursuing such approaches to security in cyberspace, the government has abandoned its national security responsibilities.

Integrating Elements of National Power

An effective response to a cyber incident of national significance requires a quick and well-coordinated response by all relevant actors. In June 2008, the Government Accounting Office (GAO) considered the integration of cybersecurity offices and centers within the U.S. government as critical for prompt government action. This included the integration of DHS/US-CERT and the National Coordinating Center for Telecommunications (NCC). The NCC is jointly run by the Federal government and the telecommunications industry to coordinate the exchange of information among participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.[495] The GAO notes that DHS/US-CERT and the NCC have overlapping missions in the areas of:

- Developing and disseminating warnings, advisories, and other urgent notifications
- Evaluating the scope of an event
- Facilitating information sharing
- Deploying response teams during an event
- Integrating cyber, communications, and emergency response exercises into operational plans and participation
- The management of relationships with others, such as industry partners[496]

Partially heeding GAO advice, DHS moved the NCC to offices adjacent to US-CERT in

---

[494] Dan Verton, Black Ice: The Invisible Threat of Cyber-Terrorism (Emeryville, California: McGraw-Hill 2006) p. 25.

[495] NCC Operating Charter < http://www.ncs.gov/ncc/nccoc/nccoc_background.html>.

[496] United States Government Accountability Office. "Report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology" (Committee on Homeland Security, House of Representatives Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks (June 2008), 11.

November 2007. The two centers now have adjoining office space and share common software used to "identify and share physical, telecommunications, and cyber information related to performing their missions."[497] However, they have not been merged into one joint operations center as recommended by GAO. Furthermore, GAO identifies the NCSD and the National Communication System (NCS) as two centers requiring integration due to overlaps and duplication of some of their functions. However, an organizational merging of the functions of the NCSD and NCS has not occurred due to competing priorities, such as implementing Presidential Directive 54.[498] A DHS-commissioned expert task force recently explained, "that without an organizationally integrated center, the department will not have a comprehensive operating picture of the nation's cyber and communications infrastructure and thus not be able to effectively implement activities necessary to prepare, protect, respond, and recover this infrastructure."[499] It is unclear from media reports whether the mission of the newly created NCSC is to eliminate this and other overlaps.

DOD and DHS

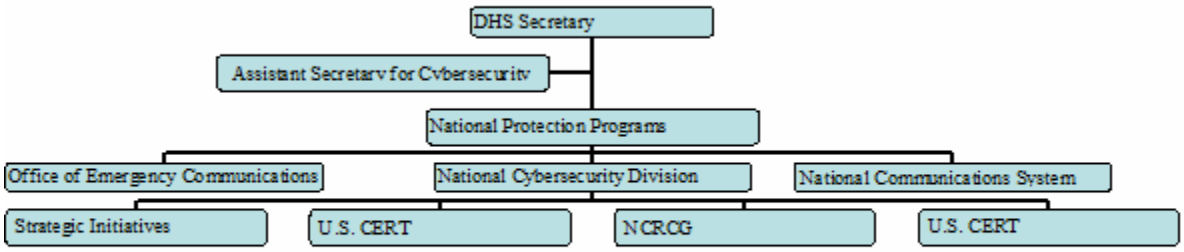
DHS and DOD are both coordinating agencies in the *Cyber Annex*. With DHS, DOD is tasked with cooperating with other Federal entities, when appropriate, to "provide attack sensing and warning capabilities, gather and analyze information to characterize the attack and to gain attribution of the cyber threat, participate in information-sharing, offer mitigation techniques perform network intrusion diagnosis and provide technical

---

[497] United States Government Accountability Office. "Report to the Subcommittee on Emerging Threats."
[498] United States Government Accountability Office. "Report to the Subcommittee on Emerging Threats" 12.
[499] United States Government Accountability Office. "Report to the Subcommittee on Emerging Threats" 14.

expertise."[500] US-CERT and the DOD's Computer Emergency Response Team Coordination Center (CERT-CC) serve as the primary communication channel between the two departments. Within the DOD, the overall responsibility for cybersecurity rests with the Joint Functional Component Command (JFCC) for Network Warfare and the JFCC-Space & Global Strike. Defending against cyber-attacks is the responsibility of the Joint Task Force-Global Network Operations and the Joint Information Operations Warfare Center. Carnegie Mellon's Software Engineering Institute is contracted to operate the DOD CERT-CC.[501] There are five core capabilities of DOD in cyberspace: (1) Psychological Operations, (2) Military Deception, (3) Operational Security, (4) Computer Network Operations, and (5) Electronic Warfare.[502]

Organizational Chart of DHS Cyber-Defense



In *Countering State-Sponsored Cyber Attacks: Who Should Lead,?* Levon Anderson questions the current strategy of having both DHS and DOD play key roles in

[500] *Cyber Annex*, 6.
[501] Clay Wilson, Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues (CRS 5 June 2007), 11.
[502] Wilson, 1.

cybersecurity.[503] While DHS does have an important role in coordinating the national defense and response to attacks on U.S. cyberspace, Anderson identifies overlapping capabilities with DHS and DOD, such as their cyber-incident response systems. Comparing DHS and DOD, he argues that overall, DOD is better suited as the focal point for responding to organized or state sponsored cyber-attacks.[504] Specifically, when responding to a cyberattack:

> DHS would also be heavily dependent on DOD for technological support as well as relying on DOD's extensive experience with information warfare. However, individual state Governors could activate and control National Guard resources through the State Adjutant General, who could coordinate cyber actions with DHS. This could alleviate DHS resource issues. This, however, will not help with legal issues where the cyber war expands across international borders via the Internet. So to recap the analysis, DOD has a clear advantage over DHS in the matter of resources (i.e., Guard, Reserve and Active forces and budget), technical operational experience (daily attacks/defense), and technological capabilities.[505]

DHS's cybersecurity response system is very important in coordinating the interagency planning to respond to cyberattack, since "total commitment by all responsible agencies is needed and expected to win the cyber war." However, Anderson recommends that "designating the DOD as the overall lead element during an actual attack will better facilitate overall command and control and unity of effort."[506] Therefore, "DOD seems to be the logical choice to lead the effort against an attack," since it still has the resources to be the lead agency responsible for military responses to events threatening U.S.

---

[503] Levon Anderson, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" in *Information as Power: An Anthology of Selected United States Army War College Student Papers*, (Eds.) Jeffrey L. Groh, David J. Smith, Cynthia E. Ayers, William O. Waddell, 105-122, http://www.carlisle.army.mil/DIME/documents/InfoasPowerVol2.pdf.117.

[504] Anderson, 110-114.

[505] Anderson, 118.

[506] Ibid.

cybersecurity.[507] However, DOD's operational ability within the United States is limited to national emergencies under the *Posse Comitatus Act* (PCA). Furthermore, DOD Directives 3025.12 and 5525.5 also regulate law enforcement-military cooperation, largely constraining their interaction to times of civil disturbances.[508] Experts have suggested that the PCA is misunderstood by soldiers and scholars, since many regard it as the codification of the founding father's fear of a standing army, rather than a Congressional limitation on use of the military in domestic law enforcement.[509] It is noted that DOD Directive 5525.5 requires updating, since the nature of threats to national security have changed since 1986 when the directive was issued.[510] Even so, the limitation to non-law enforcement activities makes the DOD of little use as the lead actor responsible for cybersecurity in cases that do not pose a national emergency. DOD and civilian law enforcement agencies operate under different rules of engagement. Thomas Lujan, in *Legal Aspects of Domestic Employment of the Army,* notes that "before decision-makers bring our military forces to bear, the situation must be so potentially harmful (seized nuclear weapon, biological or chemical weapon of mass destruction) that the United States must react to it as if it is an act of war—not just a crime."[511] This observation is also relevant in cyberspace, thus DHS may still be the appropriate lead prior to such an emergency.

State Department and DOJ

---

[507] Anderson, 119.
[508] See: U.S. Code 1385. *Use of Army and Air Force as Posse Comitatus*. See also:*DOD Directive 5525.5*, January 15, 1986, http://www.dtic.mil/whs/directives/corres/pdf/552505p.pdf.
[509] Colonel Thomas D. Cook, *The Posse Comitatus Act: An Act in Need of a Regulatory Update* (U.S. Army War College, 2008), 13.
[510] Colonel Thomas D. Cook, The Posse Comitatus Act: An Act in Need of a Regulatory Update (U.S. Army War College, 2008).
[511] Thomeas R.Lujan, "Legal Aspects of Domestic Employment of the Army" in *Parameters* (Autumn 1997) https://carlisle-www.army.mil/usawc/Parameters/97autumn/lujan.htm.

A response to any cyber-incident requires the identification of the origin of an attack. This is easier said than done. Sophisticated DDOS attacks may be launched via computers located in different countries. The owners of those computers may be completely unaware that their systems are infected with malware that allows attackers to gain access remotely. Thus, prudent national efforts alone cannot assure cybersecurity. Instead, security requires foreign policy objectives aimed at advancing a global culture of cybersecurity.

The NSSC tasks the State Department with the coordination of international outreach on global cybersecurity issues. The State Department mission includes the fostering of international cooperation in investigating and prosecuting cybercrime.[512] The International Communication and Information Policy (CIP) group, part of the Bureau of Economic, Energy and Business Affairs, is a significant component of this effort. One of the most pressing problems in investigating cybercrime is that domestic laws pertaining to the misuse of ICT vary from country to country. Double-criminality has been identified as a significant obstacle in extraditing cybercriminals.[513] If the U.S. requests the extradition of a cybercriminal so that he may be tried in U.S. courts, the nation that harbors the cybercriminal may refuse the request if they have no legislation criminalizing the action. For example, Onel A. de Guzman, creator of the "I Love You Virus" that infected ten percent of the computers connected to the Internet causing $5 billion in damages worldwide, was able to escape prosecution since no laws prohibiting computer

---

[512] White House, 51.

[513] John F. Murphy, "Computer Network Attacks by Terrorists: Some Legal Dimensions," In *Computer Network Attack and International Law,* Michael N Schmitt & Brian T. O'Donnell (eds). International Law Studies, 76 (Naval War College, Newport, Rhode Island 2002), 324-351.

virus programming existed in the Philippines.[514] Thus, the harmonization of domestic laws internationally is a key aspect of ensuring cybersecurity.

The NSSC identifies the Council of Europe's Cybercrime Convention (hereafter COE Convention) as a useful diplomatic tool that can help facilitate an effective response to a cyberattack. This convention aims to harmonize international cyber laws to enhance security by serving as a model text for national legislation.[515] States are urged to sign the convention, which eliminates problems of extradition and double-criminality (meaning a cyber criminal cannot rely on loopholes in domestic legislation). Thus, the State Department plays an important role in fostering a global culture of cybersecurity by encouraging countries to work within the framework being created to deal with the transnational aspects of cyber-crime.

The State Department's efforts complement the DOJ and FBI's investigation and prosecution of cybercriminals. However, the DOJ/FBI efforts are geared towards gathering information with which to prosecute an attacker. This can support the missions of agencies tasked with responding to attacks since DOJ/FBI use their resources to identify the source of an attack, which then allows for other agencies to respond appropriately.[516]

---

[514] Michelle Delio, "Why Worm Writers Stay Free" *Wired* (December 27, 2001) http://www.wired.com/politics/law/news/2001/12/49313.

[515] The COE cyber-crime convention is a document which aims to facilitate international cooperation on the issue of combating criminal and VNSA uses of cyberspace. The convention intends to harmonize the national legal measures of E.U. member states which pertain to cyberspace and its criminal uses. Coordinating these laws helps remove obstacles and facilitates the sharing of information between states during and after a computer crime. The U.S. ratified the convention in 2006, and the United Nations General Assembly, in relevant resolutions, encourages all U.N. Member States to adopt it as well either in full or as a model document for domestic legislation.

[516] Federal Emergency Management Agency, Cyber Annex, 7.

Department of Energy

By NSSC mandate, the Department of Energy (DOE), along with DHS, is responsible for developing best practices and new technologies to increase security of Supervisory Control and Data Acquisition (SCADA) systems. SCADA is used to remotely control industrial and critical infrastructure. A hacker may breach such a SCADA system by injecting false information, or remotely controlling critical infrastructure with potentially devastating results. Sensors in, say, an oil pipeline may provide a remote operator with information on the rate oil flows through a section of a pipeline. The rate of flow in the pipe can be adjusted by the operator with a few keystrokes thousands of miles away.[517]

Evaluation

Why Interagency is Failing: Challenge of Hierarchical Organizational Culture Where Networked Integration is Essential

In the past, the United States has faced adversarial states and VNSAs organized in relatively hierarchical vertical structures. However, today the evolution of ICT through the Internet and the intensification of globalization provides U.S. adversaries with the opportunity to organize themselves as horizontal networks with decentralized leadership.[518] John Arquilla and David Ronfeldt conceptualize this in *The Advent of Netwar* and their subsequent research.[519] While various manifestations of netwar exist, its underlying pattern is described as:

---

[517] Andrew Hildick-Smith, *Security for Critical Infrastructure SCADA Systems*, p. 1 <http://www.sans.org/reading_room/whitepapers/warfare/1644.php> .

[518] Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age." In, *Networks and Netwars*, (eds.) John Arquilla and David Ronfeldt (RAND, Santa Monica, CA, 2001) 29-60.

[519] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996).

> An emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organizations and related doctrines strategies and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command.[520]

Over the past decade, VNSAs, including terrorists groups such as Al-Qaida, have evolved into netwar actors.[521] Nation-states, such as China, also appear to be organizing their information warfare abilities along this paradigm, thereby blurring the line between nation-state and non-state hacker networks. In their article *Red Storm Rising: DOD's Efforts to Stave off Nation-State Cyberattacks Begin with China*, Dawn S. Onley and Patience Wait claim "a big part of the [Chinese] strategy is the PLA's civilian units — IT engineers drawn from universities, institutes and corporations."[522] O. Sami Saydjari, a former National Security Agency executive, has stated that the "Chinese People's Liberation Army, one of the world's largest military forces with an annual budget of $57 billion, has 'tens of thousands' of trainees launching attacks on U.S. computer networks."[523] These trainees might not officially be acting on behalf of the Chinese government, allowing the PLA to plausibly deny its involvement in an attack. Examples

---

[520] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar and Information Age Terrorism." In *Countering the new Terrorism* s (Santa Monica, CA: RAND, 1999). Also see Arquilla and Ronfeldt, 1996, 5.

[521] Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age" in *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001) 29-60.

[522] Dawn S. Onley and Patience Wait in their article "Red Storm Rising: DOD's Efforts to Stave off Nation-State Cyberattacks Begin with China" in *Government Computer News* (08/21/06.)

