Spring 2010

Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem

Jeff J. McNeil

MATURING INTERNATIONAL COOPERATION TO ADDRESS THE CYBERSPACE ATTACK ATTRIBUTION PROBLEM

by

Jeff J. McNeil
B.A. August 1992, University of Nebraska-Lincoln
M.A. May 1999, Old Dominion University

A Dissertation Submitted to the Faculty of Old Dominion University
in Partial Fulfillment of the Requirements for the Degree of

DOCTOR OF PHILOSOPHY

INTERNATIONAL STUDIES

OLD DOMINION UNIVERSITY
May 2010

Approved by:

Kurt T. Gaubatz (Director)

Regina C. Karp (Member)

Michael L. McGinnis (Member)

ABSTRACT

MATURING INTERNATIONAL COOPERATION TO ADDRESS
THE CYBERSPACE ATTACK ATTRIBUTION PROBLEM

Jeff J. McNeil
Old Dominion University, 2010
Director: Dr. Kurt T. Gaubatz

One of the most significant challenges to deterring attacks in cyberspace is the difficulty of identifying and attributing attacks to specific state or non-state actors. The lack of technical detection capability moves the problem into the legal realm; however, the lack of domestic and international cyberspace legislation makes the problem one of international cooperation. Past assessments have led to collective paralysis pending improved technical and legal advancements. This paper demonstrates, however, that any plausible path to meaningful defense in cyberspace must include a significant element of international cooperation and regime formation.

The analytical approach diverges from past utilitarian-based assessments to understand the emerging regime, or implicit and explicit principles, norms, rules, and decision-making procedures, around which actor expectations are beginning to converge in the area of cyberspace attack attribution. The analysis applies a social-practice perspective of regime formation to identify meaningful normative and political recommendations. Various hypotheses of regime formation further tailor the recommendations to the current maturity level of international cooperation in this issue area.

Examining international cooperation in cyberspace and methods for maturing international cooperation to establish attribution in other domains inform political

mitigations to the problem of cyberspace attack attribution. Potential solutions are analyzed with respect to four recent cyberspace attacks to illustrate how improved international cooperation might address the problem. Finally, a counterfactual analysis, or thought experiment, of how these recommendations might have been applied in the case of rampant Chinese cyber espionage inform specific current and future opportunities for implementation. Although timing is difficult to predict, the growing frequency and scope of cyber attacks indicate the window of opportunity to address the problem before some form of cataclysmic event is closing.

This paper is dedicated to my supportive parents, wife, and finally my children, for whom my graduate studies have spanned their entire lives.

ACKNOWLEDGEMENTS

I wish to especially thank my committee chair and members. Dr. Kurt Taylor Gaubatz provided significant guidance and many hours reviewing the numerous drafts of this and many previous papers. His tutelage and dedication surpassed that a student at any university might hope for. Dr. Regina Karp initially invited me into the doctoral program, and likewise mentored me throughout my time in the program. I thank Brigadier General Dr. Mike McGinnis, USA (ret.) for his patient and thorough review of my paper from both a technical and defense perspective.

Numerous individuals from throughout the technical and defense communities also reviewed previous revisions. I would like to especially thank Jeff Car, President and CEO of GreyLogic and Principal Investigator for Project Grey Goose, for his thorough review from a technical perspective. I also thank Lieutenant Colonel Timothy Thomas, USAR (ret.) for reviewing my China thought experiment for accuracy and content.

I thank my wife, Kim, and family and friends who have supported me in this endeavor. I am most appreciative of Kim McNeil, Karyn Doran and Linda Birge for their patient and meticulous support editing the final draft. I am especially grateful for the perspective I gained from my time as the U.S. DoD Joint Futures Lab Deputy Director for International Engagement under Colonel John "Jack" Klevecz, USA (ret.). I would also like to thank Mr. Don Murvin and the U.S. Strategic Command Global Innovation and Strategy Center for providing me time to complete it in my current capacity.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

EXECUTIVE SUMMARY

Cyberspace attacks have become a matter of daily front page news. Operation Aurora, the December 2009 to January 2010 cyber attack on Google subsequently attributed to servers in China, is an excellent case in point.[1] Additional vulnerabilities and attacks against the US electrical power grid raise the stakes even further invoking the specter of a cyber 9/11 or even World War III.[2] Loss of confidence in financial transactions and other secure communications could set global society back to the pre-information age.[3] Although timing is difficult to predict, the growing frequency and scope of cyber attacks indicate the window of opportunity to address the problem before some form of cataclysmic event is closing.

In the spring of 2009, General Kevin Chilton, commander of U.S. Strategic Command, and Mr. Tom Weaver of his Strategy and Policy Directorate noted: "The most significant deterrence challenge posed by the threat of cyberspace attack is the perceived difficulty of attributing such attacks to a specific attacker, be it a state or nonstate actor."[4]

This dissertation follows the format requirements of *A Manual for Writers of Term Papers, Theses and Dissertations* 7th edition by Kate L. Turabian.

[1] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora (accessed February 20, 2010); and John Markoff, "2 China Schools Said to Be tied to Online Attack," *New York Times*, February 18, 2010, http://www.nytimes.com/2010/02/19/technology/19china.html (accessed February 20, 2010).

[2] Jeffrey Carr, "Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats," *GreyLogic*, January 21, 2010.

[3] Eugene E. Habiger, "Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach," *Cybersecurity Institute*, February 1, 2010.

[4] Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly*, Spring 2009, 39.

Cyberspace attacks are difficult to detect and even more difficult to attribute. Even if an attack is attributed to a specific machine, the attack must be attributed to a user determined to even know their machine was involved in the attack. To prove state culpability, it must further be shown the user was acting under state direction or acquiescence. The lack of technical detection capability moves the problem into the legal realm; however, the lack of domestic and international cyberspace legislation makes the problem one of international cooperation. Given the de-facto reliance on international cooperation, this paper questions: "How might maturing international cooperation mitigate the cyberspace attack attribution problem?"

Four recent cyber attacks, including those on Estonia (2007), Georgia (2008), Kyrgyzstan (2008-2009), and the U.S. and Republic of Korea (2009) illustrate specific problems of cyberspace attack attribution. The attacks also highlight the de-facto principles and norms of the nascent cyberspace attack attribution regime, and others worth pursuing to pressure states and entities to assist in mitigation and attribution efforts.

The regime has so far been ineffective at imposing costs to shift the burden of attribution from the defender to the attacker. Past assessments have led to collective paralysis pending improved technical and legal advancements. While states and international organizations are changing their behaviors based on perceived costs and benefits, their lack of effectiveness continues to embolden and even entice violators.

The regime is, however, creating arrangements that affect more normative political behaviors, including processes of social learning. Normative and political criteria focused on attack mitigation support a very different assessment and the

identification of meaningful recommendations for advancing global security in cyberspace.

States and entities voluntarily support mitigation efforts primarily for reasons of political support for victim states and secondarily out of collective interest in Internet security. If the collective-action problem is to be addressed to realize joint gains, these priorities require reversal through mechanisms sufficiently embedded in internal state politics to appreciably enmesh state or non-state behavior.

Applying this evidence against factors prominent in theories of regime formation demonstrate the current cyberspace attack attribution regime remains in the early stages of regime development. Identifying opportunities to shape expectations, promote institutional learning, enmesh actors, and coerce compliance support specific recommendations tailored to the maturity level of the regime. Recommendations identified from successful outcomes in other domains and the unique nature of cyberspace, are integrated into a broad policy approach. This approach was evaluated through a counterfactual analysis, or thought experiment, of Chinese information warfare theory and development to develop conclusions and recommendations in the form of current and future opportunities.

First, *Internet security organizations such as computer emergency response teams (CERT) and the international telecommunications union (ITU) global response center (GRC) should work even more closely with public-private hybrid organizations to share information and assessments*. One of the key aspects of Operation Aurora is that Google broke silence. This is proving to be instrumental to future action and deterrence. Transparency of technical evidence of the majority of attacks to a broader audience

would greatly enhance power in this area. Hybrid organizations include both decentralized aspects more attuned to the decentralized nature of cyberspace as well as traditional centralized features that allow for the provision of security, authority, and accountability.

Second, *international funding tied to improved technical and legal standards* should be made available to hybrid organizations to provide incentives for cooperation and an ability to impose costs for detractors and violators. This would have to be tempting for nations ultimately desiring economic development and Internet security. International funding provides needed capacity as well as an incentive that may be withheld to coerce detractors.

Third, *technological development efforts provide cooperative opportunities to address a range of issues* such as China's outlaw mentality to software procurement and development. In the example of Operation Aurora, Google claimed intellectual property had been stolen. This opens a venue to recourse through world intellectual property organization (WIPO) and world trade organization (WTO) dispute settlement mechanisms, potentially significantly extending the shadow of the future for would-be rational attackers.

Fourth, *venues for international discussions and consensus-building in this issue area should be pursued in the form of negotiating rounds*. Such a stepwise approach shapes expectations, promotes institutional learning, enmeshes actors, and facilitates the ability of the global Internet community to coerce compliance. Current dialogue over Operation Aurora provides a specific venue, as do recent U.S.-Russian discussions. More deliberate venues such as ITU Internet governance forum (IGF) dynamic coalitions and

other established telecommunications sector discussions also provide less confrontational and more enduring opportunities.

Fifth, *power to advance the regime and coerce violators is gained through cooperative efforts, the ability to withhold funds or technologies, and a dispute settlement mechanism allowing for variance across technical, economic, social and political regions*. These efforts provide a venue to enmesh responsible actors. For example, the fact regarding Operation Aurora is that many in China now want Google to stay.

Allowing various levels of state control over the array of hubs, networks, and domains may place another potential conflict of interest aside through better understanding and informed decision-making in support of future development and investment decisions. The key point here is one of privacy versus censorship and control. Human rights advocates and civil liberties lawyers want total anonymity. Groups such as the Open Net Initiative and Electronic Freedom Foundation advance this agenda. Conversely, law enforcement officers and security officials want transparency. At the far end of this spectrum pushing beyond transparency to control is China's "Golden Shield" of censorship.

This is at the very heart of the current Operation Aurora controversy. Since Google's entry to China, the company has been subject to intense criticism for complying with censorship laws. By doing so, however, Google established a foothold, drawing China into a position of accountability and responsibility. Google declared it would stop abiding by national censorship laws only after evidence of cyber espionage, in essence, daring the Chinese government to throw them out of the country. Google has established

real bargaining power in this situation, for perhaps the first time. Only time will tell how much power Google has amassed vis-à-vis the Chinese government.

Although the focus of this paper is cyberspace as a security domain, the vast majority of the Internet is civil, commercial and recreational in nature. Attacks in cyberspace are felt across commerce and industry, and non-military activities comprise the bulk of responsibilities and authorities. Therefore, the public-private sphere provides both a first line of defense, and necessary role in response actions. Addressing cyberspace from a purely security perspective is therefore misleading, unhelpful and insufficient for formulating recommendations.

While governments and institutions spawned the Internet and have worked to subsequently control and manage it, decentralized forces have revolutionized not only the world of cyberspace, but through it the world we live in. The sheer magnitude of cyberspace and the fact the bulk of communications over it are of a business or leisure nature, place departments or ministries with these jurisdictions, such as the U.S. Department of Commerce, in a much better position to pursue these agendas than military departments or security agencies. This has an important ramification for how state security efforts in cyberspace should be viewed.

While viewing cybersecurity operations as a form of irregular or hybrid warfare may be effective in the offense, lack of control over the domain dooms it to failure in the defense. A hybrid warfare approach offers no incentives for competitors to work together to realize joint gains. The recommendations are rather focused on moving the cyberspace domain out of the grey area between peace and war where irregular warfare thrives. Regardless of how individual states chose to advance their own security in cyberspace,

this paper illuminates one immutable truth: *any plausible path to meaningful defense in cyberspace must include a significant element of international cooperation and regime formation.*

PURPOSE AND IMPORT OF RESEARCH

This paper examines international cooperation in the area of cyberspace attack attribution, identifying specific political mitigations to the problem. General Kevin Chilton, the Commander of United States Strategic Command recently noted "the most significant deterrence challenge posed by the threat of cyberspace attack is the perceived difficulty of attributing such attacks to a specific attacker, be it a state or nonstate actor."[5] As recently as January, 2010, a pentagon wargame showed "[the] enemy had all the advantages: stealth, anonymity and unpredictability. No one could pinpoint the country from which the attack came, so there was no effective way to deter further damage by threatening retaliation... [The military] lacked the legal authority to respond."[6]

This problem is further complicated by the lack of known historical track record of detection, attribution, response, or even mere definition as few nations have publicly defined what they consider to be a cyberspace "attack."[7] This lack of formal definition clearly hampers coordinated assessment and response by policy-maker and theorist alike.

---

[5] Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly*, Spring 2009, 39.
[6] John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, January 26, 2010.
[7] Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly*, Spring 2009, 39-40.

The community has recognized the difficult challenge of attribution, as well as the fact that a purely technological solution is impossible. As one further challenge, security mechanisms need to make it possible to attribute malicious behavior, as defined by society through a legal or policy process, while preserving privacy in the case of benign use. The Internet will remain a valuable medium so long as the free share of human thought unimpeded by fear of retribution is preserved.[8]

The spectrum of conflict addressed within this paper is attacks conducted or sponsored by nation-states against other nation-states or their critical infrastructure. It does not address cyber crime or recreational hackers for which other legal remedies exist or are being researched elsewhere. This scope is consistent with existing literature of deterrence, or the persuasion of one's opponent that the costs or risks of a given course of action outweigh the benefits.[9] Successful deterrence requires a sufficient probability of attack detection and attribution to be effective.

As observed in other areas of international cooperation, the vast majority of cyberspace activity routinely occurs effectively, efficiently and securely on a global scale.[10] This echoes an oft-cited response to critics of international law upon observation that most of the nations follow most of the rules most of the time.[11] The problem occurs when they do not. Kenneth Oye specifically addresses the difficulty in achieving cooperation in world politics, noting "[there] is no common government to enforce rules,

---

[8] Jeffrey Hunker, Bob Hutchinson, and Jonathon Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution," Institute for Information Infrastructure Protection, January, 2008, http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf, (accessed January 4, 2010).
[9] Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (Columbia UP, 1974), 11.
[10] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001).
[11] Malcom N. Shaw, *International Law*, Fourth Edition (Cambridge UP, 1997), 6.

and by the standards of domestic society, international institutions are weak. Cheating and deception are endemic."[12] Yet the case studies cited by Oye demonstrate that cooperation is sometimes attained, albeit with significant variance among issues and over time.

Law is not the only basis for international cooperation. Regimes are "implicit or explicit principles, norms, rules, and decision-making procedures around which actor expectations converge in a given issue-area."[13] Marcus Franda has presented a convincing case for the burgeoning cyberspace regime from the perspective of Internet and worldwide web development and operation.[14] This dissertation builds upon Franda's research with regards to the specific problem of attribution in cyberspace.

RESEARCH QUESTION AND APPROACH

Given the de-facto reliance on international cooperation, this paper inquires: "How might maturing international cooperation mitigate the cyberspace attack attribution problem?" This leads to the null hypothesis that: "Given the lack of technical attribution, deterrence in cyberspace cannot be achieved through regime-level principles and norms."

The ramifications of the null hypothesis, if true, are enormous. Without state control and provision of physical and information security, global security is at its heart jungle rules where might makes right. This means deterrence is limited to military

---

[12] Kenneth Oye, *Cooperation Under Anarchy* (Princeton UP, 1985), 226.
[13] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 2.
[14] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001).

coercion, with little room for peaceful incentives, and international cooperation is ultimately doomed to failure.

If, however, the null hypothesis is proven wrong, it not only supports international cooperative efforts in matters of global security, but it does so in perhaps the most uniquely contested environment of global cyberspace. One of defining features of the Internet is its level of decentralization. From the standpoint of the World Wide Web, Jeff McNeil holds the same position as Barak Obama or Sarah Palin. We are all users – independent, empowered, and in many ways, at least at times and places of our choosing, anonymous. If the principles and norms of international regimes stand up to this test case, it may be some of the best evidence to date for regime theorists. Finally, such analysis is critical for formulating policy recommendations for international cooperation.

First, lessons from other domains inform an approach to security regime formation to address individual findings and formulate recommendations. Key aspects of the problem are described against the backdrop of four recent cyber attacks. The facts of the attack and international cooperation to mitigate and attribute the attacks are presented for each case. Three tailored models are used to 1) assess the results of attribution efforts and their effectiveness, 2) assess the maturity of international cooperation in this area, and 3) to develop recommendations to mature the regime. These recommendations inform a policy approach applied in a counterfactual analysis, or thought experiment, in the case of countering Chinese information warfare strategy development and resulting intrusions. Finally, the concepts of international cooperation and security regime effectiveness and maturity are discussed and recommendations for the future are proposed.

KEY DEFINITIONS

Given the relatively new domain of cyberspace, it is important to be explicit with key terms. Also, cyberspace security is a large, complex and highly technical area of study, so it is equally important to be clear about the scope of what this paper does and does not address.

This paper adopts the May 12, 2008 U.S. Deputy Secretary of Defense Memorandum definition of cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[15] While the fact the cyberspace domain informs human decision-making is fully recognized, the human element is not considered part of the domain itself. Similarly, the definition does not include the electromagnetic spectrum as competing versions still do. In his work for the U.S. Center for Technical and National Security Policy (CTNSP), Dr. Dan Kuehl of the Information Resources Management College of the National Defense University has well documented the path to the above definition, and its limitations.[16]

A cyberspace attack is defined as "malicious activity targeting the computer or telecommunications networks of critical infrastructures, such as power systems, traffic

---

[15] Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc (accessed January 4, 2010).

[16] Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc (accessed January 4, 2010).

control systems or financial systems."[17] Cyber attacks may target information technology (IT) through a direct attack against an information system through the wires alone (i.e. hacking), through a physical assault against a critical IT element, or from the inside as a result of compromising a trusted party with access to the system.[18] Certainly other definitions exist, such as that adopted by Dartmouth's Institute for Security Technology Studies as a "computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it."[19] Such competing definitions are sufficiently similar to the one adopted here for the purposes of this paper.

The extent to which a cyberspace attack constitutes an act of armed aggression under international law, justifying legitimate acts of self-defense, remains in debate. This point is specifically addressed in the attacks reviewed.[20]

Susan Brenner differentiates between the three categories of cybercrime, cyber terrorism and cyber warfare:

> "Cybercrime is the use of computer technology to...engage in activity that threatens a society's ability to maintain internal order.... [Cyber] terrorist acts are designed to undermine a society's ability to maintain internal order...and should be treated as crime regardless of whether they are perpetrated locally or remotely.... Cyberwarfare is the conduct of military operations by virtual means."[21]

---

[17] Emma Nash, "How vulnerable are we to a cyber attack?" *Computing*, April 15, 2004, http://infomaticsonline.co.uk/computing/features/2072400/vulnerable-cyber-attack (accessed August 11, 2009).

[18] Emma Nash, "How vulnerable are we to a cyber attack?" *Computing*, April 15, 2004, http://infomaticsonline.co.uk/computing/features/2072400/vulnerable-cyber-attack (accessed August 11, 2009).

[19] Kevin O'Shea, "Cyberattack Investigative Tools and Technologies presentation," Institute for Security Technology Studies, May 7, 2003, http://www.ists.dartmouth.edu/library/107.pdf (accessed January 4, 2010).

[20] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008).

[21] Susan Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare," *Journal of Criminal Law and Criminology*, 97, 2007, in Jeff Wozniak and Samuel Liles, "Political and Technical Roadblocks to Cyber Attack Attribution," *IO Journal*, April 2009, 24.

An important concept in the field of international cooperation is the concept of international regimes. Regimes are defined as "implicit or explicit principles, norms, rules, and decision-making procedures around which actor expectations converge in a given issue-area,"[22] in this case the intersection of international relations and cyberspace.

- Principles are beliefs of fact, causation, and rectitude.
- Norms are standards of behavior defined in terms of rights and obligations.
- Rules are specific prescriptions or proscriptions for action.
- Decision-making procedures are prevailing practices for making and implementing collective choice.

Other definitions of regimes also exist. Oran Young defines regimes as "social institutions governing the actions of those interested in specifiable activities, (or accepted sets of activities). Like all social institutions, they are recognized patterns of behavior or practice around which expectations converge."[23] Young himself considers his definition compatible with the definition used here.

It is significant to point out that the principles and norms addressed herein are concerned with cyberspace security, and are not intended to address normal networking or computing. Marcus Franda concisely describes the origin of the "international regime for the Internet" discussing the latter, and which significantly informs portions of this paper. Franda asserts the international Internet regime began with the acceptance of the first Transmission Control Protocol/Internetwork Protocol (TCP/IP) as a de facto worldwide standard in the 1980s and 1990s.[24] This paper does not challenge or portend

---

[22] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 2.
[23] Oran Young, "Regime dynamics: the rise and fall of international regimes" in Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 93.
[24] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001), 21.

to discuss either normal cyberspace operations or technical details. This study is rather focused on political mitigations for a stated security issue, the attribution of cyberspace attacks. To this end, this research addresses emerging cyberspace security regime principles and norms.

As Stephen Krasner points out, security regimes are both especially valuable and difficult to achieve – "valuable, because individualistic actions are not only costly but dangerous; difficult to achieve, because the fear that the other is violating or will violate the common understanding is a potent incentive for each state to strike out on its own even if it would prefer the regime to prosper."[25] Krasner identifies four specific criteria for security regime formation to occur, which are used to assess international cooperation in cyberspace attack attribution.

CHAPTER SUMMARIES

Chapter two describes regime formation and methods of establishing or mitigating the lack of attribution in other, predominantly security-related domains. Observations inform assessments and recommendations in subsequent chapters, helping to identify current and future opportunities to advance the regime.

Chapter three describes key aspects of the cyberspace attack attribution problem against the backdrop of four recent cyber attacks, incorporating research not well documented in international relations literature. While great effort is being expended at

---

[25] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 174.

the technical level to address the attribution problem with limited success,[26] each of the cases posits the requirement for increased international cooperation. As former U.S. Assistant Secretary of Defense for International Security Affairs Franklin Kramer recently testified to Congress, "there is no effective international arrangement that deals with the security and law enforcement aspects of cyber. Given, however, cyber's international character, national security efforts as well as the development of enforcement will necessarily be less effective than could be accomplished by an integrated international effort."[27]

The evaluation incorporates Krasner's criteria for security regime formation and maintenance.[28] The extents to which governments exhibit coordinated action or uncoordinated behavior demonstrate international preferences for cooperation over cyberspace attacks and help to explain the outcomes of the attacks reviewed. If existing venues or incentives are insufficient to facilitate bargaining among actors, and emerging cyberspace norms do not structure sufficient incentives for governments to exercise restraint, they are unlikely to lead to mutually beneficial outcomes. If cyberspace norms are in fact self-reinforcing in a negative fashion, advancing the regime will likely require formal commitment and improved international cooperation to manage.

Chapter four describes cyberspace regime formation to explain the historical context of key aspects of the problems and their root causes. These include the decentralized nature of the domain, and the desire to maintain a free and open Internet

---

[26] Ian Gregorio-de Souza, *et al.*, "Detection of Complex Cyber Attacks," Thayer School of Engineering, Dartmouth College, Hanover, NH, 2006, http://www.ists.dartmouth.edu/library/245.pdf (accessed January 4, 2010).

[27] Franklin D Kramer, "Statement before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats," April 1, 2008.

[28] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 176-178.

preserving privacy for legitimate transactions. The chapter identifies and evaluates the significant agendas that have been developed for bringing into being principles, norms, rules and decision-making procedures that might assure international cooperation in cyberspace attack attribution into the future. The assessment examines negotiations that have taken place or are in progress to move internationally toward these goals. In so doing, the chapter informs the remaining issues of how improved international cooperation in this area can structure incentives for governments and facilitate bargaining among them.[29]

Chapter five assesses the regime's effectiveness in this area through both collective-action and social practice perspectives of international regime formation. The evaluation inquires: "To what extent has effective operationalization of an international cyberspace security regime occurred?" Evidence from recent attacks and cyberspace regime formation to date is applied against a series of hypotheses of how regimes influence behavior to evaluate regime effectiveness according to a range of criteria.

Chapter six further inquires: "How might maturing international cooperation mitigate the problem of cyber-space attack attribution?" Evidence of cyberspace regime formation and effectiveness to date is applied against a three-stage model of international regime formation – agenda formation, negotiation, and operationalization. Security regime formation criteria are incorporated to assess the maturity level of the regime. Finally, lessons learned from international cooperation in other domains inform recommendations for a policy approach tailored to the maturity level of the regime.

---

[29] Robert Keohane and Joseph Nye, *Power and Interdependence*, Third Edition (Harrisonburg: R. R. Donnelley and Sons, 2001).

Chapter seven illustrates how these recommendations might have been applied in a notional thought experiment against China's information war theory and strategy development over the years 1995-2003, and their resulting rampant intrusions into U.S. networks.[30] The experiment complements the review of recent attacks through counterfactual reconstruction of the flow of events in the relative presence or absence of cyberspace regime cooperation. The evaluation reviews the decision-making process of key actors at critical junctures including Chinese assessments of U.S. operations in Kosovo (2000) and Iraq (2003).

Chapter eight summarizes the papers conclusions and identifies concrete recommendations for addressing cyberspace attack attribution through international cooperation in the future. The chapter concludes with lessons learned in assessing security regime effectiveness and maturity, and recommendations for future work.

---

[30] "US warned of China 'cyber-spying,'" *British Broadcasting Corporation,* November 20, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7740483.stm (accessed March 27, 2009).

CHAPTER II

REGIME DEVELOPMENT AND ATTRIBUTION IN OTHER DOMAINS

Domain origination and attribution in other, predominantly security-related regimes inform assessments and recommendations in the cyberspace domain. The identification, definition and development of international security principles and norms in other domains inform potentially useful approaches for the nascent cyber security regime. While confident attribution is required for military action consistent with the international laws of armed conflict, principles and norms established in other domains provide a guide for how to proceed in the face of insufficient attribution, or for cooperative activities focused on attaining it. Lessons from other domains specifically address attribution as a collective action issue.

REGIME FORMATION

International principles and norms in today's security regime are grounded in customary international law. It is not surprising much of this chapter is rooted in the international law of armed conflict, or as it is also referred, international humanitarian law. Where useful, thoughts of influential writers are also referenced whether presently considered international law or not, which is also consistent with international law development. As the principles and norms of international law are well established and

documented,[31] detailed references are omitted, unless deemed necessary for a particular position or interpretation.

The identification, definition and development of international security principles and norms in other domains inform potentially useful approaches for the cyber security regime. The purpose is not to interpret the applicability of existing international law, or to identify specific legal remedies for areas regarding cyberspace security not covered by the law. Other efforts are already dedicated to these extremely important endeavors.[32]

The review of each domain is focused on the following questions meant to inform the current study. What was the catalyst for the principles and norms comprising the regime? What organizations are involved, such as an applicable arms control regime? What are the major principles and norms of the regime?

The Land Domain

While the principles and norms of the international law of armed conflict were initially developed through experience in the land domain, they were more importantly reflective of human experience of war. The laws of war on land effectively codified and advanced understandings of use of force for those in power, presumed to be leaders of nation-states. This moved the application of force into well-defined concepts of peace and war, belligerent and neutral, combatant and non-combatant. Certain weapons, material, and methods of warfare designed to cause superfluous injury or unnecessary suffering were prohibited or restricted in their use. These principles and norms have

---

[31] See, for example, Malcom N. Shaw, *International Law*, 4th ed. (Cambridge UP, 1997), 88-89.
[32] Rick Aldrich, "Computer Network Defense Attribution: A Legal Perspective," *Defense-wide Information Assurance Program, DIAP*, July 5, 2002.

stood the test of time despite technological development and the expansion to other domains, and we should expect the same to be true of cyberspace. Cyberspace, however, defies these well-defined assumptions, and no such restrictions apply specifically to cyberspace weapons.

Several observations from the international law of armed conflict in the land domain are applicable for consideration in our assessment of the cyber domain. First, regarding regime origination and evolution, leaders came to recognize the stake they held in their system as reflected in the 1874 Severalties of War Conference and 1899 Hague Convention. Second, everything was not accomplished at once, but rather through a series of conventions, conferences and agreements over a significant period of time. Third, it was recognized at the first Hague convention that such agreements would not be exhaustive, highlighting the use of custom as governing principles. Fourth, it included remedies for violations, including reprisals and war crimes trials.

Agendas were set as necessity demanded and not on notional or hypothetical situations. They were significantly informed by influential writers and academics. Negotiations were informed by practitioners, but conducted by diplomats and lawyers.

Key principles and norms in the land domain include the principle of self-help. There is, however, recognition that the right of belligerents to adopt means of injuring the enemy is not unlimited. The principle of necessity dictates using only that degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources. Unnecessary suffering is to be prevented.

The principle of proportionality prohibits the employment of any kind or degree of force not required for the purpose of the partial or complete submission of the enemy. The principle of humanity prohibits inflicting suffering, injury or destruction not actually necessary to accomplish a legitimate military purpose. Although deception is permitted, dishonorable conduct is forbidden.

The international law of armed conflict and deterrence principles and norms in the land domain were operationalized through actual conflict and adhered to for reasons of public support, reciprocity and an assumption of eventual restoration to peace.

Internal pressures on the international law of armed conflict are mitigated as they are largely descriptive of customary practices, and at times, normative by agreement. In this sense the law complements and supports the principles of warfare embodied in the generally universal military concepts of objective, mass, economy of force, surprise, and security.

The principles and norms associated with land warfare were in fact the crux of what we now recognize as the international law of armed conflict, or international humanitarian law, in what might be considered the preeminent security regime. It is important to understand that the international law of armed conflict we know today was at its inception primarily descriptive rather than normative. It was a matter of powers recognizing the rules of warfare as practiced at the time and not necessarily changing them except where all parties were interested. In this sense, the law then and now was meant to complement other generally recognized principles of warfare. That is to say the law of armed conflict is not intended to impede legitimate warfare. The purpose is to ensure the effects of hostilities are directed toward the enemy's forces and not used to

cause purposeless, unnecessary human suffering or physical destruction. Together, both the international law of armed conflict and the principles of warfare underscore the importance of concentrating forces against critical military targets while avoiding the expenditure of personnel and resources against persons, places, and things that are militarily unimportant.

With the rise of the nation-state, leaders came to recognize the stake they held in their nascent international system.[33] Stephen Krasner demonstrates the Concert of Europe prevailing from 1815-1823 and, in attenuated form, until the Crimean War as a security regime which deterred the individual powers from maximizing their positions at the expense of the others.[34] Alexander George and Richard Smoke portray deterrence before the atomic age, and its role in the balance of power politics of the day.[35]

In 1874 a conference of 15 states called together by Czar Alexander II drew up a document which addressed the "severalties of war." This unofficial document led the Institute of International Law at its Oxford conference to draw up the Manual of the Laws of War on Land. This document was very influential in moving states towards adoption of the first Hague treaty.

In 1899, 26 countries met at The Hague and adopted a series of Conventions and annexes. Most important was the convention with respect to the Laws and Customs of War on Land with an annexed set of regulations delineating the rules. This was the first codification of the laws and customs of war accepted by powers in a multilateral

---

[33] Henry Kissinger, *Diplomacy* (New York: Touchstone, 1994).
[34] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 178-179.
[35] Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, (Columbia UP, 1974), 12-21.

document. The drafters realized such law would not be exhaustive. The Martens Clause specifically stated customs would continue to govern "principles of the law of nations, as they result from the usages established between civilized nations, from the laws of humanity and from the dictates of public conscience."

In 1907 a further conference was held at The Hague which amended the Convention of 1899, and adopted ten others governing such things as the opening of hostilities, naval warfare, and the rights and duties of neutrals. The Geneva conventions dealt primarily with the treatment of people, clearly delineating between noncombatants and combatants. Additional conventions were added in 1864, 1906, and 1929, including two Additional Protocols in 1977.

Nations comply with the Law of Armed Conflict not only because they are legally obliged to do so, but for the practical reason that it is in the best interests of belligerents to be governed by consistent and mutually acceptable rules of conduct. Three assumptions underline the national self interest for compliance. First, violations, whether real or perceived, lead to loss of public support, both national and international. Second is an assumption of reciprocity. Belligerents treat opposing forces the way they would want to be treated or the same way they are being treated. Some obligations under the Law of Armed Conflict are reciprocal in that they are binding on the parties only so long as both sides continue to comply with them. A major violation by one side will release the other side from all further duty to abide by that obligation. For example, the 1925 Gas Protocol forbids the first use of gas, resulting in German chemical warfare restraint in World War II.

Third, there is also an assumption of the eventual restoration of peace. Violations may arouse the enemy to greater resistance and prolong the conflict resulting in greater casualties. All conflicts come to an end. It is therefore desirable to have a smooth transition from war to peace.

There are times when opposing forces step outside the limits of the international law of armed conflict. If they do, various means are available to belligerents under international law for inducing the observance of legitimate warfare to include reprisals and war crimes trials.

The right of the belligerents to adopt means of injuring the enemy is not unlimited and it is prohibited to launch attacks against the civilian population as such. Distinctions must be made between combatants and noncombatants, to the effect that noncombatants are spared as much as possible. It is prohibited to attack or bombard towns or buildings which are undefended. Undefended places are those places where no combatants or military equipment are present, either fixed or mobile, there is no hostile use made of any installations, the population is committing no acts of hostilities, and there are no activities in support of military operations. Medical units, sick and wounded, and enemy military police may be present. The definition of war-sustaining may be very broad, such as oil shipments during the Iran-Iraq War. A city or town behind enemy lines is, by definition, neither undefended nor open, and military targets therein may be attacked.

Certain weapons, material, and methods of warfare that are designed to cause superfluous injury or unnecessary suffering are prohibited or restricted in their use, including chemical, biological, incendiary, and laser weapons. No such restrictions apply specifically to cyberspace weapons.

The laws of war on land effectively codified and advanced understandings of use of force for those in power, presumed to be leaders of nation-states. This moved the application of force into well-defined concepts of peace and war, belligerent and neutral, combatant and non-combatant. Cyberspace, however, defies these well-defined assumptions. While experience in the land domain supports the concept of moving cyberspace attacks out of the grey area between peace and war, we must look further for more applicable approaches.

The Sea Domain

The sea domain is a particularly interesting metaphor for cyberspace. As in the land, air and trade domains, but unlike the nuclear or space domains, the cost of admission is low, so nations and peoples are broadly represented. As in cyberspace countless transactions occur daily on a global scale. The vast majority of these transactions are commercial or recreational and benign in nature, with some malicious elements such as piracy, smuggling, or poaching, policed by a relatively very small number of warships. A ship carrying the flag of one state may be crewed by many, carrying diverse cargo between numerous ports anywhere in the world. Ships routinely change cargo and crew, and occasionally flags, exacerbating the identification and tracking of vessels of interest. This environment has created a need for maritime domain awareness (MDA) concept of operations (CONOPS)[36] and multinational naval task

---

[36] *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security*, (Washington, D.C.: U.S. Government Printing Office, October, 2005), http://www.virginia.edu/colp/pdf/NSMS-National-Plan-to-Achieve-Maritime-Domain-Awareness.pdf (accessed July 1, 2009).

forces[37] not unlike the current situation experienced in cyberspace. The MDA concept leverages sensors, analytical fusion, and international cooperation through regional hubs.

From a security perspective, two areas inform regime-level principles and norms in the sea domain. First are specific portions of the law of armed conflict introduced in the previous section. The second is the UN Convention on the Law of the Sea, or UNCLOS.

The origination of the law of the sea is interesting and has evolved over many decades around the concept of the freedom of the high seas. That concept was modified over time in response to discovery of resources in the sea and its seabed beyond a state's territorial sea, previously considered the limit of a state's jurisdictional reach. A series of conferences in the 1950s led to four 1958 Conventions on the Law of the Sea (The 1958 Convention on the Territorial Sea and the Contiguous Zone, the 1958 Convention on the High Seas, the 1958 Convention on Fishing and Conservation of Living Resources and the 1958 Convention on the Continental Shelf).

A 1967 UN General Assembly meeting debating the preservation of the seabed and ocean floor for peaceful purposes first discussed the concept of common heritage of humankind in an international context. Elaborating a new framework convention for the law of the sea began amid numerous other economic, political and strategic factors during the negotiations of the ensuing UNCLOS III. A substantive debate emerged between several developing countries and more technologically advanced western nations

---

[37] "Multinational Task Force Targets Pirates," *American Forces Press Service*, January 8, 2009. http://www.defenselink.mil/news/newsarticle.aspx?id=52586 (accessed July 1, 2009).

regarding territorial limits and control of seabed resources on the one hand and freedom of passage and seabed exploitation on the other.[38]

Ironically, the great debate over mining deep sea resources formed in response to the 1973 purported collection of manganese nodules from the deep ocean floor by a specially engineered U.S. ship, the *Glomar Explorer*. In the spring of 1975, news broke that the real mission of the ship was to recover a Russian nuclear submarine sunk approximately 750 miles northeast of Hawaii on April 11, 1968, and mining was only a cover story.[39]

Unlike the 1958 and 1960 Law of the Sea Conferences, the UNCLOS III adopted an informal political consensus-building approach around particular issues rather than working over a pre-existing document or report.[40] The open-ended and contentiously normative approach of UNCLOS III greatly complicated and extended adoption and ratification of the convention.

Even with the principles and norms explicit in the conventions, mounting incidents at sea between U.S. and Soviet navies and the grave potential for escalation led to a 1972 agreement between the superpowers to prevent and mitigate such incidents.[41] This level of cooperation among potential adversaries occurred against the backdrop of cooperation in the nuclear domain addressed below, including the 1963 establishment of

---

[38] *United Nations Convention on Law of the Sea (UNCLOS),* 1982. http://www.eoearth.org/article/United_Nations_Convention_on_Law_of_the_Sea_(UNCLOS),_1982 (accessed July 1, 2009).
[39] *Federation of American Scientists*, s.v. "Project Jennifer," http://www.fas.org/irp/program/collect/jennifer.htm (accessed July 1, 2009).
[40] *United Nations Convention on Law of the Sea (UNCLOS),* 1982. http://www.eoearth.org/article/United_Nations_Convention_on_Law_of_the_Sea_(UNCLOS),_1982 (accessed July 1, 2009).
[41] *Agreement Between the Government of the United States of America and the Government of the Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas*, May 25, 1972.

a direct communications link, or "hot line" to prevent miscommunication in a crisis[42] and 1971 measures to prevent the escalation of potential nuclear incidents.[43] A less proscriptive U.S.-China commitment to engage in consultations was established in 1998.[44]

The Air Domain

With the development of the airplane, states recognized a new dimension to transportation which could no longer be contained within strictly national confines. World Wars I and II demonstrated the ugly potential of aviation requiring international attention. International collaboration in aviation matters born out of military necessity during and immediately following both wars led to the development of post-war civil aviation based on a belief that aviation had to be international or it would not be possible to use aviation as one of the principal elements in the economic development of the world.

Regime development in the air domain resulted in a permanent international organization centrally managing generally applicable rules and regulations requiring uniformity on a global scale. Regional offices manage practical application of specific

---

[42] *Memorandum of Understanding Between the United States of America and Union of Soviet Socialist Republics Regarding the Establishment of a Direct Communications Link*, June 20, 1963.
[43] *Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialist Republics*, September 30, 1971 http://www.fas.org/nuke/control/sea/text/sea1.htm (accessed July 2, 2009).
[44] *Agreement Between the Department of Defense of the United States of America and the Ministry of National Defense of the People's Republic of China on Establishing a Consultation Mechanism to Strengthen Military Maritime Security*, January 19, 1998. http://www.fas.org/nuke/control/sea/text/us-china98.htm (accessed July 2, 2009).

areas where operating conditions and other relevant parameters are comparable, providing they do not conflict with the world-wide activities of the organization.

These experiences are similar to the current situation in cyberspace, and two sources of security regime development in the air domain inform the current inquiry in cyberspace. The international law of armed conflict as it applies to aircraft has been sufficiently covered in the previous sections. The second area of interest is the Convention on International Civil Aviation (ICAO).

In the early years of aviation, before World War I, states recognized the advent of the airplane added a new dimension to transportation which could no longer be contained within strictly national confines. France convened the first important conference on an international air law code in Paris in 1910, attended by 18 European states. The conference successfully documented a number of basic principles governing aviation.

World War I introduced the destructive potential of aviation. Technical developments in aviation arising out of the war also created a new situation with regard to the safe and rapid transport of goods and persons over prolonged distances. A special Aeronautical Commission born from the 1917 Inter-Allied Aviation Committee addressed aviation matters at the 1919 Paris Peace Conference. Civil air transport enterprises were concurrently created in many European states and in North America, some of which were already engaged in international operations.

International collaboration in aviation matters born out of military necessity during and immediately after World War I, led to the development of post-war civil aviation out of a belief that aviation had to be international or not at all. This collaboration resulted in the French-led International Air Convention, signed by 26 of the

32 Allied and Associated powers represented at the Paris Peace Conference, and ultimately ratified by 38 states. The Convention consisted of 43 articles addressing all technical, operational and organizational aspects of civil aviation formulated by the 1910 Paris conference. The Convention also foresaw the creation of an International Commission for Air Navigation (ICAN) to monitor developments in civil aviation and to propose measures to states to keep abreast of developments. A permanent Secretariat was established in 1922 to assist the Commission under the direction of a General Secretary.