[523] Brian Grow, Keith Epstein, and Chi-Chu Tschang, "The New E-Spionage Threat; A Business Week Probe of Rising Attacks on America's Most Sensitive Computer Networks Uncovers Startling Security Gaps. In *Business Week* (21 April 2008).

of Chinese incursions in cyberspace include the Titan Rain attacks occurring during 2003-2006, and the more recent 2006-2008 Byzantine Foothold attacks. In the latter attacks, "thousands of highly customized e-mails… have landed in the laptops and PCs of U.S. government workers and defense contracting executives."[524] These e-mails differed from ordinary spam, since they were crafted in such a way that deceived the recipients into thinking it was a legitimate e-mail with an official request from another employee on behalf of a government agency. This indicates the perpetrator's intricate knowledge of U.S. government bureaucracy and interaction between government employees. Upon clicking on the e-mail, the recipient inadvertently activated malicious software, which began to spread throughout the government computer network, sending information back to servers in China. Although there is no direct link between the PLA's civilian units and the Byzantine Foothold attacks, the abundance of people trained in such units and the fact that information was sent from U.S. government computer networks to servers in China indicate that the Chinese military or government may have benefited through *ad hoc* collaboration with the perpetrators after the attacks, even if they did not directly order them.[525]

Arquilla and Ronfeldt argue that only organizations adapting networked doctrines can fight a netwar, since hierarchies are not suitable for the task. This is a challenge for nation-states since their:

---

[524] Grow, Epstein, and Tschang, 5.

[525] Grow, Epstein, and Tschang, 5.

> …sovereignty and authority are usually exercised through bureaucracies in which issues and problems can be sliced up and specific offices can be charged with taking care of specific problems. In netwar, things are rarely so clear. A protagonist is likely to operate in the cracks and gray areas of a society, striking where lines of authority crisscross and the operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash.[526]

Arquilla and Ronfeldt identify the interagency as the best Federal government mechanism with which to create netwar capabilities.[527] It appears that this is the path current cybersecurity strategies are on. While DHS/NCSD/NCSC are the main focal points for national cybersecurity, the NCRCG/IAC fosters the networking of cybersecurity efforts. Therefore, current efforts appear to be a hybrid of centralization and decentralization, in that DHS serves as a hub of interagency network cooperation. Whether this hybrid approach will be able to ensure security remains in question, especially since interagency cooperation suffers from a number of flaws outlined above and in more detail below.

Why There is Insufficient Strategy Implementation: Competing Priorities Exist and Overlapping Responsibilities

The NSSC contains numerous initiatives, such as unified cyber research and development for offensive and defensive purposes and merging overlapping capabilities. Officials do not adequately address these initiatives, as responsible agencies are often overburdened with too many tasks and limited resources. DHS and the CSNI place primary emphasis on securing federal computer systems, and not enough attention is paid

---

[526] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited) in *Networks and Netwars*, 14.

[527] John Arquilla and David Ronfeldt, "Cyber War is Coming" in *Inside Athena's Camp.*

to the fusion of multiple centers, such as US-CERT and the NCC, which are responsible for securing cyberspace. The DHS's struggle to integrate its own operations (as described above) is indicative of this. Overall, languid implementation of the existing cybersecurity strategy has resulted in continued vulnerability in the federal computing environment.

Interagency and intra-agency redundancies are also a concern. The GAO reports that:

> Overlapping responsibilities for incident response have adversely affected DHS's ability to prioritize and coordinate incident response activities. For example, private-sector firms have reported that in responding to a critical incident, DHS made time-consuming and duplicative requests for information without identifying how this information would be beneficial in helping respond to the event.[528]

In addition, DHS and DOD cybersecurity capabilities overlap significantly. DHS has performed moderately well in its role as a main coordinator for the federal response to a major cybersecurity incident but, as mentioned above, DOD may be better suited to lead U.S. national cybersecurity efforts in cases of national emergency. The preference among some analysts for DOD to lead the response to any cyber-attack is largely due to prognostications about the level of damage an attack could inflict upon the United States and the extent of resources that will be needed to respond. Thus, while at peace, DHS works well, but wartime will require a different lead.

Why There is Insufficient Strategy Implementation: Not Enough Resources, Experts are Available to Address all the Integration Priorities, and Unified Research Efforts

[528] GAO, 14.

The NSSC notes that:

> Future security requires research in cyberspace security topics and a commitment to the development of more secure products...To meet these needs, the Director of OSTP will coordinate the development, and update on an annual basis, a federal government research and development agenda that includes near-term (1-3 years), mid-term (3-5 years), and later (5 years out and longer) IT security research for Fiscal Year 2004 and beyond...DHS will ensure that adequate mechanisms exist for coordination of research and development among academia, industry, and government, and will develop new mechanisms where needed.[529]

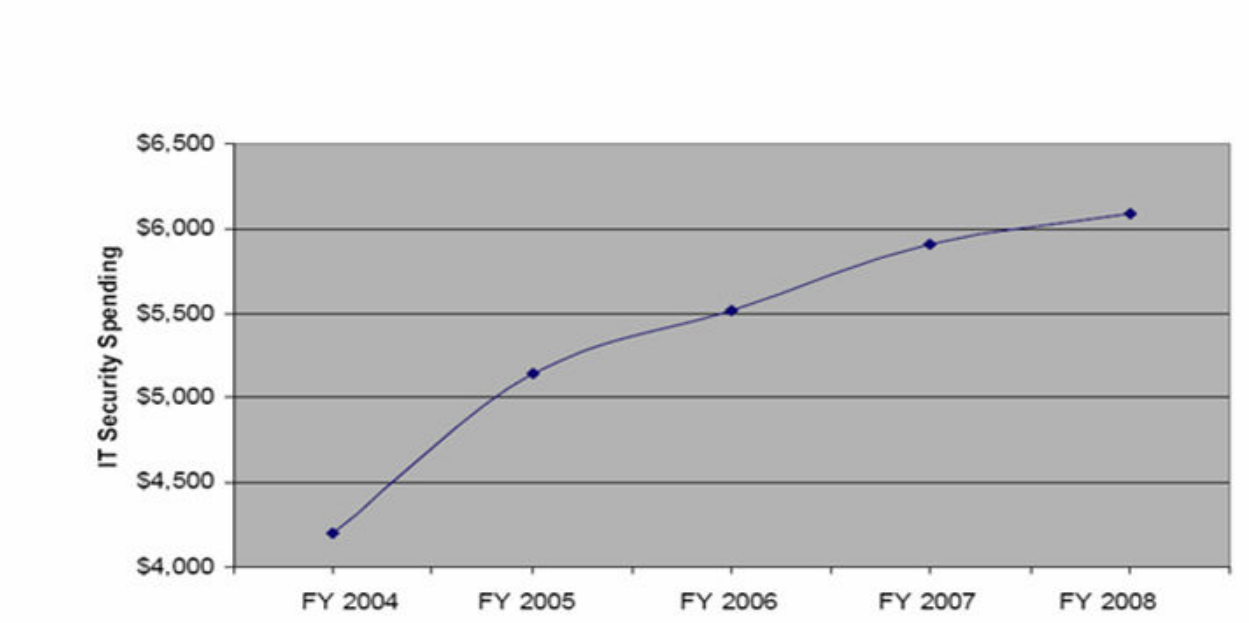
However, the President's Information Technology Advisory Committee (PITAC) identifies a lack of well-trained cybersecurity experts stemming from poor funding of the research infrastructure.[530] The lack of adequate resources places limitations on the "amount of research that can be undertaken overall and on the number of research topics that can be investigated effectively, because productive work in a topic commonly requires a critical mass of researchers."[531]

---

[529] NSSC, 34-35.

[530] PITAC, 30-31.

[531] Ibid.



PITAC suggested that Federal research and development should have a central role in long-term solutions geared towards improving computer network security.[532] The *Federal Plan for Cyber Security and Information Assurance Research and Development* provides a technical framework and baseline information for the federal research agenda.[533] However, the GAO reports that although it is a step in the right direction, it does not fulfill the objectives of the NSSC. The plan lacks elements: "(1) specifying timelines and milestones for conducting research and development activities; (2) specifying goals and measures for evaluating research and development activities; (3) assigning responsibility for implementation, including the accomplishment of the focus areas and suggested research priorities; and (4) aligning the funding priorities with

[532] PITAC 13.

[533] Interagency Working Group on Cyber Security and Information Assurance *Federal Plan for Cyber Security and Information Assurance Research and Development* (National Science and Technology Council, April 2006), http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf.

technical priorities."[534] This results in an

> …increased risk … that agencies will focus on their individual priorities for cyber security research and development, which may not be the most important national research priorities. Better coordination of research and development efforts will enable the most important topics to receive priority funding and resources and avoid duplication of effort.[535]

Furthermore, resource deficiencies affect the number of people training for cybersecurity. According to the Office of Management and Budget, for the fiscal year 2007 "agencies continued to make incremental progress in closing the Federal government's IT security performance gaps in the areas of C&A and testing of contingency plans and security controls."[536] There is also a marked decrease between FY2006-2007 in the number of federal employees being trained in computer security.[537] This exists despite a need to assure that all employees are trained in how to secure their information systems.

Why There is Insufficient Strategy Development: Focus on the Impact of Cyber Incidents on Individual Systems Rather than the Effects on the Whole Community

Current cybersecurity efforts focus on the individual impact of a crime on specific systems, rather than the effect of a crime on a network. This is due to the focus of scholarship in twentieth-century criminology on individual rather than community harm of crime. The replication of this view is evident in the NSSC, since it focuses on the

---

[534] United States Government Accountability Office, *Information Security; Coordination of Federal Cyber Security Resarch and Development* (September 2006) <http://www.gao.gov/new.items/d06811.pdf>, 18.

[535] United States Government Accountability Office, Information Security; Coordination of Federal Cyber Security Resarch and Development <http://www.gao.gov/new.items/d06811.pdf>, 17.

[536] Office of Management and Budget, Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002. http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf.

[537] Ibid, 5.

protection of critical infrastructure and federal computer-networks, while placing the burden of the responsibility of securing cyberspace on private actors.

Although a sophisticated cyber-attack targeting critical infrastructure can cause billions of dollars in damage, the harm such an action inflicts upon the network should also be considered.[538] In *The Dark Side of Private Ordering: The Network/Community Harm of Crime,* Neal K. Katyal argues that a focus on how a crime harms the community, rather than the individual, is especially important in cyberspace due to the nature of utility, or network-effects, in computer networks.[539] That is, the utility of a network increases in proportion to the number of subscribers on that network. The majority of Internet services operate on this principle. For example, online auction sites would have minimal utility if there were only a handful of subscribers, however, with millions logging on and auctioning, the utility of the service increases since there are more potential buyers browsing the auction site. The significance of this is that each instance of cybercrime, no matter how trivial, leads users to not trust their network, and subsequently reduce their use.[540] Every network intrusion leads to an increase in user mistrust, thereby leading to a decrease in the number of users. As a result, the value of that network to the remaining users decreases, since a network's utility increases along with the number of users on it.[541] Hence, in its focus on the impact of a cyber-attack against critical infrastructure and federal computer systems, the NSSC overlooks the long-term potential consequences of network attacks.

---

[538] Katyal, 217.
[539] Neal K. Katyal, "The Dark Side of Private Ordering: The Network/Community Harm of Crime" in *The Law and Economics of Cyberspace*, Mark Grady and Francesco Parisi (eds.) (Cambridge, England: CUP, 2006, 193-217).
[540] Katyal, 197.
[541] Ibid.

Why there is Insufficient Strategy Development: Focus on Hostile Conquest

> Martin Libicki suggests national security is not threatened solely by hostile acts: Friendly conquest—the creation and use of systems that contain information which others desire to access—is just as significant a threat. Such conquest occurs when a non-core operator of a system enters into partnership with a core operator in exchange for access to the desired information system. The core partner in such a coalition emerges to dominate non-core members who have come to depend on the service offered, though not without some vulnerability to the core partner's network. Fears exist, "that the full dependence that pervades one's internal systems may leave one open to manipulation…The source of such vulnerability could range from one partner's general knowledge of how the infrastructure is secure, to privileged access to the infrastructure that can permit an attack to be bootstrapped more easily."[542]

A prime example of friendly conquest is the reliance of a majority of countries on the U.S. Global Positioning Satellite (GPS) system. Access to GPS is available without a fee for the basic service after an individual purchases a device that reads the signal. Realizing that their dependence on this U.S. system makes them vulnerable, Russia has developed, and the European Union and China are developing, independent GPS systems.

The NSSC does not address threats of friendly conquest in cyberspace. Rather, it focuses on hostile conquest. However, friendly conquest of the United States by other nations is just as significant as a hostile threat. As the founder and host of ICANN and DNS, the U.S. currently enjoys the position of core provider of these services. However, Internet and digital technologies continuously evolve. The present strategy gives no guarantee that the U.S. will maintain its status as core operator of non-DNS servers. Globally, people are increasingly using Virtual Reality (VR) technology fused with the

[542] Libicki, 137.

Internet to interact socially.[543] Experts have noted:

> …that any country that succeeds in dominating the VR market may also set the technical standards for the rest of the world, and may also own and operate the VR servers that give them unique access to information about future global financial transactions, transportation, shipping, and business communications that may rely on virtual worlds.[544]

Global commerce is expected to "come to rely heavily on VR." Banking, transportation control and communications are all types of global commerce occurring in a virtual reality.[545] The potentiality of China dominating VR technology and standards is a challenge that is insufficiently addressed by the current national cybersecurity strategy.

Why There is Insufficient Strategy Development: Emphasis on P3 Security Approach.

Many sources identify the government's reliance on the private sector to carry the bulk of the responsibility in cyber security as the most significant insufficiency in the national effort to secure cyberspace. Neal K. Katyal, in *The Dark Side of Private Ordering: The Network/Community Harm of Crime,* suggests that the NSSC is flawed in this regard. He argues that:

> Far from being a breakthrough document, the *National Strategy to Secure Cyberspace* is a hodgepodge of concepts and consulting talk, devoid of serious agenda. Both simple and complicated solutions to cyber-crime were obscured by an antiregulatory, antigovernment bias that infected the strategy's outlook and thinking from the start.[546]

The reason for this bias, according to press reports, is the:

---

[543] Ibid.
[544] Clay Wilson, Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues (Congressional Research Service: April 2008), 4.
[545] Wilson, 12.
[546] Neal K. Katyal, "The Dark Side of Private Ordering: The Network/Community Harm of Crime" in *The Law and Economics of Cyberspace,* Mark Grady and Francesco Parisi (eds.) (Cambridge, England: CUP, 2006, 193-217).