The interwar period exhibited continuous growth of civil aviation in both the technical and the commercial fields. Aviation during World War II not only resulted in horror and human tragedies, but also significantly advanced the technical and operational possibilities of air transport. For the first time large numbers of people and goods were transported over long distances in an orderly and expeditious manner. In 1943, the U.S. initiated studies of post-war civil aviation problems that again confirmed the belief they needed to be tackled on an international scale or it would not be possible to use aviation as one of the principal elements in the world's economic development.[45]

The studies and subsequent consultations between the major allies led the U.S. government to invite 55 states or authorities to attend the November 1944 International Civil Aviation Conference in Chicago. Fifty-four states attended, with 52 states ultimately signing the Convention on International Civil Aviation, establishing the permanent ICAO to secure international cooperation and the highest possible degree of

[45] International Civil Aviation Organization, http://www.icao.int//cgi/goto_m.pl?icao/en/hist/history01.htm (accessed July 2, 2009).

uniformity in regulations and standards, procedures and organization regarding civil aviation matters. The most important work accomplished by the Chicago Conference was in the technical field. It established rules and regulations regarding air navigation as a whole to significantly advance flight safety and pave the way for a common, global air navigation system.[46]

In view of the inevitable delays in Convention ratification, the Conference signed an Interim Agreement creating a technical and advisory Provisional International Civil Aviation Organization (PICAO) to collaborate in the field of international civil aviation. PICAO operated from August 1945 to April 1947 when the permanent ICAO came into being, little more than a formality. By agreement, ICAO succeeded ICAN which was then dissolved.

The ICAO Secretariat covers two major activities. First, the Secretariat directly manages generally applicable rules and regulations that require uniformity on a global scale to make international air navigation possible. Second, regional offices manage the practical application of air navigation services and facilities by states and their coordinated implementation in specific areas where operating conditions and other relevant parameters are comparable. These regional offices were divided by regions with distinct and specific air navigation problems of a similar nature. For example, the North Atlantic Region primarily addresses problems concerning long-range overseas navigation, while the European-Mediterranean region focuses the coordination of trans-European operations with domestic and short-range international traffic. ICAO adopted

---

[46] International Civil Aviation Organization, http://www.icao.int/cgi/goto_m.pl?icao/en/hist/history02.htm (accessed July 2, 2009).

the concept of regions and regional offices on the understanding that any regional activities could only be undertaken provided they did not conflict with the world-wide activities of the organization. Activities were allowed to vary from region to region, however, taking into account the general economic, technical or social environment of the region concerned.[47]

The Nuclear Domain

When we think of deterrence, the basis of our interest in attribution, our natural proclivity is to consider the specific case of nuclear deterrence, especially as experienced through the Cold War. Because much of deterrence thought grows from that literature, this section considers this specific case.

As in the cyber domain, even the more determinant nuclear domain required international cooperation beyond national self-help through technical means. Just as the window of opportunity to preemptively address the cyberspace attack problem may be closing, the extreme consequences of nuclear war elevated the issue to that of high politics, forming the basis for international arms control and monitoring agreements. Even under this general threat, a specific catalyst in the form of the Cuban Missile Crisis was required for the parties to initiate formal communications and cooperation to mitigate risks including timely and accurate attribution. No cyberspace crisis has yet served as a catalyst commensurate with the Cuban Missile Crisis, with the Y2K challenge perhaps the most poignant candidate.

---

[47] International Civil Aviation Organization, http://www.icao.int/cgi/goto_m.pl?icao/en/hist/history02.htm (accessed July 2, 2009).

The nuclear arms control regime did not develop overnight, but rather over many years as the primary actors learned their own lessons of nuclear deterrence, identified the need for agreements beyond tacit communications, and developed confidence in adversary reciprocity. Agreements in the nuclear domain were not only achieved over time, but also with significant and observable benefits at modest cost to national sovereignty and self-action. We should expect the same to be true for a cyberspace security regime.

Alexander George and Richard Smoke documented the general lack of any overarching deterrence theory or regime in the first five years of the nuclear age, 1945-1950.[48] The primary catalyst for international cooperation in the nuclear domain was the overwhelming consequences of use; a premise reinforced through the preamble to the U.S.-USSR September 1971 agreement on measures to prevent the escalation of potential nuclear incidents.

> "Taking into account the devastating consequences that nuclear war would have for all mankind, and recognizing the need to exert every effort to avert the risk of outbreak of such a war, including measures to guard against accidental or unauthorized use of nuclear weapons... The Parties undertake to notify each other immediately in the event of..."[49]

Even under this general threat, a specific catalyst was required in the form of the October 1962 Cuban Missile Crisis for the parties to initiate formal communications and cooperation in the nuclear domain. The U.S. and Soviet Union agreed in June 1963 to establish a direct communications link, or "hot line" to prevent miscommunication in a

---

[48] Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, (Columbia UP, 1974), 21-26.

[49] *Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialist Republics*, September 30, 1971.

crisis.[50] The utilization of this link was further reinforced through September 1971 measures to prevent the escalation of potential nuclear incidents,[51] and a 1973 general agreement to prevent nuclear war.[52]

A 1987 U.S.-USSR agreement further established Nuclear Risk Reduction Centers (NRRC) in both capitals for the express purpose of supplementing existing means of communication and providing direct, reliable, high-speed systems to transmit notifications and communications at the government-to-government level.[53] The NRRCs may also be used by either side to transmit additional communications as a display of good will and to build confidence.[54] In 1988, an agreement was reached between the superpowers to provide advanced intercontinental and submarine-launched ballistic missile launch notifications.[55] In June 2000, the adversaries established a joint center for the exchange of data from early warning systems and notifications of missile launches.[56] A second hot line was subsequently established between the U.S. and China in 1998.[57]

It is important to note these agreements formed the basis for cooperation between principal adversaries in order to avoid miscommunication in a domain with the highest of

---

[50] *Memorandum of Understanding Between the United States of America and Union of Soviet Socialist Republics Regarding the Establishment of a Direct Communications Link*, June 20, 1963.
[51] *Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialist Republics*, September 30, 1971.
[52] *Agreement Between The United States of America and the Union of Soviet Socialist Republics on the Prevention of Nuclear War*, June 22, 1973.
[53] *Agreement Between The United States of America and the Union of Soviet Socialist Republics on the Establishment of Nuclear Risk Reduction Centers*, September 15, 1987.
[54] Federation of American Scientists, http://www.fas.org/nuke/control/nrrc/docs/nrrc1.htm (accessed June 29, 2009).
[55] *Agreement Between The United States of America and the Union of Soviet Socialist Republics on Notifications of Launches of Intercontinental Ballistic Missiles and Submarine-Launched Ballistic Missiles*, May 31, 1988.
[56] *Memorandum of Agreement Between The United States of America and the Russian Federation on the Establishment of a Joint Center for the Exchange of Data From Early Warning Systems and Notifications of Missile Launches*, June 4, 2000.
[57] Federation of American Scientists, "Voice of America Correspondent Report," http://www.fas.org/news/china/1998/980429-prc.htm (accessed June 29, 2009).

stakes, a considerable benefit exchanged for a modest cost of sovereign self-action. International cooperation was also achieved on a multilateral basis to prevent the proliferation of nuclear weapons technology as evidenced in the 1968 Nuclear Non-Proliferation Treaty,[58] 1963 Limited Test Ban Treaty,[59] 1996 Comprehensive Nuclear Test Ban Treaty,[60] and other agreements.

While these treaties focused on containing nuclear weapons technology and contributing to international peace and security, they also provided for specific and observable security guarantees at the national level while reinforcing the great power status quo at the systemic level. These incentives again provided sufficient multilateral incentives in exchange for modest encroachment on national security and sovereignty.

Paradigmatic arguments continue to complicate international dialogue and cooperation even today. Well after the height of the cold war, scholars continued to debate issues such as the impact of nuclear proliferation by Kenneth Waltz and Scott Sagan.[61] In addition to being a lively debate, this book is a classic representation of two sides arguing past each other, as they were both working under different paradigms.[62] Concentrating on systemic analysis of the increased consequences of war and actor rationality, Waltz argued more was better, while Sagan, concentrating on the competence, motives, and rationality of individual states, contended more was worse.

---

[58] *Treaty on the Non-Proliferation of Nuclear Weapons*, July1, 1968.
[59] *Treaty Banning Nuclear Weapon Test in the Atmosphere, in Outer Space and Underwater*, August 5, 1963.
[60] *The Comprehensive Nuclear Test Ban Treaty*, September 10, 1996.
[61] Kenneth Waltz and Scott Sagan. *The Spread of Nuclear Weapons: A Debate* (New York: W.W. Norton, 2002).
[62] For the definitive discussion on paradigms, see Thomas S. Kuhn, *The Structure of Scientific Revolutions*, (Chicago: University of Chicago Press, 1962).

Although there is great potential for indiscriminate effect, there are no specific prohibitions on the use of nuclear weapons under the international law of armed conflict. The general rules related to necessity and proportionality apply. The only treaty prohibitions regarding nuclear weapons relate to the placement of these weapons in certain areas.

International forums have sought to further restrict nuclear weapons technology from entire regions altogether, including Antarctica,[63] Africa,[64] Latin America,[65] South Pacific,[66] and Southeast Asia,[67] with similar efforts underway in Central Asia, Central Europe and the Mideast.[68] These agreements sought to specifically minimize the attribution requirement in observable ways. Given that participants to these agreements were not giving up nuclear weapons capability, but rather agreeing not to pursue it, observable regional security guarantees were achieved at little cost.

As an extension of nuclear ethics,[69] self-defense in the cyber domain should be considered a just, but limited cause (motives). Due to the risk of collateral effects, cyber attacks should not be treated as normal weapons, and the risk of collateral effects to innocent people should be minimized (means). Steps to reduce risks of cyber war in the near term, and reduce the reliance on cyber weapons over time (consequences) should also be taken.

---

[63] *The Antarctic Treaty*, June 23, 1961.
[64] *The African Nuclear-Weapon-Free Zone Treaty (Treaty of Pelindaba)*, December 16, 1993.
[65] *Treaty for the Prohibition of Nuclear Weapons In Latin America (Treaty of Tlatelco)*, April 22, 1968.
[66] *South Pacific Nuclear Free Zone Treaty (Treaty of Raratonga)*, August 6, 1985.
[67] *Treaty on the Southeast Asia Nuclear-Weapon-Free Zone (Treaty of Bangkok)*, December 15, 1995.
[68] Federation of American Scientists, http://www.fas.org/nuke/control/index.html (accessed June 30, 2009).
[69] Joseph S. Nye, Jr., *Nuclear Ethics*. (New York: Free Press, 1986).

The Space Domain

The space domain has been an important venue for global telecommunications development, as well as the corresponding principles and norms addressed in the next section. Several observations warrant review for the current assessment. The capabilities, principles and norms that support global information sharing through space were again developed over several decades, and much was left intentionally undefined in order to advance the regime. Just as there is wide variance in views over the limits of control in cyberspace, the limits of the commons and sovereign space did not have to be rigidly agreed upon for the two concepts to work in harmony. The legal domain of space and associated principles and norms established through state practice and opinio juris were accepted as customary international law for a decade until documented by treaty in 1967. Nations recognized the utility of the law of the commons when concepts based more heavily on national sovereignty were shown to not be viable.

With the 1957 USSR launch of the first earth satellite, Sputnik, the competition and cooperation defining the space domain burst forth with relative speed. The concept of space as commons (see discussion on the sea domain above) was initially challenged by the concept that nations maintained sovereignty over territorial airspace to an unrestricted extent (usque ad coelum); however, this was not considered viable. Beyond the separation of airspace and space, generally considered at some point between 50 and 100 miles, nations have generally agreed to apply the law of the commons (res communis). Out of concern of prematurely surrendering valuable sovereign rights in light of future technological development, nations have generally agreed to not specifically delimit this particular frontier. Also, while the law of the commons is

generally applied to low- (LEO) and mid-earth orbits, the high, geosynchronous earth orbit becomes another region of the domain that comes under dispute. UN General Assembly resolutions adopted in 1963 identified corresponding legal principles expressed in state practice, opinio juris, and accepted as customary international law. The legal domain of space was clarified in a 1967 Treaty.[70] Further Agreements followed in 1968,[71] 1972,[72] and 1975.[73]

Simply having agreements in place and the technical capability to track objects in space is not to infer all problems are solved. The number of objects in Earth orbit has increased steadily. The United States and the Soviet Union tested anti-satellite technology in the 1980s, and the United States shot down one of its orbiting satellites in 1985. Partially as a result of the debris problem, both sides stopped the programs.[74] The annual growth rate of tracked debris began to decrease in the 1990s, largely due to national debris mitigation efforts, but has been growing again since 2004.

Cooperative efforts do not always restrain aggressive powers.[75] The January 11, 2007 Chinese test of an anti-satellite (ASAT) weapon against one if its own satellites in

---

[70] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, October 10, 1967. http://www.islandone.org/Treaties/ (accessed July 2, 2009).

[71] *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*, December, 1968. http://www.islandone.org/Treaties/BH523.html (accessed July 2, 2009).

[72] *Convention on International Liability for Damage Caused by Space Objects*, September 1, 1972.http://www.islandone.org/Treaties/BH595.html (accessed July 2, 2009).

[73] *Convention on Registration of Objects Launched into Outer Space*, January 14, 1975. http://www.islandone.org/Treaties/BH653.html, (accessed July 2, 2009).

[74] Marc Kaufman and Dafna Linzer, "China Criticized for Anti-Satellite Missile Test," *Washington Post*, January 19, 2007, A01. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801029.html (accessed July 9, 2009).

[75] "Analysis: Chinese Anti-Satellite Weapons Test in Space is Provocative and Irresponsible," *Center for Defense Information,* January 22, 2007.

LEO created the largest man-made debris field in history, largely contributing to a 20 per cent increase in traceable space debris in 2007 alone.[76] While initial international reaction focused on the shared threat to space assets,[77] subsequent international concern shifted to focus on the implications of the massive amounts of space debris caused by the satellites destruction.[78] The massive amounts of space debris can feasibly limit future launches, and existing space asset maneuverability in LEO, resulting in a form of denial of space access.

Space telecommunications were specifically addressed in the 1971 INTELSAT Agreement[79] and 1976 INMARSAT Convention (with 1981 Protocol and 1985 Amendment).[80] The 1971 Agreement established an international telecommunications satellite organization INTELSAT, to design, develop, construct, establish, operate and maintain the space segment of the global commercial telecommunications satellite system. The INMARSAT Convention made provisions for the space segment necessary for improving maritime and, as practicable, aeronautical communications including

---

http://www.cdi.org/program/document.cfm?DocumentID=3800&from_page=../index.cfm (accessed July 9, 2009).

[76] SPACESECURITY.ORG, *Space Security 2008,* Executive Summary, 6. (Waterloo, Ontario: Project Ploughshares, August, 2008), http://www.spacesecurity.org/SSI2008ExecutiveSummary.pdf (accessed July 9, 2009).

[77] Marc Kaufman and Dafna Linzer, "China Criticized for Anti-Satellite Missile Test," *Washington Post*, January 19, 2007, A01. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801029.html (accessed July 9, 2009).

[78] Leonard David, "China's Anti-Satellite Test: Worrisome Debris Cloud Circles Earth," *Space.com*, February 2, 2007. http://www.space.com/news/070202_china_spacedebris.html (accessed July 9, 2009).

[79] *Agreement Relating to the International Telecommunications Satellite Organization "INTELSAT"*, August 20, 1971. http://www.islandone.org/Treaties/BH585.html (accessed July 2, 2009).

[80] *Convention on the International Maritime Satellite Organization (INMARSAT),* September 3, 1976. http://www.islandone.org/Treaties/BH688.html (accessed July 2, 2009).

radio-determination capabilities. A 1972 United Nations Declaration,[81] 1983 General Assembly Resolution,[82] and International Telecommunications Union (ITU) regulations referenced therein identify principles and procedures for establishing transmission service and content between sending and receiving states.

The Telecommunications Domain

ITU regulations establish principles and procedures for establishing transmission service and content between sending and receiving states. These are particularly applicable to the cyberspace domain as they set clear precedent regarding global communications freedom of information and state sovereignty; however, that is not to say significant tension does not remain between the two.[83]

Founded in Paris in 1865 as the International Telegraph Union, the ITU took its present name in 1934 and in 1947 became a specialized agency of the United Nations. Membership of the ITU includes all 191 countries that use the international telephone system, as well as almost 750 IT companies and other associates that are members of one or more of ITU's three sectors. The Radio-communication Sector, Telecommunication Standardization Sector, and Telecommunication Development Sector each undertake a range of technical, procedural and political measures related to cyber security.

---

[81] *United Nations Educational, Scientific and Cultural Organization (UNESCO) Declaration of Guiding Principles on the Use of Satellite Broadcasting*, 1972.
unesdoc.unesco.org/images/0000/000021/002136eb.pdf (accessed March 1, 2010).
[82] *United Nations General Assembly Resolution 37/92, Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting*, 1983.
www.un.org/documents/ga/res/37/a37r092.htm (accessed March 1, 2010).
[83] Malcom N. Shaw, *International Law*, 4th ed., (Cambridge UP, 1997), 386-389.

The ITU mission "to enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy"[84] embraces the issue of cyber security in direct terms. Dr. Paul Cornish of Chatham House has also identified ITU's relevance in cyber security[85] noting "there is clear evidence of a practical approach which bridges gaps between the worlds of public policy, technology and industry, and which assists in national capacity building."

The ITU is taking concrete steps to develop confidence in the use of cyberspace through enhanced online security in the form of concrete measures in its landmark Global Cybersecurity Agenda (GCA). The GCA was launched in 2007 as a framework for international cooperation. In a rather complicated arrangement, the GCA is comprised of five strategic pillars including legal, technical, and procedural measures, organization, capacity building and international cooperation.

The Trade Domain

The majority of cyberspace development and use occurs in the public and private sectors, as opposed to government programs. Non-military activities comprise the bulk of responsibilities and authorities in cyberspace, and therefore provide both a first line of defense, and necessary role in response actions. International cooperation and regime development in relevant non-security domains such as telecommunications and trade are

---

[84] International Telecommunications Union, http://www.itu.int/net/about/mission.aspx (accessed August 6, 2009).

[85] Paul Cornish, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, (Brussels: European Parliament, 2009, February 2, 2009), http://www.europol.europa.eu/activities/committees/studies.do?language=EN (accessed August 6, 2009).

therefore critical in any consideration of building an international cyberspace security regime.

In addition to specific agreements regarding intellectual property rights, relevant observations from international cooperation in the trade domain include problems in the functioning of the domain leading to cataclysmic events. Addressing problems of military and security necessity, temporary measures emerged which survived and remained effective through the support of member nations who valued the benefits, and desired protection from other participating nations. The measures were effective despite the absence of a rigid structure and enforcement authority, primarily through nearly continual negotiating rounds and an effective dispute settlement mechanism. The arrangement provided for exceptions without retaliation or sanction where agreed by the members.

High trade barriers among western industrialized nations were considered a contributing factor to both the Great Depression of the 1930s and the onset of World War II. U.S.-British discussions during World War II to alleviate postwar economic problems formulated a plan to join the International Monetary Fund and the World Bank by an International Trade Organization (ITO) capable of regulating commerce. A general agreement emerged from the 1947 Havana Conference as a temporary measure to stabilize world trade pending ITO charter. When the U.S. Senate refused to consent to the ITO, President Truman joined the General Agreement on Tariffs and Trade (GATT) through executive order. Twenty-two nations joined the United States in GATT which

incorporated many provisions of the ITO charter but without the envisioned enforcement powers.[86]

GATT survived and remained effective through the support of member nations who enjoy the benefits from expanded trade, and desire to avoid retaliation from other participating nations. GATT effectively and significantly reduced or eliminated high trade barriers among western industrialized nations, despite the absence of a rigid structure and enforcement authority.

The agreement's purpose to encourage member nations to lower tariffs and eliminate import or other regulatory quotas included nondiscrimination as a key principle. Nondiscrimination was operationalized through most-favored-nation provisions in tariff treaties, requiring that no signatory imposes greater burdens on one trading partner than another. A second principle is that a GATT member may not rescind any tariff concession without compensation for trading partners adversely affected. The agreement also urges all parties to rely on negotiations and consultation to resolve trade conflicts.

The arrangement provides for exceptions seemingly in contradiction to the nondiscrimination principle. Developing nations may continue relations with former colonial powers, and groups of nations may create free-trade zones, such as the European Community or the North American Free Trade Agreement (NAFTA) without retaliation or sanction from other GATT members.

A series of five negotiating rounds followed the pattern that had characterized negotiations under the U.S. Reciprocal Trade Agreements Act of 1934. Representatives

---

[86] Robert E. Baldwin and Anne O. Krueger, eds. *The Structure and Evolution of Recent U. S. Trade Policy.* (Chicago: University of Chicago Press, 1984).

of the primary supplier of a commodity or product would engage in talks with a major consumer, each party seeking reductions in rates. Once a bilateral bargain was struck and added to the multinational agreement, the most-favored-nation principle extended rates to all parties. Applying this non-discriminatory approach, the GATT successfully reduced world tariffs on industrial products to 13 percent. During the sixth Kennedy Round (1964-1967) in Geneva the United States offered broad, across-the-board reductions, focusing negotiations on what commodities or items to exclude. The Tokyo Round (1973–1979) continued tariff reduction, leading to a general overall rate of 4 percent on industrial commodities.

The first six GATT rounds were successful in reducing tariffs but less so with non-tariff barriers (NTBs), first given serious attention during the Kennedy Round and dominating the subsequent Tokyo Round. Negotiations led to a series of codes of conduct directed at NTBs to mitigate such practices as dumping, government-subsidized exports, exclusionary government procurement policies, and arbitrary customs valuations. Most were adopted by industrialized, but not developing nations. The Uruguay Round concluded seven years of expanded negotiations on December 15, 1993. In addition to further tariff reductions, it fashioned partial agreements on agricultural products, services, and intellectual property rights earlier rounds had failed to address.[87] The Uruguay Round also resulted in the formation of the present-day World Trade Organization (WTO) to embody these new trade disciplines. There are currently 145 official member countries.

---

[87] Robert E. Baldwin and Anne O. Krueger, eds. *The Structure and Evolution of Recent U. S. Trade Policy.* (Chicago: University of Chicago Press, 1984).

The Environmental Domain

Slightly diverging from the general approach of this chapter, this section builds directly on previous work of international cooperation and regime-building in the environmental domain. Environmental regime analysts have invited application of their analytical models across non-environmental security domains. Their findings are introduced here for evaluation against the cyberspace regime. Regime formation and behavioral complex descriptions are not repeated here.

Evaluation of international cooperation and regime effectiveness in the environmental domain includes regimes designed to address vessel-source pollution, Barents Sea fisheries, and acid rain in Europe and North America.[88] The international vessel-source oil pollution case detailed changes in the international regime seeking to control intentional discharges of oil from ships.[89] The analysis found broad shifts in the allocation of authority among coastal, flag, and port states through cooperation across a wide range of marine issues. These shifts supported expanded roles of port states in contrast to flag states, leading to oil-pollution regime effectiveness.

New roles were also accorded to classification societies and insurance companies to enforce compliance with tanker equipment standards. Members of the oil pollution regime recognized the legitimacy of assigning such important roles to non-state actors.[90] Granting authority to classification societies and insurance companies to police standards

---

[88] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999).
[89] Ronald Mitchell, Moira L. McConnell, Alexei Roginko, and Ann Barrett, "International Vessel Source Oil Pollution," in Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999).
[90] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 261-262.

by refusing to certify or insure ships failing to conform to equipment standards was effective because some of the key members of the regime were willing to ban or even impound non-complying tankers from their ports.[91]

In this way, the regime was successful at establishing standards users were required to meet to conduct business profitably or at all. This was accomplished less by increasing incentives to comply with the rules than through eliminating opportunities to violate regulative prescriptions. Unlike the previous situation relying upon discharge standards where operators could decide whether or not to comply while engaged in transporting oil, owners and operators were effectively barred from transporting oil by sea if they were unprepared to accept the requirements of the equipment standards. The equipment standards were effective because they coerced a variety of non-state actors to play by the rules of the regime, avoiding manipulative tactics often accompanying national regulatory efforts.[92]

Large costs of tanker building and retrofitting required owners and operators to anticipate and adopt probable equipment standard developments over several decades at a time. The decision of tanker owners and operators to adopt the technology of segregated ballast tanks appears to have reflected an assessment on their part of the probable evolution of the rules governing marine pollution, reinforcing the commitment to equipment standards and advancing the oil-pollution regime effectiveness. Informing assessments of decision-makers illustrated a tendency of regimes to influence behavior

---

[91] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 265-266.
[92] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 265-266.

by shaping expectations of various parties about rules and procedures likely to be adopted in the future, even when they do not mandate specific actions at the time of their creation. Influencing behavior through shaping expectations was particularly true where key actors were required to make large investment decisions with extended amortization schedules, such as production facilities or research and development initiatives. Shaping expectations highlights the role of assessments of current and future trends in the development of international regimes to inform decision-making under uncertainty by those responsible for investment decisions.[93]

The case of international vessel-source oil pollution showed unambiguous evidence of links among domestic politics and the operation of regimes. A diffuse public concerned with marine pollution pressured a powerful and highly organized industry to accept equipment standards; despite evidence this solution was not an efficient one in the purely economic sense.[94]

Similar to the authority allocation tendency in the oil-pollution regime, the Barents Sea Fisheries[95] case demonstrated the expansion of regulatory authority of coastal states over living resources located in marine areas adjacent to their coastlines. In this case, the authority allocation was critical to the ability of Norway and Russia to establish a bilateral management system for the Barents Sea and to phase out third-party

---

[93] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 267.
[94] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 263-264.
[95] Olav Schram Stokke, Lee G. Anderson, and Natalia Mirovitskaya, "The Barents Sea Fisheries," in Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999).

fishing. This shift also derived its legitimacy from a broader shift in the allocation of authority over marine areas.[96]

By treating the area known as the Grey Zone as a management unit and differentiating it from the area of the Barents Sea subject to conflicting jurisdictional claims, the regime encouraged cooperation while avoiding the hardening of jurisdictional claims.[97] Recognition of jurisdictional limits in this case is similar to the observation from the space domain that clear delineation between sovereign and common elements or aspects of the domain is not a prerequisite to cooperation.

The Barents Sea fisheries regime also describes an evolutionary process of pursuing conventional fisheries management approaches. The concept of maximum sustainable yield was recognized as inadequate to manage fish stocks, leading to a growing awareness of the interdependence of fish stocks and the idea of multispecies management. Continued recognition of shortcomings with these approaches and a growing interest in holistic ecosystem perspectives, allow the regime to further address problems in this area. This evolutionary regime tendency was termed a step-wise process.[98]

There is again unambiguous evidence of links among domestic politics and the operation of regimes. The Barents Sea fisheries regime subjected the actions of

---

[96] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 261-262.
[97] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 255.
[98] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 268.

bureaucratic managers to greater public scrutiny, and also institutionalized the role of scientists as contributors to the decision-making process established by the regime.[99]

Regimes can clearly shape actors behavior. In the Barents Sea case, the regime was able to overcome collective-action problems through the operation of a routine decision-making procedure that reduced transaction costs and promoted transparency. These decision-making procedures made it increasingly difficult to cheat,[100] not unlike evidence of regimes shaping behavior in the other domains.

The case study on acid rain in Europe and North America[101] describes the evolution of the regime from the 1979 Geneva Convention on Long-Range Transboundary Air Pollution (LRTAP) and its subsequent protocols. The regime has been successful without proscribing many clear cut rules or behavioral prescriptions, but rather through the establishment of a joint mechanism for information sharing regarding the problem areas and encouraging member nations to make general pledges on the understanding each government be free to fulfill the pledges any way it sees fit.[102] The LRTAP regime showed clear examples of shaping actors behavior,[103] reinforcing the observations in other domains that attribution is partially achieved through cooperative measures including observable agreements and dedicated communications mechanisms.

---

[99] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 263-264.
[100] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 260-261.
[101] Don Munton, Marvin Soroos, Elena Nikitina, and Marc A. Levy, "Acid Rain in Europe and North America," in Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999).
[102] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 9.
[103] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 260-261.

Similar to the tanker owner and operator situation in the vessel-pollution case, chemical manufacturers also faced similar choices about long-term investments in the production of alternatives to chlorofluorocarbons. Decision-making over extended amortization schedules again illustrates the tendency of regimes to influence behavior by shaping expectations of various parties about rules and procedures likely to be adopted in the future, even when they do not mandate specific actions at the time of their creation.[104]

The LRTAP regime provided further evidence of links among domestic politics and the operation of the regime. LRTAP and its North American counterpart empowered domestic critics of prevailing environmental policies, helping to create domestic constituencies capable of bringing pressure to bear on relevant government agencies. Empowerment of domestic constituencies was largely accomplished through interest groups or communities working in legislative settings and broader forums influencing public opinion to build political coalitions.[105]

The LRTAP regime demonstrated a particular tendency of launching relatively uncontroversial or seemingly unimportant programmatic activities rather than preliminarily laying down regulatory prescriptions. Over time the regime became increasingly influential as its core issues gained political prominence and the participants found themselves in a web of institutionalized activities from which they could not easily extricate themselves. The case demonstrated a regime can lend credence or authority to a set of broader principles while mandating a process that keeps the issue before national

---

[104] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 267.
[105] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 263-264.

policymakers in a politically potent manner. In this way, the regime drew governments into normatively grounded social practices they could not ignore in political terms, albeit more so for some states than others.[106]

Summary

International cooperation arises for a variety of reasons in response to particular problems. With the rise of the nation-state, leaders came to recognize the stake they held in their nascent international system, setting in motion the principles and norms codified in the laws of land warfare and eventually expanded to cover other domains. The advent of new technologies in new domains and their corresponding destructive potential led to new venues for competition and potential cooperation. States recognized emerging regimes could no longer be contained within strictly national confines. Wars also demonstrated the destructive potential of the domains requiring international attention. International collaboration born out of military necessity led to the belief that domain management had to be international or it would not be possible to use the emerging domains for purposes of global economic development.

In the nuclear domain, extreme consequences elevated the attribution issue to that of high politics, forming the basis for international arms control and monitoring agreements. Even under such a general threat, a specific catalyst was required for the parties to initiate formal communications and cooperation to mitigate risks including timely and accurate attribution.

---

[106] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 266-267.

Problems in the functioning of the trade domain were deemed to have contributed to the cataclysmic events of the great depression and World War II. Addressing problems of military and security necessity for post-war reconstruction, a general trade agreement emerged as a temporary measure which survived and remained effective through the support of member nations who valued the benefits, and desired protection from other participating nations. The arrangement provided for exceptions without retaliation or sanction where agreed by the members.

Successful formulation of principles and norms tend to focus on descriptive practice complementing other generally accepted principles, rather than normative goals except where specifically agreed for good reason. Attempts to establish normative procedures impractical in conflict prosecution lead to numerous exceptions establishing alternative customary international law. Successful implementation of international agreements in the land domain includes remedies to force adherence, including reprisals and war crimes.

Self-defense is a just, but limited cause. The distinction between neutrals and belligerents, and combatants and non-combatants and the methods for so designating will continue to be instrumental in achieving attribution, although the methods may be unique. Defensive actions designed to prevent or mitigate an attack are justified as long as the general principles of necessity and proportionality are met. Protected signs, symbols and electronic signals used to identify personnel, objects and activities entitled to protected status, and the use of exclusion zones promulgated via notices to airmen and mariners (NOTAMS) may be useful metaphors for methods to distinguish and attribute combatant status and activity in cyberspace.

Normative instruments should provide clear benefit at minimal cost. As the nuclear domain demonstrated, agreements and cooperative procedures required significant and observable benefits at modest cost to national sovereignty and self-action.

Management structures are most successful when organizational tasks and authorities are well aligned with capability and perspective. In the case of the air domain, ICAO directly manages generally applicable rules and regulations requiring uniformity on a global scale, leveraging regional offices managing practical application of regional services.

Agreements and procedures generally require years, even decades to form and the necessary catalyst to initiate them may not be present in the cyberspace domain to date. The broad and amorphous nature of cyberspace leaves significant room for paradigmatic arguments, complicating the development of international dialogue and cooperation. Negotiations gain the best traction when initiated by a few principle actors. Draft documents or provisional organizations are beneficial to begin negotiations and eventual implementation.

Well aware of the inevitable delays associated with Convention ratification, the November 1944 International Civil Aviation Conference signed an Interim Agreement creating a technical and advisory PICAO which easily transitioned to the permanent ICAO. Conversely, in the sea domain, the open-ended and contentiously normative approach of the Third UN Convention on the Law of the Sea (UNCLOS III) greatly complicated and extended adoption and ratification of the convention. The GATT was effective despite the absence of a rigid structure and enforcement authority, primarily

through nearly continual negotiating rounds and an effective dispute settlement mechanism.

Clear delineation between sovereign and common elements or aspects of the domain is not a prerequisite to cooperation. The definition of space is clearly vague, and the parsing of the geosynchronous earth orbit (GEO) is a notable compromise.

Confidence-building measures are necessary. Several principles and norms, and reasons for abiding by them presume future actions. The assumption that violations, real or perceived, lead to the loss of domestic and international support is true only if violations have a significant chance of being detected, attributed back to, and result in unfavorable consequences for the offender. Similarly, victim or community actions actually need to demonstrate a capability and willingness to respond to attacks to establish a reasonable expectation of reciprocity. If hostility in the cyberspace area is not expected to spill into other areas, such as economics, an important incentive for cooperation will be absent.[107]

The assumption of an eventual return to peace is particularly applicable to cyberspace, as attacks may occur during times of no stated conflict engaging the formal international law of armed conflict. In the absence of attacks, positive reciprocity can be exhibited through peaceful confidence-building measures. *Improved coordination and technical detection capability to attribute attacks, and such responses either through retribution or peaceful confidence-building measures may be the most promising avenue*

[107] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 176-178.

for extending the shadow of the future and aligning mutual interests among an optimal number of actors.[108]

ACHIEVING ATTRIBUTION

This section reviews lessons from other domains addressing attribution as a collective action issue. While confident attribution is required for military action consistent with the international laws of armed conflict, principles and norms established in other domains provide a guide for how to proceed in the face of insufficient attribution, or for cooperative activities focused on attaining it.

For example, low transaction costs of entry, general freedom of the environment (high seas), and the concept of commons in the sea domain provide useful constructs such as the MDA CONOPS and multinational task forces. The trade domain relies upon negotiations and consultation to resolve conflicts. Significant time is allowed to make a claim, even longer for specific findings through arguments, and both well in advance of known total damage, significantly extending the shadow of the future for rational decision-makers.

The Land Domain

Deterrence and attribution in the land domain date back to the earliest recorded history. Thucydides documents the use of walls around cities as a deterrent measure in the Peloponnesian war. Throughout history, deterrence was a function of offensive and

---

[108] Robert Axelrod and Robert O. Keohane, "Achieving Cooperation Under Anarchy: Strategies and Institutions," in Kenneth Oye, *Cooperation Under Anarchy* (Princeton UP, 1985), 1985.

defensive capabilities and alliances. Principles and norms took the form of military principles for objective achievement under such pens as Sun Tzu, Machiavelli, Clausewitz, and Jomini.

The general deterrence decision calculus of perceived benefits and costs for acting or not acting apply, with a rich historical record. For example, Paris' abduction of Helen had several precedents. Io was taken from Mycenae, Europa was taken from Phoenicia, Jason took Medea from Colchis, and the Trojan princess Hesione had been taken by Heracles, who gave her to Telamon of Salamis. According to Herodotus, Paris was emboldened by these examples to steal himself a wife from Greece, and expected no retribution, since there had been none in the other cases. To the extent attribution was a requirement, it was generally easily achieved. Even King Menelaus of Sparta sought to confirm the elopement of Paris and Helen before asking King Agamemnon to call upon all the Achaean kings to attack Troy.

Several observations from the international law of armed conflict in the land domain are applicable for consideration in our assessment of the cyber domain. Distinctions are made between belligerents and neutrals, and combatants and noncombatants, to the effect that noncombatants and neutrals are spared as much as possible. These principles of distinction inherently require attribution of belligerent or combatant status to provide the protection required by the law of armed conflict to noncombatants and their property.

Special restrictions such as exclusion, or "free fire" zones, and NOTAMS are used to distinguish between combatants and non-combatants. The international law of armed conflict recognizes protected signs, symbols and electronic signals such as "SOS" or

"May Day" to identify personnel, objects and activities entitled to protected status. These include the Red Cross and Red Crescent (Medical symbols); prisoner of war and civilian internment camps; cultural, historical, educational activities; or the white flag.

Only combatants may participate directly in hostilities. Noncombatants refrain from hostile acts, and noncombatants may not be the object of intentional attack. It is prohibited to launch attacks against the civilian population as such, and undefended places are protected. The law provides for the recognition, protection and responsibilities of neutrals and neutrality. Responsibilities of the protected are specified, such as marking protected places, not commingling activities, and not to resist or arm themselves but to cooperate with attackers. Certain conventions prohibit or restrict of certain weapons, material, and methods of warfare by principle or treaty, however, none specifically address cyberspace.

In general, deception is permitted under the law of armed conflict, to include those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce them to react in a manner prejudicial to their interests. The law of armed conflict permits deceiving the enemy through stratagems and ruses of war designed to mislead, deter, or induce the enemy to act recklessly, provided the ruses do not violate rules of international law applicable to armed conflict. Permitted deceptions include such deceptions as camouflage, deceptive lighting, dummy ships and other armament, decoys, simulated forces, feigned attacks and withdrawals, ambushes, false intelligence information, electronic deceptions, and use of enemy codes, passwords, and countersigns.

There are specifically prohibited deceptions, referred to as perfidy, which are designed to invite the confidence of the enemy to lead him to believe he is obliged to accord to the opposing force protected status under the law of armed conflict, with the intent to betray that confidence. Such acts are prohibited because they undermine the effectiveness of protective signs and thereby jeopardize the safety of noncombatants and the immunity of protected structures and activities.

The Sea Domain

From existing international law, enemy warships and military aircraft, including naval and military auxiliaries, are subject to attack, destruction, or capture anywhere beyond neutral territory. Enemy merchant vessels and civil aircraft may be captured wherever located beyond neutral territory. The targeting and lawful attack upon such vessels and aircraft depends on the circumstances on which these objects are encountered. As in the land domain, the principles of attributing belligerent or neutral, and combatant or non-combatant status apply.

The London Protocol provided that except in the case of persistent refusal to stop on being duly summoned, or of active resistance to visit and search, a warship, whether surface vessel or submarine, may not sink or render incapable of navigation a merchant vessel without having first placed the passengers, crew and ship's papers in a place of safety. Defensive arming and counter submarine tactics by merchant vessels during World War II led to widespread departures from the London Protocol.

Numerous exceptions to the rules became customary practice so that today a vessel may become a target subject to attack if it:

- refuses to stop when duly summoned;
- resists visit and search or capture;
- sails under convoy with warship protection;
- is armed, even for defensive purposes only;
- incorporates into, or assists in any way, the intelligence system of the enemy's armed forces;
- is acting in any way as a naval or military auxiliary, or is integrated into the enemy's war-fighting/war-sustaining effort; and
- if compliance with the London Protocol would, under the circumstances of the encounter, subject the surface warship to imminent danger or would otherwise preclude mission accomplishment.

Refusal by civilian passenger vessels at sea and civil airliners in flight to provide immediate identification upon demand is ordinarily sufficient legal justification for capture or destruction.

A defender may always exercise the right of self-defense if attacked or threatened with attack while in neutral territory or from neutral territory. This includes the launching of an attack by an opposing belligerent while in mere transit of a neutral's territorial waters.

Neutral merchant vessels and civil aircraft acquire enemy warship character and may be treated as such if they engage in direct hostilities on the side of the enemy, or act in any capacity as a naval auxiliary, including intelligence collection. Neutral merchant ships may acquire enemy merchant character when engaged in acts such as operating directly under enemy control, resisting visit and search, or failing to establish its identity.

Naval mines are lawful weapons, but their potential for indiscriminate effects has led to specific regulation of their deployment and employment. The extensive and

uncontrolled use of naval mines during the Russo-Japanese War inflicted great damage on innocent shipping both during and long after the conflict. More recently, the use of naval mines in the Iran-Iraq War demonstrated the potential for indiscriminate effects.

The 1907 Hague VIII delineates the rules for use of naval mines. During wartime, a nation is required to provide international notice to prevent indiscriminate effect on neutral shipping. It may not mine neutral waters. A nation may mine both its own territorial sea and the territorial sea of opposing belligerents, as well as international waters, or even international straits for the purpose of channeling shipping, but it may not cut transit passage through the strait. Torpedoes must also be designed to become harmless when they have missed their mark, such as being designed to sink to the bottom and become harmless upon the completion of their propulsion run.

One case in point is the Corfu Channel Incident, actually three separate incidents in 1946 early in the Cold War involving Royal Navy ships in the Channel of Corfu. The second incident involved Royal Navy ships striking mines and the third incident occurred when the Royal Navy conducted mine-clearing operations in the Corfu Channel, but in Albanian territorial waters, resulting in a diplomatic note to Albania. The December 21, 1946 Albanian government reply denied the British allegations and went on to elaborate that the whole affair was the work of countries which did not wish to see a normalization of relations between Albania and Britain. The reply went so far as to state vessels from Greece and other countries had trespassed recently in the area where the mines were discovered.

Albania complained about the mine-clearing operation to the United Nations leading to the Corfu Channel Case, where the United Kingdom brought a case against the

People's Republic of Albania to the International Court of Justice (ICJ). It was the first case adjudicated by the ICJ, and in December 1949 the court awarded the British the sum of £843,947 or U.S. $2,009,437. The court found that, irrespectively of who laid the mines, the Albanians ought to have observed any such action, since the minefield was so close to their coast, and thus they failed to inform the British of the danger.[109] A similar 1986 case involving the U.S. mining of Nicaraguan waters resulted in a judgment against the U.S., although the U.S. blocked any resulting action in the UN Security Council.

Within the immediate area or vicinity of operations, a belligerent may establish special restrictions upon the activities of non-belligerent ships and aircraft and may prohibit altogether such vessels and aircraft from entering the area. Exclusion zones are justified on the basis that they are reasonable measures used to contain the geographic area of the conflict or to keep neutral shipping at a safe distance from areas of actual or potential hostilities. Such exclusion zones are normally promulgated through NOTAMS. To the extent that such zones serve to warn neutral vessels and aircraft away from belligerent activities and thereby reduce their exposure to collateral damage they are lawful. The establishment of such a zone, however, does not relieve the proclaiming belligerent of the obligation under the Law of Armed Conflict to refrain from attacking vessels and aircraft which do not constitute lawful targets. In short, an otherwise protected platform does not lose that protection by crossing an imaginary line drawn in the ocean by a belligerent.

---

[109] *Digest of International Cases on the Law of the Sea,* United Nations Office of Legal Affairs, Division for Ocean Affairs and the Law of the Sea, (New York, NY: UN Press, 2007), 32-37.

As in the land domain, the principles of attributing belligerent or neutral, and combatant or non-combatant status apply. The London Protocol attempted to establish normative procedures impractical in conflict prosecution. Numerous exceptions to the rules became customary practice so that today a vessel may become a target subject to attack if it refuses to so much as provide immediate identification upon demand (attribution), let alone operate under enemy control or resisting visit and search.

As with tools used in cyberspace attacks, naval mines and torpedoes are lawful weapons, but their potential for indiscriminate effects has led to specific regulation of their deployment and employment. Neutral waters may not be mined and international lines of communication such as straights may not be cut.

The Air Domain

Two technical developments from World War II were specifically designed to address attribution and carried forward into civil air operations. One was the advent of radar and an associated command and control (C2) system to detect and identify between or attribute friendly and enemy aircraft. The other was the use of secondary radars to identify friend or foe (IFF) by assigning unique identifier codes to friendly aircraft transponders.[110] The term is a bit of a misnomer, as IFF can generally only positively identify friendly targets but not hostile ones. If an IFF interrogation receives no reply, the object can only be treated as suspicious but not as a positively identified foe. It has

[110] "Technical Surveillance Countermeasures," *Granite Island Group*, http://www.tscm.com/iff.pdf (accessed July 2, 2009).

evolved such that the term "IFF" commonly refers to all modes of operation, including civil and foreign aircraft use.[111]

The Nuclear Domain

Several observations from the nuclear domain are applicable for consideration in our assessment of the cyber domain. The lack of confidence in adversary relations and detection systems require the problem of attribution to be addressed. The attribution issue in the nuclear domain has been substantively mitigated through observable agreements and dedicated communications mechanisms between adversaries.

Traditionally, the attribution problem in the nuclear domain remained somewhat dormant due to the relative confidence of cold war adversary relations and detectable delivery systems such as heavy bombers and inter-continental ballistic missiles. Early warning also enabled limited defensive responses, although only the U.S. and Russia can reliably detect rocket launches. U.S. Defense Support Program (DSP) satellites provide early warning of conventional and nuclear ballistic missile attacks. Russia began rebuilding its aging system in 2001 by upgrading its Oko series satellites. France is developing two missile-launch early-warning satellites—Spirale-1 and -2.[112]

Nuclear detection and attribution capabilities were further developed over decades, eventually including satellites capable of detecting and locating nuclear detonations worldwide, 24 hours a day, providing a highly survivable capability to detect,

---

[111] "Technical Surveillance Countermeasures," *Granite Island Group*, http://www.tscm.com/iff.pdf (accessed July 2, 2009).
[112] SPACESECURITY.ORG, *Space Security 2008*, Executive Summary, 19-20. August, 2008. http://www.spacesecurity.org/SSI2008ExecutiveSummary.pdf (accessed July 9, 2009).

locate, and report any nuclear detonations in the earth's atmosphere or near space in near real time.[113]

For consequences as significant as nuclear war, confidence in attribution certainly does and should receive the highest of scrutiny, in accordance with the just war tradition.[114] Changes in the post-cold war, and especially post-9/11 security environment and the increasing threat of terrorist use of a man-portable "loose nuke" have forced the underlying nuclear attribution problem to resurface. Tracking, detecting, tracing and ultimately attributing a terrorist-employed nuclear device to the known producer, supplier and employer presents a similar, albeit more constrained problem than that faced in cyberspace.

The Space Domain

As in cyberspace, states expend significant resources to establish attribution of objects and activities in space. One result of these efforts has been to expand and even shift concerns from the threat of direct attack to that of collateral effects.

Articles VI-VIII of the 1967 Treaty[115] sought to establish strict attribution of objects and activities in space through registries and corresponding procedures. The 1972[116] and 1975[117] agreements specifically address the attribution issue by identifying

---

[113] Federation of American Scientists, s.v. "MASINT," http://www.fas.org/spp/military/program/masint/nds.htm, (accessed March 28, 2009).
[114] Louis A. Manzo, *"Morality in War Fighting and Strategic Bombing in World War II," Air Power History*, vol. 39, no. 3, Fall 1992.
[115] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, October 10, 1967. http://www.islandone.org/Treaties/ (accessed July 2, 2009).
[116] *Convention on International Liability for Damage Caused by Space Objects*, September 1, 1972. http://www.islandone.org/Treaties/BH595.html (accessed July 2, 2009).

all state objects in space. The 1972 Convention specified legal terms and definitions for state space objects and damages. It further established a claims process for compensation which provided the victim state a period of one year from the time it learned of the damage to establish such a claim, even if the full extent of damage is not known. The 1975 Convention further detailed the requirements for both state registries and a UN Secretary General register with free and open access.

Objects are operationally tracked by states to maintain attribution of space objects. For example, in the United States, U.S. Strategic Command's (USSTRATCOM) Joint Functional Component Command for Space (JFCC-Space) maintains space situational awareness of over 17,000 man-made objects in space 10 cm or larger through its Joint Space Operations Center (JSpOC). It is estimated that there are over 300,000 objects measuring between 1 and 10 cm in diameter, and billions smaller. Traveling at speeds of up to 7.8 kilometers per second, space debris poses a significant threat to spacecraft.[118]

JSpOC utilizes a worldwide Space Surveillance Network (SSN) of 29 military and civilian, radar and optical telescope space surveillance sensors to observe the objects. These updates form the Space Catalog, a comprehensive listing of the numbers, types, and orbits of man-made objects in space,[119] a significant level of effort to establish confident attribution. The U.S. has moderated access to its data since 2004 out of

---

[117] *Convention on Registration of Objects Launched into Outer Space*, January 14, 1975. http://www.islandone.org/Treaties/BH653.html, (accessed July 2, 2009).
[118] SPACESECURITY.ORG, *Space Security 2008*, Executive Summary, 6. August, 2008. http://www.spacesecurity.org/SSI2008ExecutiveSummary.pdf (accessed July 9, 2009).
[119] U.S. Strategic Command, "Space Control and Space Surveillance Fact Sheet," http://www.stratcom.mil/files/STRATCOM_Space_and%20Control_Fact_Sheet-25_Feb_08.doc (accessed July 2, 2009).

concern for national security. Russia maintains a Space Surveillance System using its early-warning radars and monitors some 5,000 objects (mostly in LEO), but does not widely disseminate data. The EU, Canada, China, France, Germany, and Japan are all developing independent space surveillance capabilities.[120]

The Trade Domain

Although the focus of this paper is cyberspace as a security domain, the vast majority of the Internet is civil, commercial and recreational in nature. Impacts of attacks in cyberspace are felt across commerce and industry, and non-military activities comprise the bulk of responsibilities and authorities. The public-private sector, therefore, provides both a first line of defense, and necessary role in response actions. Addressing cyberspace from a purely security perspective is therefore misleading, unhelpful and insufficient for formulating recommendations.

One example of a problem arising from this disconnect is the relevant time-horizon between cyberspace as a security domain and a tool of commerce. While the WTO provides an effective dispute settlement mechanism, significant time is allowed to make a claim, even longer for specific findings through arguments, both well in advance of known total damage. Whereas recent attacks occur in terms of millibytes per second (mps), and responses over the course of hours, days and weeks, the WTO Dispute Settlement Understanding (DSU) provides a mechanism encompassing months and years.

---

[120] SPACESECURITY.ORG, *Space Security 2008*, Executive Summary, 7. August, 2008. http://www.spacesecurity.org/SSI2008ExecutiveSummary.pdf (accessed July 9, 2009).

Should attacks violate WTO agreements, the DSU may provide recourse for compensation completely outside of traditional security channels.

The WTO serves as a platform for countries to raise their concerns regarding the trade policies of their trading partners. The DSU is a legal text containing the rules for dispute settlement in the WTO.[121] Article 2 of the DSU establishes a Dispute Settlement Body (DSB) to administer the rules, procedures, and consultation and dispute settlement provisions. The DSB has the authority to establish panels, adopt panel and appellate reports, maintain surveillance of implementation of rulings and recommendations, and authorize suspension of concessions and other obligations under the covered agreements.

A panel is restricted to addressing only those claims that are specifically set out in a Member's panel request with sufficient precision. The complainant must, therefore, include all the claims it wants the panel to address in the request for the establishment of the panel as the panel is precluded from ruling on subsequent claims. There is a significant difference, however, between the claims identified in the panel request, and the arguments supporting those claims.

A claim is an assertion the respondent has violated, nullified or impaired benefits accruing under an identified provision of a covered agreement. Arguments are put forward by the complainant to demonstrate that the respondent has indeed infringed the identified provision or otherwise nullified or impaired benefits. Arguments are not required to be included in the request for the establishment of the panel. Rather, the

---

[121] World Trade Organization, http://www.wto.org/english/docs_e/legal_e/28-dsu_e.htm#7 (accessed July 3, 2009).

parties usually develop extensive legal arguments only in the further stages of the proceedings in their written submissions and oral statements to the panel.

A panel is not limited to using the parties' arguments. Rather, a panel is free to accept or reject such arguments and has the discretion to develop its own legal reasoning to support its findings and conclusions. In other words, a panel can develop its own autonomous reasoning.

Summary

Attribution is a problem when there is lack of confidence in adversary identification and technical detection of attacks. As the nuclear domain discussion illustrated, knowing who your adversaries are coupled with detection technologies may be sufficient at a point in time; however, as relations improve or sour, new actors such as terrorists come to light, or new technologies such as stealth bypass detection systems, the attribution issue will resurface.

Attribution is achieved through a combination of detection technology and cooperative measures including observable agreements and dedicated communications mechanisms. Significant technical investment should be expected to address the attribution problem at the technological level as has been invested in maritime, sea, space and nuclear domains. IFF and airspace management tools, maritime and space surveillance capabilities, and nuclear detection capabilities are all critical in establishing attribution in other domains.

A*ny plausible path to meaningful defense in cyberspace must include a significant element of international cooperation and regime formation.* Just as technological

solutions were required in these domains, however, they were also insufficient. MDA CONOPS, space and airspace management procedures and associated international cooperative agreements are as important as the technologies themselves. In the nuclear domain, the attribution problem is specifically mitigated through observable agreements and dedicated communications mechanisms between adversaries. Given the goal of preserving non-attribution in the case of benign use, the concept of a claims approach similar to that adopted in the telecommunications, space and trade domains may be more applicable to cyberspace than that of persistent surveillance.

Behavior alone indicates intent sufficient for attribution of combatant or belligerent status in other domains. For example, a maritime vessel may become a target subject to attack if it refuses to so much as provide immediate identification upon demand. Few weapons are restricted, rather the use of certain weapons exhibiting the potential for indiscriminate effects are regulated where agreed. Few cyberspace technologies are inherently malicious. Malicious activity in cyberspace is the product of using otherwise benign technology.

Changing the focus from directly detecting and attributing attacks in cyberspace, to that of identifying the impact of collateral effects for a claims-type process may be one avenue to facilitate international dialogue in existing venues, extending the shadow of the future for rational decision-makers. One result of attribution efforts in the space domain has been to expand and even shift concerns from the threat of direct attack to that of collateral effects.

As in the space and nuclear domains, activities with the potential for indiscriminate effects should not be treated as normal operations, and the risk of

collateral effects should be minimized. Constraining attacks in cyberspace should focus on malicious activities and effects, rather than weapons per se. This is one area worth exploring for specific discourse and possible agreement. Steps might be taken to reduce the risks of cyber war in the near term and reduce reliance on cyber attacks over time.

The significant grey area between peace and war provides a notable quandary for operations in cyberspace, and difficulty in attributing belligerent and combatant status. Rules differ when in a stated conflict than during normal peacetime. Under recognized conflict, deception is permitted to include the use of feigned attacks, false intelligence information, electronic deceptions, and use of enemy codes, passwords, and countersigns. There is much room for improvement in interpreting and applying these principles in cyberspace. Few nations have even publicly defined what they consider to be a cyberspace attack. Recommendations in subsequent chapters therefore focus on moving the cyberspace domain out of the grey area between peace and war where irregular warfare thrives.

CHAPTER III

ATTRIBUTION AS A COLLECTIVE-ACTION PROBLEM IN CYBERSPACE

The nature of cyberspace attacks constitute a collective-action problem in which the uncoordinated actions of each player may not result in the best outcome each can achieve.[122] A general discussion of information warfare provides important historical context to highlight specific attribution issues encountered during four recent attacks. Together, the cases are used to evaluate the ability of the emerging regime to mitigate attacks through improved international cooperation.

The Internet was built with the goals of openness and decentralization. Security was not a priority, and the current version of the address assignment system, IP V4, provides ample opportunities for perpetrators to mask their real identity or location. "Packet flows and connections can be masked and redirected through multiple servers. A clever attacker can often highjack a machine belonging to an otherwise innocent organization and use it as a base for launching attacks."[123]

In addition, the recent shift in strategy by hackers from a central command-and-control model for controlling botnets, large numbers of hijacked computers, to a peer-to-peer (P2P) model utilizing a distributed command structure capable of spreading to computers around the world is particularly troubling. "When several hijacked computers and networks that have been compromised spread over many countries and are used to launch cyber attacks using a decentralized model (based on peer-to-peer arrangements),

---

[122] *The Concise Oxford Dictionary of Politics*, (Oxford University Press, 2003).
[123] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, 12.

no national or regional legal framework can adequately deal with such a problem. This challenge can only be addressed globally."[124]

Traditional methods for establishing attribution include passive post-attack methods to reconstruct and recreate the chain of events. These include digital forensic methods such as log inspection and reverse engineering,[125] as well as actively marking packets traveling through the network[126] through attack traceback operations including attack tree construction, attack path frequency detection, and packet to path association.[127]

Even in the exceptional example where every machine involved in an attack is positively identified, attribution efforts must reach beyond the digital realm to identify the operator. Even if the operator is identified, it must be determined that they were responsible for, or even aware of, the attack and even further if they were acting at the direction or acquiescence of a national government. While confident attribution is considered a requirement for a military response under the law of armed conflict, other measures and strategies may be pursued in the face of imperfect attribution. Thus, cyber warfare attribution moves from the digital realm to the legal realm, in which there is no uniform international framework for dealing with international acts of cybercrime, let

---

[124] *International Telecommunications Union Global Cybersecurity Agenda (GCA): Framework for International Cooperation in Cybersecurity*, 2007, 6-7.

[125] F. Enfinger, B. Neslon, A. Phillips and C. Seuart. *Guide to computer forensics and investigation,* Third edition (Boston, Massachusetts, 2008), in Jeff Wozniak and Samuel Liles, "Political and Technical Roadblocks to Cyber Attack Attribution," *IO Journal*, April, 2009, 25.

[126] B. Al-Duwairi and T.E. Daniels. "Topology based packet marking, Computer Communications and Networks," *13th International Conference on Computer Communications and Networks*, 2004, 146-151, and Y. Tang and T.E. Daniels, "A Simple framework for distributed forensics," Second International Workshop on Security in Distributed Computing Systems, 2005, in Jeff Wozniak and Samuel Liles, "Political and Technical Roadblocks to Cyber Attack Attribution," *IO Journal*, April 2009, 25.

[127] G. Manimaran and M. Muthuprasanna, "Distributed Divide-and-Conquer Techniques for Effective DDoS Attack Defenses," 28th International Conference on Distributed Computing Systems, 2008, 93-102, in Jeff Wozniak and Samuel Liles, "Political and Technical Roadblocks to Cyber Attack Attribution," *IO Journal*, April, 2009, 25.

alone cyber warfare. Current prosecutions of attacks across international borders, therefore, rely on cooperation between nations in order to investigate, extradite and prosecute.[128]

Achieving attribution is further complicated by the difficulty of identifying motivating factors behind a cyber attack. Attacks which may seem to benefit one or more states may actually be the work of third-party actors driven by a wide range of motivations. "[The] challenge of identifying perpetrators and understanding their motives gives state actors convenient plausible deniability and the ability to officially distance themselves from attacks."[129] Even when states do obtain a level of technical attribution, the desire to secure state secrets for methods of doing so inhibit the sharing of information with others or taking actions based on it. This concern with surrendering relative gains in the technical area of attribution serves to further exacerbate the security dilemma fundamental to the problem.

Relatively low barriers[130] to this kind of activity mean that cyber riots or campaigns can take on a life of their own exponentially increasing the level of uncertainty of the attacker(s) and the unpredictability of the outcome.[131] Once an attack has occurred, current approaches to attribution accomplish little toward defending or mitigating the attack. The purpose in obtaining attribution is presently viewed from the perspective of preventing or deterring future attacks; however, "[as] the critical nature of Internet-based applications and services continues to increase, the ability to deter,

---

[128] Jeff Wozniak and Samuel Liles, "Political and Technical Roadblocks to Cyber Attack Attribution," *IO Journal*, April, 2009, 26.
[129] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, 12.
[130] Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, April, 2009.
[131] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, 12.

prevent, or interrupt attacks in progress will be of greater value to society than assigning blame and collecting damages after a disaster has occurred."[132]

It is important to emphasize the underlying purpose for establishing attribution in this approach is to justify actions against the perpetrators, the *head* or *catalyst* of the attack in order to deter future attacks. Decentralized organizations, however, have no head. In fact, trying to attack the head will be shown to be one of the worst possible strategic moves. Moving forward, it is important to differentiate between technically decentralized attacks made possible by the nature of the Internet with the fact that someone is in fact behind them. Beyond the technical response, actions against the head may be effective unless the attack is spawned or supported by a similarly decentralized political movement.

The decentralized nature of cyberspace attacks over open networks pose significant issues for states to effectively cooperate on the problem. These features of the Internet mean that states possess limited control to directly negotiate, agree to, or enforce Internet behavior. While they certainly have a role to play and are ultimately responsible for the security of their citizens, much depends upon the Internet and its users directly.

Issues fundamental to Internet governance such as transparency as opposed to anonymity, capacity, and cost are compounded by significant technical and legal issues. Regardless of how or to what extent answers to these issues are found, there are also security related issues of competitiveness, uncertainty, and increasingly high stakes leading to a very real collective-action problem of relative gains.

---

[132] Howard F Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues,* Carnegie-Mellon University, November, 2002, 4.

This security dilemma resulting from real or perceived relative gains for one actor leading to real or perceived decrease for others makes international cooperation even more problematic.[133] In what can only be seen as an ironic illustration of this problem, Moscow proposed a United Nations resolution calling for new international guidelines and the banning of particularly dangerous information weapons. The Clinton administration rejected the resolution on the basis that any attempt at that time to draft overarching principles on information warfare would be premature.[134] While this position may have been partially concerned with prematurely surrendering valuable leverage, or relative gains, in light of current capabilities or future technological development,[135] it also recognized the prima facie impossibility of enforcement, a recognition still held to this day.

> "in every example of alleged [Russian Federation, RF] involvement in cyber attacks launched against other nations (Chechnya, Krygyzstan, Estonia, and Georgia), the RF Armed Services were not involved; Non-state hackers were. And any attempt by the U.S. or other nations to prosecute Russian hackers engaged in cross-border attacks is rejected out of hand by the Kremlin. In other words, The Kremlin will negotiate on military capabilities that they haven't used but will not negotiate on their civilian hacker "assets" that they have used."[136]

Attempts to address these threats have lingered at the private, public, domestic and international levels. While law enforcement agencies would prefer greater transparency to prosecute cyber crime, companies are concerned with charges of colluding with police and intelligence agencies, providing information that could

---

[133] Robert Jervis, "Security Regimes," in Stephen Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1983), 173-194.
[134] "U.S. Military Grapples with Cyber Warfare Rules," *Reuters*, November 8, 1999, http://www.hartford-hwp.com/archives/27a/021.html (accessed March 27, 2009).
[135] John Arquilla, "Click, click...counting down to Cyber 9/11," *San Francisco Chronicle*, July 26, 2009, E-2, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/07/26/IN6K18S60M.DTL, (accessed August 10, 2009).
[136] Jeffrey Carr, "Why John Arquilla's support for a Cyber Arms Control Treaty is naïve," *IntelFusion*, July 27, 2009, http://intelfusion.net/wordpress/?p=604, (accessed August 11, 2009).

subsequently be obtained through legal channels such as the U.S. Freedom of Information Act (FOIA), as well as unwanted publicity of serious intrusions. And, of course, civil liberties lawyers are concerned with Orwellian approaches to the Internet. Indeed, concerns with overreach of government control of the Internet are viewed by many as the principle threat.[137]

Responses on the continent have echoed those in the United States. The Council of Europe drafted a treaty in April 2000, and the G-8 held a Dialogue between the Public and Private Sectors on Security and Confidence in Cyberspace the following month. Although neither resulted in decision or formal adoption, a dialogue was established. Peter Ford described the varying perspectives complicating a formal consensus:[138]

- Transparency. Law enforcement officers want transparency in cyberspace to find out who did what and when.
- Anonymity. Human rights advocates and civil liberties lawyers want total anonymity in cyberspace, usually through development of secure cryptography.
- Capacity. Internet service providers (ISPs) lacked the capability to retain the data governments wanted them to retain.
- Universality. Legal and intelligence officials were concerned a single international strategy for combating cyber crime would conflict with laws of particular nations.
- Cost. Industry executives were concerned government attempts to secure cyberspace would stifle growth.

Ford summarizes part of the collective-action problem from a civil-government and legal-non-legal perspective. Clearly, the open nature of the Internet is fundamental to addressing the problem. The collective-action problem he describes is further magnified when viewed from the international security perspective.

---

[137] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001), 182-187.
[138] Peter Ford, "New Cooperation in Taming the Wild Web," *Christian Science Monitor*, May 18, 2000.

Franda concluded all four of Jervis' security dilemma factors have been prominent in international efforts toward securing cyberspace:

- Competitiveness. Security issues often involve greater competitiveness than do those related to economics and other non-security aspects of human behavior.
- Relative Gains. Protection of one's interests in non-security areas is usually costly, but it does not necessarily harm or menace others, as is often the case where security is involved.
- High Stakes. The stakes are higher in security areas, since security is usually the most highly valued goal, is a prerequisite for so many things, and is unforgiving (e.g., the costs of living up to the rules of a security regime are extremely high if other actors are not living up to the rules; even temporarily falling behind others can produce permanent harm).
- Uncertainty. Detecting what others are doing and measuring one's own security are much more difficult than gaining such intelligence in other (e.g. economic or environmental) fields; this creates much higher degrees of uncertainty and distrust in security-related areas.

Recent attacks inform an assessment of the cyberspace attack attribution regime based on security regime formation and maintenance criteria.[139] First, the great powers must want to establish such a regime. To this end, the cases inform an assessment as to what extent great powers statements and actions demonstrate a preference for a more regulated environment; as compared to one in which all states behave individualistically. Also, to what extent they are reasonably satisfied with the status quo and whatever alterations can be gained without resort to the use or threat of unlimited war, as compared with the risks and costs of less restrained competition.

Second, the cases inform an assessment as to the extent to which actors believe others share the value they place on mutual security and cooperation. To what extent do the powers perceive other powers as an aggressor?

---

[139] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 176-178.

Third, security regimes cannot form when one or more actors believe security is best provided for by expansion. War and the individualistic pursuit of security must be seen as costly. For effective cooperation, war must not be desired; or at least unlimited war or the use of certain weapons without restrictions for more limited cooperation addressing just those areas. If hostility in cyberspace is not expected to spill into other areas, such as economics, an important incentive for cooperation will be absent.

As recent attacks illustrate, uncoordinated behavior by governments leads to worse results than coordinated action, and the resulting cyberspace norms appear to be self-reinforcing, often in a negative fashion. Ultimately, it appears cyberspace security is an area where each government would prefer to cooperate except itself, resulting in the collective-action problem of relative gains in an issue fundamentally requiring coordinated global action.

INFORMATION WARFARE AND RECENT ATTACKS

There are numerous threats in cyberspace including technical, criminal, and non-state-sponsored political activists using cyberspace as a tool. The scope of this research is focused on political strategies to help attribute attacks in support of deterrence, or identify mitigations for proceeding in the face of continued lack of attribution. Although information warfare is a concept as old as deception in war, the concept of network warfare dates back to at least 2001 when John Arquilla and David Ronfeldt coined the term.[140] Capabilities for such malicious activity date back to early Internet protocols predating the World Wide Web and cyberspace as we know it today. One historical

[140] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime and Militancy* (RAND, 2001).

incident of a high-school student hacking into the North American Air Defense (NORAD) computer network was significantly glamorized in the 1983 movie *WarGames*. Other notable incidents include a 1986 infiltration into the Lawrence Livermore Berkeley computers ultimately providing sensitive information related to munitions, weapons systems, and technical data to the KGB.[141]

> "By 1995 the Government Accountability Office (GAO) reported more that 250,000 "suspected attacks" on U.S. Defense Department computers, with approximately two-thirds resulting in computer network entry, although the Pentagon claims there were "only" 500 attempts that year."[142]

By 1997, information warfare was viewed as a major security problem, and a May 1999 FBI report detailed Chinese efforts to attack U.S. government information systems through the Internet. Before September 11, 2001, the highest annual figure for cyber attacks against the Pentagon was 250,000. Attacks proliferated on such a scale that on a single day in 2008, the Pentagon was hit by would-be intruders six million times in a single day.[143]

The seminal event for Pentagon awareness and eventual response to the problem was a February 1998 widespread systemic penetration into the Pentagon's Solaris operating system. Two California youths conducted an apparently coordinated attack on the defense information infrastructure at the direction of an Israeli code-named "Analyzer." In May 2000 Russian ultranationalist Vladimir Zhirinovsky warned the U.S. that "we will bring the entire West to its knees with our Russian computer specialists."[144]

---

[141] Cliff Stoll, *The Cuckoo's Egg: Inside the World of Computer Espionage* (New York, NY: Pocket Books, 1990) in Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001), 180.
[142] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001), 180.
[143] Arnaud De Borchgrave, "Silent Cyberwar," *Washington Times,* February 19, 2009, 18.
[144] Patrick Anidjar, "Cyber Threat is Constant Worry for United States," *Agence France Press*, May 13, 2000.

A 1999 strategy for unrestricted war proposed by two Chinese colonels included the use of cyber terrorism, computer virus propagation, and disruptive penetration of strategic computer websites.[145] The U.S. briefly considered the use of cyber attacks against Serbian targets in the 1999 Kosovo conflict, however, was quickly dissuaded from doing so. A 19-page General Counsel's paper cautioned against the use of such weapons within international law and the possibility of being considered and charged with war crimes.

It is apparent information warfare is considered a legitimate form of warfare by numerous great powers, even if concerns of collateral damage may deter its use. This of course only applies to cases where attacks may be confidently attributed back to a state actor in a manner they can and will be held accountable. Therefore deterring its use as a form of plausibly deniable irregular warfare or espionage is even more problematic.

Cyberspace attacks have become a matter of daily front page news. Operation Aurora, the December 2009 to January 2010 cyber attack on Google subsequently attributed to servers in China is an excellent case in point.[146] Further vulnerabilities and attacks against the U.S. electrical power grid raise the stakes even further, invoking the specter of a cyber 9/11 or even World War III.[147] Loss of confidence in financial transactions and other secure communications could set global society back to the pre-information age.[148] Although timing is difficult to predict, the growing frequency and scope of cyber attacks indicate the window of opportunity to address the problem before some form of cataclysmic event is closing.

---

[145] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001), 180-182.
[146] Kim Zetter, "Google hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora (accessed February 20, 2010).
[147] Jeffrey Carr, "Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats," *GreyLogic*, January 21, 2010.
[148] Eugene E. Habiger, "Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach," *Cybersecurity Institute*, February 1, 2010.

The Center for Strategic and International Studies (CSIS) identified 26 significant cyber attacks between May 2006 and June 2009.[149] Recent attacks in cyberspace demonstrate a growing level of international cooperation to attribute and mitigate. The recent attacks detailed below illustrate specific aspects of this maturation. Attempts to mitigate and attribute the attacks, however, also demonstrate clear gaps in cooperation when compared to that observed in other domains. International responses to the attacks collectively highlight cooperation shortfalls emanating from, and contributing to the security dilemma in cyberspace. It is this lack of cooperation that ultimately creates the attribution vulnerability space.

Estonia – The Preemptive Strike[150]

Estonia has been a world leader in public and private sector information security efforts. While Estonia is one of the smallest NATO countries, it is also one of its most advanced in the use of Information Technology (IT). Estonians conduct nearly all of their banking over the Internet and have participated in the world's highest per capita online voting processes. The robust nature of Estonia's wired society means that the country is also IT-dependent, and therefore dependent on IT security.

Prior to the country's official accession to NATO in 2003, Estonia proposed the creation of a cyber excellence center. The 2006 Riga summit listed possible cyber

---

[149] Center for Strategic and International Studies, http://csis.org/files/publication/090612_cyber_events_2006.pdf (accessed July 10, 2009).

[150] See Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." Georgetown Journal of International Affairs, Science and Technology, Winter/Spring 2008, 121-126.

attacks among the asymmetric threats to the common security and acknowledged the need for programs to protect information systems over the long term.[151]

Political events culminating in the relocation of a Soviet war memorial monument in Estonia precipitated an unattributed April 27 – May 18, 2007 cyber attack on Estonian political, services, personal and other random targets including on-line banking, media, and ISP's. The attack, come to be known as CyberWar I, included denial of service (DoS), distributed denial of service (DDoS, overloading servers due to the influx of traffic), webpage defacement, e-mail and comment spam, targeted exploitation hacks, and attempts to use Structured Query Language (SQL) injections[152] to exploit security vulnerabilities in the database layer of applications. The cyber attacks went on for weeks, although the vast majority of the DoS attacks lasted less than an hour and only 5.5% over ten hours.[153]

Defensive actions responding to the attack included international cooperation between the Estonian computer emergency response team (CERT-EE) and an international network of specialists. Responses also included political and media coverage, law enforcement actions and technical countermeasures.[154] Estonia pushed to elevate the attack to the top of the EU-Russia summit agenda.[155]

---

[151] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, http://www.ccdcoe.org/72.html (accessed August 6, 2009).
[152] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008), 36.
[153] "Estonian DDoS – A Final Analysis," Heise Security, May 31, 2007, referenced in Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, April, 2009, 9.
[154] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008), 36.
[155] "Estonia hit by 'Moscow cyber war,'" *British Broadcasting Corporation*, http://news.bbc.co.uk/2/hi/europe/6665145.stm, May 17, 2007 (accessed July 12, 2009).

Konstantin Goloskokov, a commissar with the pro-Kremlin Nashi youth group, claimed responsibility[156] for the attack on May 2, 2007,[157] calling it a "defensive act [to] teach the Estonian regime a lesson." Although Nashi activist Anna Bukovskaya acknowledged that the group was paid by Moscow to spy on other youth movements,[158] the involvement of the Russian government in the affair could not be confirmed. The failure or unwillingness of the Russian authorities to stop the cyber riot against Estonia for over three weeks after the initial attack, however, continued to raise speculation.[159]

The use of Nashi as a cyberwarfare arm illustrates the problem of attribution. While the nominally independent group does the Kremlin's bidding, Nashi's funding comes from pro-business owners looking to ingratiate themselves with the regime. Even if they claim credit for the attacks, they are still one level removed from the Russian government, however implausible that seems.[160]

For nominal costs to volunteers and their computers, minimal coordination requirements primarily across web forums frequented by Russian hackers, and low risk of attribution and punishment (one hacker living in Estonia was identified and fined about

---

[156] "Kremlin Loyalist Says Launched Estonia Cyberattack," *Radio Free Europe Radio Liberty*, March 12, 2009, http://www.rferl.org/Content/Kremlin_Loyalist_Says_Launched_Estonia_Cyberattack/1508923.html, (accessed March 26, 2009).

[157] Victor Yasman, "Monument Dispute with Estonia Gets Dirty," *Radio Free Europe Radio Liberty*, May 8, 2007, http://www.rferl.org/content/Article/1347550.html (accessed August 11, 2009).

[158] Noah Schachtman, "Kremlin Kids: We Launched the Estonian Cyber War," *Wired*, March 11, 2009, http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ (accessed July 12, 2009).

[159] Robert Vamosi, "The Estonia cyberwar, One year later," *CNET*, http://news.cnet.com/8301-10789_3-9948720-57.html (accessed July 12, 2009).

[160] Noah Schachtman, "Kremlin Kids: We Launched the Estonian Cyber War," *Wired*, March 11, 2009, http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ (accessed July 12, 2009).

1,620 USD),[161] the attackers probably inflicted costs on the order of tens of millions of dollars in financial losses.[162]

The cyber attacks against Estonia in April 2007 showed that cyber defense issues are critical to address, and that an entire nation can, in fact, become the target of a cyber attack.[163] It also demonstrated that a skillful response, including public and private sector partnership at the international level, could substantially mitigate the effect of such cyber attacks. These conclusions led to yet one other response important to note regarding international cooperation. The attacks highlighted for the first time the potential vulnerability of NATO countries, their institutions and societies, and even NATO itself to disruption or penetration of their information and communications systems.[164]

Estonia's proposals for a NATO cyber excellence center received strong support from the alliance's Secretary-General Jaap de Hoop Scheffer. NATO completed an assessment of the situation, partly in light of Estonia's experience in October 2007, and approved a NATO policy on cyber defense in January 2008. NATO's summit communiqué in Bucharest in April announced NATO's readiness to "provide a capability to assist allied nations, upon request, to counter a cyber attack."[165] The Cooperative Cyber Defence Center of Excellence (CCDCOE) was established with seven NATO

---

[161] "Estonia Convicts First 'Cyber-War' Hacker," *AFP*, January 24, 2008 in Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, April 2009, 9.
[162] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, May 29, 2007, in Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, April 2009, 9.
[163] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, http://www.ccdcoe.org/72.html (accessed August 6, 2009).
[164] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, http://www.ccdcoe.org/72.html (accessed August 6, 2009).
[165] "NATO opens new centre of excellence on cyber defence," *NATO,* May 14, 2008, http://www.nato.int/docu/update/2008/05-may/e0514a.html (accessed March 1, 2010).

nations and Allied Command Transformation (ACT) in Tallinn, Estonia on May 14, 2008.

To further reinforce the lack of attribution surrounding the attack, in March 2009, Sergei Markov, a State Duma Deputy from the pro-Kremlin Unified Russia party, surprisingly stated: "About the cyberattack on Estonia...don't worry, that attack was carried out by my assistant. I won't tell you his name, because then he might not be able to get visas."[166] Markov, a political analyst and Putin supporter, went on to explain that this assistant happened to be in "one of the unrecognized republics" during the dispute with Estonia and had decided on his own that "something bad had to be done to these fascists,"[167] so he went ahead and launched a cyberwar. "[It] turns out it was purely a reaction from civil society," Markov reportedly said, adding ominously, "and, incidentally, such things will happen more and more."[168]

A July, 2008 Nashi Innovation Forum suffered a 50% drop in attendance from the year before, possibly coming off a high surrounding the Estonian cyberwar the previous year, or perhaps they were simply busy. On July 20, 2008, the day before this Nashi event, anonymous Russian hackers coincidently launched a DDoS attack that took the President of Georgia's website offline. Nineteen days later, a Russian sea, air, and land assault was launched against Georgia while nationalistic Russian hackers engaged their Georgian counterparts in cyber warfare.[169]

---

[166] "Sergei Markov says he knows who started the Estonia cyber war," *IntelFusion*, March 6, 2009, http://intelfusion.net/wordpress/?p=544 (accessed August 11, 2009).
[167] "Sergei Markov says he knows who started the Estonia cyber war," *IntelFusion*, March 6, 2009, http://intelfusion.net/wordpress/?p=544 (accessed August 11, 2009).
[168] "Sergei Markov says he knows who started the Estonia cyber war," *IntelFusion*, March 6, 2009, http://intelfusion.net/wordpress/?p=544 (accessed August 11, 2009).
[169] "Sergei Markov says he knows who started the Estonia cyber war," *IntelFusion*, March 6, 2009, http://intelfusion.net/wordpress/?p=544 (accessed August 11, 2009).

Georgia – Improved Coordination

The cyber attack on Georgia occurred within the broader conflict between Russia, Georgia and South Ossetia, an autonomous and de jure demilitarized Georgian region on the border of Georgia and Russia, and recognized as part of Georgia by the international community. On July 19-20, 2008, the website of the President of Georgia came under a DDoS attack. The main attack came a few weeks later. A CCDCOE report included technical details of the attack and effected websites, government, news and media, and financial institutions.

> "On August 7, 2008, following separatist provocations, Georgian forces launched a surprise attack against separatist forces, ignoring the Russian-mediated ceasefire between the two sides. Russia responded by military attack and intense international propaganda. Simultaneously, cyber attacks were launched against Georgia's websites – On August 8, 2008, a large number of Georgian websites, both government and non-government, came under attack."[170]

Ossetian, Abkhazian, and Russian websites were also affected. The attacks used methods similar to those used in Estonia the year prior, defacement of public websites and launch of DDoS attacks against numerous targets. According to the analysis of the Swedish National Defence University, stopgeorgia.ru provided DDoS attack tools for download and showed a number of Georgian .ge websites as a priority for attack. There seems widespread consensus the attacks appeared coordinated.

Attacks expanded to Turkey and the Ukraine, where servers routing traffic to Georgia were commandeered by the Russia Business Network (RBN), a multi-faceted cybercrime organization. Physically based in St. Petersburg, Russia, RBN specializes in, and in some cases monopolizes, personal identity theft for resale. It is the originator of

---

[170] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008), 3.

the now commercially available MPack malware and an alleged operator of the Storm botnet, or controlled network of zombie computers. The RBN originated as an Internet service provider for child pornography, phishing, spam, and malware distribution, and is notorious for hosting illegal and dubious businesses.[171]

The attacks left the United Telecom of Georgia router incapable of providing service for several days. The main commercial Internet service provider Caucasus Network Tbilisi was flooded with traffic, possibly also affecting smaller Internet providers as traffic was rerouted. This problem was escalated by physical disconnections in the war activity zone. As a consequence of the attacks, the National Bank of Georgia ordered all banks to stop offering electronic services for ten days, August 9-18.

Georgia received timely international cooperation to respond to the attacks. CERT Georgia, organized as an academic CERT, started to function like a national CERT and coordinated attack mitigation. CERT Poland (CERT-PL) analyzed IP data and sent out abuse messages. CERT France (CERT-FR) collected the log files. Estonian authorities pledged to provide Georgia assistance in handling the cyber incidents.

Several sites under attack had to be temporarily moved to servers outside of Georgia. The Office of the President of Poland provided their website (www.president.pl) for dissemination of information and helped to get Internet access for Georgia's government after the breakdown of local servers caused by cyber attacks. The interpress.ge news portal moved to Servage (www.servage.net), a worldwide hosting platform provider. The websites of the Ministry of Defence and the president to Tulip Systems, Inc. were relocated to Atlanta, Georgia. The websites of Georgia's Ministry of Foreign Affairs and news portal civil.ge were hosted on Estonian servers. "According to

[171] "Russian Business Network," http://rbnexploit.com/ (accessed March 1, 2010).

the information exchanged in a meeting in Estonian [Ministry of Foreign Affairs] MFA, the initiative of the Estonian MFA to host the Georgian MFA website could not have happened without Estonia learning lessons from 2007. Later, the Georgian MOD site was also moved to Estonia."[172] Finally, websites hosted on Russian domains with addresses ending in .ru, and some pro-Russian sites in other zones were reportedly briefly blocked from Georgia.

As a result of questions arising from its support to the Georgian government, NATO's CCDCOE conducted a thorough legal review of the cyber attacks on Georgia.[173] Facts were gathered from CERT-EE and distinguished IT security websites, verified with the Georgian Embassy in Estonia, and compared with international media. Except where otherwise annotated, the relevant facts and activities of this attack are summarized from the CCDCOE report.

Regarding origin and attribution of the attacks, the CCDCOE report concluded: "[the] major DDoS attacks observed were all globally sourced, suggesting a botnet (or multiple botnets) behind them."[174] As in the Estonian case, there was no actual proof of who was behind the DDoS attacks. The C2 servers used in the attacks possessed seemingly bogus registration information but did tie back to Russia. There was some indication of RBN involvement, however, perhaps no more than providing hosting services to the botnet C2 and did not commit the DDoS attacks itself. "There seems to be a rather widespread consensus that the attacks appeared coordinated; however from all

---

[172] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008), 8.
[173] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008).
[174] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008), 9.

the evidence available, the participation of the Russian government cannot be concluded."[175]

On August 22, 2008, a U.S. open source intelligence (OSINT) initiative named Project Grey Goose was launched to examine how the Russian cyber war was conducted against Georgian websites and if the Russian government was involved or if it was entirely a grass roots movement by patriotic Russian hackers. In October 2008, the project assessed that:

- The Russian government would likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions.
- Nationalistic Russian hackers are likely adaptive adversaries engaged in aggressively finding more efficient ways to disable networks.
- A journeyman-apprentice relationship will continue to be the training model used by nationalistic Russian hackers.
- Hacker forums engaged in training Russian cyber warriors will continue to evolve their feedback loop which effectively becomes their Cyber Kill Chain.[176]

Kyrgyzstan – The Unnoticed Cyber Attack

Less than five months later in December 2008, opposition groups forming a new coalition in the United Peoples Movement (UPM) were seeking a new political system for Kyrgyzstan and the removal of President Kurmanbek Bakiyev from office. The UPM was planning a series of protests for February and March against political corruption, increasing human rights abuse, and the deterioration of living standards. The coalition had been coming under increasing pressure from authorities, with the state general

---

[175] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: NATO CCDCOE, August, 2008), 9.
[176] Jeff Carr, Andrew Conway, Billy Rios, Derek Plansky, Greg Walton, Jeremy Baldwin, Preston Werntz, and Rafal Rohozinski, *Project Grey Goose Phase I Report: Russia/Georgia Cyber War – Findings and Analysis,* Project Grey Goose, October 17, 2008.

prosecutor launching criminal investigations involving a number of the opposition leaders in weeks leading up to the attack, a move analysts labeled as politically motivated.[177] Opposition party parliament deputies had not been allowed to use the parliament's press center to brief journalists, and the ensuing attack was perceived as an extension of the same repression of dissent.[178]

On January 18, 2009, a massive DDoS attack against Kyrgyzstan ISPs www.ns.kg and www.domain.kg essentially shut them down. As there are only four ISP providers for the entire country, this attack was clearly sending a message. Since the attacking Internet protocol (IP) addresses were Russian, and since the Russian government supported the standing Kyrgyzstan President, the attacks were seemingly intended to send a message to the UPM.[179] Pressure from Russia towards Kyrgyz President Bakiyevk to close U.S. access to the key Manas airbase also intensified on the same day as the DDoS attacks.