> …technology and telecommunications companies [which] lobbied hard against regulation, arguing that the private sector is better qualified to develop the most effective security… [and] White House advisers [who] held fast to their philosophical reluctance to regulate free markets or to impose industry standards that might favor one sector over another.[547]

Thus, a combination of industry lobbying and political ideology has led to the anti-regulation framework within current cyber security strategies. Katyal further notes that although law enforcement is mentioned in the strategy, it "does not even explain what the need for law enforcement is, let alone provide a blueprint for how to achieve it."[548] Contrary to the NSSC, Katyal argues that it is the responsibility of law enforcement organizations, and not private individuals or corporations, to enforce cyber-law and prosecute all infringements. Private ordering efforts, such as proprietary anti-virus or firewall software, will not prevent computer crime simply because this software or hardware is purchased and installed by a user. Private industry might:

> Promote sales of anti-virus software, intrusion systems and the like. Yet, the ability to afford and the knowledge to use such technologies will not be distributed equally. Those with fewer resources will not be able to adopt them in the same way that richer individuals and institutions can. Further, because these technologies are often complicated, there will be some who have the resources to purchase them but lack the skills necessary to use them effectively.[549]

Without adequate protective measures, those without the necessary resources will use the network less, if at all.[550] Hence, Katyal concludes, since private efforts cannot protect

---

[547] Mark D. Rasch, "Cyber-Security Strategy Depends on Power of Suggestion" in *Washington Post* < http://www.washingtonpost.com/ac2/wp-dyn/A10274-2003Feb14?language=printer>.
[548] Katyal, 215.
[549] Katyal, 199.
[550] Katyal, 194.

every user, governments must bear responsibility for network protection in order to assure that the network maintains its utility.[551]

Why There is Insufficient Strategy Implementation: Insecurity of TCP/IP

The NSSC is correct in identifying weaknesses in IP. However, its solution of implementing IPv6 is deemed flawed by some analysts since it is still based on the TCP/IP protocol. The IP protocol makes identifying the origin of an attack difficult. Tech savvy individuals can manipulate weaknesses in IP to give themselves anonymity.[552] As a result, it is highly feasible that a cyber-attacker's country of origin may never be identified.

In *How to Stop Talking About—and Start Fixing—Cyber Security Problems,* Bill Hancock notes that TCP/IP "never had any security methods built into it to ensure that even base security controls (authorized user access, protocol header verification controls, protocol filter lists, session verification, etc.) were included."[553] He criticizes the "owner" of the TCP/IP protocol, the Internet Engineering Task Force (IETF), as being "mired in politics and distracted by numerous other issues that keep it from doing a thorough housecleaning of the protocol." He also points out that the Task Force "is not funded to do basic, original research" unlike the Defense Advanced Research Projects Agency

---

[551] Katyal, 215.

[552] One such method is onion-routing (TOR). TOR is a distributed anonymous network of proxy servers connected by virtual encrypted tunnels. A computer linked to a TOR network transmitting data, sends the data through a series of proxy servers which strip the IP identification information, replace it with new IP information, and send it off to another proxy server before connecting to the final server. The effect of this is that if someone is observing the network traffic on any of the proxy servers, the observer will not be able to discern the true location of point A, nor will the observer be able to tell what the destination of the data is, unless he or she is observing the final transmission point. An observer at point B will not know where the data is really coming from, as he will only be able to detect the location of the proxy server from which the data arrived at point B. In this way, a network address is masked.

[553] Bill Hancock, "How to Stop Talking About- and Start Fixing - Cyber Security Problems" in *Cutter IT Journal* (May 2006) p. 6-11.

(DARPA), the creator of TCP/IP.[554] Also, unlike DARPA, it is an international organization, and must therefore deal with difficult political differences among its members. One might suggest that relying on IETF to rework IP protocols in such a way that U.S. cybersecurity goals are achieved is analogous with the U.S. relying on the United Nations to achieve its national security objectives. Although both the U.N. and IETF are valuable tools, dependence on them, most analysts say, is ill advised.

Hancock indicates that the absence of an influential and credible organization that has the resources to rework IP threatens U.S. security. The inability of any organization to look ahead to see what types of challenges computer networks will face in ten to twenty years is similarly detrimental.

Why There is Insufficient Strategy Implementation: Secrecy in Organizational Cultures

Threat awareness by both federal and private actors is identified as a lynchpin in securing cyberspace. However, a culture of secrecy surrounds the full extent of private sector vulnerabilities. According to Verton, this dynamic persists largely because:

> The private companies that own and operate the bulk of the nation's most critical infrastructure system continue to balk at sharing with the government the lion's share of information about cyber-vulnerabilities and security incidents. Most fear that the government, through Freedom of Information Act requests, will inadvertently disclose proprietary company data to competitors.[555]

To demonstrate his point, Verton describes the financial industry as one example where the private sector is reluctant to share data on cyber intrusions with outsiders. Beyond the protection of proprietary data, private industry is also concerned that if the full extent of their vulnerabilities is made public, people will not trust their services and stop using

[554] Hancock, 10.
[555] Verton, 25.

them.

The Federal government also appears to be less willing to share sensitive security information with both the private sector, as the classification of CNSI indicates, and within the interagency since "interagency rivalries and distrust have too often slowed progress" in organizing a networked response to security threats.[556]

Assessing Results

Federal computer systems continue to be vulnerable to attack. By drafting and adopting the NSSC, the Bush administration recognized that:

> Cyber attacks on U.S. information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructure.[557]

Putting DHS in the lead of this effort has resulted in the development of a framework for a coordinated interagency response within the DHS/ NCRCG/IAC. Although a decentralized response is limited, the current structure enables the U.S. to conduct netwar campaigns against adversaries to some degree. Still, such efforts are hindered by hierarchical structures and much work remains to be done. Competing priorities tax available resources, which at times are strained due to overlapping missions among various departments and agencies. Further, there is a weak perception of the threat in cyberspace. The focus now is on individual computer systems and hostile conquest. This overlooks community effects and the problem of friendly conquest. Finally, some

---

[556] John Arquilla and David Ronfeldt, "Afterword (September 2001): The Sharpening Fight for the Future." In, *Networks and Netwars*, (eds.) John Arquilla and David Ronfeldt (RAND, Santa Monica, CA, 2001) 363-371, 364.

[557] NSSC, 6.

analysts identify the P3 approach as a significant weakness in current strategy. The cyber threat may exist in a virtual domain, but the costs of not correcting weaknesses, or losing the current impetus, are real. Descriptions of one recent cyber attack possibly involving Chinese hackers provide an indication of potential costs. According to Grow, Epstein, and Chu Tschang:

> The attack began in May, 2006, when an unwitting employee in the State Department's East Asia Pacific region clicked on an attachment in a seemingly authentic e-mail. Malicious code was embedded in the Word document ... [which] opened a Trojan "back door" for the code's creators to peer inside the State Dept.'s innermost networks. Soon, cyber security engineers began spotting more intrusions in State Dept. computers across the globe. The malware took advantage of previously unknown vulnerabilities in the Microsoft operating system. Unable to develop a patch quickly enough, engineers watched helplessly as streams of State Dept. data slipped through the back door and into the Internet ether. Although they were unable to fix the vulnerability, specialists came up with a temporary scheme to block further infections. They also yanked connections to the Internet.[558]

Official Chinese policy is to deny any government or military involvement in this or similar attacks.

Well-executed cyber-attacks are not limited to data theft. Using the same techniques required to enter a computer-network without authorization, hackers can inject false information into a system with tragic results. Utility companies have been the targets of such attacks. Recently, the CIA warned that: "cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands,

---

[558] Grow, Epstein, and Chu Tschang, 3.

in at least one case causing a power outage that affected multiple cities."[559] Since utility companies now use SCADA to remotely monitor and access controls for their services, and because SCADA is a ubiquitous technology, U.S. utilities are just as vulnerable to these sorts of attacks. There is circumstantial evidence that Chinese hackers may have been responsible for past power blackouts in the United States, including the widespread power loss that occurred on August 15, 2003 affecting the East Coast. During this event, over one hundred power plants were shut down in part due to the disruption of communications lines used to manage the power grid. This disruption was attributed to a computer virus in circulation at the time.[560] It has been noted by "one security analyst in the private sector with close ties to the intelligence community … that some senior intelligence officials believe that China played a role in the 2003 blackout that is still not fully understood."[561] Further investigation of why there is not a full understanding of China's role is not possible due to limitations on the information available.

The threat to the power grid is very tangible. During a DHS exercise, hackers were tasked with hacking into the information system of a power generator. Succeeding in gaining remote access to the generators SCADA control system, the hackers were able to physically destroy the generator. The Aurora vulnerability, as this exploit is called, lends credence to the suggestion that the manipulation of computer code can be just as effective in destroying critical infrastructure as a missile would. In a letter to Congressman John Dingell (D-MI), Chairman of the Committee on Energy and

---

[559] Ellen Nakashima and Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says" in *Washington Post* (Saturday, January 19, 2008; A04).

[560] Shane Harris, "Chinese Hackers Pose a Clear and Present Danger to U.S. Government and Private-Sector Computer Networks and May be Responsible for Two Major U.S. Power Blackouts." In *National Journal Magazine*. (31 May 2008). <http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php>.

[561] Ibid.

Commerce, Congressmen Bennie Thompson (D-MS) and James Langevin (D-RI) emphasized that an attack exploiting the Aurora vulnerability "could enable a targeted attack on infrastructure connected to the electric grid, potentially destroying these machines and resulting in catastrophic losses of power for long periods of time."[562] The cost for a cyber-attack resulting in a three-month power outage is cited at over $700 billion.[563]

Conclusion

With the publication of the NSSC, the United States codified its strategy for securing cyberspace. This is a significant step that has had some positive results. The CNSI reiterates many of the points of the NSSC, while giving a greater cybersecurity role for the IC. The following variables emphasize the strengths and weaknesses of current cybersecurity strategy.

Strengths

- Implementation of national cyber-attack response system to coordinate the interagency in responding to cyber attacks of national significance
- Evolution to a partial decentralization of cybersecurity tasks through interagency mechanisms, such as the DHS/NCRCG/IAC, enabling netwar

Weaknesses

- Competing priorities; insufficient resources and experts to address all strategic objectives
- Overlapping responsibilities and the lack of an integrated mechanism to coordinate cybersecurity efforts
- Hierarchical organizational structures hindering networked efforts
- Weak threat perception, exhibited in strategic focus on both the individual effects of cybercrime rather than on the consequences for the network at large and on hostile conquest to the exclusion of friendly conquest

---

[562] Bennie Thompson and James Langevin, "Letter from Congressmen Bennie Thomson and James Langevin to Congressman John D. Dingel", May 29, 2008, http://homeland.house.gov/SiteDocuments/20080530130810-85574.pdf.
[563] Thompson and Langevin.

- Reliance on private industry stemming from an anti-regulatory stance prevalent in national cybersecurity policy, resulting in a lack of a federal R&D program to rework communications protocols, among other deficiencies

Overall, the government has generally been flexible in adjusting its cyber strategies as necessary, and despite its flaws, the NSSC has brought a degree of organization to the interagency. The anti-regulatory framework remains a critical flaw in current national cybersecurity strategy, since private industry is not likely to fully disclose threats and vulnerabilities to information systems.[564] This is significant since private industry controls are a substantial part of the critical information infrastructure that provides security software to the federal government. Even if the interagency performs well during a cyber attack under DHS coordination, relying on the current P3 framework might inhibit information sharing critical to mitigating effects until well after an attack is underway. Much work needs to be done to defend against ongoing cyber espionage operations by foreign governments to ensure that no group of hackers can bring down a U.S. regional power grid with a few keystrokes, causing an immeasurable amount of damage.

[564] Verton, 24.

Chapter Nine
Conclusion

Cyberspace is a (relatively) new global commonage that has enabled the emergence of an Information Society. Although the term has become synonymous with the Internet in popular culture, this project uses the strategic definition as the basis for the analysis of the global politics of its governance and militarization.

Open globe spanning networks are critical to all aspect of life in developed countries. On the other side of the digital-divide, less developed countries are eager to increase their knowledge and use of ICTs to join the Information Society. With these trends intensifying, actions taken in cyberspace will become more consequential than they already are. Cybercriminals working around the clock worldwide today have both the capability and the intent to gain access to an individuals private information, and gain access to bank accounts as if they were the legitimate user. Funds can then rapidly flow across borders appearing legitimate, but winding up in ghost accounts in foreign banks created for the purpose of electronically robbing a bank. By the time investigators have caught on, the cybercriminals will have disappeared into the electromagnetic wilderness leaving behind sparse clues that investigators can use to identify and prosecute the perpetrators of the crime.

The challenges to cybercrime investigations are both technical and political. On the technical level, the nature of the Internet, and the TCP/IP protocol in particular, make it easy for individuals to spoof their identities or locations. Some methods for doing so include bouncing a communication around the globe from country to country, or infecting potentially thousands of computers with malicious software which would allow

a cybercriminal to misuse another person's computer without being easily traced. Identifying a perpetrator requires international cooperation at the political level since gaining access to data that might reveal the identity of an attacker could involve investigators knocking on the doors of numerous Internet service providers across the globe and requesting access to their log files. The disharmonious state of cyberlaws does not guarantee such cooperation. In some cases, investigations have been thwarted in countries with non-existent cybercrime laws since authorities will argue that no criminal action has occurred under that country's legal code. Hence, the transnational nature of cybercrime highlights the need to create an international law harmonizing the response to cybercrime. Without such a legal code, cybercrime will continue. This will decrease the utility of networks since people will distrust networks since security is not guaranteed. Thus, the promise of digital technology for an information society relies on a secure cyberenvironment.

The organized use of force in cyberspace by and for the purpose of the state is the second challenge to global cybersecurity efforts. Cyberwarfare programs are proliferating at an alarming rate as state's realize that this domain can be used to project power and gather intelligence. Conflict in cyberspace is currently unregulated by laws specifically addressing this issue. The knowledge threshold for states to develop cyberwarfare capabilities is much lower than that required to build an air or nuclear forces. Attacks in cyberspace have been characterized as being potentially just as damaging as a ballistic missile strike. This is due to the migration of command and control capabilities for critical infrastructures, including energy and waste-water treatment facilities, into cyberspace. The stakes are unthinkable if one considers the U.S. and Russian positions on

possible retaliation for strategic cyberattacks include the use of nuclear weapons. The aforementioned technical and political complexities of identifying the origin of an attack present unique challenges to military responses since acts of strategic information warfare, would not offer the same evidence as the launch of a missile.

Another issue demonstrating the need for the coordinated efforts of international actors in the field of cybersecurity is the misuse of cyberspace by violent non-state actors (VNSAs), such as terrorists. Sanctions restricting access to funds, weapons and travel, such as the U.N. Security Council's 1267 sanctions regime, are futile since terrorists may circumvent sanctions using ICTs . While the Security Council has expressed its concern on the issue, it has not called for a general meeting to discuss cybersecurity despite its mandate under the U.N. Charter to address issues of global security. Although VNSAs may not have the resources available to law enforcement and intelligence services, without international cooperation in the field of cybersecurity, there is only so far an investigation can go if foreign governments do not share information pertaining to the terrorist misuse of the Internet and other ICTs. The U.N. Security Council would be the ideal awareness raising forum.

The global culture of cybersecurity agreed on at the U.N. General Assembly, represents the formulation of what are informal peremptory norms of international cyberspace law. To date, the UNGA has been the main body addressing global cybersecurity cooperation. Under its guidance, the. World Summit for the Information Society (WSIS) was the first formal conference open to all interested stakeholders, including state and non-state actors. Organized to find common ground on the vision for the Information Society, the fields of cybersecurity and Internet governance were deemed

of utmost importance. Although the outcome documents of the WSIS were political in nature, it was stressed by the U.S. in particular that they were not legally binding. These documents do form frameworks for a future treaty on the peaceful uses of cyberspace. This project focused on where state's found common ground, and where they disagreed. Focusing on the available documentation of U.S. Russian and Chinese positions at the WSIS and well as the High Level Experts Group (HLEG) of the Global Cybersecurity Agenda (GCA) provides insight into the nature of agreements and disagreements in securing cyberspace. Technogeopolitics provides insight to why these states take the positions they do at these conferences, which is primarily due to their perceived threats in the case of Russia and China, or as in the case of the U.S, the comfort of being the de facto cyberspace hegemony due to its command of the majority of the global network infrastructure.