Without network sensors similar to those used in more developed nations,[180] and without clear security ties such as NATO for assistance, unfortunately little else has been done or written regarding the attacks. With the ruling party still in power and aligned with their supposed attacker, the Kyrgyzstan attack provides little more than a stark example that technologies and global cooperation are absolutely instrumental to defending, mitigating, attributing and ultimately responding to cyber attacks.

---

[177] "The Kyrgyzstan Cyber Attack That No One Is Talking About," *IntelFusion*, January 21, 2009, http://intelfusion.net/wordpress/?p=509 (accessed March 26, 2009).
[178] "Kyrgyz Opposition Denied Use of Parliament Press Center," *Radio Free Europe Radio Liberty*, January 20, 2009, http://www.rferl.org/Content/Kyrgyz_Opposition_Denied_Use_Of_Parliament_Press_Center/1372339.html (accessed March 26, 2009).
[179] "The Kyrgyzstan Cyber Attack That No One Is Talking About," *IntelFusion*, January 21, 2009, http://intelfusion.net/wordpress/?p=509 (accessed March 26, 2009).
[180] Robert Lemons, "Cyber Attacks Disrupt Kyrgyzstan's Networks," *SecurityFocus*, January 30, 2009, http://www.securityfocus.com/brief/896 (accessed August 14, 2009).

July 4, 2009 Attack

On July 4, 2009, a distributed denial of service attack coming out of South Korea coincided with a round of North Korean missile launches and a corresponding UN decision to impose new sanctions. The attacks appeared to have originated out of Pyongyang,[181] and were reminiscent of an earlier 2007 attack.[182] The DDoS attacks were a series of coordinated cyber attacks against major government, news media, and financial websites in South Korea and the United States, involving the activation of a botnet that maliciously accessed targeted websites.[183] Most of the hijacked computers were located in South Korea.[184] The estimated number of the hijacked computers varies widely; around 20,000 according to the South Korean National Intelligence Service, around 50,000 according to Symantec's Security Technology Response group,[185] and more than 166,000 according to a Vietnamese computer security researcher who analyzed the log files of the two servers the attackers controlled.[186] Although the timing and targeting of the attacks suggest they may have originated from North Korea, it has not been substantiated.

The first wave of attacks occurred on July 4, 2009 (Independence Day holiday in the United States), targeting both the United States and South Korea. Among the

---

[181] Siobhan Gorman, and Evan Ramstad, "Cyber Blitz his U.S., Korea," *Wall Street Journal*, July 9, 2009, http://online.wsj.com/article/SB124701806176209691.html (accessed July 10, 2009).
[182] ICANN Security and Stability Advisory Committee (SSAC), "SSAC Advisory SAC008, DNS Distributed Denial of Service (DDoS) Attacks," March 31, 2006, http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf (accessed July 10, 2009).
[183] John Sudworth, "New 'cyber attacks' hit S Korea," *BBC News*, July 9, 2009, http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm (accessed August 11, 2009).
[184] Thomas Claburn, "Cyber Attack Code Starts Killing Infected PCs," *InformationWeek*, July 10, 2009, http://www.informationweek.com/news/showArticle.jhtml?articleID=218401559 (accessed August 11, 2009).
[185] Elinor Mills, "Botnet worm in DOS attacks could wipe data out on infected PCs," *CNET*, July 10, 2009, http://news.cnet.com/8301-1009_3-10284281-83.html.
[186] Martyn Williams, "UK, not North Korea, source of DDOS attacks, researcher says," *IDG News Service*, July 14, 2009, http://www.networkworld.com/news/2009/071409-uk-not-north-korea-source.html?ap1=rcb. (accessed August 11, 2009).

websites affected were those of the White House and the Pentagon.[187] An investigation revealed that 27 websites were targets in the attack based on files stored on compromised systems.[188]

The second wave of attacks occurred on July 7, 2009, affecting South Korea. Among the websites targeted were the presidential Blue House, the Ministry of Defense, the Ministry of Public Administration and Security, the National Intelligence Service and the National Assembly.[189] A third wave of attacks began on July 9, 2009, targeting several websites in South Korea, including the country's National Intelligence Service as well as one of its largest banks and a major news agency.[190]

The U.S. Department of Homeland Security issued a notice to U.S. federal departments and agencies to take steps to mitigate attacks. Despite the fact that the attacks targeted major public and private sector websites, the South Korean Presidential office suggested the attacks were meant to cause disruption, rather than steal data. The attack is estimated to have produced only 23 megabits of data per second, not enough to cause major disruptions.[191]

---

[187] "Governments hit by cyber attack," *BBC News*, July 8, 2009, http://news.bbc.co.uk/1/hi/technology/8139821.stm.

[188] John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *The New York Times*, July 9, 2009, http://www.nytimes.com/2009/07/10/technology/10cyber.html, (accessed August 11, 2009).

[189] Song Jung-a, "Pyongyang blamed as cyber attack hits S Korea," *Financial Times*, July 9, 2009, http://www.ft.com/cms/s/0/61bc6d22-6c1f-11de-9320-00144feabdc0.html (accessed August 11, 2009), and "Cyber Attacks Hit Government and Commercial Websites," *Foxreno*, July 9, 2009, http://www.foxreno.com/news/19999665/detail.html, (accessed August 11, 2009).

[190] John Sudworth, "New 'cyber attacks' hit S Korea," *BBC News*, July 9, 2009, http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm (accessed August 11, 2009), and "Official: S. Korea web sites under renewed attack," *Associated Press,* July 9, 2009, http://www.google.com/hostednews/ap/article/, (Accessed August 11, 2009).

[191] John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *The New York Times*, July 9, 2009, http://www.nytimes.com/2009/07/10/technology/10cyber.html, (accessed August 11, 2009).

It is not known who is behind the attacks, although data generated by the attacking program appeared to be based on a Korean-language browser. According to the South Korean National Intelligence Service, the source of the attacks was tracked down and the government activated an emergency cyber-terror response team. The team blocked access to five host sites containing the malicious code and 86 websites that downloaded the code, located in 16 countries, including the United States, Guatemala, Japan and the People's Republic of China, but North Korea was not among them.[192] It was later determined the malicious code responsible for causing the attack, W32.Dozer, re-used code from the Mydoom worm[193] and was programmed to destroy data on infected computers and to prevent the computers from being rebooted.[194] South Korean police stated there was various evidence of North Korean involvement, but said they may not find the culprit.[195]

The investigation itself is suspect, however, providing an excellent illustration of the complexity of attribution, and the current state of international cooperation in attaining it. The Korean CERT (KrCERT) copied the Hanoi Institute of Technology's Bach Khoa Internetwork Security Centre (BKIS) in an email to the Vietnamese CERT (VNCERT), requesting suppression of some IP addresses in Vietnam. Having been infected with the virus, the addresses had joined the DoS attack on websites in South Korea and the U.S. A July 10, 2009 email from KrCERT urgently requested members of

---

[192] Lee Jiyeon, "Cyberattack rocks South Korea," *GlobalPost*, July 11, 2009, http://www.globalpost.com/dispatch/south-korea/090710/cyberattacks (accessed August 11, 2009).
[193] Kim Zetter, "Lazy Hacker and Little Worm Set Off Cyberwar Frenzy," *Wired*, July 8, 2009, http://www.wired.com/threatlevel/2009/07/mydoom/ (accessed August 11, 2009).
[194] Thomas Claburn, "Cyber Attack Code Starts Killing Infected PCs," *InformationWeek*, July 10, 2009, http://www.informationweek.com/news/showArticle.jhtml?articleID=218401559 (accessed August 11, 2009).
[195] Kwang-Tae Kim, "S. Korea analyzes computers used in cyberattacks," *Associated Press*, July 12, 2009, http://www.google.com/hostednews/ap/article/ALeqM5jO5PtkM_1FjwMZjh3LS74g26yiUQD99CRCO80, (accessed August 11, 2009).

the Asia-Pacific CERT (APCERT) to help discover the source of the DDoS attack. KrCERT conducted its own independent research activities, providing the denial of service malware codes to BKIS only after they requested it.

BKIS analysts tracked the command and control (C2) servers to the UK. At the time BKIS made the analysis, hacking servers were sending malware to the group of robot servers, or botnet they controlled. BKIS surveyed the eight slave servers that participated in the attack and discovered two servers provided resource-sharing web services. BKIS gained control of both of the servers, subsequently finding a Virtual Private Network (VPN) tunnel from the UK to a master server in Miami:

> "In order to locate the source of the attacks, we have fought against [C2] servers and have gained control of 2 in 8 of them. After analyzing the logs of these 2 servers, we discovered the IP address of the master server...located in UK. The master server is running on Windows 2003 Server Operating System...After being requested by the Korean Computer Emergency Response Team (KrCERT), we used a method to trace back the source code of the virus and detected eight [C2] servers...We attacked them back and after we identified eight slave servers, we seized control of two of them. Through the counterattack, our experts collected useful information for analyzing and defining the master server that controlled the attacks on the websites of the South Korean and American governments. This master service has an IP address in the UK."[196]

BKIS announced on a July 12 blog that it had identified two servers located in the UK as the source of the attack, which was then reported by newspapers around the world.

[196] "Korean agency accuses BKIS of violating local and int'l law," *Bach Khoa Internetwork Security Centre (BKIS),* http://english.vietnamnet.vn/reports/2009/07/859068/ (accessed January 6, 2010).

Remarkably, Korean CERT (KrCERT) later accused BKIS of acting without its permission in uncovering the location of the servers:[197]

> "On July 16, the Vietnam Computer Emergency Response Team (VNCERT) informed the Hanoi University of Technology that it had received an 'offical complaint' from its Korean counterpart, KrCERT. Reportedly, [KrCERT]...had never requested BKIS to help investigate the attack...The KrCERT complaint alleged that the BKIS announcement of attacking and controlling two servers in the UK for analysis is a "serious violation of Vietnamese and international laws," compounded by the BKIS announcement, which caused the public to misunderstand that KrCERT and APCERT participated in this "illegal activity." VNCERT forwarded the KrCERT complaint to the Hanoi University of Technology, asking it to remind BKIS to report to VNCERT when it participates in international computer emergency response activities and to maintain secrecy. It should only provide information to related agencies based on rules agreed by the world network of computer emergency response agencies. [BKIS] said [KrCERT] did not know how BKIS succeeded in gaining control two servers in the UK, so [the] statement that the BKIS attacks "violated Vietnamese and international rules" is not accurate. He said BKIS "will work with KrCERT about this." "This is a perfectly ordinary diagnostic service, which anyone can use...Through it, BKIS acquired information that enabled us to analyze and locate a ninth, master server, that was the commander-in-chief of all the attacks on websites of the South Korean and American governments. This process obeyed Vietnamese and international rules." [BKIS] stated that seizing control of two servers used by hackers to launch DDoS attacks "doesn't require anyone's permission and anybody can do it" [and] defended [the] decision to 'go public' by quoting Article 43 of the Vietnamese government's Decree 64/2007: "In urgent cases which can cause serious incidents or network terrorism, competent agencies have the right to prevent attacks and report to the coordinating agency later" to explain for BKIS' not reporting to VNCERT. "The South Korean and American government websites were attacked and paralyzed for nearly ten days but the source of attack was not detected. This was an urgent case, which could threaten the world, including Vietnam...BKIS was allowed to hunt the source of attacks and report to the coordinating agency. We are investigating the case so we haven't time to report yet. We will perform this task after this job is accomplished."[198]

---

[197] Elinor Mills, "Researchers: Attacks on U.S., Korea sites came from U.K." *CNET*, http://news.cnet.com/security/?keyword=Bkis, July 14, 2009, and "Korean agency accuses BKIS of violating local and int'l law," *Bach Khoa Internetwork Security Centre (BKIS),* http://english.vietnamnet.vn/reports/2009/07/859068/ (accessed January 6, 2010).

[198] "Korean agency accuses BKIS of violating local and int'l law," *Bach Khoa Internetwork Security Centre (BKIS),* http://english.vietnamnet.vn/reports/2009/07/859068/ (accessed January 6, 2010).

The KrCERT accusation regarding the BKIS exercise of self-help is reminiscent of the Corfu Channel Case regarding naval mining discussed in the previous chapter. Recall the ICJ found that, irrespectively of who laid the mines, the Albanians ought to have observed any such action, since the minefield was so close to their coast, and thus they failed to inform the British of the danger. The corollary to the KrCERT-BKIS case would include state culpability for illegal activity under their sovereign jurisdiction, as well as state responsibility to take reasonable action to confront or mitigate such activity. Finally, precedent for international jurisdiction over security issues where attribution is in question has been established.

Summary

Every case demonstrated coordinated attacks, but no evidence of coordination between national governments. None of the attacks were perceived to have constituted an attack under international law. While ever-increasing coordinated behavior by governments certainly contributed to mitigating attacks in the case of Estonia, Georgia and the July 4, 2009 attacks, none were successful in attaining confident attribution in time and through a mechanism effectively enabling a meaningful response.

The Kyrgyzstan attack serves to show the importance of global coordination, capacity building, and that a lack of cooperation does in fact lead to worse results. The other cases all show that beyond the obvious incentives for victim states to cooperate, other states and organizations also appeared very willing to cooperate. With no surprise, supposed attacker states, however, were not, and no clear incentives for them to do so were evident. While some pressure was applied on Russia at the EU summit, any

corresponding pressure in the case of Georgia was trivialized by the world response to their military operations in general. No clear pressure against the DPRK in the case of the July 4, 2009 attacks was apparent.

While individual states may desire a more regulated environment and proposals for international agreements evidence collective desires, there remains no significant effort between the major powers or seemingly most egregious violators to cooperate in any meaningful way. No incentives for states significant enough to justify exposing themselves to supposed or potential adversaries were readily apparent. In this situation conflict and the individualistic pursuit of security in cyberspace are not currently seen as costly, with apparently little to no risk of major war or spilling into or being linked with other areas, such as economics. Without meaningful incentives for cooperation, nations proliferating or protecting cyberspace attackers seem more satisfied with the status quo than with negotiating away any potential leverage they currently enjoy, or expect to enjoy in the future. These states seem to be enjoying the fruits of their expansion in cyberspace, and believe it provides the best prospects for their security.

A*ny plausible path to meaningful defense in cyberspace must include a significant element of international cooperation and regime formation.* This assessment forms the basis for addressing the effectiveness and direction of international cooperation in regards to the attribution issue. The next chapter will describe the Internet and nascent cyberspace attack attribution regimes, relevant organizations, and identified agendas to confront this collective-action problem.

CHAPTER IV

INTERNATIONAL COOPERATION IN CYBERSPACE

REGIME ORIGINATION

The Internet grew out of a U.S. Department of Defense program based on the fundamental principles of decentralized authority and inclusive technical standards, providing the scalability necessary for universal connectivity and ease of expansion. The U.S. continues to hold authority over the majority of the servers and many networks comprising the physical backbone of the Internet, and a correspondingly dominant role in Internet governance decision-making. With the arrival of the World Wide Web in the 1990s, however, cyberspace as we know it today burst into the open, public sphere.

The creation and evolution of international management and technical governance arrangements that have enabled the interconnection of geographically dispersed computer networks over much of the globe within complex commercial and legal frameworks advanced relatively smoothly. As the borderless activity of this new information domain confronted traditional political, market, legal and military boundaries, however, all have been challenged as never before.

Day to day operations in cyberspace transformed from a free and open technological breakthrough to an increasingly controlled public institution. Thousands of corporate and government-run ISPs established rules for users of their services within the boundaries of network agreements providing global access. Many ISPs joined to create regional associations forming a basis for international cooperation.

Responsibility for the Internet's technical infrastructure gradually moved from the U.S. Department of Defense (DOD) Defense Advanced Research Projects Agency (DARPA) Internet Architecture Board (IAB) to the totally private international organization, Internet Corporation for Assigned Names and Numbers (ICANN) in 1999.[199] The U.S. Commerce Department white papers leading to ICANN's mandate typified three principles for Internet governance: openness, representation, and due process. To the extent security and attribution of attacks might have been considered under this mandate, it appears the Commerce Department and ICANN envisioned a claims process conforming to due process and other democratic norms,[200] similar to the WTO DSU claims and appellate process.[201]

Other relevant international organizations include the:

- World Intellectual Property Organization (WIPO) and Internet Trademark Association concerned with intellectual property matters;
- Internet Society (ISOC) and subordinate Internet Engineering Task Force (IETF) and IAB concerned with technological growth of the Internet;
- ITU and International Organization for Standardization (ISO) for international standards, coordination and settlements; and
- WTO regarding matters of global e-commerce.

The roles of the ITU and WTO have already been addressed for the roles they have played in the formation of principles and norms in other domains.

This list is illustrative and not exhaustive as other organizations and forums have certainly played extensive roles, particularly with respect to engineering advancements. These include a number of vendor-driven forums and consortiums instrumental in setting

---

[199] Marcus Franda, *Governing the Internet: the emergence of an international regime*, (Lynne Rienner Publishers, Inc., 2001), 6-8.
[200] Marcus Franda, *Governing the Internet: the emergence of an international regime*, (Lynne Rienner Publishers, Inc., 2001), 61-72.
[201] World Trade Organization, http://www.wto.org/english/docs_e/legal_e/28-dsu_e.htm#7 (accessed July 3, 2009).

early standards. Similarly, Switzerland's Centre Européen pour la Recherche Nucléaire (CERN) Laboratories contributed significant work to develop major building blocks of the World Wide Web including Hypertext Transfer Protocol (HTTP), Hypertext Markup Language (HTML), and Universal Resource Locator (URL). In coordination with CERN, the World Wide Web Consortium (W3C) developed new protocols including Extensible Markup Language (XML) and Hardware Markup Language (HML).[202]

In the aftermath of the 1998 Morris worm incident, the Defense Advanced Research Projects Agency charged the Software Engineering Institute, Carnegie Mellon University, to establish a capability to coordinate communications among experts during computer security incidents and prevent future incidents. The result was the Computer Emergency Response Team, CERT (later renamed CERT® Coordination Center, CERT/CC), whose mission is: "[To] work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents."[203]

CERT/CC has built a solid reputation for objectivity and discretion based on the center's proven ability to keep identities and sensitive information confidential. The level of trust is evident in its receipt of over 235,000 e-mail messages, 16,200 hotline calls, 17,800 computer security incidents, and more than 1,100 vulnerability reports in the first decade of its existence. [204] CERT/CC grew from handling six security incidents in 1998 to 52,658 in 2001, and had handled over 73,000 for 2002 by the end of September

---

[202] Marcus Franda, *Governing the Internet: the emergence of an international regime*, (Lynne Rienner Publishers, Inc., 2001), 7-11.

[203] Steven M. Rinaldi, "Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security," *USAF Institute for National Security Studies (INSS)* Occasional Paper 33 (Colorado Springs, CO: USAF Academy, May, 2000), 47.

[204] Steven M. Rinaldi, "Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security," *USAF Institute for National Security Studies (INSS)* Occasional Paper 33 (Colorado Springs: USAF Academy, May, 2000), 47-48.

alone.[205] CERT/CC is an excellent example of the importance of trust and ability to protect confidential information to effectively coordinate responses to cyberspace attacks.

The Y2K Challenge

The first global test of responding to a failure in cyberspace was focused on an internal engineering threat rather than an attack per se. The public-private and international cooperation experienced in its mitigation was the most significant to date, laying the groundwork for current cooperation in the area of attack attribution. The year 2000 date conversion (Y2K) was a result of how dates were entered into computers, resulting in a variety of computer malfunctions. States identified national Y2K coordinators and at the First Global Meeting of National Y2K Coordinators at the United Nations in December 1998, coordinators from over 120 countries advocated for the creation of an International Y2K Cooperation Center (IY2KCC). The IY2KCC was established in February 1999 under the auspices of the UN with funding from the World Bank to "promote increased strategic cooperation and action among governments, peoples, and the private sector to minimize adverse Y2K effects on the global society and economy."[206]

---

[205] Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Carnegie-Mellon University, November, 2002, 5.

[206] Charles Babbage Institute, *International Y2K Cooperation Center Records (CBI 153)* (Minneapolis: University of Minnesota) http://special.lib.umn.edu/findaid/xml/cbi00153.xml (accessed July 3, 2009).

Activities of IY2KCC were conducted in six areas before closing down in March, 2000:

- National Readiness to promote Y2K programs worldwide;
- Regional Cooperation to promote and support coordination within defined geographic areas;
- Sector Cooperation to promote and support coordination within and across defined economic sectors;
- Continuity and Response Cooperation to promote and support coordination to ensure essential services and provisions for emergency response;
- Information Cooperation to promote and support international information sharing; and
- Publicity, and Facilitation and Assistance responsible for organizing global meetings of Y2K coordinators and to identify resources.[207]

A U.S. Senate special committee identified ascertaining the status of international preparation their greatest challenge in the months leading up to the Y2K conversion and the IY2KCC created a useful mechanism for governments from member countries to share information and lessons learned.[208] The committee's final report noted some type of similar international coordination mechanism could be useful in addressing future IT issues.[209]

Y2K preparations also formalized domestic cyber incident monitoring and response procedures. Within the U.S., CERTs and international Forum of Incident Response and Security Teams (FIRST) provided the national information coordination center (ICC) reports on incidents in their respective areas. The Federal Bureau of

---

[207] The United States Senate Special Committee on the Year 2000 Technology Problem, *Statement of Bruce W. McConnell, Director, International Y2K Cooperation Center Director* (Washington, DC: U.S. Government Printing Office, July 29, 1999).

[208] The United States Senate Special Committee on the Year 2000 Technology Problem, *Investigating the Year 2000 Problem: The 100 Day Report* (Washington, DC: U.S. Government Printing Office, September 22, 1999).

[209] The United States Senate Special Committee on the Year 2000 Technology Problem, *Y2K Aftermath – Crisis Averted Final Committee Report* (Washington, DC: U.S. Government Printing Office, February 29, 2000), 20.

Investigation (FBI), National Security Council (NSC), DOD Decision Support Activity and other agencies similarly reported to the ICC.

More generally, the massive effort to address the Y2K problem forged new relationships and partnerships among industry and government sectors, particularly in the areas of critical infrastructure. The U.S. alone estimated to have spent $100 billion on the problem.[210] Again, the Senate found it important that domestic and international industry and government partnerships nurtured during Y2K preparations were maintained and continued to grow.[211] The final committee report starkly identified examples of Y2K glitches around the globe representational of the potential impact of a concerted attack in cyberspace.[212]

The Decentralized Nature of Cyberspace

This description of cyberspace origination so far is informative from a traditional organizational, rational utility point of view; however, it would be deeply flawed and skewed to discuss the story from only this perspective. For while governments and institutions spawned the Internet and have worked to subsequently control and manage it, decentralized forces have revolutionized not only the world of cyberspace, but through it the world we live in. "The absence of structure, leadership, and formal organization,

---

[210] The United States Senate Special Committee on the Year 2000 Technology Problem, *Y2K Aftermath – Crisis Averted Final Committee Report* (Washington, DC: U.S. Government Printing Office, February 29, 2000), 3-12.
[211] The United States Senate Special Committee on the Year 2000 Technology Problem, *Y2K Aftermath – Crisis Averted Final Committee Report* (Washington, DC: U.S. Government Printing Office, February 29, 2000), 23.
[212] The United States Senate Special Committee on the Year 2000 Technology Problem, *Y2K Aftermath – Crisis Averted Final Committee Report* (Washington, DC: U.S. Government Printing Office, February 29, 2000), 37-49.

once considered a weakness, has become a major asset. Seemingly chaotic groups have challenged and defeated established institutions. The rules of the game have changed."[213]

From the Internet's inception in the mid-1990s with the first popular web browser, grass-roots movements with no strategic plan collectively advanced in a newly decentralized fashion. With no one in charge, individuals throughout the net contributed as they were able creating not only the industry standard, but a new standard of industry. These standards outpaced development efforts by large actors such as Microsoft and Netscape, circumventing a major clash, an important note for addressing collective-action relative gains problems in cyberspace.

Decentralization powered by the Internet soon expanded beyond technical web development, shifting underlying power structures within numerous industries. This shift is evidenced in areas as diverse as:

- Information sharing (e.g. Wikipedia);
- Telecommunications (e.g. Skype and other voice over Internet protocol (VOIP) companies);
- Music (e.g. Napster and Apple's iTunes);
- Marketing (e.g. eBay, CraigsList, and Amazon);
- Environmental activism (e.g. ALF); and even
- Conflict (e.g. al Qaeda).[214]

Wikipedia demonstrates one of the key aspects of cyberspace development lost in a purely organizational-perspective discussion: "There's no schedule, there's no direction for these people at all. Nobody's the boss of anybody. People just pick up projects and work on them. They remotely log into servers to work on them when they need

---

[213] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 7.
[214] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 62-74.

maintenance. They reconfigure the networks when they need reconfiguring. It's all done completely willy-nilly, I mean with no organization at all. And yes, it works."[215]

Another aspect of Wikipedia is important to note for this topic. Not only are the quality of articles outstanding, but users police the sites from malicious or erroneous entries with incredible diligence, speed, and accuracy. "[An] investigation led by Nature magazine found that Wikipedia and the Encyclopedia Britannica are almost equally accurate. Like concerned and thoughtful neighbors, members of the Wikipedia community care enough to contribute regularly and are mindful to keep the content accurate."[216] Some users even volunteer as Wikipedia cops. Additionally, Wikipedia can lock down certain pages exceptionally prone to vandalism perhaps due to its controversial nature until a compromise is reached among users, or the controversy subsides.[217]

This highlights an important conclusion for the current study: "Open systems can't rely on a police force...there's freedom to do what you want, but [you] become responsible for your own welfare and that of those around you."[218] While this may have disturbing consequences for states and organizations responsible for providing stability and security, we should not lose sight of the fact that differences across domains require a similar variance in potential solutions. Models that would clearly be unacceptable in more centralized domains exhibiting high transaction costs of entry, such as nuclear or major war, might be those that should in fact be embraced, at least to some extent, in more decentralized domains. Domains with low costs of entry are strongly represented

---

[215] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 112.
[216] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 74.
[217] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 76-77.
[218] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 80.

by society, and policing mechanisms reflect similarly decentralized approaches ranging from civil air patrols, merchant marines, paramilitary forces, and even neighborhood watches. This may also mean what is acceptable for some open democracies may be the most feared by more authoritarian regimes.

Another relevant point to make is that when attacked, a decentralized organization tends to become even more open and decentralized. When established institutions took early P2P music sharing entities such as Napster to court, they only exacerbated the problem. As it turned out, waging this battle was the worst strategic move the music labels could have made. Each successive court case simply contributed to the proliferation of P2P services, as well as their level of decentralization making each successive case more difficult than the previous one. Further, those convicted often became heroes of the movement. Removing the catalyst only shifts the power in circles, further decentralizing the organizations and making them stronger.[219]

The Internet has drastically lowered the barrier to entry to numerous domains in this way, irrevocably shifting power to the people. In the above example, not only did the P2P industry become more decentralized, revenues among the four leading record labels dropped 25% between 2000 and 2001. This revenue did not shift to the P2P players; it simply disappeared from the industry.[220] From a government perspective, such a loss may or may not equate to lost revenues (e.g. taxes), but almost certainly to a corresponding loss of control over the domain.

---

[219] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 139-143.
[220] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 45.

In decentralized societies, the power resides with the individual, resulting in flexibility, shared power and ambiguity. Everyone becomes a leader, spawning accountability and self-policing among peers, and so it is with the Internet. It is not like a spider with a centralized nervous system, but rather like the neural net of a starfish. If you cut off a leg, or even all five legs, a new starfish will grow from each. "[It's] easy to mistake starfish for spiders."[221]

It is important to acknowledge decentralized organizations do not necessarily make better decisions; however, those decisions are better informed and the organizations are able to adapt more quickly to external and internal stimuli. In this way, it can grow very rapidly. "Since the industrial revolution, people had communicated by mail, telegraph, or telephone, but the Internet changed everything in less than a decade."[222]

In decentralized organizations, the people who use the site are also responsible for it. Craigslist is an example of such a site, promoting and relying almost entirely upon a culture of trust and community. No one tells anyone else what they can or cannot do. If something is offensive, users themselves can take it down. "It's a fully user-controlled democratic system."[223] In an open system, what matters most is leadership trusting members enough to leave them alone. People remain happy as long as they're given freedom to do what they want to do. Again, sites such as Craigslist have had a similarly devastating impact on newspaper revenues. Major newspapers responded in the same

---

[221] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 36.
[222] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 39-41.
[223] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 65-66.

fashion as the music industry becoming more centralized and suffering similarly negative strategic consequences.[224]

The simple mechanism of feedback, for example through eBays user ratings, was a simple, but crucial innovation to developing trust and confidence on the part of users.

> "In empowering the community, eBay shifted the burden of policing from the company to its users—knowledge and power became distributed throughout the network... [Sellers] gained a huge incentive to stay honest and trustworthy...Items sold by users with an established record of positive feedback fetched an 8.1 percent premium over identical items sold by nonestablished sellers."[225]

Although eBay hosts P2P interactions and relies on a decentralized user rating system, it retains important centralized organizational aspects. EBay also relies on a subsidiary PayPal based on rigid controls and secure interaction to allow users to transfer funds to one another via a trusted intermediary. As it turns out, when it comes to money, people want structure, safety and accountability.[226]

EBay is a hybrid organization. A hybrid organization operates in both the public and private sectors, simultaneously fulfilling public duties and developing commercial market activities. It deliberately mixes organizational forms in an attempt to blend the advantages of two or more different types or because the organization changing. Hybrid organizations include both decentralized aspects more attuned to the decentralized nature of cyberspace, as well as traditional centralized features that allow for the provision of security, authority, and accountability.

---

[224] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 67-68.
[225] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 163.
[226] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 164-165.

Ultimately, Apple cashed in on the power shift in the music industry brought about by P2P services through its iTunes software, allowing consumers to buy and share (e.g. podcast) individual songs as opposed to entire albums. This also combined the features of a decentralized marketplace with accountable and revenue-producing structures of a centralized company in a safe and legal environment, providing premium services with security. This type of hybrid organization is one possible adaptation approach for addressing cyberspace attacks and attribution.

There are two recognized approaches to forming *hybrid organizations*, centralized organizations that decentralize the customer experience and those that decentralize internal parts of themselves. In the case of the former, organizations introduce decentralized elements by giving their users a role. For example, eBay introduced user ratings. Amazon incorporated a similar feature allowing users to review books. Some have gone even farther inviting users to actually make the products themselves. Google relies upon user input. The more it is used, the more feedback is provided and the more accurate its popularity-based search engine becomes, making it more useful for the customer. As the 2005 Intuit-launched TaxAlmanac.org (a Wikipedia equivalent for tax issues) site explains: "One of the things we've learned is that the community wants to interact with one another."[227]

The second type of hybrid organization need not radically change its structure. Although it may mean separating units into distinct organizations, it may be as simple is incorporating a form of appreciative inquiry to spread information, and therefore ownership around the organization.

---

[227] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 171-172.

What does this portend for efforts toward attack attribution? In order to continue to provide premium services with security, states would do well to not only recognize the loss of control over the domain, but to embrace it through hybrid organizations. States should focus controls toward specific areas where it is desired by users, such as monetary transactions and official information content, allowing and empowering Internet users themselves to help police the rest. Passing this information exchange and ownership to the broader Internet community as opposed to individual states may in fact be instrumental in circumventing clashes between major actors and addressing the problem of relative gains.

Such a state-sponsored hybrid approach might be accomplished through continued decentralization and improvement to the user experience, promoting feedback, ownership, and direct interaction among Internet users themselves. At the very least, such a cyber-civil air patrol approach will spread information and ownership around the Internet, allowing them to adapt more quickly to stimuli, such as an attack.

Cyberspace as a Security Regime

International cooperation in the security arena, however, is more problematic due to the security dilemma resulting from a real or perceived relative gain in security for one actor leading to the real or perceived decrease in security of others.[228] Marcus Franda conducted the first, and perhaps most significant research for this current study. He specifically inquired how such activity might inform current theories of international

---

[228] Robert Jervis, "Security Regimes," in Stephen Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1983), 173-194.

relations through the concept of international regimes,[229] as espoused by Robert Keohane,[230] Stephen Krasner[231] and others.

One representational area squarely in the crosshairs of this debate was control of country code top level domains (ccTLD, such .uk, .il, .pt, etc.) identified through ITU country codes. This sovereign vs. common space issue was exacerbated in an October 1998 letter to the Commerce Department stating it would "respect each nation's sovereign control over its individual top-level domains." The debate ultimately favored a counter position that: "It was never intended that just because it had a two-letter country code that the computers were in that country, much less under some sort of sovereign ownership...In fact, the sovereign ownership concept doesn't make sense because this is a shared computer network."[232] This concept of cyberspace as international commons is instrumental to its nature as a domain as established in others, notably the sea and space domains. The negotiation process between ICANN and individual government or private ccTLD managers continues to this day as continually documented through the exchange of letters and agreements.[233]

The test of whether agreed upon technical principles and norms can survive as a bona fide international regime will depend upon global leaders' ability to adapt to rapid change while managing divergent cultural, political, social, and economic behavior and

---

[229] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001), 1.
[230] Robert Keohane, "The Theory of Hegemonic Stability and Changes in International Economic Regimes, 1967-1977," in Ole R. Holsti, Randolph M. Siverson, and Alexander L. George, *Changes in the International System* (Boulder, Colorado: Westview Publishing, 1980), 131-162.
[231] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1983).
[232] Jeri Clausing, "New Internet Board Could Shake up Country Domains," *New York Times*, November 27, 1998. 4. Quoted in Marcus Franda, *Governing the Internet: the emergence of an international regime*, (Lynne Rienner Publishers, Inc., 2001), 69-70.
[233] ICANN, http://www.icann.org/en/cctlds/agreements.html (accessed July 6, 2009).

practices with divergent expectations of the Internet.[234] In the absence of a formal ITU-like intergovernmental institution, ICANN may be "the most acceptable organization for carrying out negotiations for the principles, norms, rules, and procedures of a new governance regime for the Internet simply because it already exists."[235]

The decentralized nature of the Internet yields specific consequences and evidence for recommendations in addressing relative gains in cyberspace. Are ICANN and other relevant intergovernmental institutions passing information exchange and ownership to the broader Internet community as opposed to states to address the problem of relative gains and circumvent clashes between major actors? Are they promoting premium services with security, recognizing and addressing the loss of control over the domain through hybrid organizations? Are controls focused toward specific areas where desired by Internet users, such as monetary transactions and official information content, allowing and empowering users themselves to help police the rest? If so, are hybrid organizations decentralizing to continually improve the user experience, promoting feedback, ownership, and direct interaction among users themselves? Are they spreading information and ownership around the Internet, allowing users to adapt more quickly to stimuli, such as an attack? The rest of the chapter explores these questions.

REGIME MATURATION

For some of the reasons related to decentralization and relative gains discussed above, the cooperation exhibited in addressing the Y2K problem did not directly translate

---

[234] Marcus Franda, *Governing the Internet: the emergence of an international regime*, (Lynne Rienner Publishers, Inc., 2001), 2-33.
[235] Marcus Franda, *Governing the Internet: the emergence of an international regime*, (Lynne Rienner Publishers, Inc., 2001), 75.

into addressing the threat or attribution of cyberspace attacks. In 2002, Dr. Howard Lipson of the CERT®/CC in a special report for the U.S. Department of State noted:

> "[The] current state of the practice regarding the technical ability to track and trace Internet-based attacks is primitive at best. Sophisticated attacks can be almost impossible to trace to their true source using current practices. The anonymity enjoyed by today's cyber-attackers poses a grave threat to the global information society, the progress of an information-based international economy, and the advancement of global collaboration and cooperation in all areas of human endeavor."[236]

Numerous organizations have since attempted to advance security in cyberspace since then, with mixed accomplishments.

OECD and COE Roles, Agendas and Accomplishments

In August 2002 the Organization for Economic Cooperation and Development (OECD) released revised Guidelines for the Security of Information Systems and Networks. The guidelines sought to increase public awareness, education, information sharing, and training to promote a better understanding of online security and the adoption of best practices. The Guidelines represented consensus views of all 30 OECD member countries toward "A Culture of Security,"[237] replacing similar guidelines previously issued in 1992.

The Council of Europe (COE) continued to press forward with the convention on cybercrime,[238] which entered into force in July 2004, and is the only binding international treaty on the subject to have entered into force. It identifies guidelines for all

---

[236] Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues,* (Carnegie-Mellon University, November, 2002), ix.
[237] Federal Trade Commission, "OECD Issues Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," August 23, 2002, http://www.ftc.gov/opa/2002/08/oecdsecurity.shtm (accessed July 7, 2009).
[238] Council of Europe Convention on Cybercrime, (Budapest: Council of Europe, November 23, 2001) http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (accessed July 7, 2009).

governments wishing to develop legislation against cybercrime, and is open to signature by non-European states, providing a framework for international cooperation.[239]

Internet Governance and ICANN, ITU and WSIS Roles, Agendas and Accomplishments

In January 2002, the United Nations General Assembly endorsed a proposal for a global summit on Information and Communication Technology (ICT) issues. The International Telecommunications Union (ITU) took the lead in organizing the World Summit on the Information Society (WSIS), including the participation of more than 50 heads of state.

The summit process began with a preparatory committee, or Prepcom, in July 2002 for the first phase in December 2003 in Geneva. The last Prepcom, held in September 2005 in Geneva, ended without securing final agreement on Internet governance, and with the U.S. rejecting a European Union proposal to relinquish control of ICANN. The dominant role of U.S. policy making in Internet governance was at the crux of the issue with alternatives put forth as radical as adopting a civil society approach to Internet governance.[240] Such an approach would be composed of the totality of voluntary civic and social organizations and institutions that form the basis of a functioning society as opposed to the force-backed structures of a state (regardless of that state's political system) and commercial institutions of the market. In essence, this would completely decentralize Internet governance as opposed to creating hybrid organizations, inhibiting capacity to provide secure services where desired.

---

[239] Council of Europe, "Cybercrime: a threat to democracy, human rights and the rule of law," http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp (accessed July 7, 2009).
[240] International Telecommunications Union, "World Summit on the Information Society," http://www.itu.int/wsis/index.html (accessed March 1, 2010).

In 2003 at Geneva, delegates from 175 countries took part in the first phase of WSIS where they adopted a Declaration of Principles as a road map for achieving an information society accessible to all and based on shared knowledge:

> "Strengthening the trust framework...is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies...supported by increased international cooperation...to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. [We] support the activities of the United Nations to prevent the potential use of ICTs 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. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights...Cyber-security should be dealt with at appropriate national and international levels."[241]

A Plan of Action set the goal of bringing 50 percent of the world's population online by 2015, but did not spell out any specifics of how this might be achieved. The Geneva summit also left unresolved more controversial issues, including the question of Internet governance and funding.

When the 2003 summit failed to reach agreement, the Working Group on Internet Governance (WGIG) was formed to develop ideas on the future of Internet governance. Civil society delegates from non-governmental organizations (NGOs) produced a document titled "Shaping Information Societies for Human Needs,"[242] assembling a wide range of issues under a human rights and communication rights umbrella.

---

[241] "Building the Information Society: a global challenge in the new Millennium," *World Summit on the Information Society Declaration of Principles*, December 12, 2003, http://www.itu.int/wsis/docs/geneva/official/dop.html (accessed March 1, 2010).

[242] International Telecommunications Union, "World Summit on the Information Society," http://www.itu.int/wsis/index.html (accessed March 1, 2010).

In a document released on December 3, 2003, the United States delegation to the WSIS advocated a strong private sector and rule of law as the critical foundations for development of national ICT efforts. Ambassador David Gross, the U.S. coordinator for international communications and information policy, outlined the three pillars of the U.S. position, identifying specific focus areas for Internet state control and security through ostensibly hybrid organizations:

- Commitment to the private sector and emphasis on the rule of law, so that countries can attract the necessary private investment to create the infrastructure as nations attempt to build a sustainable ICT sector;
- Content creation and intellectual property rights protection in order to inspire ongoing content development; and
- Ensuring security on the Internet, in electronic communications and in electronic commerce. "All of this works and is exciting for people as long as people feel that the networks are secure from cyber attacks, secure in terms of their privacy."[243]

Gross stated the United States was achieving broad consensus on the principle that a culture of cyber security must develop in national ICT policies to continue growth and expansion in this area. He related considerable national legal and international information sharing advances towards addressing exponentially increasing criminal threats in cyberspace to make his case.

Many governments expressed concern that various groups used U.S.-based servers to spread anti-Semitic, nationalist, or regime critical messages. This controversy is, at its root, a consequence of the American position on free speech which does not consider speech as criminal without direct appeals to violence. The U.S. argued that giving the control of Internet domain names to international bureaucrats and governments

---

[243] United States Department of State, "U.S. Outlines Priorities for World Summit on the Information Society," December 3, 2003 http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2003&m=December&x=20031203163730retropc0.0570032&t=usinfo/wf-latest.html (accessed August 13, 2009).

may lead to massive censorship that could destroy the freedom of the Internet as a public space. This would seem to reinforce the earlier assertion that rules for open, decentralized systems acceptable for some open democracies may also be the most feared by more authoritarian regimes, and demonstrates a significant variance of views over the limits of control of the Internet. On June 30, 2005, the U.S. Department of Commerce made it clear it intends to retain control of the Internet's root servers indefinitely.

The second WSIS phase took place in November 2005 in Tunis, Tunisia. The Association for Progressive Communications (APC), an international network of civil society organizations, participated extensively in the Internet governance process at the WSIS. APC attended with the stated goal of empowering and supporting groups and individuals working for peace, human rights, development and protection of the environment through the strategic use of ICT, including the Internet. On the eve of the Tunis event, the APC proposed specific actions in each of the following five areas:[244]

- The establishment of an Internet Governance Forum;
- The transformation of ICANN into a global body with full authority over DNS management, and an appropriate form of accountability to its stakeholders in government, private sector and civil society;
- The initiation of a multi-stakeholder convention on Internet governance and universal human rights that will codify the basic rights applicable to the Internet, which will be legally binding in international law with particular emphasis on clauses in the universal declaration of human rights specifically relevant to the Internet, such as rights to freedom of expression, freedom of association and privacy;
- Ensuring Internet access is universal and affordable; and
- Measures to promote capacity building in developing countries with regard to increasing developing country participation in global public policy forums on Internet governance.

---

[244] International Telecommunications Union, "World Summit on the Information Society," http://www.itu.int/wsis/documents/listing-all.asp?lang=en&c_event=s|2&c_type=all (accessed March 1, 2010).

APC argued: "The Internet is a global public space that should be open and accessible to all on a non-discriminatory basis. The Internet, therefore, must be seen as a global public infrastructure. In this regard we recognize the Internet to be a global public good related to the concept of the common heritage of humanity and access to it is in the public interest, and must be provided as a global public commitment to equality."[245]

A dispute over control of the Internet threatened to derail the conference; however, a last-minute decision to leave control in the hands of the U.S.-based ICANN for the time being avoided a major clash. The conference resulted in agreement on the Tunis Commitment, and a compromise to establish the called for international Internet Governance Forum, with a purely consultative role. The Commitment specifically recognized "the involvement, cooperation and partnership of governments and other stakeholders, i.e. the private sector, civil society and international organizations, and that international cooperation and solidarity at all levels"[246] were indispensible in addressing achieving their goals.

The IGF similarly addressed security, however with an emphasis on protecting children, and child pornography in particular. The IGF recognized other security issues to include cyber-terrorism, hacking, and other virus and cyber threats, and resulted in the formation of a wide number of Dynamic Coalitions. These coalitions are relatively informal, issue-specific groups consisting of stakeholders that are interested in the particular issue, and most coalitions allow participation of anyone interested in contributing. Thus, these groups gather not only academics and government

---

[245] International Telecommunications Union, "World Summit on the Information Society," http://www.itu.int/wsis/documents/listing-all.asp?lang=en&c_event=s|2&c_type=all (accessed March 1, 2010).

[246] World Summit on the Information Society, *Tunis Commitment*, November 18, 2005.

representatives, but also members of the civil society interested in participating on the debates and engaged in the coalition's works. None of the dynamic coalitions, however, specifically address cyber attacks or attack attribution within the context of this paper.[247]

As of May 2009 there continued to be calls for the U.S. to give up control of ICANN;[248] however, as recently as August, 2009 a U.S. Senate version of the Cyberspace Security Act of 2009 continued to advocate the counter position, going so far as to provide the President essentially emergency control of the Internet and the ability to shut down online traffic by seizing private networks. The legislation would allow the President to declare a cybersecurity emergency, which remained undefined, related to nongovernmental computer networks and respond to the danger.[249]

On May 17, 2007, the ITU launched the Global Cybersecurity Agenda (GCA), to provide a comprehensive framework to coordinate and address international responses to growing cybersecurity challenges. The ITU Secretary-General benefited from the advice of an expert panel, the High-Level Experts Group, representing expertise in policy making, government, academia and the private sector. This advisory group met for the first time in Geneva on October 5, 2007, to develop strategies to combat cybercrime and promote cybersecurity, formulating proposals to the ITU Secretary-General in a Global Strategic Report.

In September 2008 the ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT) entered into an agreement collocating the ITU Global

---

[247] Internet Governance Forum, www.intgovforum.org/, (accessed March 1, 2010).
[248] "Europeans: U.S. Should Give Up Control of the Internet," *Fox News*, May 4, 2009 http://www.foxnews.com/story/0,2933,518808,00.html (accessed September 7, 2009).
[249] "Senate Bill Would Give President Emergency Control of Internet," *Fox News*, August 28, 2009 http://www.foxnews.com/politics/2009/08/28/senate-president-emergency-control-internet/ (accessed September 7, 2009).

Cybersecurity Agenda (GCA) with IMPACT headquarters in Cyberjaya, Malaysia to provide ITU membership with the expertise, facilities and resources to effectively address the world's most serious cyber-threats. The partnership was intended to provide:

- Real-time analysis, aggregation and dissemination of global cyber-threat information;
- Early warning system and emergency response to global cyber-threats; and
- Training and skills development on the technical, legal and policy aspects of cybersecurity.

IMPACT is an international public-private initiative dedicated to enhancing the global community's capacity to prevent, defend and respond to cyber threats. The Global Response Centre (GRC) plays a pivotal role in realizing ITU GCA's objective of putting technical measures in place to combat new and evolving cyber-threats, and the ITU maintains a virtual showcase in Geneva of the early warning system, crisis management and real-time analysis of global cyber-threats available in Cyberjaya.

The two prime highlights of GRC are Network Early Warning System (NEWS) and Electronically Secure Collaboration Application Platform for Experts (ESCAPE). Working with leading partners in the industry, academia, and governments, NEWS provides the global community with a real time early warning system, serving as a vehicle for information sharing and collaboration of up to date information on security trends. NEWS features include:

- Real time threat monitoring and assessment whereby member countries can see the global severity threat level and solutions to mitigate the threat;
- Statistical cyber threat trend analysis whereby member countries can see minute views of current cyber trends and threats around the world, presented as a collection of easy to read charts, graphs, maps and tables; and
- Malware threat centre where members can upload malware and receive feedback on the full technical details of the malware analysis.

IMPACT also provides its member countries with ESCAPE, an electronic tool that enables authorized cyber experts across the different countries to pool resources and remotely collaborate with each other in a secure and trusted environment. ESCAPE features a comprehensive and growing database of key resources around the world – including IT experts, empowered persons (e.g. government regularity officials), and other trusted bodies (e.g. CERTS), who can be called in to assist during a crisis. Thus, members can rapidly create a response team to deal with almost any emerging cyber threat. ESCAPE enables GRC coordination and response for countries during emergencies, enabling swift identification and the sharing of available resources across borders.

The ITU provides crucial expertise, both in its research on cyber security as well as its experience with developing online collaborative platforms. With a state of the art team collaboration platform and access to experts from government, academia and private industry, IMPACT represents a significantly empowered hybrid organization for global emergency response.

The ITU Centre for Policy & International Cooperation partners with United Nations agencies, Interpol, Council of Europe, OECD and others to contribute to the formulation of new policies and the harmonization of national laws around a variety of issues relating to cyber-threats, including cybercrimes. The Centre provides advisory services to interested ITU Member States on policy and regulatory matters for cybersecurity. With the support of ITU, the Centre fosters international cooperation through specific programs such as coordinated cyber-drill exercises between countries.

IMPACT's Centre for Training & Skills Development also provides world-class cyber-training in support of ITU's objective of capacity building among member states.

Other Related Efforts and Hybrid Organizations

Any number of related efforts and hybrid organizations may be identified around the globe through even a cursory survey of the community. The previous chapter alluded to several including the NATO CCDCOE, national CERTs, IntelFusion, and Project Grey Goose. Chapter seven will further describe a rather expansive organizational approach from a uniquely Chinese perspective. A few organizations are highlighted here for illustrative purposes.

Established in 2004, the Shadowserver Foundation gathers intelligence on the darker side of the Internet. Comprised of volunteer security professionals from around the world that gather, track, and report on malware, botnet activity, and electronic fraud, their goal is to understand and help put a stop to high stakes cybercrime in the information age. Its mission is to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware. The Shadowserver Foundation supports:

- Capturing and receiving malicious software, or information related to compromised devices;
- Disassembling, sandboxing, and analyzing viruses and Trojans;
- Monitoring and reporting on malicious attackers;
- Tracking and reporting on botnet activities;
- Disseminating cyber threat information; and
- Coordinating incident responses.

The Shadowserver Foundation works alongside other security agencies to develop strategies against the threats and to form action plans to help mitigate the threats as they develop.[250]

On August 22, 2008, a U.S. open source intelligence (OSINT) initiative was launched to examine how the Russian cyber war was conducted against Georgian websites and if the Russian government was involved or if it was entirely a grass roots movement by patriotic Russian hackers. Since that time, Project Grey Goose has evolved into a formal business entity providing consulting services to governments.[251] GreyLogic represents a unified approach to collection and analysis mimicking the non-traditional, multi-faceted strategies used by non-state actors in cyber conflicts.

GreyLogic applies an open innovation intelligence model focusing on identifying and tracking non-state hackers and the companies and governments that support them. The company provides a proprietary blend of social network analysis and server-level data, hosted on a platform provided by Palantir Technologies. GreyLogic's Hacker Alias Knowledge Repository (HAKR) used in the Project Grey Goose proof-of-concept provides a mechanism for agencies to leverage their work against present and future threats.[252]

GreyLogic's blog, *IntelFusion* represents a true grass-roots effort using only open source data pulled from the Web. Leveraging large groups of volunteer users is demonstrating an ability to meaningfully supplement technical and social investigations

---

[250] Shadowserver, http://www.shadowserver.org/wiki/ (accessed August 11, 2009).
[251] Jeff Carr, Billy Rios, Derek Plansky, Greg Walton, Matt Devost, Ned Moran, Rebecca Givner-Forbes, and Shannon Siverstein. "Project Grey Goose Phase II Report: The evolving state of cyber warfare," *GreyLogic*, March 20, 2009.
[252] GreyLogic, http://greylogic.us/ (accessed August 10, 2007).

on the part of government intelligence analysts.[253] In this sense, it both leverages and contributes to transparency in cyberspace.

The Canadian-based Information Warfare Monitor (IWM) is an independent and advanced research activity tracking the emergence of cyberspace as a strategic domain with a mission to educate and inform, building and broadening the evidence base available to scholars, policymakers, and others. IWM is a public-private venture between two Canadian institutions: The SecDev Group, an operational think tank based in Ottawa, and the Citizen Lab at the Munk Centre for International Studies, University of Toronto. The SecDev Group conducts field-based investigations and data gathering. Advanced research and analysis facilities are located at the Citizen Lab, and part of the Citizen Lab's network of advanced research projects, which include the OpenNet Initiative (ONI) and ONI Asia. The Information Warfare Monitor also benefits from donations from a variety of sponsors including Psiphon Inc, and Palantir Technologies (associated with GreyLogic above). IWM conducts three primary activities:

- Case studies including field-based investigations and technical scouting and laboratory analysis such as the aforementioned "Tracking Ghostnet: Investigating a Cyber Espionage Network;"
- Open source trend analysis; and
- Analytical workshops and outreach.[254]

Summary

It is clear ICANN and other relevant intergovernmental institutions are embracing a culture of security, at least as to the extent funding is provided. It is also evident national and intergovernmental organizations are attempting to co-opt and empower

---

[253] Jeff Wozniak and Samuel Liles, "Political and Technical Roadblocks to Cyber Attack Attribution," *IO Journal*, April 2009, 27.

[254] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, 51-52.

Internet users by passing information exchange and thus ownership to the broader Internet community through hybrid organizations with the express intent of enabling the community at large to react more quickly to an attack. There is, however, wide variance in how actors view the limits of control over the Internet and approaches to addressing it.

Given the technical challenges of attribution highlighted in chapter three and the state of the community reflected here, the following emerging principles and norms summarize the emerging attack attribution regime:

- State and hybrid organizations focus on mitigation as opposed to attribution;
- States and hybrid organizations are empowered to assist in mitigation and attribution efforts, working together to mitigate the impact of attacks, and sharing attribution information where possible; and
- Cyber attacks are considered a legitimate form of declared conflict, commensurate with established principles and norms of the laws of armed conflict (international humanitarian law).

The following principles and norms appear to be worth pursuing to advance the emerging regime, pressuring states and entities to assist in mitigation and attribution efforts:

- Costs are imposed for failing to assist in mitigation and attribution efforts, imposing de facto costs on those responsible or complicit. Such costs could be economic in nature, tied to current or future access to the Internet or the conduct of certain transactions over it, or the expectation of future cooperative security efforts or agreements.
- Those states and entities not supporting mitigation and attribution efforts are considered complicit (or even responsible) for them, shifting the burden of attribution from the defender to the attacker.

The effectiveness of international efforts to address the problem of attack attribution and the issue of relative gains to circumvent clashes between major actors is the topic of the next chapter.

CHAPTER V

CYBERSPACE REGIME EFFECTIVENESS IN ADDRESSING THE ATTRIBUTION ISSUE

A 2002 assessment of cyberspace attack attribution through direct problem-solving and legal criteria reflects a collective paralysis pending improved technical attribution and formal legal agreements:

> "There are no universal technical standards or agreements for performing the monitoring and record keeping necessary to track and trace attacks. Moreover, there are no universal laws or agreements as to what constitutes a cyber-attack, and what punishments, economic sanctions, or liability should ensue. There are no universal international agreements for the monitoring, record keeping, and information sharing necessary to track and trace intruders. No existing privacy laws span the Internet as a whole. Existing international laws and agreements that might touch on these issues were not written for the Internet and need to be tested on cases involving Internet cyber-attacks."[255]

Revisiting this assessment based on cyberspace attack mitigation-based objectives provide meaningful normative and political criteria for information sharing to empower states and hybrid organizations. Such normative and political criteria may even lead to the identification of opportunities to impose costs to shift the burden of attribution from the defender to the attacker, while clearly defining acceptable attacks.

Table 1 below introduces a series of hypotheses of how regimes influence behavior across a range of criteria[256] according to both utility and social-practice perspectives. Assessments of each criterion inform an assessment of regime effectiveness according to each hypothesis.

---

[255] Howard F Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Carnegie-Mellon University, November, 2002), 17.

[256] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 3-6.

Table 1: Cyberspace attack attribution regime effectiveness

Perspective	Regime Effectiveness Criteria			
	Problem-solving (Economic)	Legal	Normative	Political
	Degree to which a regime eliminates or alleviates the problem that prompts its creation (Economic criteria add the concept of efficiency to evaluate not only outcomes, but the cost)	Meeting of contractual obligations	Advancement of principles and norms	Changes in the behavior of actors, interests of actors, or the policies and performance of institutions in ways that contribute to positive management of the targeted problem
Collective-Action	As a *utility maximizer*, how do specific rules and regime activities influence the costs and benefits that established actors factor into their utilitarian calculus? Have actors possessing well-defined utility functions altered their behavior if and when social practices made it worth their while to do so?			
Social-Practice	As an *enhancer of cooperation*, has the regime affected behavior by mitigating these collective-action problems standing as barriers to the realization of joint gains otherwise available to parties engaged in interactive decision-making?			
	As a *bestower of authority*, have social norms rooted in considerations of legitimacy or authoritativeness often guided the behavior of individuals and collective entities?			
	As a *learning facilitator*, to what extent have institutions achieved their effects by initiating processes giving rise to individual and especially social learning?			
	As a *role definer*, to what extent has the regime shaped the identities and interests of actors and, in the process, influenced the way actors behave as occupants of the roles to which they are assigned?			
	As an *agent of internal alignment*, to what extent does the regime affect behavior by creating new constituencies or shifting the balance among factions or subgroups vying for influence within individual states or other actors?			

Regimes influence behavior in a variety of ways, often through a complex of causal mechanisms rather than a single one. Regimes may alter the alternatives available to actors, structuring debate during negotiation about alternative policies to exclude those that backtrack while facilitating discussion of those advancing the regime, thereby preventing or deterring violations.[257]

Because regimes generate their effects by influencing the behavior of actors involved in the relevant issue areas,[258] the evaluation focuses on the behavioral pathways or mechanisms through which institutions produce effects. The social-practice hypotheses adopted here advance the concept of behavioral complexes as "specific

[257] Ronald Mitchell, Moira L. McConnell, Alexei Roginko, and Ann Barrett, "International Vessel-Source Oil Production," in Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 87.
[258] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 20.

constellations of actors, interests, and institutions."[259] Relevant behavioral complexes taken from the accounts of recent attacks identify the stakeholders and their interests and resources, and the principal attributes of the regime for addressing them. Recent attacks are reviewed against cyberspace regime formation to date to assess the effectiveness of the regime toward addressing the attribution problem, and causal connections between the relevant behavior and the operation of the regime.

With only a few cases to evaluate, the analysis focuses on tendency analysis as opposed to variation analysis framing hypotheses linking various factors to anticipated levels of effectiveness. The latter worthwhile evaluation is left to future research involving larger numbers of cases. Rather, the evaluation of recent attacks here seeks to identify the particular combination of forces at work in each case to show how they account for the outcomes.

This analysis identifies and evaluates the significant agendas that have been developed for bringing into being principles, norms, rules and decision-making procedures that might assure international cooperation in cyber attribution in the future. It considers negotiations to date and progress to move internationally toward these goals.

There is a major division between two broad categories of processes through which regimes affect international cooperation. For mechanisms intended to solve collective-action problems, "the role of the regime is to alter incentives in such a way as to prevent individualistic behavior likely to lead to collective-action problems in situations involving strategic interaction."[260] From a social-practice perspective,

---

[259] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999).
[260] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 269.

"regimes are arrangements that affect behavior through non-utilitarian mechanisms like inducing actors to treat prescriptions as authoritative, enmeshing actors in communities that share a common discourse, or stimulating processes of social learning."[261]

The key point between these two perspectives is not only the research agendas, but also the resulting conclusions and recommendations. Recommendations from collective-action oriented research lead to:

- Utilitarian assessments of regime member behavior regarding compliance with institutional commitments;
- Relative merits of different policy instruments; and
- Problems of avoiding or resolving differences on the application of rules to particular circumstances.

These recommendations are more closely aligned to a formal organizational discussion of regime origination.

Recommendations from social-practice oriented research lead to:

- Sources of behavioral change in general rather than specific compliance;
- Prospects for socializing actors to conform to rules without making conscious calculations concerning the benefits and costs of doing so; and
- Processes through which regimes integrate individual actors into communities engaged in practices not governed by utilitarian calculations.[262]

These recommendations are more closely aligned to cyberspace regime formation from the perspective of more informal aspects of decentralization and hybrid organizations.

Both perspectives are leveraged here to evaluate cyberspace regime influence on actor behavior. First, the regime as a utility-maximizer is assessed from a collective-action perspective. This analysis is then extended from the social-practice perspective,

---

[261] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 270.
[262] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 270-271.

evaluating the regime as an enhancer of cooperation, bestower of authority, learning facilitator, role-definer, and agent of internal realignment.

The Regime as a Utility Maximizer

How do specific rules and regime activities influence the costs and benefits that established actors factor into their utilitarian calculus? Have actors possessing well-defined utility functions altered their behavior if and when social practices made it worth their while to do so?

Recall the examples in the form of equipment standards for oil pollution and the role the Long-Range Transboundary Air Pollution (LRTAP) regime played in shaping actors behavior. The Barents Sea case demonstrated a regime overcoming collective-action problems through the operation of a routine decision-making procedure that reduced transaction costs and promoted transparency making it increasingly difficult to cheat. While utilitarian considerations were important sources of effectiveness, each regime presents a complex dynamic in which several types of mechanisms operate in tandem to produce the observable behavioral effects.[263]

Accounts of the four recent attacks in chapter three provide a seemingly consistent answer to this question in regards to cyberspace attack attribution. *While states and international organizations are changing their behaviors based on perceived costs and benefits, their lack of effectiveness continues to embolden and even entice violators.*

---

[263] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 260-261.

In each case the actual attacker likely does not have a well-defined utility function, while those ultimately directing such coordinated attacks likely do. The inability to attribute attacks to them, however, makes this venture impractical to pursue except in theory. To the extent state sponsors of the attack do have reasonably well-defined utility functions; they are able to hide behind non-state actors for plausible deniability. Other actors including victim states and hybrid organizations, to include national CERTs and other technical organizations they coordinate with, do possess reasonably well-defined utility functions based on constituencies, political agendas, formal agreements, mission statements, and in the case of industry, revenue streams.

Recent international cooperation reflected in regime maturation and responses to recent attacks provide evidence states and relevant intergovernmental organizations at large are changing behaviors based on perceived costs and benefits. The IY2KCC proved useful for governments from member countries to share information and lessons learned while building relationships fundamental to attack response activities to this day. The massive effort to address the Y2K problem forged new relationships and partnerships among industry and government sectors, particularly in the areas of critical infrastructure.

The Kyrgyzstan attack serves to show the importance of global coordination, capacity building, and that a lack of cooperation does in fact lead to worse results. Through continuing efforts to reform Internet governance, states and intergovernmental organizations are investing heavily in capacity-building measures. They also appear to be focusing controls toward specific areas where it is desired by users, such as monetary transactions and security-related issues, allowing and empowering Internet users themselves to help police the rest. Hybrid organizations do appear to be spreading

information and ownership around the Internet, allowing them to adapt more quickly to stimuli, such as an attack. However the lack of effectiveness of their behaviors continues to embolden and even entice violators.

While ever-increasing coordinated behavior by governments certainly contributed to mitigating attacks in the case of the Georgian and July 4, 2009 attacks, none were successful in attaining confident attribution in time and through a mechanism effectively enabling a meaningful response. None of them were perceived to have constituted an attack under international law to elicit an armed response.

With the exception of the Kyrgyzstan attack, the other cases all show that beyond the obvious incentives for victim states to cooperate, other states and organizations also appeared very willing to cooperate. With no surprise, however, supposed attacker states were not, and no clear incentives for them to do so were evident. While some pressure was applied on Russia at the EU summit, any corresponding pressure in the case of Georgia was trivialized by the world response to their military operations in general. No clear pressure against the DPRK, or any other potentially responsible party, in the case of the July 4, 2009 attacks was apparent.

Does a shift in emphasis from attribution to mitigation change this assessment? It is clear international response and information sharing to mitigate the effects of the attack was superior to efforts focused specifically toward attribution. The Georgian and DPRK attacks demonstrated increasing cooperation between states and ever-increasing and empowered hybrid organizations to mitigate the impact of attacks, ostensibly sharing attribution information where possible. For security concerns, however, this is difficult to state with confidence, an illustrative implication of the security dilemma in cyberspace.

It is apparent states and entities voluntarily supported these mitigation efforts. This was likely a combination of political support for victim states, as well as collective interest in Internet security per se. There was, after all, no evidence of adversaries supporting victim states, while CCDCOE efforts in the Georgian case were tied to the formal NATO security umbrella. Although academic and industry members are relatively apolitical, they remain vested in network security.

There was some evidence of pressure on the Kremlin in the case of the Estonian and Georgian attacks, as reported at the EU summit, however, no significant concrete costs were imposed, and once the broader Georgian conflict erupted, concerns over the cyber attacks faded to a distant consideration. Although the lack of response or support for victim states on the part of the supposed attackers fed international suspicions, there was no particular burden shifted to the supposed attackers to prove they were not complicit in the attack.

In other words, *there is little evidence to show the current regime is sufficiently embedded in internal state politics to appreciably enmesh state or non-state behavior.* The current regime proved unable to impose costs to coerce compliance or eliminate opportunities to violate (largely non-existing) regulatory prescriptions to positively shape future expectations and deter future attacks. This appears to have rather emboldened supposed Russian attackers from one conflict to the next, and exposed continuing weaknesses for less capable aggressors as evidenced in the July 4, 2009 attack.

States did seem to recognize or acquiesce to the emerging norm that cyber attacks are considered a legitimate form of declared conflict, commensurate with established principles and norms of international humanitarian law. This norm is reflected in all

major powers security strategies, international response to the Georgian conflict, and central to U.S. opposition to Russia's proposed international agreement.

Just as an organizational, rational utility approach alone was insufficient to understanding the cyberspace domain in the previous chapter, this assessment is incomplete without considering normative and political criteria. Analysis of the following three models are combined as they all retain the unitary actor assumption, but emphasize sources of behavior difficult or impossible to interpret in utilitarian terms. These non-utilitarian sources of behavior and how they interact in complex ways are evaluated to identify findings utilitarian analyses are poorly equipped to explain.[264] These variables also tend to work together to produce a combined effect, so we should expect similarly spurious findings in the area of international cooperation in cyberspace.

While less analytically tractable, these models still provide ample evidence of the roles non-utilitarian forces play as drivers of regime behavior. The evaluation therefore focuses towards genetic tendencies within individual case studies as opposed to predictable variance between them, as we can expect the behavioral mechanisms at work to be closely tied to certain characteristics of the particular behavioral complex, and therefore situation specific.[265]

The Regime as an Enhancer of Cooperation

Rational actors engaged in interactive decision-making often fail to achieve joint gains or avoid joint losses due to the effects of strategic behavior. Barriers to a

---

[264] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 263.
[265] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 265.

collective-action consensus identified in chapter three identify some of the possible joint gains that could be realized by the community if the security dilemma could be overcome. These include increased capacity for global Internet access, universal legal instruments for combating cyber crime, and transparency to investigate and prosecute cyber crime while protecting anonymity of lawful users in ways as to not stifle future economic growth. These could include increased international cooperation to realize efficiencies and cost savings through global economies of scale.

Recalling the security dilemma in cyberspace, however, while individual states may desire a more regulated environment and proposals for international agreements evidence collective desires, there remains no significant effort between the major powers or seemingly most egregious violators to cooperate in any meaningful way. There are no readily apparent incentives significant enough to justify exposing themselves to supposed or potential adversaries. In this situation conflict and the individualistic pursuit of security in cyberspace are not currently seen as costly, with apparently little to no risk of major war or spilling into or being linked with other areas, such as economics. Without meaningful incentives for cooperation, nations proliferating or protecting cyberspace attackers seem more satisfied with the status quo than with negotiating away any potential leverage they currently enjoy, or expect to enjoy in the future. These states seem to be enjoying the fruits of their expansion in cyberspace, and believe it provides the best prospects for their security.

Has the regime affected behavior by mitigating these collective-action problems standing as barriers to the realization of joint gains otherwise available to parties engaged in interactive decision-making? The IY2KCC created a useful mechanism for

governments from member countries to share information and lessons learned and built relationships fundamental to attack response activities to this day. The massive effort to address the Y2K problem forged new relationships and partnerships among industry and government sectors, particularly in the areas of critical infrastructure. CERT/CC provides an excellent example of the importance of trust and ability to protect confidential information to effectively coordinate responses to cyberspace attacks.

It is apparent states and entities voluntarily support mitigation efforts primarily for reasons of political support for victim states and secondarily out of collective interest in Internet security. These priorities require reversal if the collective-action problem is to be addressed to realize joint gains. As stated above, observed international response and information sharing to mitigate the effects of attacks was superior to cooperative attribution efforts, although for reasons implicit in the cyberspace security dilemma, this is difficult to state with confidence. One policy choice that could be considered would be to increase emphasis on securing the Internet as a priority over securing the state. Given the history, cooperative efforts to accomplish the former would leverage and continue to advance the global and apolitical nature of Internet governance and a worldwide information society.

Through continuing efforts to reform Internet governance, states and intergovernmental organizations do appear to be focusing controls toward specific areas where it is desired by users, such as monetary transactions and security-related issues, allowing and empowering Internet users themselves to help police the rest. Passing information exchange and ownership to the broader Internet community does present opportunity for circumventing clashes between major actors and addressing the problem

of relative gains; however, recent attacks provide insufficient evidence to state this as a finding to date. Further, there remains wide variance in how actors view the limits of control over the Internet and approaches to addressing it.

The Regime as a Bestower of Authority

The normative status or authoritativeness of regime rules and activities may trigger the behavioral response rather than some calculation of the anticipated benefits and costs of different options available to decision-makers. Have social norms rooted in considerations of legitimacy or authoritativeness often guided the behavior of individuals and collective entities?

This is clearly a major shortfall of the cyberspace attack attribution regime. Although international law and the chance of being considered and charged with war crimes deterred the United States from conducting cyber attacks against Serbian targets in the 1999 Kosovo conflict, this restraint on the part of the community appears short-lived. The EU Convention on Cybercrime remains the only international agreement to have entered into force, and in its current form provides minimal legislation specifically focused on cyberspace attacks or attack attribution within the scope of this paper.

The ITU WSIS has demonstrated the ability to influence decisions related to Internet governance. IGF dynamic coalitions continue to advance specific issue areas through relatively informal, issue-specific groups of interested stakeholders, although again none specifically address cyber attacks or attack attribution within the context of this paper. As stated above, there is little evidence to show the current regime is sufficiently embedded in internal state politics to appreciably enmesh state or non-state

behavior. *The lack of effectiveness in imposing costs to coerce compliance or positively shape future expectations to significantly deter future attacks appears to have rather emboldened attackers from one conflict to the next, and exposed continuing vulnerabilities for less capable aggressors.*

The Regime as a Learning Facilitator

Regimes can facilitate learning in the form of:

- New perspectives on the nature of a particular problem;
- New ideas about measures likely to prove effective in solving the problem;
- New insights into the process of implementing these measures; or
- New solution concepts for larger classes of problems to which the specific case belongs.

Social learning in the evolution of regimes may lead to devising new means with which to pursue unchanging objectives. It may alternatively lead to major changes in how regimes understand problems and, as a result, in ideas about how to cope with them.[266] To what extent have institutions achieved their effects by initiating processes giving rise to individual and especially social learning?

It is clear ICANN and other relevant intergovernmental institutions are embracing a culture of security, at least to the extent funding is provided. It is also evident national and intergovernmental organizations are attempting to co-opt and empower Internet users by passing information exchange and thus ownership to the broader Internet community through hybrid organizations with the express intent of enabling the community at large to react more quickly to an attack.

---

[266] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 262.

The ITU WSIS enjoys broad participation and the GCA-IMPACT partnership is one example significantly empowering member states. The proliferation of hybrid organizations discussed in the previous chapter provides further evidence of expanding public-private partnerships.

The Regime as a Role-Definer

Regimes also operate at the constitutive level with actors taking on new roles under the terms of institutional arrangements. To what extent has the regime shaped the identities and interests of actors and, in the process, influenced the way actors behave as occupants of the roles to which they are assigned?

As thousands of corporate and government-run ISPs established rules for users of their services within the boundaries of network agreements providing global access, many ISPs joined to create regional associations forming a basis for international cooperation. The IY2KCC further paved the way for organizational and institutional advancement based on cyberspace threats. Internet governance decisions, such as those over ccTLD, have established the concept of the Internet as global commons as formalized in the WSIS and associated commitments. The WSIS has also provided a venue for various interest groups such as the APC to exert influence.

In the aftermath of the 1998 Morris worm incident CERT/CC was formed, and CERT/CC and national CERTs have continued to mature. In response to the Georgian attack, CERT Georgia, organized as an academic CERT, started to function like a national CERT and coordinated attack mitigation, and the OSINT Project Grey Goose was initiated maturing into GreyLogic. In response to the Estonian attack, NATO

established its CCDCOE. The GCA-IMPACT partnership has resulted in the creation of the GRC to address the world's most serious cyberspace threats.

The decentralized nature and subsequent loss of centralized control of the Internet has spurred a decentralized approach to policing the net through hybrid organizations. The Internet has drastically lowered the barrier to entry to numerous domains, irrevocably shifting power to the people. Hybrid organizations do appear to be spreading information and ownership around the Internet, allowing them to adapt more quickly to stimuli, such as an attack.

The Regime as an Agent of Internal Realignment

Finally, by relaxing the unitary actor assumption, regimes may play some role in restructuring the alignment of domestic groups endeavoring to influence governmental behavior or factions seeking to redirect corporate behavior. The creation of a highly visible regime can have an enabling effect over time leading to the emergence of an associated community of governmental and nongovernmental actors. These actors can become a powerful pressure group dedicated to the achievement of the regime's goals. In this sense, the regime becomes a focal point for activities of state and non-state actors that act as watchdogs on key prescriptions, increasing the transparency of the behavior of regime members.

Environmental regime formation demonstrated unambiguous evidence of links among domestic politics and the operation of regimes. A diffuse public concerned with a particular issue area was able to pressure a powerful and highly organized industry to accept equipment standards; despite evidence this solution was not an efficient one in the

purely economic sense. Environmental regimes also empowered domestic critics, helping to create domestic constituencies capable of bringing pressure to bear on relevant government agencies. This was largely accomplished through interest groups or communities working in legislative settings and broader forums influencing public opinion to build political coalitions. Environmental regimes have proven able to subject the actions of bureaucratic managers to greater public scrutiny and institutionalize the role of scientists as contributors to the decision-making process established by the regime.[267] Interactions between regimes and domestic politics are likely to vary greatly from one country to another and, probably, from one type of regime to another, so reviewing this interaction from the perspective of cyberspace bears considerable merit.

To what extent does the regime affect behavior by creating new constituencies or shifting the balance among factions or subgroups vying for influence within individual states or other actors? The Internet grew out of a DARPA program and the U.S. continues to hold authority over the majority of the servers and many networks comprising the physical backbone of the Internet. Despite pressures from various domestic and international groups, the U.S. maintains a correspondingly dominant role in Internet governance decision-making, although responsibility for the Internet's technical infrastructure gradually moved to ICANN.

Y2K preparations also formalized domestic cyber incident monitoring and response procedures. Within the U.S., CERTs and international FIRST provided the national ICC reports on incidents in their respective areas. The FBI, NSC, DOD Decision Support Activity and other agencies took on similar roles reporting to the ICC.

---

[267] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 263-264.

More generally, the massive effort to address the Y2K problem forged new relationships and partnerships among industry and government sectors, particularly in the areas of critical infrastructure. In the U.S., this paved the way for moving responsibility for Internet security from the DOD to the Department of Homeland Security (DHS), with the new U.S. Cyber Command (USCYBERCOM) focused on and limited to defending DoD networks.

Decentralization powered by the Internet has shifted the underlying power structures of numerous industries and aspects of life, irrevocably shifting power to the people with a corresponding loss of government control. In areas involving monetary transactions and issues related to security, however, users continue to desire structure, safety and accountability.[268] The formation and proliferation of hybrid organizations such as GreyLogic, the Shadowserver Foundation, and others have combined features to provide premium services with security. *There remains, however, wide variance in how various domestic and international actors view the limits of control over the Internet and approaches to addressing it.*

Summary

An international cyberspace security regime has emerged through collective interests in mitigating attacks in cyberspace. Its effectiveness, however, is another matter. Attack mitigation-based objectives do seem to provide meaningful normative and political criteria for assessing and advancing cyberspace attack attribution regime effectiveness. From the social-practice perspective, the regime is creating arrangements

---

[268] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations*, (London: Penguin Books, 2006), 164-165.

that affect some behaviors such as stimulating processes of social learning. Other non-utilitarian mechanisms, however, to induce actors to treat prescriptions as authoritative, or enmesh actors in communities that share a common discourse have so far been ineffective at imposing costs to shift the burden of attribution from the defender to the attacker. While states and international organizations are changing their behaviors based on perceived costs and benefits, their lack of effectiveness continues to embolden and even entice violators.

While individual states may desire a more regulated environment and proposals for international agreements evidence collective desires, there remains no significant effort between the major powers or seemingly most egregious violators to cooperate in any meaningful way. There are no readily apparent incentives significant enough to justify exposing themselves to supposed or potential adversaries. In this situation conflict and the individualistic pursuit of security in cyberspace are not currently seen as costly.

States and hybrid organizations are focusing on mitigation as opposed to attribution. States and a growing number of hybrid organizations are increasingly empowered to assist in mitigation and attribution efforts, working together to mitigate the impact of attacks, and share attribution information where possible. In apparent support for the U.S. position, cyber attacks do appear to have gained legitimacy in declared conflict, commensurate with established principles and norms of the laws of armed conflict.

States and entities appear to voluntarily support mitigation efforts primarily for reasons of political support for victim states and secondarily out of collective interest in Internet security. These priorities require reversal through mechanisms sufficiently

embedded in internal state politics to appreciably enmesh state or non-state behavior if the collective-action problem is to be addressed to realize joint gains.

The regime currently brings little pressure to states and entities to assist in mitigation and attribution efforts. This has created the situation that when states and entities do not support mitigation and attribution efforts or are even considered complicit or even responsible for them, the burden of attribution remains on the victim, with no power to shift the burden of attribution from the defender to the attacker.

There still remains wide variance in how various domestic and international actors view the limits of control over the Internet and approaches to addressing it. The current regime has not been successful at imposing, or even identifying, costs for failing to assist in mitigation and attribution efforts, and by extension those responsible or complicit in instigating the attacks in the first place. Such costs could be economic in nature, tied to current or future access to the Internet or the conduct of certain transactions over it, or the expectation of future cooperative security efforts or agreements.

This assessment informs prospects for socializing actors to conform to rules without making conscious calculations concerning the benefits and costs of doing so, and processes through which the regime might integrate individual actors into communities engaged in practices not governed by utilitarian calculations. Advancing the domain in these areas requires a nuanced appreciation for the maturity of the emerging regime, and practical approaches successfully applied in other domains. These approaches are explored in the next chapter.

CHAPTER VI

CYBERSPACE ATTACK ATTRIBUTION REGIME MATURITY

> *"[The] process through which new institutional arrangements come into existence virtually always encompasses several distinct stages...Only by successfully navigating all three stages can a regime that has real consequences for the nature of collective outcomes come into existence."*[269]

Various stages of regime formation involve differing political dynamics. Efforts to explain regime formation require evaluating discrete influences across several stages of the overall process.[270] Evidence of cyberspace regime formation and effectiveness to date is now applied against a three-stage model of international regime formation to assess the maturity level of the current regime. Table 2 provides a roadmap to the assessment based on six hypotheses relating to the stages of regime formation: agenda formation, negotiation, and operationalization.

Table 2. Hypotheses relating to the stages of regime formation[271]

	Agenda Formation	Negotiation	Operationalization
Driving Forces	Ideas	Interests	Material conditions
Players	Intellectual leadership	Entrepreneurial leadership	Structural leadership (all stages)
Collective-Action Problems	Miscommunication	Stalemate or gridlock	Asymmetries in levels of effort
Context	Broad changes in the political environment	More specific exogenous events	Domestic constraints
Tactics	Efforts to influence the framing of the problem	Classic concern with threats and promises	Administrative or bureaucratic politics
Design Perspectives	Focus on the big picture	Focus on agreement language	Focus on domestic concerns

[269] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 2-3.
[270] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 2-3.
[271] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 21.

Informed by this assessment, the chapter then inquires: "How might maturing international cooperation mitigate the problem of cyber-space attack attribution?" The inquiry incorporates security regime formation criteria and observations from international cooperation in other domains to formulate a policy approach tailored to the maturity level of the regime.

Stages of Regime Formation

The agenda formation stage "encompasses the processes through which an issue initially finds its way onto the international political agenda and rises to a sufficiently prominent place on this agenda to justify the investment of time and political capital needed to embark on explicit negotiations."[272] It is at this point issues are often adopted by actors, or champions, that push the issue to the top of their own priorities and expend political capital in an effort to persuade others to see them as priority agenda items.[273] The dominant political dynamic that sets the agenda formation stage apart from the others is an atmosphere of openness and fluidity. "Issues are not cast in concrete at this stage; the identity of those who will play major roles in subsequent stages is not fully determined, and the timing (or even the likelihood) of a move to the front burner of the policy agenda is difficult to predict."[274]

The negotiation stage is dominated by institutional bargaining, beginning with the initiation of direct and focused negotiations and ending with the signing of an agreement.

---

[272] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 5.
[273] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 7.
[274] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 10.

While international regimes typically emerge from explicit negotiations between two or more actors, unrecorded secret side agreements, informal deals and tacit understandings are also prolific. These also become important to the success of the resultant social practices over time. Negotiations regularly involve hard bargaining among participants to best exploit whatever bargaining leverage is available to them. At this stage, participants seldom have a clear picture of the payoff structure and much of the negotiation process is exploratory in nature to expand the range of available possibilities.

Unlike bargaining in other settings, the negotiation stage of regime formation seeks to build a consensus among as many participants as possible rather than assembling a winning coalition. This provides every potential participant real bargaining power as the ability of each participant to hold out for preferred provisions greatly exceeds the ability of individual participants to get their way. Although the negotiation stage is considerably more structured than the agenda formation stage, the process of institutional bargaining at the international level is multidimensional and open-ended. Further, governments simply do not act as rational utility maximizers as they are subjected to pressures from a variety of domestic and international interest groups.[275]

The operationalization stage advances the provisions of an international regime from paper to practice. This includes domestic actions such as treaty ratification within the political systems of prospective regime members, and international actions like setting up the administrative apparatus called for in the relevant agreement.[276] This process is distinct from other stages as it involves the commitment of material resources

---

[275] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 11-15.
[276] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 16-20.

as opposed to agreement language. The operationalization stage therefore typically involves representatives from implementing agencies in addition to foreign service personnel. These additional actors often have different incentives than those handling negotiations, meaning material resources may not be as forthcoming as envisioned during negotiation.[277]

Assessment

What stage of maturity is the cyberspace attribution regime? As Table 3 below illustrates, while evidence of various stages of regime formation are evident throughout chapters two and three, the weight shows those criteria specific to attack attribution cooperation remain in the agenda formation stage. We must be careful to differentiate this from Internet governance negotiations, and cooperative attack mitigation efforts which, managing to ride on the governance negotiation stage have entered into day-to-day operations.