The more critical obstacles to forging a secure cyberenvironment for the Information Society are rooted in the militarization and geopolitics of cyberspace. The lens of technogeopolitics is used to explain and understand these impediments. It is argued that since states develop and use specific technologies to enhance their geopolitical positions, and the United States is the cyberspace's hegemon, the U.S. will continue to block those efforts to make ICANN and the DNS system more transparent, in addition to efforts to create an international law for cyberspace. One might suggest that since most Internet traffic passes through the U.S. due to its role of core technical operator of the Internet's foundation, there may be classified capabilities which the U.S. would lose if it succumbed to international pressure to open up ICANN and DNS.

However, an investigator using only open sources is not able to explore this possibility further.

Other states are reacting to the U.S. technical developments geopolitically through their militarization of this domain. Russia in particular, which is technologically immature when compared to the U.S. in terms of ICT development and distribution on a global scale, is using forums such as the WSIS process and the ITU to urge for an international law of cyberspace which would restrict U.S. dominance of ICANN, DNS and use of special technical intelligence collection capabilities. The U.S. uses these same forums to urge for liberal policies such as the free flow of information. It is predicted that the U.S. dominance is not permanent. Russia and China in particular are developing their own ICT manufacturing base, as well as their own national networks not interoperable with the Internet. In the long term, any geopolitical gains the U.S. has today might be wiped out causing the U.S. to reexamine its policies as a result of the shifts towards national private networks due to U.S. resistance to open up the global network infrastructures to the rest of the world.

Unanimous agreement exists on the issue of the private-ordering of cybersecurity in documents pertaining to global cooperation in this field. This guiding tenet of global and national cybersecurity efforts is flawed since public-private partnerships (P3) in which there is no federalized effort to guarantee the security of privately owned networks will erode trust in the networks over the long term. The Greek cyberespionage case demonstrates the pitfalls of this strategy. Foreign companies offering their services to consumers may not follow their legal obligations in cases where the security of an information system is breached. One might suggest that the P3 model of cybersecurity

applies better in the U.S. case where many ICT corporations, including those overseeing the day-to-day functioning of the Internet such as ICANN, interact with the government in formal meetings of an advisory nature. Further, Greece lacks a National Security Council to coordinate its responses to security threats at an interagency level. The U.S. National Security Council (NSC) has existed since the end of the Second World War. This has allowed it reform itself over time as an organ of interagency and cooperation.

However, the P3 model is flawed, even in the U.S. case. This project emphasizes the point that if private industry is relied on to secure information systems, the full utility of those networks will not be realized since users will not trust systems that they cannot be expected to know how to secure. Preventing a computer to be hijacked by malicious code is not as simple as putting a lock on one's house. This is not to say that private industry plays no role in securing cyberspace, only that it is the state that should take on the brunt of the effort.

With rampant criminal activity and the militarization of cyberspace, the consequences of not having more proactive national efforts to secure cyberspace on the basis of international cooperation paints a bleak picture of the future of cyberspace. If current trends observed in international conferences and national cybersecurity efforts continue, cyberspace will come to mirror the Balkans just prior to the outbreak of the First World War rather than a unifying global village envisioned for the Information Society.

BIBLIOGRAPHY

Geography of Cyberspace

Abler, R.F., "The Geography of Communications" in *Transportation Geography: Comments and Readings*. Michael E. Eliot Hurst (Ed.) (New York, New York: McGraw-Hill Book Company, 1974).

Affel, H.A., et. al. "The New Key West-Havana Carrier Telephone Cable," in *Bell System Technical Journal* 11:197-212 (January 1932).

Black, Robert M., *The History of Electric Wires and Cables*, (London: Peter Peregrinus Ltd. 1983).

Buckley, O.E., "The Future of Transoceanic Telephony" *Bell System Technical Journal* 1-19 (January 1942).

Glover, Bill, *Cable Timeline: 2001-* <http://www.atlantic-cable.com/Cables/CableTimeLine/index2001.htm>

Hägerstrand, Torsten, "Aspects of the Spatial Structure of Social Communication and the Diffusion of Information," *Papers of the Regional Science Association* (16) 27-42.

Innis, Donald, Q "The Geography of Radio in Canada" in *The Canadian Geographer* (1953 (3) 89-97.

Kellerman, Ahoron. *Telecommunications and Geography* (New York: Belhaven Press, 1993), 12.

Kidorf, Howard, "Network Architecture for Submarine Systems" in José Chesnoy, Govind Agrawal, Ivan P. Kaminow, Paul Kelley (eds.), *Undersea Fiber Communication Systems* (Academic Press, 2002, 413-415).

Newall,R.S., *Facts and Observations Relating to the Invention of the Submarine Cable and to the Manufacture and Laying of the First Cable Between Dover and Calais in 1851* (London: E & F.N Spon 1882).

Malcolm, H.W., *The Theory of the Submarine Telegraph and Telephone Cable* (London: Benn Bros 1917).

Markoff, John, "Internet traffic begins to bypass the U.S." *New York Times,* (August 31, 2008).

Nichols, Russell T. *Submarine Telephone Cables and International Communications* (Santa Monica, CA: Rand Corporation 1963).

Solomon, Louis, *Voiceway to the Orient: The First U.S.-Japan Telephone Cable* (New York: McGraw Hill 1964).

Van Cleef, Eugene, *Trade Centers and Trade Routes* (New York, New York: D. Appleton Century, 1937).

Williams, David, O. "An Oversimplified Overview of Undersea Cable Systems". European Laboratory for Particle Physics (CERN), Geneva, Switzerland. Last revision March 1999. < http://nicewww.cern.ch/~davidw/public/SubCables.html>

Zipf, George Kingsley, "Some Determinants of the Circulation of Information" in *American Journal of Sociology* 1946 (59) 401-421.

Environment of Cyberspace

Aitken, Hugh G.J. *Syntony and Spark: The Origins of Radio* (New York: Wiley Interscience 1976).

Davis ,Eric W., Teleportation Physics Study (Edwards Air Force Base, CA: AIR FORCE RESEARCH LABORATORY 2004)

Feynman, Richard P., *Six Easy Pieces: Essentials of Physics Explained by its Most Brilliant Teacher*, (California Institute of Technology:) 1995, 28.

Franklin, Benjamin, *The Autobiography of Benjamin Franklin* (Philadelphia, PA: University of Pennsylvania Press, 2005), 43.

Franklin, Benjamin, "The Kite Experiment," in *The Papers of Benjamin Franklin, Volume 4: July 1, 1750 through June 30, 1753*, Ed. Leonard W. Labaree, (New Haven, CT: Yale University Press) 1961.

Hastings, Daniel *Issues in Space* Talk to the Federation of American Scientists 20th Feb 2003.

Jackson, William, "A Faster Internet Lane" in Government Computer News (29 September 2008) < http://www.gcn.com/print/27_24/47246-1.html?page=1>

Larmor L., "The Origins of Clerk Maxwell's Electric Ideas, as Described in Familiar Letter to W Thomson" in *Proceedings of the Cambridge Philosophical Society*, 32:695-750 (1936).

Leighton, Tom. "The Net's Real Security Problem." In *Scientific American*. (September 2006), 44.

Lodge, Oliver J., Space Without Wires: Being a Description of the Work of Hertz and His Successors (Arno Press 1974).

Lord, L.E., "Watchtowers and Fortresses in Argolis," *American Journal of Archeology* (1939) 78-84.

Lord, L.E. "Blockhouses in the Argolide" *Hesperia* 10 (1941) 93-109.

March, Robert H., *Physics for Poets*, Fifth Edition (New York: McGraw Hill,2003), 66.

Marconi, Guglielmo,"On Methods Whereby the Radiation of Electric Waves May be Mainly Confined to Certain Directions," *Proceedings of the Royal Society*, Series A. Vol. 77 No. A518: 413-421 (April 20, 1906).

Molyneux, Robert E. , The Internet Under the Hood: An Introduction to Network Technologies for Information Professionals (Westport, CT: Libraries Unlimited, 2003) pp. 85-86.

Poincare, H. and Vreeland, Frederick K.. *Maxwell's Theory and Wireless Telegraphy* (New York McGraw Hill, 1904).

Tunzelmann, G.W. de "Hertz Reserces on Electrical Oscillations" *Annual Report of the Board of Regents of the Smithsonian Institute* (1889).

White, Gene. *Internetworking and Addressing* (New York, NY: McGraw Hill, 1992) 12.

Whittaker, Edmund T., *A History of the Theories of Aether ad Electricity* (London: Longmans Green 1910.)

United States Patent 4866704, *Fiber optic voice/data network*

Cyberspace and Culture

William Gibson, *Neuromancer. (*Ace Books 1984).

Bell David, "Moments in Cyberculture" in *Cybercultural Theorists: Manuel Castells and Donna Haraway* (New York, New York: Routledge 2007, 2-3).

Gibson, William "Academy Leader" in *Cyberspace: First Steps (ed)* (Cambridge, MA: MIT Press, 1991.

Politics of Cyberspace

Global Governance, Regimes and Emerging Cyberspace Norms,

Bederman, David J. , Globalization and International Law (New York: Palgrave-Macmillan, 2008) pp. 36-49.

Biermann, Frank, "Global Governance and the Environment," in *International Environmental Politics*, Michele M. Betsil, Kathryn Hochstetler and Dimitris Sevidis (eds), (New York: Palgrave Macmillan, 2006), 237-261.

Bonnici, Jeanne Pia Mifsud. *Self Regulation in Cyberspace* (The Hague, Netherlands: TMC Asser Press, 2008) 1.

Delio, Michelle, "Why Worm Writers Stay Free" Wired (December 27, 2001) http://www.wired.com/politics/law/news/2001/12/49313

Garcia, Greg, "Forging a Private-Public Partnership: The Wonk-Free Approach to Cybersecurity" in *Cutter IT Journal* (Vol. 19 No. 5, 2006) 21-35.

Goodman, Marc D. and Brenner, Susan W., "The Emerging Consensus on Criminal Conduct in Cyberspace" in *International Journal of Law and Information Technology* (Vol. 10 No. 2, 2002) 139-223, 140-143

Hancock, Bill, "How to Stop Talking About- and Start Fixing - Cyber Security Problems" in Cutter IT Journal (May 2006) p. 6-11.

Kamal, Ahmad. *Law of Cyber-Space: An Invitation to the Table of Negotiations* (Geneva, Switzerlan: United Nations Institute for Training and Research, 2005). Available at: <http://www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf>

Katyal, Neal K. , "The Dark Side of Private Ordering: The Network/Community Harm of Crime" in The Law and Economics of Cyberspace Mark Grady and Francesco Parisi (eds.) (Cambridge, England: CUP, 2006, 193-217).

Lessig, Lawrence, *Code and Other Laws of Cyberspace* (Basic Books, 1999).

Lipschutz, R., The National Origins of International Environmental Policies and Practices: My Country is in the World, in *Global environmental politics – power, perspectives, practice* CQ Press, 177-222.

Raboy, Marc and Landry, Normand, *Civil Society Communication and Global Governance: Issues from the World Summit on the Information Society* (New York, New York: Peter Lang, 2005).

Rasch, Mark D., "Cyber-Security Strategy Depends on Power of Suggestion" in Washington Post < http://www.washingtonpost.com/ac2/wp-dyn/A10274-2003Feb14?language=printer>

Simpson, Richard, "Creating Trust and Confidence Through Collaboration" (Athens, Greece: Internet Governance Forum 31 October 2006)

Stokke, Olav Schram, "Regimes as Governance Systems," in *Global Governance: Drawing Insights from the Environmental Experience*, Oran R. Young (ed), (MIT Press, Cambridge, Massachusetts, 1997), 28-63, 28.

Wapner, Paul, "Governance in Global Civil Society," in *Global Governance: Drawing Insights from the Environmental Experience*, Oran R. Young (ed), (MIT Press, Cambridge, Massachusetts, 1997), 66-84, 73.

Young, Oran R., "Global Governance: Toward a theory of Decentralized World Order," in *Global Governance: Drawing Insights from the Environmental Experience*, Oran R. Young (ed), (MIT Press, 1997), 274-299, 294.

Zittrain, Johnathan, *The Future of the Internet and How to Stop It* (New Haven, Connecticut: Yale University Press 2008).

Geopolitics and International Relations

Abbot, Kenneth W. and Snidal, Duncan, "Hard and Soft Law in International Governance" *Internat*ional Organization*,* Vol. 54, No. 3. (Summer 2000) 421-456.

Applebaum, Arthur, "Knowledge and Negotiation: Learning Under Conflict, Bargaining Under Uncertainty," Ph.D. dissertation, Harvard University, Cambridge, Massachusetts, 1987.

Arquilla, John & Ronfeldt, David: *The Emergence of Noopolitik: Toward an American Information Strategy*, Rand 1999

Betsill, Micele M., Transnational Actors in International Enviromental Politics," in *International Enviromental Politics*, Michele M. Betsil, Kathryn Hochstetler and Dimitris Sevidis (eds), (Palgrave Macmillan: New York, 2006), 173-202, 174.

Butler, David L., "Technogeopolitics and the Struggle for Control of World Air Routes," 1910-1928. in *Political Geography* (20, 2001) 635-658.

Cohen,Saul R., *Geography and Politics in a Divided World* (London: Methuen, 1960, p. 24

Comor, Edward A. "Communication Technology and International Capitalism: The Case of DBS and U.S. Foreign Policy" in *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy*. Ed. Edward A. Commor (New York, NY: St Martins Press, 1994, 83-102).

Eriksson, Johan and Giacomello, Giampiero, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", in *International Political Science Review* (2006, Vol. 27, No. 3, 221-244, 228.

Feather, John, "Information Rich and Information Poor" in *The Information Society: A Study of Continuity and Change* 4th Edition (London, UK: Facet Publishing, 2004, 111-136).

Ferguson, Yale H. and R Mansbach, Richard W., "Technology and Change" in *Remapping Global Politics: History's Revenge and Future Shock* (Cambridge, UK: Cambridge University Press, 2004), 273-311.

Frieden, Rob, "Balancing Equity and Efficiency Issues in the Management of Shared Global Radiocommunication Resources," in *University of Pennsylvania Journal of International Economic Law* (*Summer, 2003) 24 U. Pa. J. Int'l Econ. L. 289*

Foerstel, Herbert N., *Secret Science: Federal Control of American Science and Technology* (Westport, Connecticut: Praeger 1993).

Giacomello, Giampiero, *National Governments and Control of the Internet: A Digital Challenge* (New York: Routledge, 2005, 16-17).

Goldstein, Judith, Kahler, Miles, Keohane, Robert O., and Slaughter, Anne-Marie, "Introduction: Legalization and World Politics" *International Organization,* Vol. 54, No. 3 (Summer 2000) 385-399.

Graham, E.M., "Negotiating and Implementing and Investment Accord" in *Global Corporations and National Governments*, Washington DC: Institute for International Economics.

Gray, Colin S, "The Continued Primacy of Geography." *Orbis* 40, no. 2 (Spring 1996): 247. *Academic Search Premier*, EBSCO*host* (accessed September 22, 2008), 251.

Haggard, Stephen and Simmons, Beth A., "Theories of International Regimes" *International Organization* Vol. 41, No. 3 (Summer 1987) 491-517.

Herrera, Geoffrey L., *Technology and International Transformation: The Railroad, the Atom Bomb and the Politics of Technological Change* (Albany, New York: State University of New York Press, 2006), 3.

Hills, Jill. *The Struggle for Control of Global Communications: The Formative Century* (Chicago, Illinois: University of Illinois Press 2002.)

Jervis, Robert, "Cooperation Under the Security Dilemma" *World Politics*, Vol. 30, Issue 2 (Jan 1978) 167-214.

[John Doe] China To Produce Low-Cost Computers of Its Own"
Xinhua Tuesday, March 14, 2006 NewsEdge Document Number: 200603141477.1_22a40018245f4430

Jusdanis, Gregory, *The Necessary Nation*, (Princeton, NJ: Princeton University Press, 2001).

Keohane, Robert O. and Nye, Joseph S., "Power and Interdependence in the Information Age" in *Democracy.com: Governance in a Networked World* (Hollis, NH: Hollis Publishing Company, 1999), 197-214, 199.

Ibid., in *Foreign Affairs*, v. 77 no. 5 (September/October 1998).

Kobrin, Stephen J., "Sovereignty @ Bay: Globalization, Multinational Enterprise and the international Political System," 184.

Koremenos, Barbara, Charles Lipson and Duncan Snidal, "The Rational Design of International Institutions" *International Organization*, 5, 4 (Autumn 2001 761-799).

Krasner, Stephen D., "Global Communications and National Power: Life on the Pareto Frontier" *World Politics* Vol. 43, No. 3 (April 1991), 336-366.

Liebich, Andre, *Nationalizing the Globe, Globalizing the Nation*.

Libicki, Martin, "The Emerging Primacy of Information", *Orbis* Volume 40, Issue 2 (Spring 1996) 261-274.

Mackinder, Halford John, Democratic Ideals and Reality: A Study in the Politics of Reconstruction (New York, New York, Henry Holt and Company, 1919).

Martin, Lisa L., "Interests, Power, and Multilateralism" in *International Organization*, Vol. 46, No. 4 (Autumn 1992 765-792).

Mahan, Alfred Thayer: *The Influence of Sea Power Upon History: 1660-1783*. (Boston, Massachusetts: Little Brown and Company, 1898).

Mukerji, Chandra, *A Fragile Power: Scientists and the State* (Princeton, New Jersey: Princeton University Press, 1989.

Ostry, S.. The Multilateral Trading System, in *The Oxford Handbook of International Business,* Rugman, AM and Brewer, TL (eds) New York: OUP, 2001.

Ostry, S. and Nelson, R.R., 'Coping with System Friction: Deeper Integration and Other Means," in Techno-Nationalism and Techno-Globalism: Conflict and Cooperation, Washington DC: The Brookings Institute, 81.

Oye, Kenneth A., "Explaining Cooperation Under Anarchy: Hypothesis and Strategies, *World Politics* Vol. 38, No. 1 (October 1985) 1-24.

Ruggie, John Gerard, "International Responses to Technology: Concepts and Trends" in *International Organization*, Vol. 29, No. 3, (Summer, 1975), pp. 557-583

Rosendorff, B. Peter and Milner, Helen V., "The Optimal Design of International Trade Institutions: Uncertainty and Escape" *International Organization*, Vol. 55, No. 4

Sebenius, James K., "Challenging Conventional Explanations of International Cooperation: Negotiation Analysis and the Case of Epistemic Communities" *International Organization* 46 I (Winter 1992) 323-365, 331.

Slaughter, Ann-Marie , "International Law and International Relations Theory: A Dual Agenda" *The American Journal of International Law,* Vol. 87, No. 2 (April 1993) 205-239.

Sprout,Harold and Margaret, "Geography and International Politics in an Era of Revolutionary Change" in *The Journal of Conflict Resolution,* IV, No. 1 (1960), 145-161. (Autumn 2001) 829-857.

Wendt, Alexander, "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organizations* Vol 46, No. 2 (Spring 1992), 391-425.

Ibid., "Driving with the Rearview Mirror: On the Rational Science of Institutional Design. *International Organization*, Vo. 55, No. 4 (Autumn 2001 (1019-1049).

Cyberconflict

Cyberspace Militarization

"Experts Announce Agreement on the 25 Most Dangerous Programming Errors - And How to Fix Them
Agreement Will Change How Organizations Buy Software."
"Offensive Cyber Capabilities Sought" in *The Journal of Electronic Defense* (July 2008, 20).
< http://home2.nyc.gov/html/nypd/html/nypd/pdf/dcpi/NYPD_Report-Radicalization_in_the_West.pdf> cited on 17 August 2007.
<http://www.sans.org/top25errors/>

Adams, James, "The New Arms Race" in *The Next World War: Computers are the Weapons and the Frontline is Everywhere* (London, IK: Hutchinson 1998, 233-244, 233). Advantages', *International*

Anand, A, "Threats to India's Information Environment" *Information Technology: The Future Warfare Weapon* (New Delhi, India: Ocean Books Pvt. Ltd 2000 56-62).

Anderson, Levon, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" in Information as Power: An Anthology of Selected United States Army War College Student Papers, Eds. Jeffrey L. Groh, David J. Smith, Cynthia E. Ayers, William O. Waddell (Carlisle Barracks, Pennsylvania: U.S. Army War College) pp. 105-122, 106.

Arquilla John, Ronfeldt David, and Zanini Michele, "Networks, Netwar and Information Age Terrorism." In *Countering the new Terrorism* s (Santa Monica, CA: RAND, 1999).

Arquilla, John and Ronfeldt, David, "Afterword (September 2001): The Sharpening Fight for the Future." In, Networks and Netwars, eds. John Arquilla and David Ronfeldt (RAND, Santa Monica, CA, 2001) 363-371, 364.

Arquilla, John and Ronfeldt, David, "Cyber War is Coming" in Inside Athena's Camp

Arquilla, John and Ronfeldt, David, "The Advent of Netwar (Revisited) in Networks and Netwars, 14.

Arquilla, John and Ronfeldt, David, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996).

Arquilla, John, Ronfeldt, David, and Zanini, Michele, "Networks, Netwar and Information Age Terrorism." In *Countering the new Terrorism* s (Santa Monica, CA: RAND, 1999).Also see Arquilla and Ronfeldt, 1996, 5.

Attack on Syria shows Israel is master of the high-tech battle" in *Aviation Week & Space Technology*, Vol. 167 No. 21 (November 26, 2007, 28)

Barrington, Barrett M Jr., 'Information Warfare: China's Response to U.S. Technological

Barth, Richard C. and Smith, Clint N., "International Regulation of Encryption: Technology Will Drive Policy" in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, Eds. Brian Kahin, Charles Nesson (Cambridge, Massachsetts, MIT Press 1998, 283-299).

Berkowitz, Bruce, "The New Terrain" in *The New Face of War: How War Will be Fought in the 21st Century* (New York, New York: The Free Press 2003, 1-8)

Berkowitz, Bruce, "Command of the Nets" in *The New Face of War: How War will be Fought in the 21st Century* (New York, New York: The Free Press 2003, 179-195).

Cass, Stephen, "Antipiracy Software Opens Door to Electronic Intruders: Sony BMG shoots itself—and its customers—in the foot" in *IEEE Spectrum* (January 2006) 12-13.

China Information Technology Security Certification Center Source Code Review Lab Opened (September 26, 2003) <http://www.microsoft.com/presspass/press/2003/sep03/09-26gspchpr.mspx>.

Claburn, Thomas, "25 Most Dangerous Programming Errors Exposed," in *InformationWeek* (January 12, 2009) <http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=212701491&subSection=News>

Cook, Thomas D., *The Posse Comitatus Act: An Act in Need of a Regulatory Update* (U.S. Army War College, 2008).

Crepeau, Claude, Slakmon, Alain, "Simple backdoors for RSA key generation" (Lecture Notes in Computer Science, 2003 – Springer) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69.1878&rep=rep1&type=pdf

Delibasis, Dimitrios, "Information Warfare Operations Within the Concept of Individual Self Defense" in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni (London, Routledge 2009, 95-111).

Denning, Dorothy E., "Cyberspace Attacks and Countermeasures" in *Internet Besieged: Countering Cyberspace Scofflaws (*Eds) Dorothy E. Denning and Peter J. Denning (New York, New York: ACM Press 1998, 29-55).

Denning, Dorothy E., "Cyberspace Attacks and Countermeasures" in *Internet Besieged: Countering Cyberspace Scofflaws (*Eds) Dorothy E. Denning and Peter J. Denning (New York, New York: ACM Press 1998, 29-55).

Espiner, Tom. "Security Experts Lift Lid on Chinese Hack Attacks." ZdNet

Everard, Jerry, "The @ of War" In *Virtual States: The Internet and the Boundaries of the Nation-State*, (London, UK: Routledge 2000, 97-118, 117).
for Online Crime, CERT Coordination Center, 1 December 2005.

Frezza, Bill, "The Militarization Of Cyberspace," *Network Computing* (March 15, 1997) 35.

Fulghum, David A. and Barrie, Douglas, "Off The Radar; Israel used electronic attack in air strike against Syrian mystery target," in *Aviation Week & Space Technology*, Vol. 167 No. 14 (October 8, 2007, 28)

Fulghum, David A., "Cyber, Kinetic War Collide; Two-seat fighters take on multiple missions as bombing and network-attack combine" in *Aviation Week & Space Technology*, Vol. 167, No. 13 (October 1,2007, 27).

Fulghum, David A., Wall,Robert and Butler, Amy, "Cyber-Combat?s First Shot;

Gardner, Hall, “War and the Media Paradox” in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni (London, Routledge 2009, 11-30).

Gordon, Joshua. *Illegal Internet Networks in the Developing World*. (The Berkman Center for Internet and Society at Harvard Law School: Research Publication No.2004-03 2/2004).

Grant, Ian, "Kids responsible for Estonia attack" *Computer Weekly* (13 Mar 2009) http://www.computerweekly.com/Articles/2009/03/13/235262/kids-responsible-for-estonia-attack.htm

Grow, Brian, Epstein, Keith, and Tschang Chi-Chu, “The New E-Spionage Threat: A Business Week probe of rising attacks on America's most sensitive computer networks uncovers startling security gaps.” In *Business Week* (April 21, 2008).

Harris, Shane, “Chinese Hackers Pose a Clear and Present Danger to U.S. Government and Private-Sector Computer Networks and May be Responsible for Two Major U.S. Power Blackouts.” In National Journal Magazine. (31 May 2008). < http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php>

Hildick-Smith, Andrew, *Security for Critical Infrastructure SCADA Systems*, <http://www.sans.org/reading_room/whitepapers/warfare/1644.php>, 1 (cited on 27 April 2009).

Ianelli, Nicholas and Hackworth, Aaron, *Botnets as a Vehicle*

Internet Corporation for Assigned Names and Numbers, *Factsheet: Root Server Attack on February 7, 2007* <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>, cited on 27 April 2007.

Josh, Rogin,. “Cyber Officials: Chinese hackers attack ‘anything and everything’”.*Journal of Intelligence and CounterIntelligence*,18:4, (2005) 682 -706.

Knowles, John, “Spectrum Warfare” in *The Journal of Electronic Defense* (September 2008, 6).

Kohlmann, Evan. “The Real Online Terrorist Threat.” In *Foreign Affairs* Sep/Oct 2006, vol 58 issue 5 p 115-124.

Kopp, Carlo, "The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction *Air," & Space Power Journal.*

Kunkel, M., “New Cyber Definition Excludes EW” in *The Journal of Electronic Defense* (November 2008, 26).

Lazarev, Yury, Petrov, Peter, “Generation of an intense, directed, ultrashort electromagnetic pulse” *SPIE* Vol. 2557, 512-515

Lewis, James A.. "Cybersecurity and Critical Infrastructure Protection," In *Homeland Security*: *Protecting America's Targets*. Vol. III: Critical Infrastructure. ed. James J.F. Forest (Praeger Security International: Westport, CT, 2006), 324-338, 332.

Libicki, Martin, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: CUP, 2007) pp. 74-84.

Lonsdale, David J., "How Strategic is Strategic Information Warfare?" in *The Nature of War in the Information Age: Clausewitzian Future* (London, UK: Frank Cass 2004, 135-176, 135).

Lyda, Robert and Hamrock, James, "Using Entropy Analysis to Find Encrypted and Packed Malware," in IEEE Security and Privacy (March/April 2007 VOl. 5 No. 2), 41-45.

Mannes, Aaron. 'The Terrorist Threat to the Internet," In *Homeland Security*: *Protecting America's Targets*. Vol. III: Critical Infrastructure, ed. James J.F. Forest (Westport, CT: Praeger Security International, 2006), 339-353.

Markoff, John, "Web becomes a battleground in Russia-Georgia conflict" Intenrational Heral Tribune (August 12, 2008) <http://www.iht.com/articles/2008/08/12/technology/webcyber.php>

Markoff, John, "Attack of the Zombie Computers is a Growing Threat Experts Say", *The New York Times*, 7 January 2007 (Section 1; column 5).

Mitchell, Paul T., "U.S. Military Primacy and the New Operating System" in *Network Centric Warfare: Coalition Operations in the Age of U.S. Military Primacy* (London, UK: Internation Institute for Strategic Studies 2006, 11-26). <Adelphi Paper 385>.

Murphy, John F., "Computer Network Attacks by Terrorists: Some Legal Dimensions," In *Computer Network Attack and International Law*, Michael N Schmitt & Brian T. O'Donnell (eds). International Law Studies, Volume 76 (Naval War College, Newport, Rhode Island 2002), 324-351.

Murphy, John F., "Computer Network Attacks by Terrorists: Some Legal Dimensions," In Computer Network Attack and International Law, Michael N Schmitt & Brian T. O'Donnell (eds). International Law Studies, Volume 76 (Naval War College, Newport, Rhode Island 2002), 324-351.

Nakashima, Ellen and Mufson, Steven, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says" in Washington Post (Saturday, January 19, 2008; A04).

Nakashima, Ellen and Mufson, Steven, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *Washington Post* January 19, 2008; Page A04

Nakashima, Ellen, “Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions,” *Washington Post*, January 26, 2008 p. A03.

Onley, Dawn S. and Wait, Patience in their article “Red Storm Rising: DOD’s Efforts to Stave off Nation-State cyberattacks Begin with China” in Government Computer News (08/21/06.)