Driving Forces

Regarding driving forces, it is clear ICANN and other relevant intergovernmental institutions are embracing a culture of security, at least as to the extent funding is provided; however, this culture of security, and related agreements and declarations focus on cybercrime and not state-sponsored attacks. This has meant that even the rare instances of formal agreements, such as the COE Convention on Cybercrime, have not provided a venue for negotiation over state-sponsored cyberspace attacks or attack

---

[277] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 5.

attribution. As the previous chapters demonstrated, while individual states may desire a more regulated environment and proposals for international agreements evidence collective desires, there remains no significant effort between the major powers or seemingly most egregious violators to cooperate in any meaningful way.

Table 3. Cyberspace attack attribution regime formation evidence

	Agenda Formation	Negotiation	Operationalization
Driving Forces	Ideas: *-Culture of security focused on cybercrime* *-Focus on mitigation and securing critical infrastructure*	Interests	Material conditions
Players	Intellectual leadership: *-WSIS IGF Dynamic Coalitions*	Entrepreneurial leadership: *-Hybrid organizations* *-ITU GCA GRC* *-NATO CCD COE*	Structural leadership (all processes): *-State and non-state actors* *-ICANN* *-ITU* *-CERTs*
Collective-Action Problems	Miscommunication: *-Wide variance in views over the limits of control over the Internet and approaches to addressing it* *-Focus on state security as opposed to securing the Internet*	Stalemate or gridlock: *-Violators believe expansion best provides for security*	Asymmetries in levels of effort: *-Inability to impose costs*
Context	Broad changes in the political environment: *-Lowered the barrier to entry in numerous domains, broadly decentralizing numerous power structures* *-Terms still largely undefined internationally*	More specific exogenous events: *-Recent attacks*	Domestic constraints
Tactics	Efforts to influence the framing of the problem: *-Tacit bargaining to increase leverage*	Classic concern with threat and promises	Administrative or bureaucratic politics
Design Perspectives	Focus on the big picture	Focus on agreement language	Focus on domestic concerns

States and hybrid organizations are focusing on mitigation as opposed to attribution. Attribution efforts continue to focus on protecting the individual state and critical infrastructure (the target) as opposed to securing the Internet (the attack vector, or domain). Further, unlike the mitigation challenge spurred by the Y2K threat to mature, at

this point it is unlikely the attribution issue will be championed as a priority agenda item. The political dynamic regarding attack attribution remains one of openness and fluidity, the identity of actors who will play major roles in subsequent stages is not fully determined, and the timing, or even the likelihood, of a move to the front burner of the policy agenda is difficult to predict.

Players

Recent attacks portray the primary actors in the current attribution regime. These included state security agencies and state and distributed non-state actors that provided the plausible deniability at the root of the attribution problem. Cyberspace regime formation also identified the numerous players involved in Internet governance and attack mitigation efforts. Governance and mitigation efforts have demonstrated entrepreneurial leadership in assembling innovative and hybrid organizations such as the ITU GCA GRC, NATO CCDCOE, and GreyLogic. Formal attribution efforts, however, largely remain firmly within closely held state security organizations. So far, other analysts from academia and industry that may participate in attribution efforts from an academic perspective lack the capacity of state intelligence and security agencies to move to a more entrepreneurial stage.

Collective-Action Problems

Attribution efforts continue to focus on protecting the individual state and critical infrastructure as opposed to securing the Internet. This exacerbates the collective

security problem rooted in the wide variance of how various domestic and international actors view the limits of control over the Internet and approaches to addressing it.

Attribution efforts are a largely relative gains approach. There is no benefit for the attacker to be identified. Joint gains can only be realized when identifying attackers is in all states best interests, such as non-state-sponsored cyber attacks, crime or terrorism. This implies a largely unwelcome level of persistent surveillance and state control or oversight over Internet activities, as the next chapter will detail in the case of China. Focusing on mitigation efforts leverages more mature efforts and organizations while circumventing the relative gains issue. It provides opportunities for broad participation in activities without disclosing state secrets that may be involved in attribution efforts.

Without meaningful incentives for cooperation or ability to impose costs, nations proliferating or protecting cyberspace attackers seem more satisfied with the status quo than with negotiating away any potential leverage they currently enjoy, or expect to enjoy in the future. As long as states believe their expansion in cyberspace provides the best prospects for their security, there remains insufficient interest to move to the next stage of domain formation. To posit miscommunication over attribution describes the current regime would be to imply there is any communication at all. Focusing on mitigation efforts through hybrid organizations may be the most promising approach to negotiating this obstacle to regime formation.

Context

The Internet has drastically lowered the barrier to entry to numerous domains, irrevocably shifting power to the people. The world has had to come to terms with the impact of decentralization powered by the Internet shifting underlying power structures within numerous industries. This is clearly a broad change in the political environment indicative of the agenda formation stage.

Recent attacks have provided more specific exogenous events forcing actors to address the problem within a more defined context. This has led to some specific actions such as pressure on Russia at the EU summit following the Estonian attacks. The only draft agreement addressing the scope of this paper, however, is the stillborn Russian proposal which focuses on information weapons rather than securing the domain. The further inability to so much as agree upon definitions of cyberspace, and attacks and attribution therein continues to retard cooperative action on the issue.

The lack of domestic constraints that would be indicative of a more mature regime provides a partial answer to the noted lack of ability to enmesh actors identified in chapter four. Without specific issues championed to an elevated place on the agenda, or specific agreements to negotiate and base cost-benefit analysis on, there is little substance or power to enmesh any actor. The next three hypotheses of regime maturation reinforce this point.

Tactics

Current attribution tactics portrayed in recent attacks include passive post-attack digital forensics, and attack trace back operations. Recent attacks also introduced the

limitations of current legal instruments and the resulting reliance upon cooperative efforts. Given the scope of the current collective-action problem evidenced in cyberspace, tacit bargaining best describes attribution negotiation tactics to date. These include attacks showcasing certain capabilities while leaving significant doubt as to others. This is again consistent with the agenda formation stage of regime formation. The lack of regime maturity to enmesh actors is again evidenced by the absence of bureaucratic politics.

Design Perspectives

With no plausible draft agreement in sight, the attack attribution regime is clearly at a big picture stage of design perspective. This lack of definition of the regime also leads to the lack of domestic concerns with the power to enmesh actors over this issue area.

MATURING THE REGIME

The purpose in languishing over the lack of maturity of the attack attribution regime serves more than academic interest. Understanding the regime with respect to various hypotheses of regime formation leads to specific recommendations tailored to the maturity level of the regime. For where there is lack of progress, lies opportunity. Given the regime is still immature and in the agenda formation stage, how might the regime be matured?

Factors in Regime Origination

What factors determine whether issues rise to the point parties are willing to commit resources?[278] There is no accepted single causal mechanism for international regime formation. Lessons learned from other domains identify numerous origins. While early work favored hegemonic theories, subsequent knowledge-based theories emphasizing the role of technological epistemic communities are most cited for explaining the origin of the Internet:

> "[the] development of broad rules of governance for the Internet fits the definition of an international regime in many ways, but the Internet has no central governing authority and the principles, norms, rules and decisionmaking procedures around which actor expectations are converging to manage it are evolving from the interaction of, among others, a wide variety of private business firms, governments, universities, and scientific, professional, and epistemic communities spread across the globe."[279]

Recall, however, the collective-action problem experienced in recent attacks based on Krasner's criteria for security regime formation and maintenance.[280] While individual states may desire a more regulated environment and proposals for international agreements evidence collective desires, there remains no significant effort between the major powers or seemingly most egregious violators to cooperate in any meaningful way. There are no readily apparent incentives significant enough to justify exposing themselves to supposed or potential adversaries.

In this situation conflict and the individualistic pursuit of security in cyberspace are not currently seen as costly. There is apparently little risk of being linked with other areas,

---

[278] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance*, (Ithaca, NY: Cornell UP, 1998), 184.
[279] Marcus Franda, *Governing the Internet: the emergence of an international regime,* (Lynne Rienner Publishers, Inc., 2001), 5.
[280] Stephen D. Krasner, *International Regimes* (Ithaca, NY: Cornell UP, 1991), 176-178.

such as economics. Without meaningful incentives for cooperation, nations proliferating or protecting cyberspace attackers seem more satisfied with the status quo than with negotiating away any potential leverage they currently enjoy, or expect to enjoy in the future. These states seem to be enjoying the fruits of their expansion in cyberspace, and believe it provides the best prospects for their security.

This stark assessment makes prospects for a formal agreement to advance to the negotiation stage of regime formation highly unlikely. *Prospects for advancing the regime therefore reside in social-practice perspectives to advance cooperative efforts focused on attack mitigation.* Historical lessons from other domains highlight specific considerations for advancing cyberspace attack mitigation and attribution cooperation during the agenda formation stage. States and organizations across the globe have come to recognize the stake they hold in Internet security, and as a new technology the world has discovered a new venue for competition and cooperation. With the recognition of cyberspace as global commons, states understand it cannot be contained within strictly national confines, and that it must be viewed internationally to use cyberspace as a principal element in global economic development.

Unlike other domains, however, the world has yet to experience or accept the ramifications of a cataclysmic cyber attack to elevate the issue to that of high politics. The community lacks such a catalyst to form the basis for international arms control and monitoring agreements, or initiate formal communications and cooperation to mitigate risks including timely and accurate attribution.

Numerous temporary measures have emerged, of which some such as CERTs and hybrid organization development and coordination have survived, and others such as the

formal IY2KCC have not. Further advancement of the regime in this way will require such temporary measures to gain the support of member nations who value their benefits or desire protection from other participating parties. Given the wide variance of views over the limits of control of the Internet, exceptions where agreed by the members should be considered without retaliation or sanction.

Attribution in other domains is achieved through a combination of detection technology and cooperative measures including observable agreements and dedicated communications mechanisms. Significant technical investment should be expected to address the attribution problem at the technological level as has been invested in maritime, sea, space and nuclear domains. IFF and airspace management tools, maritime and space surveillance capabilities, and nuclear detection capabilities are all critical in establishing attribution in other domains. Just as technological solutions were required in these domains, they were also, however, insufficient. MDA CONOPS, space and airspace management procedures and associated international cooperative agreements are as important as the technologies themselves.

The attribution problem is specifically mitigated through observable agreements and dedicated communications mechanisms between adversaries. Given the goal of preserving non-attribution in the case of benign use, the concept of a claims approach similar to that adopted in the telecommunications, space and trade domains may be more applicable to cyberspace than that of persistent surveillance.

One result of attribution efforts in the space domain has been to expand and even shift concerns from the threat of direct attack to that of collateral effects. Changing the focus from directly detecting and attributing attacks in cyberspace, to that of identifying

the impact of collateral effects for a claims-type process may be one avenue to facilitate international dialogue in existing venues. This could prove to be a significant variable in extending the shadow of the future for potential rational attackers.

The significant grey area between peace and war provides a notable quandary for operations in cyberspace, and difficulty in attributing belligerent and combatant status. Rules differ when in a stated conflict than during normal peacetime. Even under recognized conflict, deception is permitted to include the use of feigned attacks, false intelligence information, electronic deceptions, and use of enemy codes, passwords, and countersigns.

In other domains, behavior alone indicates intent sufficient for attribution of combatant or belligerent status. Few weapons are restricted, rather the use of certain weapons exhibiting the potential for indiscriminate effects are regulated where agreed. Malicious activity in cyberspace is the product of using otherwise benign technology. Few technologies are inherently malicious. Just as a maritime vessel may become a target subject to attack if it refuses to so much as provide immediate identification upon demand, a vessels actions may provide sufficient justification for attack.

Activities with the potential for indiscriminate effects should not be treated as normal operations, and the risk of collateral effects should be minimized. This is one area worth exploring for specific discourse and possible agreement. Steps might be taken to reduce the risks of cyber war in the near term and reduce reliance on cyber attacks over time. Constraining attacks in cyberspace should focus on malicious activities and effects, rather than weapons per se.

Lessons from other domains reinforce the point that management structures are most successful when organizational tasks and authorities are well aligned with capability and perspective. The sea domain has created a need for MDA and multinational naval task forces[281] not unlike the current situation experienced in cyberspace. The MDA concept leverages sensors, analytical fusion, international cooperation through regional hubs, not unlike International Civil Aviation Organization (ICAO) regional offices in the air domain, or ccTLD managers and hybrid organizations in cyberspace. Activities are allowed to vary from region to region taking into account the general economic, technical or social environment of the region concerned.[282]

Decentralizing management of certain issues may be another approach to addressing the wide variance of views over the limits of control of the Internet. Potential solutions to issues of significant variance might include granting exceptions to technical standards, operating procedures or Internet governance where agreed by the members without retaliation or sanction.

Confidence-building measures are necessary. Several principles and norms, and reasons for abiding by them presume future actions. The assumption that violations, real or perceived, lead to the loss of domestic and international support is true only if violations have a significant chance of being detected and attributed back to, and result in unfavorable consequences for the offender. Victim or community actions actually need to demonstrate a capability and willingness to respond to attacks to establish a reasonable expectation of

---

[281] "Multinational Task Force Targets Pirates," *American Forces Press Service*, January 8, 2009. http://www.defenselink.mil/news/newsarticle.aspx?id=52586 (accessed July 1, 2009). Manama, Bahrain.
[282] International Civil Aviation Organization, http://www.icao.int/cgi/goto_m.pl?icao/en/hist/history02.htm (accessed July 2, 2009).

reciprocity. If hostility in the cyberspace area is not expected to spill into other areas, such as economics, an important incentive for cooperation will be absent.[283]

In the absence of attacks, positive reciprocity can be exhibited through peaceful, confidence-building measures. The assumption under the international law of armed conflict of an eventual return to peace is particularly applicable to cyberspace, as attacks may occur during times of no stated conflict engaging the formal international law of armed conflict. Improved coordination and technical detection capability to attribute attacks, and such responses either through retribution or peaceful confidence-building measures may be the most promising avenue for extending the shadow of the future and aligning mutual interests among an optimal number of actors.[284]

Addressing Decentralization

Advancing the regime through agenda formation should leverage the proliferation and empowerment of hybrid organizations. Decentralized organizations are not invincible, however, defeating them require new strategies. Decentralization through hybrid organizations includes empowering regular Internet users and especially trusted circles to assist in mitigation, attribution and response. By placing Internet users in a position of trust and power, hackers will be ostracized as opposed to glorified. Empowering users further leverages hybrid organizations as catalysts to plant the principle and champions to proliferate the norm. Hybrid organizations should consider recruiting hackers into new and independent virtual watchdog organizations. Maturing

---

[283] Stephen D. Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1991), 176-178.
[284] Robert Axelrod and Robert O. Keohane, "Achieving Cooperation Under Anarchy: Strategies and Institutions," in Kenneth Oye, *Cooperation Under Anarchy* (Princeton UP, 1985), 226-254.

hybrid organizations to advance cyberspace security principles and norms is a long-term strategy. Changing people's ideology will take time.[285]

Hybrid organizations provide the opportunity to create small circles, recruiting and utilizing people well-trained in conducting network operations, defense, and attack to combat would-be attackers. Circles should be empowered through resources commensurate with the level of trust in and within the circle, and then allowed a level of autonomy consistent with the role of a catalyst. Circle members do not need to know how many other circles there are, or their membership. Feedback mechanisms develop trust and confidence in circles and their members over time.

Decentralization shifts the burden of policing from the organization to its users, is already prevalent on the Internet, and may be leveraged by centralized governments to various extents. Organizations that want to preserve the freedom and utility of the Internet from a position of anonymity, and agencies that want to police cyberspace from a position of transparency can both create such movements. Because they share the similar ideology of preserving the Internet, the two mechanisms are not mutually exclusive. In fact, while decentralization encourages creativity, it also increases variance, increasing odds of the community having the necessary tool or access to attribute and respond to future attacks.

Decentralizing the user experience may also provide the opportunity for the global Internet community to swarm around an attack, helping to defend, mitigate, attribute and ultimately even respond. It brings the collective knowledge of world to bear. Providing information to power holders rapidly arms them with information to

---

[285] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 144-151.

respond or to demand answers from those facilitating or acquiescing to the attack.[286] Consider for example Emergency Services integrators' (ESi) software WebEOC, a crisis information management system that enables a decentralized community of first responders and managers. Open communication on the scene provides information from the edge of the network.[287]

Decentralization should mitigate the relative gains problem by substantially increasing capacity and transparency while reasonably preserving anonymity, and decreasing cost while leveraging existing technical and legal expertise. Formal and informal communication mechanisms within and between circles provides an important confidence-building measure, and facilitates others. Through increased transparency, states are kept more honest, moving state-sponsored cyber warfare out of the grey area between peace and war. Because so much cyberspace development and attack analysis and mitigation happens in the open, previously perceived relative gains are recognized as joint gains by Internet users in a non-threatening way. Attacks and attackers are ostracized as Internet users are empowered to police the net on their own.

As achieved in other domains, such a strategy provides numerous incentives while ceding little, if any sovereignty. Cyberspace attack capabilities can still be developed. Cyberspace attacks may even be employed when in a stated conflict. Although attacks come increasingly at risk of attribution, clearly detrimental to criminal attacks, attacks during a stated conflict are simply restrained within other generally recognized laws of war.

---

[286] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 155-158.
[287] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 210.

While decentralization is a core element of hybrid organizations, centralization is good in many areas to include security and finances. Search for a centralized-decentralized sweet spot should be a continuing priority to remain competitive.[288]

In order to centralize hacker organizations, incentives should be considered to shift hackers' power from symbolic to material. Hacker organizations gaining material resources provide leaders power to reward and punish by giving or withholding resources. The power to reward and punish shifts once flat power structures into hierarchical, centralized organizations, able to be identified, targeted, and ultimately controlled.

Centralizing hacker organizations is also a difficult task. Offering lucrative property rights to hacker tools might be one method in confronting the problem. "The moment you introduce property rights into the equation, everything changes...with power over property rights, the catalyst turns into a CEO and circles become competitive."[289] In cases where organizations are so decentralized there is no one to grant property rights to, other financial incentives should be considered for hackers to keep things legal.

Variables in Regime Formation

Ideas, power, cooperative efforts, and non-state actors[290] all play a role in shaping expectations and advancing institutional learning to enmesh and coerce actors.

---

[288] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 188-189.
[289] Ori Brafman and Rod Beckstrom, *The starfish and the spider: the unstoppable power of leaderless organizations* (London: Penguin Books, 2006), 151-154.
[290] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance* (Ithaca, NY: Cornell UP, 1998), 184-193.

Table 4 below illustrates how stepwise processes might be applied to enmesh actors and coerce compliance in this case.

Table 4. Recommendations for regime maturation

	Shaping Expectations	Institutional Learning	Enmeshing Actors	Coercing Compliance
Ideas	-Focus on descriptive practice -Address de-centralization	-Understand clear delineation between sovereign and common elements or aspects of the domain is not a prerequisite to cooperation -Shift emphasis on attribution to justify action to effects to support claims	-Allow activities across regions or domains to vary taking into account the general economic, technical or social environment of the region concerned	-Extend the shadow of the future through dispute settlement mechanism(s) -Focus on effects as opposed to technologies
Power	-Use future Internet versions to inform future investments and adopt specific measures to shape decision-making under uncertainty	-Use negotiating rounds to recognize joint gains and advance the regime piecemeal	-Create transparency to elicit compliance in cases where actors have incentives to violate rules -Incorporate property rights and financial incentives to centralize hacker organizations	-Include remedies to force compliance -Secure international funding to spur development and provide a tool to enmesh actors through bureaucratic bargaining and impose costs through the withholding of funds to detractors and non-participants
Cooperative Efforts	-Leverage sensors, analytical fusion, international cooperation through regional or domain hubs, such as ccTLD managers and hybrid organizations -Promote confidence-building measures focusing on relatively uncontroversial programmatic activities rather than preliminarily laying down regulatory prescriptions	-Leverage venues such as WSIS dynamic coalitions -Place Internet users in position of power and trust to change ideology	-Advance temporary organizations operating under loose authorities -Align organizational tasks and authorities with capabilities and perspectives	-Focus on behavior in addition to technical attribution -Incorporate improved technical standards such as new versions of the Internet, and ISP requirements to operate over it to inform investment decisions and shape decision-making
Non-State Actors	-Proliferate and empower hybrid organizations			

Coercing Compliance

Environmental regimes were successful at establishing standards users were required to meet to conduct business profitably or at all. This was accomplished less by increasing incentives to comply with the rules than through eliminating opportunities to violate regulative prescriptions. The use of standards was effective because they coerced a variety of non-state actors to play by the rules of the regime, avoiding manipulative tactics often accompanying national regulatory efforts.[291]

In cyberspace this approach would incorporate improved technical standards such as new versions of the Internet, and ISP requirements to operate over it. Given current Internet governance arrangements, ICANN may be in the best position to advance this approach. The combination of particular technical standards and operating requirements might be taken up by a WSIS IGF dynamic coalition to achieve greater international consensus and capital.

Similarly, the trade domain relies upon negotiations and consultation to resolve trade conflicts. Significant time is allowed to make a claim, even longer for specific findings through arguments, and both well in advance of known total damage. While such a feature does little to mitigate an attack in progress, *the prospect of lengthy litigation and significant penalties in the face of world opinion may serve to significantly lengthen the shadow of the future, impacting the cost-benefit analysis of prospective rational aggressors*. Either approach provides a mechanism to impose costs through operating authorities or dispute settlement.

---

[291] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 265-266.

Coercing compliance with international agreements in the traditional security domains includes remedies to force adherence, including reprisals and war crimes tribunals. Defensive actions designed to prevent or mitigate an attack are justified as long as the general principles of necessity and proportionality are met.

Distinctions between neutrals and belligerents, and combatants and non-combatants, and the methods for so designating continue to be instrumental in achieving attribution, although the methods in cyberspace may be unique. Protected signs, symbols and electronic signals used to identify personnel, objects and activities entitled to protected status. The use of exclusion zones promulgated via NOTAMS may be useful metaphors for methods to distinguish and attribute combatant status and activity in cyberspace. Just as CERTs and other Internet security organizations send out alerts, specific mitigation procedures based on current practice and authorized in the event of a cyber attack might provide enhanced ability to mitigate and attribute the attack, while preserving normal Internet operations over the rest of cyberspace.

Enmeshing States

Regimes tend to launch relatively uncontroversial or seemingly unimportant programmatic activities rather than preliminarily laying down regulatory prescriptions. Over time the regime becomes increasingly influential as its core issues gain political prominence and the participants find themselves in a web of institutionalized activities from which they cannot easily extricate themselves. In this way, the regime draws governments into normatively grounded social practices they cannot ignore in political

terms, albeit more so for some states than others.[292] Again, WSIS dynamic coalitions provide one such venue for this approach.

Temporary organizations operating under loose authorities serve to advance regimes in the absence of formal agreements. As one example from the air domain, in view of the inevitable delays in ICAO Convention ratification, the Chicago Conference signed an Interim Agreement creating a technical and advisory PICAO to collaborate in the field of international civil aviation. This is similar to the current status of ICANN or WSIS IGF in Internet governance.

Shaping Expectations

Another tendency of regimes is to influence behavior by shaping expectations of various parties about rules and procedures likely to be adopted in the future, even when they do not mandate specific actions at the time of their creation. Regimes influencing behavior through shaping expectations is particularly true where key actors are required to make large investment decisions with extended amortization schedules. Shaping expectations highlights the role of assessments of current and future trends in the development of international regimes to inform decision making under uncertainty by those responsible for investment decisions.[293]

Shaping expectations is an especially insightful consideration for the current stage of agenda formation as new versions of the Internet are being considered. A specific engagement plan and metrics based on actors consideration or adoption of

---

[292] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 266-267.
[293] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 267.

specific measures might be a useful mechanism to inform decision-making under uncertainty and track regime maturation progress.

Institutional Learning

Cooperative efforts might leverage existing venues such as WSIS dynamic coalitions to place Internet users in a position of power and trust, and to advance certain ideas fundamental to addressing the relative gains dilemma over cyberspace attacks. Regimes tend to initiate stepwise processes leading to desired results over time.[294] For example, clear delineation between sovereign and common elements or aspects of cyberspace is not a prerequisite to cooperation. The use of negotiating rounds advances the regime piecemeal to recognize joint gains. One of the goals of such a stepwise process would be to shift the dialogue from one of attribution in order to justify military action, to identifying effects of cyberspace attacks to support a civil claims process.

Significant Intervening Variables

Any number of intervening variables may enter the equation in specific cases. The influence of intervening variables requires viewing regime effectiveness through the linkages or interactions among the institutional properties of regimes and sources of behavior, as well as various features of the specific behavioral complex.[295]

---

[294] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 268.
[295] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 271-272.

Key variables that seem to apply to the current situation in cyberspace, include:

- The extent to which victims were able to acquire jurisdiction over those responsible for the problem;
- The willingness of national governments to translate regime rules, procedures, and programmatic commitments into practices successful in directing the behavior of the right set of subjects; and
- The presence and importance of a variety of non-state actors other than those whose behavior was the source of the problem itself.

Perhaps the most poignant intervening variable in cyberspace is its level of decentralization addressed in the hybrid organization strategies above.

Mitigating Cyberspace Attack Attribution through Agenda Formation

A concerted effort leveraging hybrid organizations during agenda formation can significantly shape the character of the discourse employed in subsequent stages.[296] In designing effective institutions, environmental regimes were more effective when they were able to:[297]

- Embed themselves in the internal political dynamics of member states, as their effectiveness varied considerably among issue areas, cases, and even time;
- Contribute to an improved understanding of the problem to be solved and to evolve the handle new tasks was similarly instrumental to regime effectiveness;
- Create transparency to elicit compliance in cases where actors have incentives to violate rules;
- Redirect the interplay of political forces within the domestic policymaking arenas of key members, especially key members critical to the success of the overall arrangement and arrangements involving large numbers of members;
- Maximize their force in a number of different domestic political settings; and
- Focus on the behavior of actors giving rise to problems, commensurate with the extent to which behavioral change serves to alleviate the problems.

---

[296] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance* (Ithaca, NY: Cornell UP, 1998), 196.

[297] Oran Young, *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* (MIT, 1999), 274-278.

Maturing international cooperation to mitigate the problem of cyber-space attack attribution may best be approached along the following policy approach based on Table 4 recommendations:

- Cooperative technical development through joint investment allowing for variance in views over control of the Internet across technical, economic, social and political regions;
- International funding tied to improved technical and legal standards to spur development and provide a tool to enmesh actors through bureaucratic bargaining and impose costs through the withholding of funds to detractors and non-participants;
- Empowerment of hybrid organizations cooperating in practical areas of global Internet security in order to:
    - Advance cooperative Internet sensing and analysis through regional or domain hubs incorporating behavioral analysis, activities and effects;
    - Place Internet users in a position of power and trust, capitalizing on temporary organizations; and
- International consultations, such as the current IGF dynamic coalitions, in the form of negotiating rounds to:
    - Initially focus on descriptive practice as opposed to normative efforts such as addressing the wide variance in views over control of the Internet, and delineate between sovereign and common elements, or agree to the limits of such delineation;
    - Promote regulatory prescriptions in a stepwise approach as identified through cooperative efforts, such as property rights and penalties for software and malware, and Internet crime legislation and recourse; and
    - Develop a dispute settlement mechanism focusing on effects, again allowing for variance across technical, economic, social and political regions.

Such an approach recognizes that formal agreements and procedures generally require years, even decades to form and the necessary catalyst to initiate them may not be present in the cyberspace domain to date. The broad and amorphous nature of cyberspace leaves significant room for paradigmatic arguments, complicating the development of international dialogue and cooperation. *Keeping in mind negotiations gain the best traction when initiated by a few principle actors, draft documents or*

provisional organizations will be beneficial to begin negotiations and eventual implementation.

Normative instruments should provide clear benefit at minimal cost. Agreements and cooperative procedures require significant and observable benefits at modest cost to national sovereignty and self-action for adoption.

Finally, it is necessary to clearly distinguish between conflicts of interests and misunderstandings arising out of differences in the political structure and policy culture of participants during the agenda formation stage. This requires an analysis of the links between interests and policy preferences, and the relative contributions of problem structures and processes.[298] These are matters of comparative politics left for limited analysis in the next chapter in the case of China.

[298] Oran R. Young, *Creating Regimes: Arctic Accords and International Governance* (Ithaca, NY: Cornell UP, 1998), 186-196.

CHAPTER VII

THOUGHT EXPERIMENT ON THE APPLICATION OF RECOMMENDATIONS IN THE CASE OF CHINA

Cyberspace attacks in the form of espionage have become a matter of daily front page news. Operation Aurora, the December 2009 to January 2010 cyber attack on Google subsequently attributed to servers in China is an excellent case in point.[299]

A March 2009 Information Warfare Monitor report promulgated findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions. The investigation, consisting of fieldwork, technical scouting, and laboratory analysis, discovered much more, including a network of over 1,295 infected hosts in 103 countries. Targets included computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs.

> "Significantly, close to 30% of the infected computers can be considered high-value and include the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters...Documentation and reverse engineering of the *modus operandi* of the *GhostNet* system—including vectors, targeting, delivery mechanisms, data retrieval and control systems—reveals a covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems."[300]

From the evidence at hand, however, it was not clear whether the attacker(s) really knew what they had penetrated, or if the information was ever exploited for

---

[299] Kim Zetter, "Google hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora (accessed February 20, 2010).
[300] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, 5-6.

commercial or intelligence value. While some may conclude the evidence points definitively to China as the culprit, attributing all Chinese malware to deliberate or targeted intelligence gathering operations by the Chinese state would be wrong and misleading. The numbers can tell a different story. China is presently the world's largest Internet population. The sheer number of young digital natives online can more than account for the increase in Chinese malware. With more creative people using computers, it is expected that China, and Chinese individuals, will account for a larger proportion of cybercrime.

China is particularly susceptible to being used as a platform for third country attacks as its networks are especially vulnerable for a variety of reasons. Chinese networks often employ legacy equipment, poor security practices, and perhaps most important, the widespread use of pirated software. "[Up] to 90% of the software (such as operating systems) used in China is pirated."[301]

The threshold for engaging in cyber espionage is falling. Cybercrime kits are now available online, and their use is clearly on the rise, in some cases by organized crime and other private actors. Socially engineered malware is the most common and potent; it introduces Trojans onto a system, and then exploits social contacts and files to further propagate infections.

Certainly Chinese cyber espionage is a major global concern. Chinese authorities have made it clear they consider cyberspace a strategic domain, which helps redress the military imbalance between China and the rest of the world, particularly the U.S. They

---

[301] James A. Lewis, "Computer Espionage, Titan Rain and China," *Center for Strategic and International Studies, Technology and Public Policy Program*, December, 2005, 1.

have correctly identified cyberspace as the strategic fulcrum upon which U.S. military and economic dominance depends.[302]

In 2007 it was reported: "Chinese hackers, some believed to be from the People's Liberation Army, have been attacking the computer networks of British government departments."[303] An April 2009 article identified no less than eight significant cyber espionage U.S. government breaches, including the Analyzer attacks mentioned in chapter two, e-mail invasions of the Obama and McCain campaign systems and White House e-mail archives in 2008, as well as the following:[304]

- A 1999 case dubbed "Moonlight Maze" involved Russian hackers accessing Department of Defense computers for an entire year before being detected. The cyber thieves stole mountains of sensitive data, including information from nuclear weapon labs, NASA, and various defense contractors' networks.
- In 2004, a group of Chinese hackers called "Titan Rain" started making their way into U.S. military systems. It is believed the cybercrooks gained access to all sorts of sensitive information, including military vehicle plans and the Army and Air Force's flight-planning software. Investigators think their techniques were used at the U.S. Army Information Systems Engineering Command at Fort Huachuca, AZ; the Defense Information Systems Agency in Arlington, VA; the Naval Ocean Systems Center in San Diego; and the U.S. Army Space and Strategic Defense installation in Huntsville, AL.
- The first week of April 2009, someone breached the U.S. electrical grid and left behind malware meant to shut down power service. The cyberspies, thought to have been from China and Russia, installed software tools that could potentially disable parts of the grid system.
- Also in April 2009 it was discovered cyberspies hacked into government computers and stole sensitive information on a next-generation stealth fighter, lifting terabytes of data on the Pentagon's $300 billion Joint Strike Fighter project, including details about the aircraft's design that could expose vulnerabilities. The hack is believed to have happened through a hole in a contractors' network including Lockheed Martin, Northrop Grumman, and BAE Systems.

---

[302] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, 5.

[303] Richard Norton-Taylor, "Titan Rain – how Chinese hackers targeted Whitehall," *The Guardian*, September 5, 2007. http://www.guardian.co.uk/technology/2007/sep/04/news.internet (accessed December 14, 2009).

[304] Jr Raphael, "Fighter Jet Hack Far From First Government Breach," *PC World*, April 21, 2009. http://www.networkworld.com/news/2009/ 042109-fighter-jet-hack-far-from.html?ry=gs (accessed December 13, 2009).

The recommendations identified in the previous chapter are now applied in a notional thought experiment against China's information war theory and strategy development over the years 1995-2003, and their resulting rampant intrusions into United States networks.[305] As such, the assessment complements the earlier case studies through counterfactual reconstruction of the flow of events in the relative presence or absence of cyberspace regime cooperation. The evaluation reviews the decision-making process of key actors at critical junctures including Chinese assessments of U.S. operations in Kosovo in 2000 and Iraq in 2003.

The previous chapter also identified the need to clearly distinguish between conflicts of interests and misunderstandings arising out of differences in the political structure and policy culture of participants during the agenda formation stage. Understanding the influence of Chinese political structures and policy cultures requires an exhaustive review of source literature beyond the scope of this current study to compare to the primarily U.S. perspective of regime formation and maturation presented in chapter four. Fortunately, such an effort has been undertaken by the Fort Leavenworth U.S. Army Foreign Military Studies Office (FMSO). FMSO researches, writes, and publishes from unclassified sources about the military establishments, doctrines, and practices of selected foreign armed forces, and studies a variety of civil-military and transnational security issues affecting the U.S. and its military forces. Timothy Thomas completed such an exhaustive compilation, translation with the assistance of the Foreign Broadcast Information Service (FBIS), and analysis over the years 1995-2003 in his 2004 book, *Dragon Bytes, Chinese Information-War Theory and Practice*. The following

---

[305] "US warned of China 'cyber-spying,'" *British Broadcasting Corporation*, November 20, 2008. http://news.bbc.co.uk/2/hi/asia-pacific/7740483.stm, (accessed March 27, 2009).

thought experiment applies the recommendations against major tenants of Thomas' research in the area of Chinese computer confrontation operations, augmented with supporting references where appropriate.

Chinese Information Warfare Theory and Practice 1995-2000

Although Chinese analysts had written about information warfare (IW) theory since about 1985, the Chinese military had done little to advance or apply the concept. They were somewhat surprised when IW articles began to appear in the U.S. in the early 1990s, and when concepts and tactics were later inserted into field exercises.

The 1991 Gulf War presented Chinese leadership with the stark realization of the power and precision of an information-based force, and that without advancements, the People's Liberation Army (PLA) would risk becoming an anachronism of the mechanized-warfare age.[306] In the words of Major General Wang Pufeng, former Director of the Academy of Military Science Strategy Department in Beijing: "In the near future, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness."[307] Early Chinese thoughts mirrored U.S. developments; however, a distinctly Chinese approach was being debated behind the scenes, crystallizing around the 1997-1998 timeframe.

By conceptualizing underlying cultural, cognitive, and ideological characteristics, the Chinese began to instantiate IW theory and practice to allow a quality IW force to

---

[306] Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" *Strategic Studies Institute* (Carlisle Barracks: U.S. Army War College, November, 2001), 8.
[307] Wang Pufeng, "The Challenge of Information Warfare," *China Military Science*, 1995. http://fas.org/irp/world/china/docs/iw_mg_wang.htm (accessed December 14, 2009).

empower China, as well as other less capable nations, to theoretically threaten more powerful nations through electronic attacks against a nation's financial institutions. Such a capability could further hold the worldwide economy at risk through dependence on the Internet for financial transactions.[308]

As of 1996, Chinese thoughts on IW focused on controlling the flow of information and intelligence, protecting one's own systems while attacking the enemy's. Through 1997-1998 Chinese definitions and approaches still closely paralleled U.S. and international development. One translation emphasized IW as rendering the operational space unclear and indistinct to the enemy while making it transparent to one's own forces. Chinese emphasis remained on hindering adversary decision-making as opposed to attacking enemy information or information systems. "To achieve victory in information warfare, the central issue is control of information."[309]

A serious debate over IW reemerged in 1999 reflecting IW as a "pitched battle against one another in the political, economic, cultural, scientific, social, and technological fields...forcing enemy troops to surrender without a fight,"[310] still implying IW as more of a cognitive than systems-related process. Another author emphasized the struggle to seize and maintain control over information, "capitalizing on and sabotaging the enemy's information resources, information system, and informationized-weapon systems...as well as utilizing and protecting one's own."[311]

---

[308] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 5-6.
[309] Wang Pufeng, "The Challenge of Information Warfare," *China Military Science*, 1995. http://fas.org/irp/world/china/docs/iw_mg_wang.htm (accessed December 14, 2009).
[310] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 12-13.
[311] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 12-13.

Another Chinese general further distinguished between fighting an IW-enabled complete war while defining "informationized" warfare as an entirely new form of warfare; one that would not be realized until twenty-first century informationized forces were available, but that would constitute the soul of Sun Tsu's "subduing the enemy without battle." Three areas of IW included command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), electronic warfare, and finally computer attack and defense methods. The concept of information-network warfare (INW) was advanced as a confrontation on the network between two opposing sides in war. Another author recommended the PLA establish an authoritative, centralized and united network People's War organ able to control information operations and networking activities. Such an organ would also support mobilization exercises and education on People's war on the net.

It was clear China intended to uphold the principle of combining military and civilian dual-use networks, while developing limited Internet service. Chinese focus, however, remained on cognitive processes, perceptions and beliefs, reflecting a competition to gain the initiative over information resources and control over information production, transmission, and processing. The strategic role of communications and the media was noted, particularly the deterrent effect it might possess through its ability to manipulate the populace.

There was also considerable work specifically in the area of cyberspace attack operations, or in Chinese terminology, computer confrontation operations:

> "There will be point-to-point confrontation between computers as well as theater-to-theater confrontation. There will be wireless confrontation as well as confrontation via cables...there will be wartime confrontation as well as confrontation in peacetime. There will be confrontation between military computers as well as between civilian computers."[312]

"In the final analysis, information warfare is conducted by people. The basic great plan is to cultivate talented people suited to information warfare...Scientific research institutions should also engage in research on information warfare."[313] The PLA advanced IW organizations and training over this timeframe to include the lead Communications Command Academy well respected for an IW curriculum analyzing strategic, operational, and tactical IW requirements. The Academy is located near the reserve component IW regiment, an important link to China's emphasis on a reserve force structure. Also the Information Engineering University, the Science and Engineering University, National Defense Science and Technology University, and the Navy Engineering College helped to cultivate professionals for high-tech warfare. Disciplines include electronic engineering, information engineering, network engineering, and other key information-warfare technologies as their core. One conclusion from an April-June 1999 event involving some sixty senior officers studying high-tech warfare during the Kosovo conflict was that the information umbrella is the

---

[312] "Computer Confrontation," *Information Warfare*. Chap. Five, January 1999, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice*. (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 14-17.

[313] Wang Pufeng, "The Challenge of Information Warfare," *China Military Science*, 1995. http://fas.org/irp/world/china/docs/iw_mg_wang.htm (accessed December 14, 2009).

most important factor, and the opponent's nerve center the most important military target.[314]

The universities and colleges reflected a PLA vision of IW as a strategic combat effectiveness multiplier. Computer confrontation training included hardware, software, electromagnetic and virus confrontation, in times of both peace and war, and military versus civilian systems. Offensive training included virus design, organizing virus invasions and control contagions, conducting electromagnetic jamming, deciphering data and gaining unauthorized access to the other side's computer networks. Numerous significant training events were undertaken between 1997 and 2000. Events included the development of a computer-virus warfare capability, development and use of a military information network superhighway, computer attack tactics to hit information networks, links and points, and confrontational campaign exercises on the Internet.[315]

In their book *Information War*, Zhu Wenguan and Chen Taiyi noted the necessity of a preemptive, active offense to disrupt and destroy enemy computer offensive forces, and that the PLA had established small brigades of offensive and defensive computer confrontation forces to conduct such attacks. They noted the units must be trained together using one another as targets, implying the units already existed and were practicing against each other. A November 1999 *PLA Daily* article stated China may develop an IW branch of service. The branch would constitute a net force including

---

[314] Xi Qixin and Zhao Yongxin, "Advancing toward High Technology—High Ranking Military Cadres Attending a Hi-Tech Training Course," *Xinhua Domestic Service*, June 13, 1999, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 18-19.

[315] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 20-24.

scanning, offensive, defensive, recovery, and masquerade, or deception technologies that could assist someone to masquerade as a commander and take over the net.[316]

Chinese analysts meticulously studied the use of armed force during the 1991 Gulf War, the fight for Kosovo,[317] and subsequent fighting in Iraq, noting the integration of military strikes and psychological-warfare activities and the increased strategic role of mass media during these operations. A number of Chinese authors identified networks as the most important aspect of the technological battle.

> "Network psychological warfare is a new topic in psychological-warfare defense, but networks will become the main psychological-warfare battlefield in the future. Global networks provide more space in which to engage in propaganda. Network data can be put online in secrecy by almost anyone; it is difficult to verify who the providers of network data are; and access to information is not subject to restrictions of time or place. Network attacks can throw a country's social, political, and economic life into chaos, producing a shock effect on people's minds and leading to political instability. In order to develop network defense, China must develop network sovereignty, establish laws for network activities, and establish information protection forces. Creating competent forces for information war and psychological warfare will help ensure China's information security and psychological security."[318]

China uniquely integrated its IW theory into its People's War concept. A multitude of computer operators conducting cyber warfare were to defend the nation against an electronic invader from laptops even from their own homes,[319] in the form of a decentralized and empowered hybrid cyber army. "The people's war of the past was

---

[316] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 57.
[317] Wang Baocun, "Information Warfare in the Kosovo Conflict," *Jiefangjun Bao*, May 25, 1999, and Yao Yunzhu, "Federal Republic of Yugoslavia Crisis Shows Need to Strenthen PLA: Discussion of the Kosovo Crisis Among Experts and Scholars," *Jiefangjun Bao*, April 13, 1999, referenced in Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" *Strategic Studies Institute* (Carlisle Barracks: U.S. Army War College, November, 2001), 9.
[318] Li Yuankui, Wang Yanzheng and Yang Xiaoli, "On Defense in Modern Psychological Warfare," *Zhongguo Junshi Kexue* (China Military Science), Number 6, 2000, 117-126, quoted from Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 102.
[319] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 1-2.

conducted in tangible space, but information war...is conducted even more in intangible space, such as in electromagnetic fields. It is...also a "computer battlefield" in the sheltered laboratories and control rooms."[320]

> "Some Chinese theorists have recommended organizing network special warfare detachments and computer experts to form a shock brigade of "network warriors" to accomplish this task. These detachments will look for critical nodes and control centers on networks and sabotage them."[321]

Beginning in the late 1990s, the Chinese Defense Ministry established the NET Force research organization to evaluate Chinese vulnerabilities. NET Force soon expanded to evaluating vulnerabilities of other nations, especially the U.S., Japan and South Korea. NET Force continued to grow, and was soon joined by an irregular civilian militia known as the Red Hackers Union (RHU), several hundred thousand patriotic Chinese programmers and Internet engineers wishing to defend and support the homeland.[322]

The emphasis on reserve personnel was a critical link to Chinese People's War and local-war theories and effectively decentralized the force structure. By 2000, China had built a networked civil-military force to conduct network People's War. This consisted of a reserve telecom force structure that included a reserve telecom regiment with an information industrial base, and a reserve contingent of high-tech telecom and transmission personnel. These personnel specialized in satellite, radio, relay, digital, telegraph and telephone, and optical-fiber telecoms.

---

[320] Wang Pufeng, "The Challenge of Information Warfare," *China Military Science*, 1995. http://fas.org/irp/world/china/docs/iw_mg_wang.htm (accessed December 14, 2009).
[321] Le Yinnina, in Huang Youfu, Zhang Bibo, and Hang Song, "New subjects of Study Brought about by Information War—Summary of Army Command Academy Seminar on 'Confrontation of Command on Information Battlefield,'" *Jiefangjun Bao* (Liberation Army Daily), November 11, 1997, 6, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice*. (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 6-7.
[322] "The Internet Is Tamed In China," *StrategyWorld*, July 9, 2009. http://www.strategypage.com (accessed December 14, 2009).

This hybrid organizational structure was further empowered through partnering at the technical level. By the end of December 2000, the PLA and reserve forces had reportedly developed their own web sites and simulation centers. On January 7, 2001 "several unidentified companies agreed to form the China C-Net Strategic Alliance, a second-generation, Internet-like network for China's government and industry."[323] Subunits of the People's Armed Police Corps underwent intensive IW training, and by 1999 emergency communications subunits were providing support to combat troops. The Shenyang military region alone included over one hundred militia high-tech subunits covering seventeen specialized fields such as modern communications, computers, automatic control, and electronic countermeasures.

> "In order to stem the tide of Internet crime, China reportedly increased the size of its Internet police force in 2000 to some 300,000 personnel. These crime fighters are part of the Ministry of Public Security and, thus, may have jobs other than fighting crime (espionage, etc.). The Internet police are mainly responsible for analyzing information content flowing through local communication systems or the Internet, fighting computer viruses, cracking down on Internet crimes, and stopping the spread of "harmful information."[324]

In response to Allied operations in the battle for Kosovo, Chinese analysts noted NATO prevented third parties from providing intelligence information to the Federal Republic of Yugoslavia (FRY), creating a NATO information blockade. The Serbs also used the Internet to fight NATO by setting up websites describing NATO air strikes, and trying to overload NATO systems with excessive numbers of e-mail.

---

[323] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 7-10.
[324] "China's Reserve Defense Might Is Markedly High-Tech," *Xinhua Hong Kong Service*, July 20, 1999 quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 73.

> "Active, protective measures taken by NATO were well advised and paid dividends. The Chinese *Liberation Army Daily* disclosed on 27 July 1999 that a "network battle" was fought between Chinese and US hackers following the 8 May bombing of the Chinese embassy. US hackers, according to the report, aimed their counterattack at the following Web sites:
>
> Xin Lang Wang or Sina—http://home.sina.com.cn
> Zhongwen Re Xun or Yesite—http://www.yesite.com
> Shanghai Wang Sheng or Shanghai Web Boom (no http listed)
>
> The Chinese initiated the short cyber war by altering the home page of the US Embassy in Beijing, writing on it "down with the Barbarians." The Chinese also reported that they caused a blackout at a few US political and military Web sites and some three hundred civilian Web sites. The methodology for performing these hacks, according to the *PLA Daily* article, was the mobilization of thousands and thousands of net users to issue a ping command to certain Web sites at the same time. This caused servers to overload and paralyzed these Web sites. In addition, thousands and thousands of e-mails were sent daily that blocked mail servers. Viruses were sent via e-mail, and attacks were launched with "hacker tools" hidden in certain programs. The *PLA Daily* article called for developing a computer network warfare capability, training a large number of network fighters in PLA academies, strengthening network defenses in China, and absorbing a number of civilian computer masters to take part in future network wars."[325]

The Kosovo conflict convinced the PLA it must use short-term solutions while modernizing. China did not expect to catch up to the U.S. in the next decade, however, the interdependence of PLA IW capability with building the nations information economy provided serious will to attempt just that.[326]

---

[325] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 27.
[326] June Teufel Dreyer, "The PLA and The Kosovo Conflict," *Strategic Studies Institute* (Carlisle Barracks: U.S. Army War College, May 2000), 12-15.

The battle for Kosovo was a catalyst to speed PLA modernization from mechanized to informationized forces.

> "China, instead of building bigger and better, in the mid-1980's decided to place emphasis on economic construction and cut its army by one million men. At the same time the information age began to emerge, and...there is a vast gray between peace and war in which the struggle will be largely decided."[327] "Thus, the 1995-2000 period represented five years of learning and advancement for the Chinese military...watching coalition actions in the Gulf War in 1991 and...the war over Kosovo in 1999. Not only was theory advanced, but exercises were held and new training methods presented."[328]

In the U.S., the FY2000 National Defense Authorization Act (Section 1202) directed the Secretary of Defense to submit a report on the current and future military strategy of the People's Republic of China addressing the current and probable future course of military-technological development on the People's Liberation Army. The report also included the tenets and probable development of Chinese grand strategy, security strategy, and military strategy, and of the military organizations and operational concepts, through the next 20 years.[329]

Summary 1995-2000

In the wake of the 1991 Gulf War, Chinese leadership recognized the power and precision of an information-based force. A distinctly Chinese approach crystallized around the 1997-1998 timeframe to allow a quality IW force to threaten more powerful nations through electronic attacks against a nation's financial institutions, or even the

---

[327] Shen Weiguang, *World War, The Third World War—Total Information Warfare*, (Beijing, Xinhua Publishing House, January, 2000), Postscript, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 50.
[328] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 30.
[329] U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China 2009*, (Washington, DC: U.S. Government Printing Office, 2009), 3.

worldwide economies financial transactions. Early efforts focused on the control of information, computer confrontation capabilities and forces were developed, and exercises and operations were conducted. Networks were identified as the most important aspect of the technological battle, and China uniquely integrated its IW theory into its People's War concept to include a multitude of computer operators conducting cyber warfare in the form of a decentralized and empowered hybrid cyber army. By 2000, China had built a networked civil-military force to conduct network People's War, including reserve telecommunications forces incorporated into the PLA force structure. The battle for Kosovo was a catalyst to speed PLA modernization from mechanized to informationized forces.

Over the 1995-2000 timeframe it is clear China recognized new technologies in the emerging domain of cyberspace and their corresponding destructive potential leading to new venues for competition. Unlike similar stages in other domains, however, areas for potential cooperation seem to have been either missed, or not capitalized upon. Catalyzing events including the 1991 Gulf War and 1999 Kosovo conflict spurred competition; however, even in the shadow of Y2K no cataclysmic cyber event demonstrated the destructive potential of cyber attacks requiring international attention. Even though the open access of the Internet was clearly recognized as a principal element in global economic development,[330] it did not lead to increased international cooperation to secure cyberspace. Rather, the militarization and effectiveness of cyber-enabled military forces led directly to a situation of competition and relative gains.

---

[330] Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" *Strategic Studies Institute* (Carlisle Barracks: U.S. Army War College, November, 2001), 6.

Chinese Information Warfare Theory and Practice 2001-2003

In October 2000, Major General Xu Xiaoyan, head of the General Staff's Communications Department, spoke of the tightening coordination between military and civilian information resources, and the need for "information mobilization" to be conducted during peacetime to strengthen and further enable networks to assist economic policy and national security. He noted information attacks in peacetime can cause social disorder and achieve the art of winning without fighting.

> "All locations where networks can extend will become IW battlefields. No matter if it is the citizens of any country, no matter what locality, as long as they possess certain computer knowledge and master certain network attack skills, they can then apply the mouse under their thumb to war on the network, enabling the global nature of IW."[331]

In the fall of 2001 Shanghai's National Defense Mobilization Committee reportedly established an Information Mobilization Office with the goal of creating a synchronous and real-time coordination mechanism with reliable communications to improve military-civilian war exercises and mobilization capacities. "To improve its skill base, the PLA has been recruiting specialists via its reserve officer selection program in order to design, comprehend, and execute a full-spectrum information operations/information warfare (IO/IW) campaign."[332]

C4I systems were considered both China's and the enemy's center of gravity,[333] and according to at least one author "the main forms of future combat operations would

---

[331] Xu Xiaoyan, "Establishing an Information Resource Mobilization Mechanism with Chinese Characteristics," *Zhongguo Junshi Kexue* (China Military Science), October 20, 2000, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice*. (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 70-72.

[332] U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China 2002*, (Washington, DC: U.S. Government Printing Office, 2002), quoted in M.E. Kabay, "US DoD Annual Estimates of Information Warfare Capabilities and Commitment of the PRC 2002-2009," (Northfield, VT: Norwich University Press, 2009), 3.

[333] Chong-Pin Lin, "Info Warfare Latecomer," *Defense News*, April 12, 1999, 23

be electronic warfare, network warfare, computer virus warfare, noncontact operations, and space warfare."[334] By 2003 network attacks were a popular topic across the board in Chinese writings, and it was clear reserve forces continued to play an important role in PLA IW planning and offensive strategies. In February 2003 the U.S. Strategic Command announced plans to develop a network attack task force, and China announced its own units the following month at the March 2003 People's Congress.[335]

As a result of work over this timeframe, China's military leaders began to speak of leading military transformation by information warfare themes. Chairman of the Central Military Commission, Jiang Zemin, pointed out in April 2003: "The essence of high-tech warfare is informationization and...IW will be the major form of warfare in the twenty-first century." Whereas analysts seldom, if ever, mentioned an active offense prior to 2000, in that year the main IW proponent on the General Staff, Major General Dai Qingmin, stated: "In the age of IW the active offense is necessary...to maintain the initiative." In 2001, China's National Defense University published a book discussing "the development of preemption strategies and the conduct of a "war of annihilation" strategy against enemy networks."[336]

Strategy was also advanced over this timeframe, with an emphasis on thirty-six traditional Chinese stratagems. The three thousand year-old stratagems remain very applicable in today's high-tech world.

---

[334] Liu Aimin, "The Characteristics of Informationized War," *Zhongguo Junshi Kexue* (China Military Science), August 1, 2001, 69-72, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 74.
[335] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 60.
[336] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 53.

For example:

> "Strategem One is "fool the emperor to cross the sea." This means that in order to lower an enemy's guard you must act in the open while hiding your true intentions under the guise of common, daily activities. The IW application would be to use regular e-mail services or business links over the Internet to mask the insertion of malicious code or viruses. Strategem Two is "Besiege Wei to rescue Zhao." This means that when the enemy is too strong to attack directly, then attack something he holds dear. The IW application is that if you can't hit someone with nuclear weapons due to the catastrophic effects on your own country, then attack the servers and nets responsible for Western financial, power, political and other systems stability with electrons. Strategem Three is "Kill with a borrowed sword." This means that when you do not have the means to attack your enemy directly, then attack using the strength of another. The IW application is simple—send your viruses or malicious code through a surrogate of another country. Strategem Four is "Await the exhausted enemy at your ease." This means that it is an advantage to choose the time and place for battle. Encourage your enemy to expend his energy in futile quests while you conserve your strength. When he is exhausted and confused, you attack with energy and purpose. The IW application here is to use the People's War theory to send out multiple attacks while saving the significant attack for the time when all of the West's computer emergency response teams (CERT) are engaged. Finally Strategem Five is "Loot a burning house." This means that when a country is beset by internal conflicts, then it will be unable to deal with an outside threat. The IW application is to put hackers inside the West (under the guise of a student or business) and attack from the inside. While chaos reigns, steal from information resource bases."[337]

By 2003, Chinese IW specialists offered fewer definitions, indicating the end of the debate:

> "[It] is clear that from 2000-2003 some conclusions were reached by the Chinese leadership regarding the nature of future war and IW's role in it...Real-world incidents, such as the hacker confrontation over the collision between a US EP-3 plane and a Chinese jet fighter, have affected Chinese IW perceptions...The number of IW related training exercises has risen sharply...In short, China's IW theory is much more reflective of China's culture and traditions, and the requirements of the times, than it was some nine years ago."[338]

---

[337] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 91.

[338] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 53.

A January 2003 issue of *Jiefangjun Bao* called for enhancing China's capability to launch electronic and network-based warfare. PLA representatives at the 2003 National People's Congress revealed the PLA was transitioning from mechanized to high-tech information warfare units with the ability to conduct network warfare on the Internet, and had the capability to transfer data via remote sensing satellites. Little mention was made in open sources of specific reserve units' activities between 2000 and 2003; however, the monthly journal of the PLA Academy of Military Science, *Guofang*, provided specific instructions in late 2003 on network attack activities to reserve units. Li Mingrang stated an auxiliary combat force system with People's War requirements must be built in China out of the reserves, and called for the development of "network People's War:"

> "[There] now are nearly twenty million network subscribers in China, and there is no shortage of computer experts and network jockeys among them, any one of whom could become a network guerilla who could open up a gunpowderless battlefield all by himself by harassing attacks on the network, namely by releasing large volumes of data from many directions concentrated on some enemy network station to jam up its network router and bring the network station to a standstill...and once there is a military requirement, either enter the network system to steal intelligence, or to activate viruses or detonate "bombs' to achieve the combat target of destroying the network."[339]

The People's War concept was refined over the 2000-2003 timeframe; with one writer emphasizing the concept under high-tech conditions should focus on cities to make the most of their high-tech information force, arming the masses through established units, militia and reserves, even recommending a mobilization database on the nationwide Internet to improve planning and mobilization. Delegates to the 2003 People's Congress continued to emphasize the requirement for an information-age

---

[339] Li Mingrang, "Develop the Advantage of People's War under the conditions of Innovation and Informatization," *Guofang*, November 15, 2003, 7-8, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice*. (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 59-60.

People's War, noting: "Even under informationized conditions, China's military strategic guiding policy of active defense will still uphold the ideology of Peoples War."[340]

China again observed U.S. operations in Iraq with intense interest over the March-August 2003 timeframe. In addition to television, the Internet provided great transparency through pluralistic reporting by Arab, Chinese, and Western media, even allowing CNN and FOX News pictures to be broadcast. "Instead of causing instability in Chinese society, the reporting showed that a new round of reform might be underway in the Chinese media."[341] China is undergoing rapid social and economic change that has gradually undermined the capacity of the authorities to control the flow of ideas. The proliferation of the Internet, as well as a flourishing publishing business not under direct government control, produced works unthinkable a decade earlier.[342]

Other observations noted that: "Information war should not only be conducted in the sphere of computer network war but should proceed in coordination with traditional mechanized modes of war."[343] The value of psychological warfare could not be overstated, and it was recommended military propaganda include modern mass communications and advanced information technology. A June 15, 2003 conference at the Academy of Military Science in Beijing discussed psychological operation methods employed by the U.S., including an Internet and cell phone campaign to persuade senior

---

[340] Bai Ruixue, "Chinese Military Delegates Say War in the Information Age Still Requires the Support of People's War," *Xinhua Asia-Pacific Service*, March 12, 2003, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 72-73.

[341] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 111.

[342] Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" *Strategic Studies Institute* (Carlisle Barracks: U.S. Army War College, November, 2001), 22.

[343] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 115.

Iraqi officials to give up resistance.[344] It was recommended China should "cultivate as many as possible highly qualified military professionals and professional military officers who are experts in computer systems and the Internet and information technology."[345] In 2003, former Chairman Jiang Zemin noted:

> "[No] matter what changes occur in the form of warfare, even IW, People's War remains China's magic key to beat any enemy. In the information era, China is laying the material foundation for the armed forces to launch a People's Informationized War. Information resources must be mobilized and specialized forces combined with nonspecialized forces. High technology allows the masses to participate in and support war more easily. The military-civilian compatibility of high technology allows for greater diversity in how masses can take part. People's War is more dependent on the buildup of war energy, is intense and fast paced. The new characteristic is exploiting the country's overall national strength to the maximum extent. New strategies and tactics of People's War should be developed."[346]

China's militia continued to advance along these lines, apparently even assuming offensive missions. The Guangzhou City's militia organized a battalion headquarters, provincial telecommunications company, computer network warfare company, and an electronic warfare company. The computer network company included network defense and attack platoons. "NetEase Guangdong (gz.163.com) and the China Unicom Paging Company have already secured arrangements with the unit to provide equipment."[347]

---

[344] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 126-128.

[345] Li Xuangqing, Chai Yongzhong, and Bao Guojun, "Directly Facing the Roaring Tide of New Institutional Changes of the Military around the World—Dialogue with Experts and Scholars form the Academy of Military Sciences" (Internet version), July 16, 2003, 12, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 140.

[346] Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 132.

[347] Ye Youcai and Zhou Wenrui, "Building a High-quality Militia Information Technology Element," *Guofong*, September 15, 2003, 45, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 133.

By 2003 China recognized cyberspace attacks as a means to enable economic growth and national security central to military planning, causing other nations to match this relative gain in cyberspace security. "China will use power projection as a means of achieving success in influencing the activities of foreign nations. Its centralized leadership system will continue to exert control over the news, propaganda, and public opinion."[348] "Apparently, other nations have noticed China's focus on psychological warfare and have responded. In January 2002, Taiwan, taking advice from U.S. military officials, activated its first modern psychological-warfare unit to counter China's buildup."[349]

A September 2003 network break-in at Lockheed Martin was followed several months later by an attack at Sandia government laboratories in Albuquerque, NM. Sandia analyst Shawn Carpenter noted the similarities and with unfortunately loose coordination with the labs, Army intelligence, and the FBI, pursued the cyber infiltrators.

> "Methodical and voracious, these hackers wanted all the files they could find, and they were getting them by penetrating secure computer networks at the country's most sensitive military bases, defense contractors and aerospace companies. Carpenter had never seen hackers work so quickly, with such a sense of purpose. They would commandeer a hidden section of a hard drive, zip up as many files as possible and immediately transmit the data to way stations in South Korea, Hong Kong or Taiwan before sending them to mainland China. They always made a silent escape, wiping their electronic fingerprints clean and leaving behind an almost undetectable beacon allowing them to re-enter the machine at will. An entire attack took 10 to 30 minutes...They never hit a wrong key."[350]

---

[348] Wang Lianshui, Ma Jingcheng, and Yan Jianhong, "Comparison of Psychological Warfare between China and the West," *Zhongguo Junshil Kexue* (China Military Science), Number 6, 2000, 102-110, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 105.

[349] Brian Hsu, *Taipei Times* (Internet Version), December, 2001, quoted in Timothy L. Thomas, *Dragon Bytes, Chinese Information-War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 104.

[350] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," *TIME*, August 29, 2005. http://www.time.com/time/magazine/article/0,9171,1098961,00.html (accessed December 14, 2009).

Carpenter accomplished the rare achievement of locating the attackers' country of origin to just three Chinese routers in the southern Chinese province of Guangdong. He carefully installed a homemade bugging code in the primary router's software, sending him an e-mail to his anonymous Yahoo! account every time the gang made a move on the net. Within two weeks, his account was filled with nearly 23,000 messages, one for each connection the router made in its quest for files. The aforementioned Titan Rain operation had been discovered, compromising secure networks ranging from the Redstone Arsenal to NASA to the World Bank.

The FBI lacked sufficient cyber experts in 2004, however, to track down such foreign rings, and their hands were often tied by strict rules of engagement (ROE). While the FBI "aggressively" pursued the possibility the Chinese government was behind the attacks, they cautioned they did not know yet whether the spying is official, a private-sector job or the work of many independent, unrelated hands. China did not cooperate with the U.S. investigation, and the Chinese government replied to the charges about cyber spying and Titan Rain as "totally groundless, irresponsible and unworthy of refute." Highlighting the differences between state-sponsored cyber vigilantism, and paralyzing U.S. ROE in cyberspace, Carpenters' reward was the loss of his job and Top Secret security clearance for gaining unauthorized Internet access.[351]

For the interested reader, Thomas has published a subsequent book,[352] and M. E. Kabay has assimilated significant PRC IW references from the DoD Annual Report over

---

[351] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," *TIME*, August 29, 2005. http://www.time.com/time/magazine/article/0,9171,1098961,00.html (accessed December 14, 2009).

[352] Timothy Thomas, *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy*. (Fort Leavenworth, KS: Foreign Military Studies Office, 2007).

the years 2002-2009, extending the baseline for this experiment.[353] The 2009 Annual Report noted:

> "The 2000 edition of this report observed that China is "working to ameliorate weaknesses in C4I training and [place] increased emphasis on 'electromagnetic warfare' to degrade or destroy enemy operational systems." At that time, the PLA's electronic warfare (EW) systems were derived mostly from a combination of "1950s-1980s technologies." By the 2006 edition of this report, China's investments in advanced EW programs had given the PLA Air Force "technological parity with or superiority over most potential adversaries." By improving space-based and terrestrial C4ISR and by moving communications infrastructure to fiber, China is hardening its own capabilities while making gains in developing weapon systems (e.g., counterspace, computer network operations, and anti-radiation systems) to deny these capabilities to others. The 2004 introduction of the PLA concept of "local wars under conditions of informatization" has guided development in this area, positioning the PLA to contest electromagnetic dominance in the early phases of future campaigns."[354]

Summary 2001-2003

By 2000, China recognized the need to go on the offense through peacetime, preemptive attacks,[355] and identified the need for "information mobilization" to be conducted during peacetime to strengthen and further enable networks to assist economic policy and national security. The focus of future combat operations development focused on electronic, network, computer virus, noncontact, and space warfare. By 2003 network attacks were a popular topic across the board in Chinese writings, and it was clear reserve forces continued to play an important role in PLA IW planning and offensive strategies.

---

[353] M.E. Kabay, "US DoD Annual Estimates of Information Warfare Capabilities and Commitment of the PRC 2002-2009," (Northfield, VT: Norwich University Press, 2009), 2.
[354] U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China 2009*, (Washington, DC: U.S. Government Printing Office, 2009), viii.
[355] James Mulvenon, "The PLA and Information Warfare," in James Mulvenon and Richard H. Yang, *The People's Liberation Army in the Information Age*, (Washington, D.C.: RAND, 1999), 184-185.

China sought to enhance its capability to launch electronic and network-based warfare. At the 2003 National People's Congress, PLA representatives revealed the PLA was transitioning from mechanized to high-tech information warfare units with the ability to conduct network warfare on the Internet, and to transfer data via remote sensing satellites. The People's War concept was further refined over the 2000-2003 timeframe, even extending into the militia. Chinese observations of the U.S. war in Iraq in 2003 spurred the development and incorporation of psychological operations into Chinese activities along thirty-six traditional strategems. Other nations noticed China's focus on psychological warfare and responded with development of their own units.

Over this timeframe it is clear China recognized technological and operational advances through the wars in Kosovo and Iraq. Rather than seeking further cooperation through an IY2KCC-like instrument, or proposing a draft agreement as Russia did, China seemed to recognize its security would be best served through expansion. Few, if any, incentives seem to have been offered for them to cooperate in any meaningful way. This led to the militarization and build-up of cyber-enabled military forces exacerbating the relative gains dilemma.

Counterfactual Application of Recommendations 1995-2003

The unfortunate truth over this timeframe is that China obviously shared a number of goals with her global neighbors, including using the Internet for economic development, controlling and securing information, and protecting critical infrastructure. In 2006, Liu Zhengrong, Deputy Chief of the Internet Affairs Bureau of the State Council Information Office argued China's efforts to control the Internet were no different from

those of Western countries. "After studying Internet legislation in the West, I've found we basically have identical legislative objectives and principles...It is unfair and smacks of double standards when [they] criticize China for deleting illegal and harmful messages while it is legal for U.S. Web sites to do so."[356] Along these lines, China advanced Internet policing, and created hybrid organizations in a distinctly Chinese approach through the People's War concept.

How might this history have differed had the following approach been applied?

- Cooperative technical development through joint investment allowing for variance in views over control of the Internet across technical, economic, social and political regions;
- International funding tied to improved technical and legal standards to spur development and provide a tool to enmesh actors through bureaucratic bargaining and impose costs through the withholding of funds to detractors and non-participants;
- Empowerment of hybrid organizations cooperating in practical areas of global Internet security in order to:
    - advance cooperative Internet sensing and analysis through regional or domain hubs incorporating behavioral analysis, activities and effects;
    - place Internet users in a position of power and trust, capitalizing on temporary organizations; and
- International consultations, such as the current IGF dynamic coalitions, in the form of negotiating rounds to:
    - Initially focus on descriptive practice as opposed to normative efforts such as addressing the wide variance in views over control of the Internet, and delineate between sovereign and common elements, or agree to the limits of such delineation;
    - Promote regulatory prescriptions in a stepwise approach as identified through cooperative efforts, such as property rights and penalties for software and malware, and Internet crime legislation and recourse; and
    - Develop a dispute settlement mechanism focusing on effects, again allowing for variance across technical, economic, social and political regions.

First, consider the 1995-2000 timeframe leading up to Y2K and the war in Kosovo. Suppose ISP regional associations centralized development and security efforts

---

[356] Sumner Lemon, "China defends right to censor Internet," *IDG New Service*, February 15, 2006. http://www.networkworld.com/news/2006 (accessed December 14, 2009).

at the regional level, extended through hybrid private-public partnerships, and loosely coordinated, as they were, through IAB-IETF efforts. *A joint program would have facilitated the pooling of resources, and promulgation of the Internet in a transparent environment.* The Internet itself provided the collaboration mechanism necessary to coordinate such disparate grass-roots efforts.

This would have allowed regional hubs to focus on the areas of interest and concern to the region or domain, without penalizing other hubs for addressing their own. For example, the Chinese have pursued control and censorship unique to their political structure. These efforts to prevent domestic Internet users from reaching blacklisted web sites or content have included:

- Monitoring all incoming and outgoing traffic using mirroring routers to scan for forbidden information;
- Using tens of thousands of censors to monitor bloggers and delete offensive or subversive material; and
- DNS blocking, reset commands, connection breaking, URL keyword blocking and content scanning.[357]

Second, *international funding tied to improved technical and legal standards would have provided not only much desired resources, but also an ability to impose costs through the withholding of funds or technologies from detractors and non-participants.* Cooperative monitoring activities would have increased transparency of individual or criminal activities while empowering all participants to address identified risks. Finally, it would have greatly facilitated international Y2K efforts, with potential cost savings in the billions of dollars for the U.S. alone.

Certainly some opportunities could have been recognized by numerous actors including the U.S. and China. International Monetary Fund (IMF) or World Bank

[357] "10 Ways the Chinese Internet is Different From Yours," *Networkworld*, 2008. http://www.networkworld.com/slideshows/2008 (accessed December 14, 2009).

funding following the IY2KCC model would have had to have been very appealing to a nation that cut a million men from its army over the 1980s to focus on economic construction. *The availability of such funds would have immediately pulled the Chinese government into a position of accountability, effectively enmeshing at least certain aspects of the government.*

While it is doubtful in the wake of the Gulf War China would have forgone a move to an "informationized" force, there is no reason to believe the incorporation of computer confrontation operations as an offensive weapon or espionage capability was a foregone conclusion. The weight of evidence is in fact to the contrary, highlighting one potentially significant area of miscommunication during this agenda formation stage of the regime. Recall China's initial concerns over this timeframe were defensive in nature, with the PLA clearly recognizing a gap in capability with the U.S. and perhaps others. In fact given the Chinese emphasis on controlling as opposed to exploiting information, and concerns over the impact of open Internet access on domestic stability, there is every reason to believe China may have favored such an approach. In the wake of incidents such as the 1998 Morris worm, *security coordination efforts such as those taken by CERT/CC would have been in a position to provide true joint gains for the entire community. Incorporating behavioral analysis would have helped to bridge divides between technical attribution and political action, as well as the public and private sectors through hybrid and state security organizational relationships.*

Significantly, none of this would have restricted ongoing grass-roots efforts around the Internet. Internet development and enhanced use through P2P technologies could have largely progressed as described in chapter four. The visibility over criminal

activities, however, would have been much higher, potentially facilitating improved legal or political instruments to address them. In essence, states would have been indirectly empowered through such regional efforts. If the 25% loss of revenue in a single year from the music industry due to the loss of control of information in the form of recordings is any indicator, states stood, and continue to stand, much to lose by failing to address decentralization empowered by the Internet.

Third, *regional and international partnering would have provided funds and technology transfers in a secure, accountable, and transparent environment.* This would have promoted, as opposed to skirted, property rights in the same way Apple's iTunes has proven to be more favorable than less secure options. It would have most certainly contributed to improved understanding of the problems to be solved and evolved the handling of new tasks. In such cases as actors had reasons to violate the evolving principles and norms, *international transparency of violators' actions would have supported concerted action on the part of the international community.*

In short, it is quite plausible China would have welcomed such opportunities to support Internet security efforts while advancing its force modernization efforts. This would have circumvented China's advancement of computer confrontation operations except perhaps in the most extreme circumstances of national survival. Such opportunities would have provided real incentives and the opportunity to impose costs to deter actively offensive measures during peacetime at the risk of losing international support and resources. It would not be too bold to say that even in the case of the 1999 U.S. bombing of the Chinese embassy during the war in Kosovo; such incentives might have deterred the ensuing cyber battle, even if the Chinese had developed the capability

to carry out such an attack, which is questionable under these conditions. *At the very least, the attack would have been more transparent, actors would have been more empowered to mitigate it, attackers would have been more likely to act in accordance with the principles of the international law of armed conflict, and awareness of these factors would have most certainly extended the shadow of the future in their decision-making.*

Such efforts would have further facilitated national and international response to the first global threat to the Internet, Y2K. Facing such a potential catastrophe was probably the first opportunity for efforts in cyberspace to reach a level of high politics to force Internet security onto the international agenda.

Fourth, over the 2000-2003 timeframe, consider that in the wake of Y2K the international community widely perceived the same benefits of the IY2KCC as did the U.S. Senate. These included awareness of international risks and mitigating activities, and nurturing the domestic and international industry and government partnerships. Suppose the IY2KCC was left intact as an international partnership focusing on technical development through joint investments. In this role, the center would have acted as a central monitoring hub of Internet activity, as it performed leading up to Y2K, and similar to CERT/CC and the ITU's GRC.

Suppose this provisional organization in concert with the ITU, WTO, ISO, CERN laboratories, ICANN and others initiated a series of negotiating rounds addressing Internet crime, software and malware property rights and penalties, and a dispute settlement mechanism focusing on the effects of cyber activity along the lines of the WTO DSU. Perhaps the May 1999 U.S.-Chinese cyberwar, had it occurred, might have

been one of the first test cases. Such a venue would have provided the opportunity for any number of negotiating rounds to address topics as improved technical standards, the application of international law, the development of domestic legislation, and multilateral or bilateral agreements regarding reciprocity, rendition, and extradition.

Negotiations could have facilitated not only the high politics of international cyber attacks and the law of armed conflict, but also domestic legislation and ratifications further enmeshing participating states. *With the emphasis on securing the Internet as opposed to securing any individual state or entity, this cause could be advanced under a condition of realized joint gains as opposed to perceived relative gains.* Under these conditions, real legal and monetary costs as well as more subjective political costs could be imposed upon violators, further extending the shadow of the future into rational actor decision-making. *While the deterrence of non-rational actors such as juvenile hackers is questionable at best, their resources, opportunities and incentives for hacking may have been considerably curtailed.*

Negotiations would have directly facilitated the 2002 OECD Guidelines for the Security of Information Systems and Networks, and 2004 COE Convention on Cybercrime, *effectively maturing the regime to the negotiation stage.* In essence, it would have provided a more substantive initiation to what in reality became a sluggish start to the 2002 WSIS, and resulting IGF efforts, to include the 2007 GCA and 2008 GRC. The provisional organization may have advanced operational and legal foundations not unlike PICAO in the air domain, as opposed to the contentious and open-ended approach adopted more closely resembling negotiations over the UNCLOS III in the sea domain.

In this specific case, these approaches would not have restricted or deterred the focus of China's approach to digitizing their force. In truth, it may have enabled it in an open and legal manner. It would almost certainly, however, have mitigated their perceived risks of cyber attack, and likely deterred them from dedicating resources to develop the force structure history now presents. While China recognized technological and operational advances through the wars in Kosovo and Iraq, incentives and opportunities for cooperation, as opposed to expansion in cyberspace may have been realized. Certainly *firm incentives and the ability to impose costs would have been more available to the international community and individual states alike. Ultimately, there is every reason to believe such opportunity for joint gains would have deterred the use, if not limited the development of, offensive cyberspace capabilities*, even as China's force modernization progressed in other areas.

During the agenda formation stage, we need to clearly distinguish between conflicts of interests and misunderstandings arising out of differences in the political structure and policy culture of participants. In this case at least two areas of friction with China over Internet security warrant serious consideration as cases in point. The first identified above is that the primary rationale for China's expansion in cyberspace was originally defensive in nature. The second lies in the wide variance of views over control of the Internet, and merit in discussing regional or domain approaches to addressing such technological, organizational, social, economic, and political differences.

Allowing various levels of state control over the array of hubs, networks, and domains may place another potential conflict of interest aside through better understanding and informed decision-making in support of future development and

investment decisions. Allowing all of this to happen in an open, transparent web of relevant hybrid organizations provides for grass-roots development opportunities. *These efforts offer the opportunity to bypass potential clashes between major actors*, as early web browser development prevented between Microsoft and Netscape. In this way, this limited experiment identifies some of the links between interests and policy preferences, and the relative contributions of problem structures and processes.[358]

[358] Oran Young, *Creating Regimes: Arctic Accords and International Governance*, (Cornell UP, 1998), 186-196.

CHAPTER VIII

DISCUSSION AND CONCLUSIONS

This paper has explored the question: "How might maturing international cooperation mitigate the problem of cyberspace attack attribution." Cyberspace is a unique domain, and international cooperation in cyberspace security policy decisions poses a fundamental test of security regime theory developed from experience in other domains. Lessons from regime development in other security-related domains informed the analysis and recommendations for the cyberspace domain.

The lack of incentives to cooperate or ability to impose costs has led to conflict and expansion in offensive cyberspace capabilities. Four recent attacks illustrated specific problems of attribution in cyberspace. The application of P2P C2 and other technologies are increasing the lack of transparency into mounting threats. The cases also illustrated growing international cooperation in the area of mitigating attacks, while highlighting hurdles to sharing sensitive information that might lead to more confident attribution. This was a key observation informing subsequent analysis and recommendations. The cases demonstrated that while individual states may desire a more regulated environment, no readily apparent incentives significantly justified exposing themselves to potential adversaries.

Hybrid organizations facilitate information exchange and a sense of ownership with the express intent of enabling the Internet community at large to react more quickly to an attack. A review of cyberspace domain development makes clear relevant intergovernmental institutions are in fact embracing a culture of security; at least to the

extent funding is provided. These efforts, however, continue to focus on security for individual users as opposed to the Internet as a whole, and therefore individual states and critical infrastructures. Recent events also provide evidence of national and intergovernmental organizations such as CERTs, the ITU GRC, NATO CCDCOE, GreyLogic and numerous others attempting to address the decentralized nature of the domain through co-opting and empowering Internet users.

The following emerging principles and norms summarize the current cyberspace attack attribution regime:

- State and hybrid organizations focus on mitigation as opposed to attribution;
- States and hybrid organizations are empowered to assist in mitigation and attribution efforts, working together to mitigate the impact of attacks, and sharing attribution information where possible; and
- Cyber attacks are considered a legitimate form of declared conflict, commensurate with established principles and norms of the laws of armed conflict (international humanitarian law).

The following principles and norms appear to be worth pursuing to advance the emerging regime, and pressure states and entities to assist in mitigation and attribution efforts:

- Costs are imposed for failing to assist in mitigation and attribution efforts, imposing de facto costs on those responsible or complicit. Such costs could be economic in nature, tied to current or future access to the Internet or the conduct of certain transactions over it, or the expectation of future cooperative security efforts or agreements.
- Those states and entities not supporting mitigation and attribution efforts are considered complicit (or even responsible) for them, shifting the burden of attribution from the defender to the attacker.

The regime has so far been ineffective at imposing costs to shift the burden of attribution from the defender to the attacker. Past assessments of the capability and effectiveness of the regime have led to the collective paralysis of the community pending improved technical and legal advancements described by General Chilton. While states

and international organizations are changing their behaviors based on perceived costs and benefits, their lack of effectiveness continues to embolden and even entice violators.

The regime is, however, creating arrangements that affect more normative political behaviors, including processes of social learning. Normative and political criteria focused on attack mitigation support a very different assessment and the identification of meaningful recommendations for advancing global security in cyberspace.

States and entities voluntarily support mitigation efforts primarily for reasons of political support for victim states and secondarily out of collective interest in Internet security. If the collective-action problem is to be addressed to realize joint gains, these priorities require reversal through mechanisms sufficiently embedded in internal state politics to appreciably enmesh state or non-state behavior.

Applying this evidence against factors prominent in theories of regime formation demonstrate the current cyberspace attack attribution regime remains in the early stages of regime development. Understanding the maturity level of the regime led to specific recommendations tailored to the agenda formation stage. Table 4 summarized the role of ideas, power, cooperative efforts, and non-state actors to shape expectations, advance institutional learning through stepwise processes, and enmesh actors to ultimately develop capacity to coerce compliance. The level of decentralization in cyberspace was identified as a significant intervening variable, and informed specific recommendations regarding the advancement of hybrid organizations.

Lessons from regime development in other security-related domains demonstrated strong correlation to relevant aspects of the cyberspace domain, informing the following proposed policy approach:

- Cooperative technical development through joint investment allowing for variance in views over control of the Internet across technical, economic, social and political regions;
- International funding tied to improved technical and legal standards to spur development and provide a tool to enmesh actors through bureaucratic bargaining and impose costs through the withholding of funds to detractors and non-participants;
- Empowerment of hybrid organizations cooperating in practical areas of global Internet security in order to:
    - Advance cooperative Internet sensing and analysis through regional or domain hubs incorporating behavioral analysis, activities and effects;
    - Place Internet users in a position of power and trust, capitalizing on temporary organizations; and
- International consultations, such as the current IGF dynamic coalitions, in the form of negotiating rounds to:
    - Initially focus on descriptive practice as opposed to normative efforts such as addressing the wide variance in views over control of the Internet, and delineate between sovereign and common elements, or agree to the limits of such delineation;
    - Promote regulatory prescriptions in a stepwise approach as identified through cooperative efforts, such as property rights and penalties for software and malware, and Internet crime legislation and recourse; and
    - Develop a dispute settlement mechanism focusing on effects, again allowing for variance across technical, economic, social and political regions

Finally, these recommendations were applied through a counterfactual thought experiment of Chinese information warfare theory and development to develop conclusions and recommendations in the form of current and future opportunities. The experiment provided an opportunity to distinguish between conflicts of interests and misunderstandings arising out of differences in the political structure and policy culture of participants during the agenda formation stage.

The evaluation showed that despite China's ambitions to modernize their force and spur economic growth, there is no reason to believe that offensive expansion in cyberspace was a foregone conclusion. Rather, the evidence showed a preference for investments in other areas as long as technological advances respected their political system and their security in cyberspace could be assured through transparent and multilateral efforts. The potential for international investment to promote cooperative development and monitoring ultimately leading to transparency, as well as mitigation and attribution capability, would have ultimately provided one source of power to impose costs on violators which the current regime lacks.

CURRENT AND FUTURE OPPORTUNITIES

Although opportunities have certainly been missed, the objectives are far from lost considering the early stage of regime formation in this issue area. China has invested heavily in modernizing its force structure in addition to advancing cyber attack and espionage capabilities. China now likely considers its cyber espionage capabilities as critical for its economic development and force modernization. Similarly, Russian hackers now enjoy a plausibly deniable instrument to carry out an increasingly expansionist foreign policy with little risk for the Kremlin. "[The] Chinese – and the Russians – are very comfortable with the deniability and using proxies, even through the actions of those proxies could have enormous strategic consequences."[359]

The cyberspace attack attribution regime is still clearly at a stage of agenda formation, proceeding in an atmosphere of openness and fluidity with all significant

---

[359] Simon Elegant, "Cyberwarfare – The Issue China Won't Touch," *Time,* November 18, 2009. http://www.time.com/time/world/article/0,8599,1940009,00.html (accessed December 13, 2009).

actors advancing their position through tacit communications and bargaining. "The world is just getting around to dealing with information warfare activities...Spies will have to match counterspies and hackers will have to match counter-hackers. The smarter of the two will carry the day,"[360] and it isn't affecting just the U.S. "In the past few years, sources ranging from the German Chancellor's office to government mainframes as far afield as New Zealand and Belgium have made loud public allegations that they had been the subject of cyber infiltration from China, all to no avail."[361] Chinese espionage efforts have cost Germans an estimated 30,000 jobs lost.[362] This means it is not too late to apply such an approach, despite the fact the window is closing.