Palfrey, John G., Jr, "Local Nets: Filtering and the Internet Governance Problem," in *The Global Flow of Information* (XXXXX 2005)

Prevelakis, Vassilis and Spinellis, Diomidis, “The Athens Affair: how Some Extremely Smart Hackers Pulled off the Most Audacious Cell-Network Break-In Ever” in *IEEE Spectrum* (July 2007) 25-33.

Qiu, Jack Linchuan, “Virtual Censorship in China: Keeping the Gate Between the Cyberspaces,” *International Journal of Communications Law and Policy* Issue 4, (Winter 1999/2000) 1-25.

R.Lujan, Thomeas, "Legal Aspects of Domestic Employment of the Army" in Parameters (Autumn 1997) https://carlisle-www.army.mil/usawc/Parameters/97autumn/lujan.htm

Sherman, Erik, “DNS: Definitely Not Safe, New Attacks on the Internet’s Domain Name Systems Keep CISOs Guessing,” in *CSO* (February 2007) 38-41.

Sherman, Erik, “DNS: Definitely Not Safe, New Attacks on the Internet’s Domain Name Systems Keep CISOs Guessing,” in CSO (February 2007) 38-41.

Silber, Mitchell D. and Bhatt, Arvin, *Radicalization in the West: The Homegrown Threat* (New York Police Department, New York, 2007)

The risk: The usual hazards of not having a good data backup plan?, Wall Street Journal, January 17, 1996; [Brian_Mulvaney@intersolv.com via risks-digest Volume 17, Issue 65].

Thomas, Timothy L., "China's Electronic Long-Range Reconnaissance" *Military Review*, (November-December 2008) 47-54.

Thomas, Timothy L., “Dialectical Versus Empirical Thinking: Ten Key Lements of Russian Understanding of Information Operation” in *The Journal of Slavic Military Studies*, Vol. 11, No. 1 (March 1998).

Thomas, Timothy L., “Russian View on Information Based Warfare” Originally Appeared in *Airpower Journal* Vol. X, EE, Special Edition 1996 25-35, 26.

Thomas, Timothy L.. “Al Qaida and the Internet: The Danger of ‘Cyberplanning.’ In *Parameters* (*Spring 2003, Vol. XXXIII, No. 1).* U.S. Army War College, Carlisle, PA, 112-123, 113.

Verton, Dan, *Black Ice: The Invisible Threat of Cyber-Terrorism* (Emeryville, California: McGraw-Hill 2006) p. 25.

Waltz, Edward, *Information Warfare: Principles and Operations*, (Boston, MA: Artech House, 1998), 1-3.

Wilson Clay, *Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues* (Congressional Research Service: April 2008), 4.

Wilson, Clay, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* (CRS 5 June 2007), 11.

Wingfield Thomas C., *The Law of Information Conflict: National Security Law in Cyberspace (*Falls Church, Virginia: Aegis Research Corporation, 2000), 17.

Winston, Thomas, "Intelligence Challenges in Tracking Terrorist Internet Fund Transfer Activities." In *International Journal of Intelligence and Counterintelligence* (20:2, 2007) 327-343, 330.

Yannakogeorgos, Panayotis A. "Blogs, Libel and Anonymity: The New Face of Cybercrime in Greece" (Hellenic News of America, 28 February 2008) <http://www.hellenicnews.com/readnews.html?newsid=8135&lang=US> Cited on 3 June 2008.

Zanini, Michele and Edwards, Sean J.A., "The Networking of Terror in the Information Age" in *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001) 29-60.

Zheng, Jiexun Li, Rong and Chen, Hsinchun, "From Fingerprint to Wireprint," in *Communications of the ACM* (April 2006 Vol 49. No. 4).

Government Documents

United States

Chertoff, Michael, "Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference," 8 April 2008, < http://www.dhs.gov/xnews/speeches/sp_1208285512376.shtm> cited on 9 April 2008.

Department of Defense, *Information Operations Roadmap* (30 October 2003).

Federal Communications Commission, *Voice Over Internet Protocol: Frequently Asked Questions*: <http://www.fcc.gov/voip/> (Cited on 27 April 2007).

Federal Emergency Management Agency, National Response Framework, Cyber Incident Annex, December 2004, < http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf>, 1.

Federal Emergency Management Agency, Emergency Support Function #2 – Communications Annex, January 2003, http://www.fema.gov/pdf/emergency/nrf/nrf-esf-02.pdf

Federal Emergency Management Agency, National Response Framework, Cyber Incident Annex, 2.

ICANN, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority" March 1, 2000, http://www.icann.org/en/general/ietf-icann-mou-01mar00.htm.

ICANN, Factsheet: Root Server Attack on February 7, 2007 <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>.

Interagency Working Group on Cyber Security and Information Assurance *Federal Plan for Cyber Security and Information Assurance Research and Development* (National Science and Technology Council, April 2006)), http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

National Telecommunications and Information Administration, *Domain Names: U.S. Principles on the Internet's Domain Name and Addressing System (30 June 2005) < http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm>*

NCC Operating Charter < http://www.ncs.gov/ncc/nccoc/nccoc_background.html>

Nightingale, Stephen, Montgomery, Doug, Frankel, Sheila and Carson, Mark, "A Profile for IPv6 in the U.S. Government – Version 1.0" (National Institute of Standards) <http://www.antd.nist.gov/usgv6-v1-draft.pdf>, 2.

Office of Management and Budget, Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002. http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf

Report to Congress of the U.S.-China Economic and Security Review Community (November 2007). I thank Josh Lampen for providing the exact number of terabytes and for other insights on cybersecurity that informed this paper.

The National Military Strategy for Cyberspace Operations, 2006. As read in: Sgt. C. Todd Lopez, Fighting in Cyberspace Means Cyber Domain Dominance, (Air Force Print News, 28 February 2007) <http://www.af.mil/news/story.asp?id=123042670> (cited on 28 April 2007).

Thompson, Bennie and Langevin, James, "Letter from Congressmen Bennie Thomson and James Langevin to Congressman John D. Dingel", May 29, 2008, http://homeland.house.gov/SiteDocuments/20080530130810-85574.pdf

U.S. Code 1385. *Use of Army and Air Force as posse comitatus*. See also:*DOD Directive 5525.5*, January 15, 1986, http://www.dtic.mil/whs/directives/corres/pdf/552505p.pdf.

United States Government Accountability Office, Information Security; Coordination of Federal Cyber Security Resarch and Development (September 2006) <http://www.gao.gov/new.items/d06811.pdf>, 18.

United States Government Accountability Office, Information Security; Coordination of Federal Cyber Security Resarch and Development <http://www.gao.gov/new.items/d06811.pdf>, 17.

United States Government Accountability Office. "Report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology" (Committee on Homeland Security, House of Representatives Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks (June 2008), 11.

White House, National Strategy to Secure Cyberspace, February 2003. http://www.whitehouse.gov/pcipbcyberspace_strategy.pdf, 30.

U.S. Joint Chiefs of Staff, *Joint Publication 3-13.1: Electronic Warfare* (25 January 2007).

U.S. Army Training and Doctrine Command, *Handbook No. 1.02: Cyber Operations and Cyber Terrorism* (Fort Leavenworth, Kansas 15 August 2005).

Congressional Research Service, *Information Operation, Electronic Warfare and Cyberwar: Capabilities ad Related Policy Issues* (20 March 2007).

Greek Documents

"Κανονισμός Για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπερεσιών" in *Εφημερίς της Κυβερνυσεώς* (No. 629a, 26 January 2005) 1013-1020.

Bafoutsou, Georgia, Antoniadis, Nikolaos, Nikolouzou, Eugenia, Panagopoulos, Athanassios, *Regulatory Framework for Communications Security and Privacy in Greece* Presentation at the ETSI Security Workshop: Future Security (16-17 January 2007, Sophia-Antipolis, France), 4.

Bouyatsou, Aristeas "Ακτινογραφία του Μηχανισμού Υποκλοπων" (X-Ray of the Tapping Mechanism) in *Kathimerini* (30, June 2006). Translation is mine. See also: Prevelakis and Spinellis.

Bouyatsou, Aristeas, "Δεκατέσσερα Ερωτήματα που Ζητούν Απάντηση" (Fourteen Questions Without Answers) in *Kathimerini* 2 February 2006.

Bouyatsou, Aristeas, «Η «Άλωση» Vodafone από το λογισμικό των Υποκλοπών" (The Fall of Vodafone from Eavesdropping Software) in *Kathimerini* 3 February 2006.

Evert, Miltiadis, "Εβερτ: 'Δεν Μπορώ να έχω εμπιστοσύνη στη Vodafone'" (Evert: "I cannot trust Vodafone at All.") In Kathimerini (02 February 2006). Translation is mine.

Hadjiyakis, Sotiris, Ομιλία του Υπουργού Δικαιοσύνης στη Βουλή για τις Τηλεφωνικές Υποκλοπές (Statement of the Minister of Justice on the Eavesdropping of Cellular Phones). 3 March 2008.

Hellenic Government. Law No. 3115 "Σύσταση Αρχής Διασφάλισης του Απορρήτου των Επικκοινονίων" (Recommendation of the Committee on the Security and Confidentiality of Communications) 27 February 2003. See also, Hellenic Government, Regulations for the Internal Management of the Authority for the Assurance of Communications Security and Privacy (7 November 2003)

Hellenic Government. Law No. 3115 "Σύσταση Αρχής Διασφάλισης του Απορρήτου των Επικκοινονίων" (Recommendation of the Committee on the Security and Confidentiality of Communications) 27 February 2003. See also, Hellenic Government, Regulations for the Internal Management of the Authority for the Assurance of Communications Security and Privacy (7 November 2003)

Unknown Author, "Η «Εισβολή» της 10ης Αυγούστου του 2004" (The "Invasion" of the 10th of August 2004.) In *Kathimerini* (30 June 2006).

Unknown Author. "Τα Μυστήρια της Παιανίας, ο Eric ο Listener και η Ericsson" (Paianias' Mysteries, Eric, the Listener and Ericsson) in *Kathimerini* (30 June 2006).

Foreign Ministry Archives

Most important to this project have been the voluminous collections of government documents kept by foreign ministries recording the diplomatic processes relevant to the topic of investigation. These were made available to me for the purpose of completing this project. I list here only the documents that have been of use in the making of this dissertation. This is by no means a complete record of government sources I have consulted, but it does indicate the substance and range of documents available in the archives.

Bavaro Declaration, 1.h <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0007!!PDF-E.pdf>

Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions, "Toward a Global Partnership in the Information Society: Translation the Geneva Principles into Actions: Commission Proposals for the Second Phase of the World Summit on Information Society (WSIS)" (13 July 2004) [Com 2004 480 Final]

Council of the European Union General Secretariat, "Main Items Raised at the Working Lunch at Ambassador Level between the Troika and China (Geneva, 5 December 2002 (TGN.1205.02), 3.

Council of the European Union Working Party on Telecommunication and Information Society World Summit on Information Society (WSIS): Internet Governance- Guidelines for Discussions in the WSIS Framework (7 October 2004)

Council of the European Union, Ad Hoc Working Party on Preparation of International Conference for Development- World Summit on Information Society (WSIS), "I/A Item Note: SU Strategy Paper on WSIS (7 June 2004), 3.

Council of the European Union, *Transmission Note: Principal Results of the Regular Meeting of Heads of Mission)(Geneva 15 December 2004),* 3.

Denmark, speech on behalf of the European Union, http://www.itu.int/wsis/docs/pc1/statements_general/denmark.doc.

Diplomatic dispatch dated 16 May 2003 on the results of the E.U. Commissions meeting at the level of delegate-expert.

Diplomatic note on the theme of the Paris intersessional meeting.

DRAFT DECLARATION Based on the DISCUSSION IN THE WORKING GROUP OF SUB-COMMITTEE" in *Report of the Second Meeting of the Preparatory Committee* <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0012!R1!PDF-E.pdf> c.5.20

Draft Declaration of Principles refined on April 22/23.

DRAFT REPORT OF THE CHAIRMAN OF SUB-COMMITTEE 2, <http://www.itu.int/dms_pub/itu-s/md/02/wsispc1/doc/S02-WSISPC1-DOC-0010!!PDF-E.pdf>. *Report of the First Meeting of the Preparatory Committee*, 26.

E.U. Presidency Non-Paper, "The Composition of the U.N. Task Force on Financial Mechanism and the U.N. Working Group on Internet Governance" (9 March 2004), 1)

Email from Ole Neutrup, Mission of Denmark to Ambassador Fillp 10/29/2002 *Bucharest Declaration E.U. Reaction*.

European Commission Working Party on Telecommunications and Information Society, *Preparation of the Transport/Telecommunications and Energy Council of 1/10 December 2004* (6423/04 TELECOM 30 DEVGEN 37 CONUN 6)

European Commission Working Party on Telecommunications and Information Society, *Preparation of the Transport/Telecommunications and Energy Council of 1/10 December 2004* (6423/04 TELECOM 30 DEVGEN 37 CONUN 6), 7.

Final Declaration of the Pan European Regional Conference <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-E.pdf>

Final Declaration of the Pan European Regional Conference<http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-E.pdf>

First Deputy Minister of the Russian Federation for Communications and Informatization of the Preparatory Committee for the World Summit on the Information Society
for the Tunis Phase of the Summit, http://www.itu.int/wsis/docs2/pc1/contributions/eutext.pdf

Greek Delegation, Preliminary Thoughts on the State of Play Regarding the Preparatory Process of Phase Two (22 June 2004) 1.

Hellenic Ministry of Foreign Affairs, Diplomatic Note (27 January 2003).

Kummer, Markus *Report by Mr. Markus Kummer, Head of the Secretariat of the Working Group on Internet Governance,* <http://www.itu.int/wsis/docs2/pc1/wgig/kummer.pdf>.

Letter from Yoshio Utsumi, "World Summit on the Information Society, Tunis Phase, Tunis, 16-18 November 2008" (2 June 2004). (DM-1138).

Note by the WSIS Executive Secretariat, *ACCREDITATION OF NGOS, CIVIL SOCIETY AND BUSINESS SECTOR ENTITIES TO THE WORLD SUMMIT ON THE INFORMATION SOCIETY*, (9 June 2004) <WSIS-II/PC-1/DOC/3-E>.

Number of entities represented as recorded by the World Summit for the Information Society, *About WSIS*, <http://www.itu.int/wsis/tunis/newsroom/index.html>

Number of participants recorded by the World Summit for the Information Society, *About WSIS*, <http://www.itu.int/wsis/tunis/newsroom/index.html>

Office of the United Nations High Commissioner for Human Rights prepared a "Background Note on the Information Society and Human Rights" (October 2003)

Preliminary E.U. Views on the Preparatory Process

Presidency of the Council of the European Union, World Summit for the Information Society-Guidelines for the Exchange of Views at the Council (Brussels 20 June 2005: 10144/05).

President of the Preparatory Committee, *Proposal of an Orientation Document for PrepCom-2*, *

Proposal for the Russian Federation for the text of Principle VI.

Report of the Second Meeting of the Preparatory Committee <http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0012!R1!PDF-E.pdf> b.20

See also Denmark, speech on behalf of the European Union Content and Themes for the World Summit on the Information Society (WSIS) < http://www.itu.int/wsis/docs/pc1/statements_content/denmark.doc>

Statement by Chinese Ambassador SHA Zukang at the First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society, <http://www.itu.int/wsis/docs/pc1/statements_general/china.doc>

Summary of the WSIS Bureau meeting held on Wednesday 8 January 2003.
The Different Actors in the Information Society, http://www.itu.int/wsis/basic/actors.html

Transcript of Ambassadorial meeting in Geneva regarding latest developlents on the WSIS process.

Transcript of the First Meeting at the Ambassadorial level of the European Commission Regarding the World Summit on the Information Society (27 January 2003), 3

Transmission Note for the Attention of E.U. Heads of Mission. *WSIS: Information Exchange of Views Between E.U. Heads of Mission and the ITU Secretary General, Mr. Utsumi* (Geneva, 17 November 2004).
U.N. Charter and the *Universal Declaration of Human rights*

U.N. ICT Task Force Global Forum on Internet Governance to be Held in March http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html

U.S. comments on the Russian text for Principle 6, received October 29.

U.S. Revision to the Russian Proposal.

United Nations Department of Economic and Social Affairs Secretariat of the Working Group on Internet Governance, "Consultations on the Establishment of the Working Group on Internet Governance, Geneva, 20-21 September 2004" (19 August 2004)

United Nations Economic Commission for Europe, *The Information Society in Europea and Nrth America: Contributions from the UNECE to the WSIS Prep Com 2* (December 2002), 3.

United Nations Press Release, "Global Internet Governance System is Working But Needs to Be More Inclusive, U.N. Forum on Internet Governance Told" (26 march 2004) PI/1568. http://www.un.org/News/Press/docs/2004/pi1568.doc.htm

United States Contribution document WSIS/PC-1/CONTR/9-E < http://www.itu.int/dms_pub/itu-s/md/02/wsispc1/c/S02-WSISPC1-C-0009!!MSW-E.doc>, 2.

United States Contribution document WSIS/PC-1/CONTR/9-E < http://www.itu.int/dms_pub/itu-s/md/02/wsispc1/c/S02-WSISPC1-C-0009!!MSW-E.doc>, 2.

United States Position on Phase II of the World Summit on theInformation Society, http://www.itu.int/wsis/docs2/pc1/contributions/us.pdf

World Summit for the Information Society, *Draft Declaration of Principles* (19 September 2003 <WSIS/PC-3/DT/1-E>.

World Summit for the Information Society, *Draft Declaration of Principles* (26 September 2003 <WSIS/PC-3/DT/1(rev.2B)-E>. Para. 28.

World Summit for the Information Society, *Draft Declaration of Principles* (19 September 2003 <WSIS/PC-3/DT/1-E>. Para. 42, alternatives b & c.

World Summit for the Information Society, *Note by the President of PrepCom* (WSIS-II/PC-1/DOC/5-E), http://www.itu.int/wsis/docs2/pc1/doc5.pdf

World Summit for the Information Society, *Tunis Agenda for the Information Society*.

World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration- The Asia-Pacific Perspective to the WSIS*.

World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration- The Asia-Pacific Perspective to the WSIS*. 3.f

World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration- The Asia-Pacific Perspective to the WSIS*, 1.i, 3.p

World Summit on the Information Society, Final Report of the Preparatory Meeting: PrepCom-1 of the Tunis phase (WSIS-II/PC-1/DOC/6-E) <http://www.itu.int/wsis/docs2/pc1/doc6.pdf>.

World Summit on the Information Society, *Plan of Action*, section.

World Summit on the Information Society, *Roles of HLSOC, WSIS-ES, host country Executive Secretariats, and ITU* <http://www.itu.int/wsis/basic/roles.html>

World Summit on the Information Society. *Civil Society Facility Fund*

World Summit on the Information Technology. *Declaration of Principles*.

WSIS, Note by the President, (18 July 2003).

United Nations Security Council

1267 Monitoring Group, *Fifth Report of the Monitoring Team* (20 September 2006) <http://daccessdds.un.org/doc/UNDOC/GEN/N06/529/76/PDF/N0652976.pdf?OpenElement> cited on 4 October 2007.

Independent International Investigation Commission, *Sixth Report of the International Independent Investigation Commission* <http://daccessdds.un.org/doc/UNDOC/GEN/N06/654/33/PDF/N0665433.pdf?OpenElement>, 18. cited on 4 October 2007

U.N. Security Council 1267 Committee, *The Consolidated List established and maintained by the 1267 Committee with respect to Al-Qaida, Usama Bin Laden, and the Taliban and other individuals, groups, undertakings and entities associated with them* <http://www.un.org/sc/committees/1267/consoltablelist.shtml> Cited on 4 October 2007

U.N. Security Council resolutions: 1595

United Nations Security Council, "Marking of Plastic or Sheet Explosives for the Purpose of Detection," Resolution 635 (1989).

United Nations Security Council, Resolution 1535

United Nations Security Council, Resolution 1267.

United Nations Security Council, Resolution 1333

United Nations Security Council, Resolution 1363.

United Nations Security Council, Resolution 1373.

United Nations Security Council, Resolution 1390.

United Nations Security Council, Resolution 1526.

United Nations Security Council, Resolution 1624.

United Nations Security Council, Resolution 1636.

United Nations Security Council, Resolution 1644.

United Nations Security Council, Resolution 1664.

United Nations Security Council, Resolution 1699.

United Nations Security Council, Resolution 1735.

United Nations Security Council, Resolution 1970.

United Nations Security Council, Resolution 732.

United Nations, *Charter of the United Nations*.

United Nations General Assembly

U.N. General Assembly, "Creation of a Global Culture of Cybersecurity." A/RES/57/239. 31 January 2003.

U.N. General Assembly, "Creation of a Global Culture of Cybersecurity." A/RES/57/239. 31 January 2003, Preliminary Paragraph 5.

U.N. General Assembly, "Creation of a Global Culture of Cybersecurity." A/RES/57/239. 31 January 2003, Operational Paragraph 3.

U.N. General Assembly. "Developments in the field of information and telecommunications in the context of international security." A/RES/56/19, PP7. 7 January 2002.

U.N. General Assembly. "Developments in the field of information and telecommunications in the context of international security." A/RES/56/19, PP7. 7 January 2002, PP8.

U.N. General Assembly, Resolution 56/121 (2002), preliminary paragraph 5

U.N. General Assembly. "Creation of a global culture of cybersecurity and the protection of critical information infrastructures." A/RES/59/199. 30 January 2003.

Other International Organizations

Interpol, *Connecting Police: I-24/7* <http://www.interpol.int/Public/ICPO/FactSheets/GI03.pdf> cited on 4 October 2007.

Council of Europe, Convention on Cybercrime (2000), III.4.

Romano, Benjamin J. "Microsoft device helps police pluck evidence from cyberscene of crime" *The Seattle Times* (April 29, 2008) http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html

Sund, Christine. *Building Confidence and Security in the Use of ICT's and the International Cooperation Agenda*. Presentation at UNITAR Symposium on ICT Policy Issues for Development, (notes taken at symposium on 30 August 2006).

Appendix A
Relevant United States Federal Policy and Legislative Initiatives

National Security Council Intelligence Directive 9
Homeland Security Presidential Directive-5 (HSPD-5)
Homeland Security Presidential Directive-7 (HSPD-7)
Executive Order 13133: Working Group on Unlawful Conduct on the Internet
National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems
The Homeland Security Act (Section 223 of P.L. 107-276)
December 2004 Cyber Incident Annex CYB-1 National Response Plan
Executive Order 12333: United States Intelligence Activities
Executive Order 12472: The Assignment of National Security Emergency Preparedness Responsibilities for Telecommunications
Section 706, Communications Act of 1934, as amended (47 U.S.C. 606)
National Security Act of 1947
H.R. 2889: The Computer Security and Training Act of 1985
H.R. 145: The Computer Security Act of 1987
Federal Information Security Management Act (FISMA)
H.R. 9011: The Security and Freedom Through Encryption Act of 1996
S.1726: Promotion of Commerce On-Line in the Digital Era (Pro-Code) Act of 1996
National Strategy to Secure Cyberspace [2003]
S.982: The National Infrastructure Protection Act of 1995 Executive Order 13010: Critical Infrastructure Protection
S.982: The National Information Infrastructure Protection Act of 1996
H.R. 4095: The National Information Infrastructure Protection Act of 1996
H.R. 2413: The Computer Security Act of 1999
H.R.4246: Cyber Security Information Act (2000)
H.CON.RES. 285 Expressing the Sense of Congress Regarding Internet Security and Cyberterrorism
S.2439: Internet Security Act of 2000
S.2448: Internet Integrity and Critical Infrastructure Protection Act of 2000
H.R. 1903: The Computer Security Enhancement Act of 1997
S.376: The Encrypted Communications Privacy Act of 1997
S.377: The Promotion of Commerce On-Line in the Digital Era Act
S.798: Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT Act H.R. 850: Security and Freedom Through Encryption (SAFE) Act
S.854: The Electronic Rights for the 21st Century Act
H.R.2413: The Computer Security Enhancement Act of 1999 H.R. 2616: Encryption for the National Interest Act H.R. 2617 Tax Relief for Responsible Encryption Act of 1999

H.R. 4246: Cyber Security Information Act (2000)
2002 Cyber Security Research and Development Act
HR 285: Department of Homeland Security Cybersecurity Enhancement Act of 2005

Appendix B

Interview Survey: An Assessment of Relevant Stakeholders in the Global Cybersecurity Agenda

If this questionnaire is not given in person, please request for an electronic copy of this document, and send the completed questionnaire to:

Panayotis A. Yannakogeorgos: yannakog@post.harvard.edu

Name of organization: .....

I. Completed by: .....
Position in the organization:……..
Contact information:…….

II. Completed by: .....
Position in the organization:……..
Contact information:……

III. Completed by: .....
Position in the organization:…….
Contact information:…….

Date and place: .....

QUESTIONAIRE

Please kindly fill out the below questionnaire to the best of your ability.

- **General information about your organization**

- **Description of your organization's specialization pertaining to the global cybersecurity agenda/ global culture of cybersecurity:** *please check more then one if you need to describe your organization.*

O Cybersecurity (O *Planning*, O *Development*, O *Design*, O *Operation*, O *Management*)	O Standardization	O Risk-Assessment
O Awareness Raising	O Promotion of Best Practices	O Lobbying (O *national* O *regional* O *local*)
O Scientific Research	O Promoting International Cooperation	O Training

- **In what year was your organization officially founded/registered? ……..**

- **What is the main level of your organizations main operations?**

O local level	O regional level	O national level
O international	O other (please explain)*	

***** Explanation of other:
……
……
……
……
……
……

- **Briefly describe your organizations with regard to the global culture of cybersecurity/global cybersecurity agenda, and how your organization strives to achieve its goals.**

……
……
……
……
……
……
……
……

- **Physical Resources**

- **Does your organization have a central office?**
  O No O Yes

If you answered yes to question 2.A, please answer questions 2.B – 2.D. Otherwise proceed to question 2.E.

- **Does your organization own or rent the central office space?** O Own O Rent

- **Where is your central office located?**

.....

- **If your central office is located within the United Nations, do you have offices in other cities, towns or villages in the world? Please list the locations of these offices, and indicate after each if it is owned by your organization, or rented.**

.....
.....
.....
.....

- **What Information and Communication Technology does your organization operate?**

Equipment	***Available***		**Number**
	Yes	*No*	
PC			
Notebook			
Printer			
Telephone			
Fax			
Copy machine			
Scanner			
Internet access			O dial-up O ISDN O DSL O T1 /T3 O Other, specify:……
LCD projector			
Website			URL: _____ average number of domestic hits ____ average number of international hits ____ Which country has the most visits? _____

o Human Resources

- **Members**

* members	O < 6	O 7-15	O 16-29	O 30-50	O > 50
* gender	Female=		Male=		
* main profile (you may chose more than one)	O Academics	O Scientists	O Government. Officials	O Private-Sector	O Civil Society

- **Staff and volunteers**

Permanent staff	O 1	O 2	O 3-5	O 5-10	O .....
Contractors	O 1	O 2	O 3-5	O 5-10	O .....
Volunteers	O <5	O 5-10	O 10-25	O 25-50	O .....
Internets	O <5	O 5-10	O 10-25	O 25-50	O .....

- ***Do volunteers contribute to your organization?***

O No O Yes Number: . . . . . .

If you answered yes to question B.1, then please answer questions 1.a -1.g. If you need more space, please continue writing on the back of this page. If you have internal memos available that provide answers to these questions, please feel free to include it along with the questionaire.

o *Do you actively recruit new staff members/volunteers? How?*

.....

.....

.....

.....

.....

o *What is the role of volunteers in your organization?*

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

- *How do you support/t new volunteers or train new volunteers that require new skills to fulfill your organizations objectives?*

  .....

  .....

  .....

- *Is there a membership fee? (if yes, can you circle what percentage represents the annual budget)*

- *Do members pay?*

- *Are all members registered with your organization?*

- *Do members receive updated information about your organization?*

· ***Dedicated Staff***

O No O Yes Number: . . . . . .

If yes, then please proceed with folowing questions:

- *What is the expertise of staff?*

- *How are they recruited?*

- *Do they receive support? If so, what kind of support do they recieve? (if not monetary, then list fringe benefits).*

- *Does their professional background or education fit with the work?*

- *When a position becomes vacant, are there people immediately available to fill that position?*

▪ **Meetings**

· ***Annual meetings***

Regular membership meetings: O No O Yes Number/year: .....

Minutes of meetings recorded: O No O Yes
Minutes of meetings distributed: O No O Yes
Number of People who attend your organization's meetings?: .....

· ***Board / Executive Body***

Number of board members: .....

Can staff members also be members of the board? O no O yes
Number of staff member of board:.....

Board Members are elected by: O board members O members of annual meeting

· ***Board meetings***

Regular board meetings: O No O Yes Number/year: .....
Minutes of meetings available: O No O Yes

· ***Minutes of meetings distributed:***

O No O Yes
If yes describe how: ……

- **Financial Information**

  - What is the size of your annual budget (for the last two fiscal years 2006 and 2007)

    ……

  - Who is responsible for making annual budget?

    ……

  - Who is responsible for writing financial reports?

    ……

  - What is your planned annual budget for 2008?

    ……

  - Do you conduct a yearly financial audit?

……

- What are your domestic sources of funding?

……

- What are your international sources of funding?

……

- **Achievements to Date**

- Please provide a list of publications that you have produced in the last years? Include author, title, publisher, date of publication.

.....
.....
.....
.....
.....

- What is the most significant contribution your organization has made to the global cybersecurity agenda/global culture of cybersecurity in the past 2-3 years?

.....
.....
.....
.....

- How many projects did you complete over the previous two years?

.....
.....
.....
.....

- What challenges has your organization encountered in its efforts over the past 2-3 years. In what areas does your organization need the most improvement?

.....
.....
.....
.....

1. What was the total duration of the project in days, months or years?

.....

.....
.....
.....

2. If the projects are ongoing, what is their current stage?

.....
.....
.....
.....

3. Were there changes in the execution of the project from the original plan? Was there delay? What were the reasons for the delay? Please include any problems with the civil society, private sector, national government, international organization, or internal problems within your organization.

.....
.....
.....
.....

4. How closely did the accomplishments meet your initial goals?

.....
.....
.....
.....

5. Where there any failures in meeting your goals?

.....
.....
.....
.....
.....

- **Institutional Development**

  - **Networking**

    - **Partnerships with other organizations**

1 Do you invite people of other organization to attend your seminars, training sessions or meetings as participants?

O Always O Often O Sometimes O Occasionaly O Never

2 Do you make use of the expertise of other organizations, such as trainers, an expert, guest speaker for your activities (e.g. training seminars)?

O Always O Often O Sometimes O Occasionaly O Never

3 Do you involve people from other organizations in working groups to prepare and organize joint activities?

O Always O Often O Sometimes O Occasionaly O Never

4 Do you have project in which other organizations are involved in the development of applications. (joint project proposal to a source of funding?)

O Always O Often O Sometimes O Occasionaly O Never

5 Are you interest in joint projects with other organizations? What are some barriers for cooperation in joint projects?

O Always O Often O Sometimes O Occasionaly O Never

....
....
....
....
....
....

- **Political Cooperation with other organizations**

1 Do you do lobby work towards official institutions of national governance?

O Always O Often O Sometimes O Rarely O Never

2 Do you lobby together with other organizations? Which one(s)?

O Always O Often O Sometimes O Rarely O Never

....
....

3 How? For example: joint documents, joint visits of meetings with the ministry?

....

....
....
....

4 Are there representatives of all interested stakeholders in the global culture of cybersecurity participating in meetings with higher councils, committees, Ministries of Communications, etc?

O Always O Often O Sometimes O Rarely O Never

....
....
....
....

Note: Please mention few NGOs, private-sector actors, other organizations, personnel, institutions of diplomacy that are applicable to questions 6.A. 1-a and 1-b)?

.....
.....
.....
.....
.....

- **Publicity**

· Do you have a media strategy that includes media outlets in your activities?

O Always O Often O Sometimes O Occasionaly O Never

· Do you invite press to your activities?

O Always O Often O Sometimes O Occasionaly O Never

· Do you send articles to magazines or other publications of other organizations?

O Always O Often O Sometimes O Occasionaly O Never

· Do you issue press releases which aim to inform the public of your activities?

O Always O Often O Sometimes O Occasionaly O Never

· Do you receive feedback from the media on your activities? How?

O Always O Often O Sometimes O Occasionaly O Never

.....

- **Contact with the Government (if you are a government organization, you may skip this section).**

· Do you involve government authorities in your work?

LOCAL O Always O Often O Sometimes O Occasionaly O Never
NATIONAL O Always O Often O Sometimes O Occasionaly O Never
REGIONAL O Always O Often O Sometimes O Occasionaly O Never
INTERNATIONAL O Always O Often O Sometimes O Occasionaly O Never

· Do you inform the government about your activities? If so, which ministry(ies) is/are your main point(s) of contact?

O Always O Often O Sometimes O Occasionaly O Never

.....
.....
.....

· Are you aware of domestic legislation relevant to the global cybersecurity agenda?

O Yes O No

· Do you use domestic legislation to justify your activities? Please list laws relevant to your activities.

O Always O Often O Sometimes O Occasionaly O Never

.....
.....
.....
.....
.....
.....
.....
.....
.....

· Do you use international or European Union law to justify your activities? Please list which laws.

O Always O Often O Sometimes O Occasionaly O Never

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

Note: Can you mention few NGOs, organizations trainers institutes applicable (under 6.C. 1 to 4)?

.....
.....
.....
.....
.....

- **Organizational Experience**

  - Do you have experience with private-sector or national cybersecurity development plans?
    O No O Yes

  - Briefly describe activities which your organisation has recently organised on a local level to contribute to cybersecurity development/cybersecurity education and describe the:

    Aims

    Methods

    Results

    Partners in the Activity

  - If you have none, do you have plans for such type of work? What are these plans?

  - Do you have experience with public-private partnerships in forums, planning processes or similar events that you attended and gave your comments? If yes, please describe below:

.....
.....
.....
.....
.....

- **Further Variables for Consideration**

  - **Decision Making Structures and Processes**

    - **Multilateral Decision Mechanisms**: How did existing institutions of diplomacy (in the United Nations, national, regional and/or local) facilitate or impede progress?

.....
.....
.....
.....
.....

    - **How has the landscape of cyber security within your area of jurisdiction changed in the past 2-3 years?**

.....
.....
.....
.....

    - **Briefly describe any emerging threats that were not previously considered under your original mission and how your organization currently plans to address these threats?**

.....
.....
.....
.....
.....

    - **Multilateral Authorities**: How well empowered were lead multilateral diplomatic bodies in the scope of their authority to exercise effective control over policy implementation?

.....
.....
.....
.....

    - **Lead agency Approach**: Did existing bodies assign implementation to a lead agency? To what extent did this assignment produce unity of effort with other agencies?

.....

.....

.....

.....

- **Informal-Informal Decision Mechanisms**: Did informal and ad hoc bodies have to be established? Did these bodies work well or did they suffer from problems (e.g., take too long to become effective)?

.....

.....

.....

.....

.....

- **Organizational Cultures**

  - **Individual Agency Behaviors**: How did strong individual department and agency bureaucracies of member-states promote or resist sharing information and implementing decisions with multilateral bodies?

.....

.....

.....

.....

  - **Interagency Culture**: How did different agency and department cultures, including leadership styles and behavior, reinforce collaboration or competition among organizations?

.....

.....

.....

.....

  - **Shared Values**: How did existing organizational cultures and personnel systems discourage or reward individual agency performance over unity of global cybersecurity purposes and efforts?

.....

.....

.....

.....

- **Missions and Mandates**: Were government and private sector partners able or unprepared to apply their expertise rapidly in a risky global environment?

- **Expeditionary Mindset**: Did government and private-sector partners have a culture that embraces operational activities (i.e. making success in the field as important as success at Headquarters or member-states capitals?

.....

.....

.....

.....

- **Capabilities and Resources**

  - **Staff**: Were multilateral diplomatic staff capabilities sufficient enough to provide rapid policy, planning and implementation direction? If not, what capabilities were lacking?

.....

.....

.....

.....

  - **Sufficient Resources:** Did private sector, civilian and government departments and agencies have sufficient resources to carry out their cybersecurity responsibilities? If not, what resources were lacking?

.....

.....

.....

.....

  - **Multilateral Resourcing**: To what extent did relevant U.N. bodies (e.g ITU) provide the necessary resources and the authorities to permit their effective use?

.....

.....

.....

.....

  - **Resource Management**: To what degree were agencies and departments able to effectively administer the resources and programs they controlled?

.....

.....

.....

- **Information Management**: To what extent were bodies able to generate, find, and quickly access relevant information and analysis?

.....

.....

.....

.....

- **Legal**: Were there any specific legal issues that affected decision-making processes and structures, organizational culture, or capabilities and resources?

.....

.....

.....

.....

The questionaire is complete. Your assistance with this project is greatly appreciated.

Appendix C
Council of Europe Convention on Cybercrime

For their part, governments have been working on harmonizing domestic cybercrime laws. The UNGA resolutions urge U.N. Member States to consider the Council of Europe's *Convention on Cybercrime* (COE Convention) as model law, along with other international and regional efforts, as they "develop their national law, policy and practice to combat the criminal misuse of information technologies."[565] The Convention is an international effort, albeit one primarily between European states, and provides further insight into the role of government in cybersecurity. The COE Convention intends to facilitate the harmonization of national legal measures pertaining to cyberspace and its criminal uses. Since this Convention was signed, various states outside of the Europe Union, including the United States, have signed and ratified the convention, though most signatories have not ratified it as of this writing.[566] It should be noted that cases exist where non-ratifying signatories have worked within the scope of the COE Convention to investigate cybercrimes.[567]

The COE Convention focuses on the criminal misuse of ICT. Key elements of the COE convention identified in the UNGA resolutions include provisions on the

---

[565] CITE RESOLUTION, OP1.

[566] The following COE member states have ratified the COE Cybercrime Convention: Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Latvia, Lithuania, Netherlands, Norway, Romania, Slovakia, Slovenia, the Former Yugoslav Republic of Macedonia (FYROM), Ukraine; United States (Not a member of the Council of Europe). <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG> cited on: 8 May 2008.

[567] Panayotis A. Yannakogeorgos "Blogs, Libel and Anonymity: The New Face of Cybercrime in Greece" (Hellenic News of America, 28 February 2008) <http://www.hellenicnews.com/readnews.html?newsid=8135&lang=US> Cited on 3 June 2008.

harmonization of procedural law and the establishment of an international 24/7 Network staffed by properly equipped and trained personnel who can address instances of cybercrime. Overall, the COE Convention forms an important part of global cybersecurity efforts in addition to the relevant UNGA resolutions, WSIS. It is an emerging customary international law of cyberspace.

The preamble of the COE Convention outlines the basic assumptions underlying the European effort to deal with cybercrime. In line with the view held by the U.N. General Assembly, the Council of Europe identifies a:

> ..need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights…. including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy…[and is] mindful also of the right to the protection of personal data.

Emphasis is placed on upholding the principles of human rights, including access to the free-flow of information, which is considered a fundamental ideal of the Information Society. However, one might argue that these are not the ambitions of all states, and thus could pose problems for the universal adoption of the COE Convention.

Article I.2 of the COE Convention pertains to illegal access, illegal interception, data interference, system interference, misuse of devices, computer related forgery and fraud, child pornography offences, infringement of copyrights and the aiding or abetting and corporate liability of any of the above offences. The COE Convention requires that parties to the convention have domestic laws making infringement of these elements punishable by "proportionate and dissuasive sanctions, which include deprivation of liberty… [and that legal persons] shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary

sanctions."[568] However, as previously highlighted, the private sector is mandated as being primarily accountable for providing cybersecurity, thereby making companies and individuals responsible for reporting instances of cybercrime to law enforcement authorities and implementing their own security.

The COE Convention elements harmonizing national procedural cybercrime investigations are notable in that they guide law enforcement authorities with the best practices for gathered information pertaining to a cybercrime on the basis of which a perpetrator might be prosecuted. [569] Articles sixteen and seventeen oblige the signatories to preserve stored computer data or traffic data that might be useful in an investigation. To prevent problems associated with information sharing, article eighteen requires that parties to the COE Convention adopt domestic legislation facilitating international cooperation between law enforcement authorities. In passing such legislation, information gleaned from equipment seized in the course of a cybercrime investigation can be made available to parties in a third country within the framework of the COE Convention.

While an investigation of the actual computers used in a crime is important, article twenty covers issues pertaining to the real-time collection of traffic data by service providers. Once again, the brunt of an important aspect of providing security is placed on the private sector stakeholders who, as demonstrated in the case study below, might not preserve important data for law enforcement since data storage space is a scare resource. Traffic data competes with billing data, and the latter is often deemed more important to

[568] CITE 1.2

[569] CITE: second section of the COE Convention

the interests of service-providers.[570] The COE Convention legally binds service providers, such as the operators of Internet cafes, to cooperate with officials investigating a case of cybercrime when they request traffic and content data.[571]

Section three, article twenty-two pertains to determining which state has jurisdiction over a cyber-criminal. The assumption is that the private sector has abided by the best practices of data storage outlined above, and through its cooperation with law enforcement the identity of a cybercriminal has been determined. In such cases, jurisdiction over the criminal is given to a state if the act occurs:

> a) in its territory; or b) on board a ship flying the flag of that Party; or c) on board an aircraft registered under the laws of that Party; or d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.[572]

This section encourages parties to the convention to bilaterally resolve conflicts over jurisdictional claims if more than one party considers an offender to have been acting in its jurisdiction. A theoretical case illustrating potential complexities is useful here. Assume a cybercrime occurs in the exclusive economic zone of State X against State X by a national of State Y on a ship flying the flag of State Y. Both States X and Y would have jurisdictional claim over the offender. Under the COE, the two countries would have to consult with each other to solve these jurisdictional issues.

---

[570] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair: how Some Extremely Smart Hackers Pulled off the Most Audacious Cell-Network Break-In Ever" in *IEEE Spectrum* (July 2007) 25-33.

[571] CITE

[572] CITE

Double-criminality and extradition is one of the most problematic areas for the investigation of cybercrimes and the prosecution of cybercriminals operating in states that lack domestic laws protecting ICT.[573] Crimes committed using ICT originating in State X (a State where no domestic cybercrime laws exist) targeting a computer in State Y (which does have cybercrime laws) are resolved if both parties have signed and ratified the COE Convention. Addressing this issue is a key provision of the COE Convention. Specifically, it establishes that:

> The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[574]

This eliminates the possibility of a cybercriminal to act without the certainty that he or she will avoid extradition from a country lacking domestic laws criminalizing the misuse of ICT. While encouraging the adoption of such domestic laws, parties to this convention agree to act concordant with the COE Cybercrime Convention.

Article twenty-five outlines general principles of mutual assistance, whereas article twenty-six covers issues of spontaneous information. That is, if law enforcement authorities in State X discover information pertinent to an investigation in State Y, and

---

[573] John F. Murphy, "Computer Network Attacks by Terrorists: Some Legal Dimensions," In *Computer Network Attack and International Law*, Michael N Schmitt & Brian T. O'Donnell (eds). International Law Studies, 76 (Naval War College, Newport, Rhode Island 2002), 324-351.

Marc D. Goodman and Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace" in *International Journal of Law and Information Technology* (10 No. 2, 2002) 139-223, 140-143.

[574] Council of Europe, Convention on Cybercrime (2000), III.4.

State Y has not requested the information, then State X may forward the information to State Y. State X has the right to request that the information be kept confidential or to place conditions on the use of the information.

While in a presentation of this length it is not possible to cover all aspects of the COE Convention, important elements have been summarized in order to emphasize its importance in the creation of a global culture of cybersecurity. It is encouraging to see that international efforts recognize the importance of this convention as a model treaty that can help overcome the various hurdles countries will face when conducting investigations.

Curriculum vitae

Place of Birth:

Atlanta, Georgia, United States, 31 May 1982

Secondary Schools:

American Community Schools of Athens (Greece) 1995-2000

Brookline High School (Brookline, Massachusetts, 2000-2001 (U.S. High School Diploma

University Education:

Harvard University 2002-2005, ALB in Philosophy (2005)

Rutgers University 2005-2009, M.Sc. Global Affairs (2007) , Ph.D. Global Affairs (2009)

Principal Occupations During Time of Doctoral Research:

Permanent Mission of Greece to the United Nations (2006) Adviser for Security Council desk.

Rutgers University, Teaching Fellow (2007-2009).

Hellenic Ministry of Foreign Affairs (June 2008) Delegate-Expert to International Telecommunications Union