As illustrated in the assessment of regime maturity, *direct confrontation or negotiation is likely not the answer.*

> "[Even] if U.S. officials try to raise the issue of what they believe is a constant and growing campaign by China to infiltrate U.S. networks, steal secrets and hone Beijing's ability to wreak havoc in case of military conflict, the likelihood is that Chinese officials will simply deny that the problem exists, as they have done with great success in the past. From the American point of view, there's unfortunately currently little Washington can do to change the state of affairs."[363]

Indeed, "playing dumb" [364] to elude issues is a known Chinese facilitating tactic. In one recent example, China forcefully protested the DoD Annual Report on the Military Power of the People's Republic of China pointing to the doubling of Chinese defense spending over the last decade and areas of expansion. China insisted its military

---

[360] Hari Sud, "Chinese and U S lead information warfare," *UPI Asia*, July 17, 2009. http://www.upiasia.com/Security (accessed December 14, 2009).
[361] Simon Elegant, "Cyberwarfare – The Issue China Won't Touch," *Time,* November 18, 2009. http://www.time.com/time/world/article/0,8599,1940009,00.html (accessed December 13, 2009).
[362] "Chinese Bandits Can't Be Touched," *StrategyWorld*, July 28, 2009. http://www.strategypage.com (accessed December 14, 2009).
[363] Simon Elegant, "Cyberwarfare – The Issue China Won't Touch," *Time,* November 18, 2009. http://www.time.com/time/world/article/0,8599,1940009,00.html (accessed December 13, 2009).
[364] Richard Solomon, *Chinese Negotiating Behavior, Pursuing Interests Through 'Old Friends,"* (Washington, D.C.: USIP Press, 1999), 89.

spending was purely for defensive purposes, although much spending is hidden under budgets of other offices. Since China does not allow translation of certain sanctioned media activities, such as decades of writings portraying the U.S. as the opponent in future war, China's reaction to the report is based on the idea that anything published in Chinese doesn't count.[365]

Hybrid organizations should be technically, financially, and organizationally empowered in accordance with the level of trust within and between them. International cooperation in cyberspace to date highlight a number of multilateral and hybrid organizations. Funds tied to improved technical and legal standards should be made available to their efforts to provide incentives for cooperation and an ability to impose costs for detractors and violators. Given the billions that might have been saved in international Y2K efforts, these funds would indeed be worth their weight in "global cyber financial transaction gold." The U.S. reportedly spent $100 million over six months in 2009 alone to repair damage caused by cyber attacks, most of which originated in China.[366]

Efforts such as IPv6, providing the backbone to the China Next Generation Internet,[367] and Web 3.0 development provide cooperative joint opportunities. The Service Web 3.0 support action project funded by the European Commission as a part of the 2008-2009 Seventh Framework Programme (FP7) provides but one clear example.[368] China is currently mandating government computers adopt a Chinese developed and

---

[365] "China Has a Secret Plan," *StrategyWorld*, March 29, 2009. http://www.strategypage.com (accessed December 14, 2009).
[366] Hari Sud, "Chinese and U S lead information warfare," *UPI Asia*, July 17, 2009. http://www.upiasia.com/Security (accessed December 14, 2009).
[367] M.E. Kabay, "Chinese information warfare capabilities," *Networkworld*, April 7, 2009. http://www.networkworld.com/newsletters (accessed December 14, 2009).
[368] European Union, "Seventh Framework Program (FP7)," http://cordis.europa.eu/fp7/dc/index.cfm (accessed March 1, 2010).

subsidized Unix variant called Kylin. Chinese interest in moving away from Windows to Unix and Linux operating systems for security reasons present additional cooperative opportunities to address China's outlaw mentality to software procurement and development.[369]

Decentralized technical development efforts should be promoted, allowing for variances across technical, economic, social and political regions and domains. For example, as of December 2009, China continued to advance Internet controls to enhance the nation's already strict control of political opposition. China justifies this under goals such as protecting children from pornography, and limiting media piracy and Internet scams. The "Internet has become an important avenue through which anti-China forces infiltrate, sabotage and magnify their capabilities for destruction,"[370] so the trend has been toward ever tightening control through improving censorship capabilities. The new measures restrict citizens' ability to establish personal websites under China's .cn ccTLD, now limited to registered businesses, or to view hundreds of others. This appears a continuation of China's blocking of Facebook, Twitter, YouTube and thousands of other websites in 2008. China's censorship also extends to the telecommunications, and de facto space, domains as the government has similarly pressured cell phone companies to "prevent transmissions of online pornography."[371]

Internet security organizations (e.g. CERT/CC and GRC) *should work even closer with private-public hybrid organizations* (e.g. IWM, GreyLogic and

---

[369] "China Turns Unix Into A Weapon," *StrategyWorld*, May 14, 2009. http://www.strategypage.com (accessed December 14, 2009).
[370] Meng Jianzhu, Public Security Minister, *Quishi* (Communist Party's Central Committee magazine) , December 1, 2009, quoted in Sharon LaFraniere, "China Imposes New Internet Controls," *New York Times*, December 18, 2009. http://www.nytimes.com (accessed December 19, 2009).
[371] Sharon LaFraniere, "China Imposes New Internet Controls," *New York Times*, December 18, 2009. http://www.nytimes.com (accessed December 19, 2009).

ShadowServer) *to expand Internet sensing and analysis capabilities in an open and transparent venue*. Clearly, multilateral and bilateral efforts directly between state security organizations would further the ability of allies to share information in the pursuit of more definite attribution. Incorporating behavioral analysis inherent in traditional state intelligence agencies would help bridge the technical attribution-political action divide. Such a cooperative approach provides the opportunity to place numerous scatter-shot efforts within more comprehensive global and national strategies, which according to some at least remain a "ship adrift."[372] These include smart-card identity credentials and more secure Internet protocols

These combined efforts provide more opportunities for actors to cooperate in the area of cyberspace security, while pressing non-participants and detractors to cooperate, or acknowledge their activities as a matter of policy. Together, the efforts provide a first step to shift the burden of attribution from the victim to the attacker, and reduce the legal grey area between peacetime domestic legislation, international criminal legal cooperation, and the international law of armed conflict.

For example, how is it a country with extensive control over the Internet and an estimated 30,000 strong force of secret police technicians (known as the Golden Shield Project, or The Great Firewall of China)[373] allow such expansive malicious activity on their nets?[374] China is clearly willing to resist discussion or play dumb with individual actors. The recommendations presented here would pressure China to do so in the face of

---

[372] Jaikumar Vijayan, "Internet Warfare: Is the focus on the wrong things?" *Networkworld*, April 27, 2009. http://www.neworkworld.com/news/2009 (accessed December 14, 2009).
[373] "The Internet Is Tamed In China," *StrategyWorld,* July 9, 2009. http://www.strategypage.com (accessed December 14, 2009).
[374] "The Curious China Connection," *StrategyWorld*, July 1, 2008. http://www.strategypage.com (accessed December 14, 2009).

broad international consensus and scrutiny. Perhaps most importantly, the recommendations focus on providing capacity to all states that chose to play by the rules, thus realizing joint gains. Sharing cyberspace attack information and gaining joint stakes in cooperative Internet development would stiffen the international community's resolve to confront prolific violators such as China and impose costs through bilateral or multilateral venues.

WSIS IGF dynamic coalitions and other venues for international discussions and consensus-building in this issue area should be pursued in the form of negotiating rounds. *A stepwise approach shapes expectations, promotes institutional learning, enmeshes actors, and facilitates the ability of the global Internet community to coerce compliance. Power to do so is gained through cooperative efforts, the ability to withhold funds or technologies, and a dispute settlement mechanism again allowing for variance across technical, economic, social and political regions. Such empowerment provides real prospects for extending the shadow of the future for rational decision-makers.*

These provide meaningful steps for advancing the regime and for discussion in such formal negotiations as may present themselves. For example, in November 2009, a U.S.-Russian delegation met in Washington, reportedly bridging long-standing divisions between the two countries. Two weeks later in Geneva, the U.S. agreed to discuss cyberwarfare and cybersecurity with representatives of the United Nations committee on disarmament and international security, breaking with policies of previous administrations that insisted on addressing those matters in the committee on economic issues.

Russia characterized this new round of discussions as the opening of negotiations between Russia and the U.S. on a possible disarmament treaty for cyberspace, noting the American position on Internet security had shifted perceptibly in recent months. A U.S. State Department official, however, disputed the Russian characterization of the American position. "While the Russians have continued to focus on treaties that may restrict weapons development, the United States is hoping to use the talks to increase international cooperation in opposing Internet crime," maintaining that strengthening defenses against Internet criminals would also strengthen defenses against any military-directed cyberattacks.[375] Such discussions provide opportunities for finding common ground.

These efforts should be taken in coordination with related efforts, such as cooperation in the space domain. For example, managing issues which threaten the common interest in the peaceful use of space also require broader international cooperation. Perhaps no state will be more important in developing stable solutions to these problems than China. The U.S. and China share a common interest in preserving the peaceful use of outer space over such pressing items such as improvements to orbital-debris mitigation, space traffic control, and transparency.[376]

States expend significant resources to establish attribution of objects and activities in space. Russia maintains a Space Surveillance System using its early-warning radars and monitors some 5,000 objects (mostly in LEO), but does not widely disseminate data. The EU, Canada, China, France, Germany, and Japan are all developing independent

---

[375] John Markoff and Andrew Kramer, "In Shift, U.S. Talks to Russia on Internet Security," *New York Times,* December 12, 2009, 1.

[376] Jeffrey Lewis, "Engage China, Engage the World," *adAstra Online: The Magazine of the Space Society*, http://www.space.com/adastra/china_engagement_0505.html (accessed December 7, 2009).

space surveillance capabilities.[377] One result of these efforts has been to expand and even shift concerns from the threat of direct attack to that of collateral effects. Similarly, such efforts, if assumed cooperatively, provide recurring opportunities to establish dialogue and engage in confidence-building measures to realize joint gains in areas of common interest. These areas include using the Internet for economic development, controlling and securing information, and protecting critical infrastructure.

> "China races to embrace its destiny as a global player to be reckoned with...For decades, the world's most populous nation lived in self-imposed isolation, but now it moves to engage the world as an economic, cultural, and, inevitably, a military power. Just as the Cold War spawned the space race and put a man on the moon, much of today's quest for space is rooted in the desire to gain--and keep--the military advantage, the "higher ground"...With a space program deeply rooted in its military, America remains skeptical and wary of China's intentions...But if the Cold War taught us anything, it is that measured responses and tentative steps can open channels of communication and cooperation."[378]

Although the focus of this paper is cyberspace as a security domain, the vast majority of the Internet is civil, commercial and recreational in nature. Attacks in cyberspace are felt across commerce and industry, and non-military activities comprise the bulk of responsibilities and authorities. The public-private sphere, therefore, provides both a first line of defense, and necessary role in response actions. Addressing cyberspace from a purely security perspective is therefore misleading, unhelpful and insufficient for formulating recommendations.

While governments and institutions spawned the Internet and have worked to subsequently control and manage it, decentralized forces have revolutionized not only the

---

[377] Space Security 2008, Executive Summary, 7. August, 2008. http://www.spacesecurity.org/SSI2008ExecutiveSummary.pdf (accessed July 9, 2009).
[378] Anthony Duignan-Cabrera, "Special Report: Emerging China, Engaging China," *adAstra Online: The Magazine of the Space Society*, http://www.space.com/adastra/china_special_report.html (accessed December 7, 2009).

world of cyberspace, but through it the world we live in. The sheer magnitude of cyberspace, and the fact the bulk of communications over it are of a business or leisure nature, place departments or ministries with these jurisdictions, such as the U.S. Department of Commerce, in a much better position to pursue these agendas than military departments or security agencies. This has an important ramification for how state security efforts in cyberspace should be viewed.

While viewing cybersecurity operations as a form of irregular or hybrid warfare may be effective in the offense, lack of control over the domain dooms it to failure in the defense. A hybrid warfare approach offers no incentives for competitors to work together to realize joint gains. The recommendations are rather focused on moving the cyberspace domain out of the grey area between peace and war where irregular warfare thrives. Regardless of how individual states chose to advance their own security in cyberspace, this paper illuminates one immutable truth: a*ny plausible path to meaningful defense in cyberspace must include a significant element of international cooperation and regime formation.*

ADDITIONAL RECOMMENDATIONS

While the thrust of this research was policy-oriented, it was fundamentally an important study of regime theory. *The evaluation showed that regimes do matter as evidenced by other domains and Internet development to date.* Regimes can achieve deterrence through the proliferation of principles and norms. These venues also serve to advance technical and legal instruments in the process.

Assessing Security Regime Effectiveness

This study reinforces previous research showing security dilemma factors have been prominent in international efforts toward securing cyberspace:[379]

- Security issues in cyberspace involve greater competitiveness than do those related to economics and other non-security aspects of human behavior;
- Expansion in cyberspace as a defensive approach does threaten others, exacerbating the issue of relative gains, as opposed to protecting one's interests in non-security areas which does not necessarily harm or menace others;
- The stakes are higher in cyberspace security areas, since security is the most highly valued goal, is a prerequisite for so many things, such as economic development, and is unforgiving; and
- Detecting what others are doing and measuring one's own security in cyberspace is much more difficult than gaining such intelligence in other (e.g. economic or environmental) fields; creating much higher degrees of uncertainty and distrust in security-related areas.[380]

Criteria for security regime formation and maintenance informed assessments of recent attacks and the regime from a security perspective. Analysis of the land, air, sea, space, nuclear, trade and telecommunications domains, also inform an outstanding agenda item to apply environmental regime models on security regimes. The social-practice perspective proved both applicable, and most informative in assessing security aspects of the non-environmental regime of cyberspace.

Significantly, it was the social-practice perspective that provided opportunities to address the collective-action problem in cyberspace, largely through peaceful, constructive incentives with the occasional power to withhold them as opposed to technical defenses or threats of retaliation that we know are not working. The lack of state control over the domain, and corresponding lack of maturity of the regime, meant

---

[379] Marcus Franda, *Governing the Internet: the emergence of an international regime* (Lynne Rienner Publishers, Inc., 2001).
[380] Robert Jervis, "Security Regimes," in Stephen Krasner, *International Regimes* (Ithaca, New York: Cornell UP, 1983), 173-194.

that normative and political criteria were most helpful in this case. It was in fact recommendations resulting from an evaluation of behavioral changes not governed by utilitarian calculations that led to a very different utilitarian assessment than previous analyses. This should not be lost on the students of international cooperation, and more formal treatment of the models applied here on more traditional security regimes should be a priority for addressing the range of security-related collective-action problems. Similarly, decentralization powered by the Internet should be considered a significant intervening variable in updating past assessments.

The Concept of Maturity in International Security Regime Formation

The three-stage model of agenda formation, negotiation, and operationalization was applicable and informative for understanding the sources of the regime ineffectiveness and formulating specific recommendations tailored to the maturity level of the regime. Failing to consider the maturity level of the regime has led to any number of failed approaches, such as Russia's premature treaty proposal, and the recommendations presented inform more recent calls for an Internet arms control agreement.

Reevaluating previous assessments in other regimes informed by their maturity level may lead to both differing results and recommendations. This may present a fresh approach to organizational learning on the global scene that has previously proven but a lofty and elusive goal.

Final Thoughts

Finally, the analysis significantly informed the role of the nation-state as opposed to global society in securing cyberspace, and how it is viewed. The Internet has irrevocably decentralized numerous aspects of our lives. Just as the music industry witnessed a 25% loss of revenue over a single year resulting from the loss of control over information in the form of recordings, states should recognize a corresponding loss of control over the domain. *Conflict in cyberspace presents a direct challenge to the centuries-old state monopoly over legitimate conflict, and may represent a nail in the coffin of future state-controlled propaganda. The path to regaining some semblance of state control over cyberspace is in fact through global cooperation.*

The other side of the coin is that activities in cyberspace are an ideal test bed for evaluating issues of governance, and political mobilization. Here in the U.S., we need look no further than; for example, Sarah Palin's use of Facebook and Twitter to help mobilize the Tea Party movement for evidence of this. While most topics of international study occur over extended time periods, opaque exchanges, and often scant data, the Internet provides a transparent and data rich living laboratory to observe them, often at the moment they are occurring. Even focused study of discrete phenomena, such as cyberspace attack attribution, quickly translates into important evidence regarding deterrence theory, transnational relations, and global society. Use of cyberspace venues to document, analyze, and collaborate on such matters of human behaviors and global relations should continue to be encouraged.

REFERENCES

The African Nuclear-Weapon-Free Zone Treaty (Treaty of Pelindaba). December 16, 1993.

Agreement Between the Department of Defense of the United States of America and the Ministry of National Defense of the People's Republic of China on Establishing a Consultation Mechanism to Strengthen Military Maritime Security. January 19, 1998.

Agreement Between the Government of the United States of America and the Government of the Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas. May 25, 1972.

Agreement Between the United States of America and the Union of Soviet Socialist Republics on Notifications of Launches of Intercontinental Ballistic Missiles and Submarine-Launched Ballistic Missiles. May 31, 1988.

Agreement Between the United States of America and the Union of Soviet Socialist Republics on the Establishment of Nuclear Risk Reduction Centers. September 15, 1987.

Agreement Between the United States of America and the Union of Soviet Socialist Republics on the Prevention of Nuclear War. June 22, 1973.

Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialist Republics. September 30, 1971.

Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space. December, 1968.

Agreement Relating to the International Telecommunications Satellite Organization "INTELSAT." August 20, 1971.

Aimin, Liu, "The Characteristics of Informationized War." *Zhongguo Junshi Kexue (China Military Science),* August 1, 2001.

Aldrich, Rick, "Computer Network Defense Attribution: A Legal Perspective." *Defense-wide Information Assurance Program (DIAP)*, July 5, 2002.

Al-Duwairi, B. and T.E. Daniels. "Topology based packet marking, Computer Communications and Networks." *13th International Conference on Computer Communications and Networks*, 2004.

Anidjar, Patrick. "Cyber Threat is Constant Worry for United States." *Agence France Press*. May 13, 2000.

The Antarctic Treaty. June 23, 1961.

Arquilla, John. "Click, click...counting down to Cyber 9/11." *San Francisco Chronicle*, July 26, 2009, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/07/26/IN6K18S60M.DTL (accessed August 10, 2009).

Arquilla, John and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime and Militancy*. RAND, 2001.

Axelrod, Robert and Robert O. Keohane. "Achieving Cooperation Under Anarchy: Strategies and Institutions." In *Cooperation Under Anarchy*, edited by Kenneth Oye. Princeton, UP. 1985.

Baldwin, Robert E., and Anne O. Krueger, eds. *The Structure and Evolution of Recent U. S. Trade Policy*. Chicago: University of Chicago Press, 1984.

Baocun, Wang, "Information Warfare in the Kosovo Conflict." *Jiefangjun Bao,* May 25, 1999.

Brafman, Ori, and Rod Beckstrom. *The starfish and the spider: the unstoppable power of leaderless organizations*. London: Penguin Books, 2006.

Brenner, Susan. "At light speed: Attribution and response to cybercrime/terrorism/warfare." Journal of Criminal Law and Criminology, 2007.

Carr, Jeffrey. "Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats." *GreyLogic*, January 21, 2010.

Carr, Jeffrey. "Why John Arquilla's support for a Cyber Arms Control Treaty is naïve." *IntelFusion*, July 27, 2009. http://intelfusion.net/wordpress/?p=604 (accessed August 11, 2009).

Carr, Jeff, Andrew Conway, Billy Rios, Derek Plansky, Greg Walton, Jeremy Baldwin, Preston Werntz, and Rafal Rohozinski. "Project Grey Goose Phase I Report: Russia/Georgia Cyber War – Findings and Analysis." *GreyLogic*, October 17, 2008.

Carr, Jeff, Billy Rios, Derek Plansky, Greg Walton, Matt Devost, Ned Moran, Rebecca Givner-Forbes, Shannon Siverstein. "Project Grey Goose Phase II Report: The evolving state of cyber warfare." *GreyLogic*, March 20, 2009.

Center for Defense Information. "Analysis: Chinese Anti-Satellite Weapons Test in Space is Provocative and Irresponsible." January 22, 2007.

http://www.cdi.org/program/document.cfm?DocumentID=3800&from_page=../index.cfm (accessed July 9, 2009).

Center for Strategic and International Studies (CSIS). "Cyber Incidents Since 2006." http://csis.org/files/publication/090612_cyber_events_2006.pdf (accessed July 10, 2009).

Chilton, Kevin and Greg Weaver, "Waging Deterrence in the Twenty-First Century." *Strategic Studies Quarterly*, Spring 2009.

"China Has a Secret Plan." *StrategyWorld*, March 29, 2009. http://www.strategypage.com (accessed December 14, 2009).

"China Turns Unix Into A Weapon." *StrategyWorld,* May 14, 2009. http://www.strategypage.com (accessed December 14, 2009).

"China's Reserve Defense Might Is Markedly High-Tech." *Xinhua Hong Kong Service*, July 20, 1999.

"Chinese Bandits Can't Be Touched," *StrategyWorld,* July 28, 2009. http://www.strategypage.com (accessed December 14, 2009).

Claburn, Thomas. "Cyber Attack Code Starts Killing Infected PCs." *InformationWeek*, July 10, 2009. http://www.informationweek.com/news/showArticle.jhtml?articleID=218401559 (accessed August 11, 2009).

Clausing, Jeri. "New Internet Board Could Shake up Country Domains." *New York Times*, November 27, 1998.

The Comprehensive Nuclear Test Ban Treaty. September 10, 1996.

The Concise Oxford Dictionary of Politics. Oxford University Press, 2003.

Convention on International Liability for Damage Caused by Space Objects. September 1, 1972. http://www.islandone.org/Treaties/BH595.html (accessed July 2, 2009).

Convention on Registration of Objects Launched into Outer Space. January 14, 1975. http://www.islandone.org/Treaties/BH653.html, (accessed July 2, 2009).

Convention on the International Maritime Satellite Organization (INMARSAT). September 3, 1976. http://www.islandone.org/Treaties/BH688.html (accessed July 2, 2009).

Cornish, Paul. "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks." European Parliament, February 2, 2009.

http://www.europol.europa.eu/activities/committees/studies.do?language=EN (accessed August 6, 2009).

Council of Europe Convention on Cybercrime. Budapest, November 23, 2001. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (accessed July 7, 2009).

Council of Europe, http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp (accessed July 7, 2009).

"The Curious China Connection," *StrategyWorld,* July 1, 2008. http://www.strategypage.com (accessed December 14, 2009).

"Cyber Attacks Hit Government and Commercial Websites." *Foxreno.com*, July 9, 2009. http://www.foxreno.com/news/19999665/detail.html, (accessed August 11, 2009).

David, Leonard. "China's Anti-Satellite Test: Worrisome Debris Cloud Circles Earth." *adAstra Online: The Magazine of the Space Society*, February 2, 2007. http://www.space.com/news/070202_china_spacedebris.html (accessed July 9, 2009).

De Borchgrave, Arnaud. "Silent Cyberwar." *Washington Times*, February 19, 2009.

Denning, Dorothy E., "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, April 2009.

Dreyer, June Teufel. "The PLA and The Kosovo Conflict." *Strategic Studies Institute*, May, 2000.

Duignan-Cabrera, Anthony. "Special Report: Emerging China, Engaging China." *adAstra Online: The Magazine of the Space Society*, http://www.space.com/adastra/china_special_report.html (accessed December 7, 2009).

Elegant, Simon. "Cyberwarfare – The Issue China Won't Touch." *Time,* November 18, 2009. http://www.time.com/time/world/article/0,8599,1940009,00.html (accessed December 13, 2009).

Enfinger, Fl, B. Neslon, A. Phillips and C. Seuart. *Guide to computer forensics and investigation,* 3rd ed. Boston, Massachusetts, 2008.

"Estonia Convicts First "Cyber-War' Hacker." *AFP*, January 24, 2008.

"Estonia hit by 'Moscow cyber war.'" British Broadcasting Corporation (*BBC),* May 17, 2007. http://news.bbc.co.uk/2/hi/europe/6665145.stm (accessed July 12, 2009).

"Estonian DDoS – A Final Analysis." *Heise Security*, May 31, 2007.

European Union. "Seventh Framework Program (FP7)," http://cordis.europa.eu/fp7/dc/index.cfm (accessed March 1, 2010).

"Europeans: U.S. Should Give Up Control of the Internet." *Fox News*, May 4, 2009. http://www.foxnews.com/story/0,2933,518808,00.html (accessed September 7, 2009).

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs*, Science and Technology, Winter/Spring (2008): 121-126. http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf.

Federal Trade Commission, "OECD Security," August 23, 2002. http://www.ftc.gov/opa/2002/08/oecdsecurity.shtm (accessed July 7, 2009).

Federation of American Scientists. "Military Space Programs, Nuclear Detection System." http://www.fas.org/spp/military/program/masint/nds.htm, (accessed March 28, 2009).

Federation of American Scientists. "Project Jennifer: Hughes' Glomar Explorer." http://www.fas.org/irp/program/collect/jennifer.htm (accessed July 1, 2009).

Federation of American Scientists. "Weapons of Mass Destruction: Arms Control Agreements." http://www.fas.org/nuke/control/index.html (accessed June 30, 2009).

Ford, Peter. "New Cooperation in Taming the Wild Web." *Christian Science Monitor*, May 18, 2000.

Franda, Marcus. *Governing the Internet: the emergence of an international regime*. Lynne Rienner Publishers, Inc., 2001.

George, Alexander, and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. Columbia UP, 1974.

Gorman, Siobhan and Evan Ramstad. "Cyber Blitz his U.S., Korea." *Wall Street Journal*, July 9, 2009.http://online.wsj.com/article/SB124701806176209691.html (accessed July 10, 2009).

"Governments hit by cyber attack." *BBC*, July 8, 2009. http://news.bbc.co.uk/1/hi/technology/8139821.stm (accessed July 12, 2009).

Granite Island Group. "Technical Surveillance Countermeasures," http://www.tscm.com/iff.pdf (accessed July 2, 2009).

Gregorio-de Souza, Ian, and Vincent H. Berk, Annarita Giani, George Bakos, Marion Bates, George Cybenko, and Doug Madory. "Detection of Complex Cyber Attacks," *Thayer School of Engineering*. Hanover, NH: Dartmouth College, 2006. http://www.ists.dartmouth.edu/library/245.pdf.

GreyLogic, http://greylogic.us/ (accessed August 10, 2007).

Habiger, Eugene E. "Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach." *Cybersecurity Institute*, February 1, 2010.

Hsu, Brian. *Taipei Times* (Internet Version), December 7, 2001.

Hunker, Jeffrey, Bob Hutchinson, and Jonathon Margulies. "Role and Challenges for Sufficient Cyber-Attack Attribution." January, 2008. http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf.

International Civil Aviation Organization. "History." http://www.icao.int//cgi/goto_m.pl?icao/en/hist/ (accessed July 2, 2009).

International Telecommunications Union. "Building the Information Society: a global challenge in the new Millennium." *World Summit on the Information Society Declaration of Principles*, December 12, 2003. http://www.itu.int/wsis/docs/geneva/official/dop.html (accessed March 1, 2010).

International Telecommunications Union. "World Summit on the Information Society," http://www.itu.int/wsis (accessed March 1, 2010).

International Telecommunications Union. "Global Cybersecurity Agenda (GCA): Framework for International Cooperation in Cybersecurity," 2007.

International Telecommunications Union (ITU). "Mission," http://www.itu.int/net/about/mission.aspx (accessed August 6, 2009).

Internet Corporation for Assigned Names and Numbers (ICANN), "Country Code Top Level Domain Agreements." http://www.icann.org/en/cctlds/agreements.html (accessed July 6, 2009).

Internet Corporation for Assigned Names and Numbers (ICANN). "DNS Distributed Denial of Service (DDoS) Attacks." *Security and Stability Advisory Committee (SSAC)*, Advisory SAC008, March 31, 2006. http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf (accessed July 10, 2009).

Internet Governance Forum. www.intgovforum.org/ (accessed March 1, 2010).

"The Internet Is Tamed In China," *StrategyWorld,* July 9, 2009. http://www.strategypage.com (accessed December 14, 2009).

Jervis, Robert. "Security Regimes." In *International Regimes*, edited by Stephen Krasner. Ithaca, NY: Cornell UP, 1983.

Jiyeon, Lee. "Cyberattack rocks South Korea." *GlobalPost*, July 11, 2009. http://www.globalpost.com/dispatch/south-korea/090710/cyberattacks, (accessed August 11, 2009).

Jung-a, Song. "Pyongyang blamed as cyber attack hits S Korea." *Financial Times*, July 9, 2009. http://www.ft.com/cms/s/0/61bc6d22-6c1f-11de-9320-00144feabdc0.html (accessed August 11, 2009).

Kabay, M.E. "Chinese information warfare capabilities." *Networkworld*, April 7, 2009. http://www.networkworld.com/newsletters (accessed December 14, 2009).

Kabay, M.E. *US DoD Annual Estimates of Information Warfare Capabilities and Commitment of the PRC 2002-2009.* Northfield, VT: Norwich University Press, 2009, 3.

Kaufman, Marc and Dafna Linzer. "China Criticized for Anti-Satellite Missile Test," *Washington Post*, January 19, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801029.html (accessed July 9, 2009).

Keohane, Robert. "The Theory of Hegemonic Stability and Changes in International Economic Regimes, 1967-1977." In *Changes in the International System*, edited by Ole R. Holsti, Randolph M. Siverson, and Alexander L. George. Boulder, CO: Westview Publishing, 1980.

Keohane, Robert and Joseph Nye. *Power and Interdependence*, 3rd ed. Harrisonburg: R. R. Donnelley and Sons, 2001.

Kim, Kwang-Tae. "S. Korea analyzes computers used in cyberattacks." *Associated Press*, July 12, 2009. http://www.google.com/hostednews/ap/article/ALeqM5jO5PtkM_1FjwMZjh3LS74g26yiUQD99CRCO80 (accessed August 11, 2009).

Kissinger, Henry. *Diplomacy*. New York: Touchstone, 1994.

"Korean agency accuses BKIS of violating local and int'l law." *Bach Khoa Internetwork Security Centre (BKIS),* July 20, 2009. http://english.vietnamnet.vn/reports/2009/07/859068/ (accessed January 6, 2010).

Kramer, Franklin D. *Statement before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats*. Washington, DC: U.S. Government Printing Office, 1 April 2008.

Krasner, Stephen D. *International Regimes*. Ithaca, NY: Cornell UP, 1991.

"Kremlin Loyalist Says Launched Estonia Cyberattack." *Radio Free Europe Radio Liberty,* March 12, 2009. http://www.rferl.org/Content/Kremlin_Loyalist_Says_Launched_Estonia_Cyberattack/1508923.html (accessed March 26, 2009).

Kuehl, Dan. "From Cyberspace to Cyberpower: Defining the Problem." 2009. http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc (accessed December 19, 2009).

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press, 1962.

"The Kyrgyzstan Cyber Attack That No One Is Talking About." *IntelFusion*, January 21, 2009. http://intelfusion.net/wordpress/?p=509 (accessed March 26, 2009).

"Kyrgyz Opposition Denied Use of Parliament Press Center." *Radio Free Europe Radio Liberty*, January 20, 2009. http://www.rferl.org/Content/Kyrgyz_Opposition_Denied_Use_Of_Parliament_Press_Center/1372339.html (accessed March 26, 2009).

LaFraniere, Sharon. "China Imposes New Internet Controls." *New York Times*, December 18, 2009. http://www.nytimes.com (accessed December 19, 2009).

Landler, Mark and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." *The New York Times*, May 29, 2007.

Lemon, Sumner. "China defends right to censor Internet," *IDG New Service*, February 15, 2006. http://www.networkworld.com/news/2006 (accessed December 14, 2009).

Lemons, Robert. "Cyber Attacks Disrupt Kyrgyzstan's Networks." *SecurityFocus*, January 30, 2009. http://www.securityfocus.com/brief/896, (accessed August 14, 2009).

Lewis, James A. "Computer Espionage, Titan Rain and China." *Center for Strategic and International Studies, Technology and Public Policy Program*, December, 2005.

Lewis, Jeffrey. "Engage China, Engage the World." *adAstra Online: The Magazine of the Space Society*, http://www.space.com/adastra/china_engagement_0505.html, (accessed December 7, 2009).

Lianshui, Wang, Ma Jingcheng, and yan Jianhong. "Comparison of Psychological Warfare between China and the West." *Zhongguo Junshil Kexue (China Military Science)*, Number 6, 2000.

Lin, Chong-Pin. "Info Warfare Latecomer." *Defense News*, April 12, 1999.

Lipson, Howard F. "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues." Carnegie-Mellon University, November, 2002.

Manimaran, G., and M. Muthuprasanna. "Distributed Divide-and-Conquer Techniques for Effective DDoS Attack Defenses." *The 28th International Conference on Distributed Computing Systems,* 2008.

Manzo, Louis A. "Morality in War Fighting and Strategic Bombing in World War II." *Air Power History*, vol. 39, no. 3, Fall 1992.

Markoff John. "2 China Schools Said to Be tied to Online Attack." *New York Times*, February 18, 2010. http://www.nytimes.com/2010/02/19/technology/19china.html (accessed February 20, 2010).

Markoff, John. "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea." *New York Times*, July 9, 2009. http://www.nytimes.com/2009/07/10/technology/10cyber.html, (accessed August 11, 2009).

Markoff, John and Andrew Kramer. "In Shift, U.S. Talks to Russia on Internet Security." *New York Times*, December 12, 2009.

Markoff, John, David E. Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *New York Times*, January 26, 2010.

Memorandum of Agreement Between The United States of America and the Russian Federation on the Establishment of a Joint Center for the Exchange of Data From Early Warning Systems and Notifications of Missile Launches. June 4, 2000.

Memorandum of Understanding Between the United States of America and Union of Soviet Socialist Republics Regarding the Establishment of a Direct Communications Link. June 20, 1963.

Mills, Elinor. "Botnet worm in DOS attacks could wipe data out on infected PCs." *CNET News*, July 10, 2009. http://news.cnet.com/8301-1009_3-10284281-83.html (accessed January 6, 2010).

Mills, Elinor. "Researchers: Attacks on U.S., Korea sites came from U.K." *CNET News*, July 14, 2009. http://news.cnet.com/security/?keyword=Bkis (accessed January 6, 2010).

Mingrang, Li. "Develop the Advantage of People's War under the conditions of Innovation and Informatization." *Guofang*, November 15, 2003.

Mitchell, Ronald, Moira L. McConnell, Alexei Roginko, and Ann Barrett. "International Vessel-Source Oil Production." In *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms,* edited by Oran Young. MIT, 1999.

"Multinational Task Force Targets Pirates." *American Forces Press Service*. January 8, 2009. http://www.defenselink.mil/news/newsarticle.aspx?id=52586 (accessed July 1, 2009).

Mulvenon, James. "The PLA and Information Warfare." In *The People's Liberation Army in the Information Age,* edited by James Mulvenon and Richard H. Yang. Washington, D.C., 1999.

Munton, Don, Marvin Soroos, Elena Nikitina, and Marc A. Levy. "Acid Rain in Europe and North America." In *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms*, edited by Oran Young. MIT, 1999.

Nash, Emma. "How vulnerable are we to a cyber attack?" *Computing,* 15 April 2004. http://infomaticsonline.co.uk/computing/features/2072400/vulnerable-cyber-attack.

National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security. October, 2005. http://www.virginia.edu/colp/pdf/NSMS-National-Plan-to-Achieve-Maritime-Domain-Awareness.pdf (accessed July 1, 2009).

North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Center of Excellence (CCD-COE). http://www.ccdcoe.org/72.html (accessed August 6, 2009).

North Atlantic Treaty Organization (NATO). "NATO opens new centre of excellence on cyber defence." May 14, 2008. http://www.nato.int/docu/update/2008/05-may/e0514a.html (accessed March 1, 2010).

Norton-Taylor, Richard. "Titan Rain – how Chinese hackers targeted Whitehall," *The Guardian*, September 5, 2007. http://www.guardian.co.uk/technology/2007/sep/04/news.internet (accessed December 14, 2009).

Nye, Joseph S. Jr. *Nuclear Ethics*. New York, Free Press. 1986.

O'Shea, Kevin. "Cyberattack Investigative Tools and Technologies presentation." Dartmouth University, May 7, 2003. http://www.ists.dartmouth.edu/library/107.pdf.

Oye, Kenneth. *Cooperation Under Anarchy*. Princeton UP. 1985.

Pufeng, Wang. "The Challenge of Information Warfare," *China Military Science*. 1995.

Qixin, Xi and Zhao Yongxin. "Advancing toward High Technology—High Ranking Military Cadres Attending a Hi-Tech Training Course." *Xinhua Domestic Service*, June 13, 1999.

Quishi (Communist Party's Central Committee magazine). December 1, 2009.

Raphael, Jr. "Fighter Jet Hack Far From First Government Breach." *PC World*, April 21, 2009. http://www.networkworld.com/news/2009/ 042109-fighter-jet-hack-far-from.html?ry=gs (accessed December 13, 2009).

Rinaldi, Steven M. "Occasional Paper 33, Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security." *USAF Institute for National Security Studies (INSS)*. Colorado Springs, CO: USAF Academy, May, 2000.

Ruixue, Bai. "Chinese Military Delgates Say War in the Information Age Still Requires the Support of People's War." *Xinhua Asia-Pacific Service*, March 12, 2003.

"Russian Business Network." http://rbnexploit.com/ (accessed March 1, 2010).

Schachtman, Noah. "Kremlin Kids: We Launched the Estonian Cyber War." *Wired.com*, March 11, 2009. http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ (accessed July 12, 2009).

"Senate Bill Would Give President Emergency Control of Internet." *Fox News*, August 28, 2009. http://www.foxnews.com/politics/2009/08/28/senate-president-emergency-control-internet/ (accessed September 7, 2009).

"Sergei Markov says he knows who started the Estonia cyber war," *IntelFusion*, March 6, 2009. http://intelfusion.net/wordpress/?p=544 (accessed August 11, 2009).

Shadowserver. http://www.shadowserver.org/wiki.

Shaw, Malcom N. *International Law*, 4th ed. Cambridge UP. 1997.

Solomon, Richard. *Chinese Negotiating Behavior, Pursuing Interests Through 'Old Friends.'* Washington, D.C.: USIP Press, 1999.

South Pacific Nuclear Free Zone Treaty (Treaty of Raratonga). August 6, 1985.

"Space Security 2008," *SpaceSecurity.org*, August, 2008. http://www.spacesecurity.org/SSI2008ExecutiveSummary.pdf (accessed July 9, 2009).

Spang-Hanssen, Henrik. *Cyberspace & International Law on Jurisdiction: Possibilities of Dividing Cyberspace into Jurisdictions with help of Filters and Firewall Software*. Copenhagen: DJØF Publishing, 2004.

Stokke, Olav Schram, Lee G. Anderson, and Natalia Mirovitskaya. "The Barents Sea Fisheries." In *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms* edited by Oran Young. MIT, 1999.

Stoll, Cliff. *The Cuckoo's Egg: Inside the World of Computer Espionage*. New York, NY: Pocket Books, 1990.

Sud, Hari. "Chinese and U.S. lead information warfare." *UPIASIA*, July 17, 2009. http://www.upiasia.com/Security (accessed December 14, 2009).

Sudworth, John. "New 'cyber attacks' hit S Korea." *BBC News*, July 9, 2009. http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm (accessed August 11, 2009).

Sudworth, John. "Official: S. Korea web sites under renewed attack." *Associated Press,* July 9, 2009. http://www.google.com/hostednews/ap/article/ (Accessed August 11, 2009).

Tang, Y. and T.E. Daniels. "A Simple framework for distributed forensics." paper presented at the *Second International Workshop on Security in Distributed Computing Systems*. 2005.

"Ten Ways the Chinese Internet is Different From Yours." *Networkworld*, 2008. http://www.networkworld.com/slideshows/2008 (accessed December 14, 2009).

Thomas, Timothy L. *Dragon Bytes, Chinese Information-War Theory and Practice*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

Thomas, Timothy. *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy*. Fort Leavenworth, KS: Foreign Military Studies Office, 2007.

Thornburgh, Nathan. "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)." *TIME*, August 29, 2005. http://www.time.com/time/magazine/article/0,9171,1098961,00.html (accessed December 14, 2009).

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Ann-Maria Talihärm, and Liis Vihul. "Cyber Attacks Against Georgia: Legal Lessons Identified." *NATO CCDCOE*. Tallinn, Estonia: August, 2008.

"Tracking GhostNet: Investigating a Cyber Espionage Network." *Information Warfare Monitor*, March 29, 2009.

Treaty Banning Nuclear Weapon Test in the Atmosphere, in Outer Space and Underwater. August 5, 1963.

Treaty for the Prohibition of Nuclear Weapons In Latin America (Treaty of Tlatelco). April 22, 1968.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies. October 10, 1967. http://www.islandone.org/Treaties/ (accessed July 2, 2009).

Treaty on the Non-Proliferation of Nuclear Weapons. July 1, 1968.

Treaty on the Southeast Asia Nuclear-Weapon-Free Zone (Treaty of Bangkok). December 15, 1995.

"Tunis Commitment." *World Summit on the Information Society (WSIS)*. November 18, 2005.

United Nations Convention on Law of the Sea (UNCLOS). 1982. http://www.eoearth.org/article/United_Nations_Convention_on_Law_of_the_Sea_(UNCLOS),_1982 (accessed July 1, 2009).

United Nations Educational, Scientific and Cultural Organization (UNESCO) Declaration of Guiding Principles on the Use of Satellite Broadcasting. 1972. unesdoc.unesco.org/images/0000/000021/002136eb.pdf (accessed March 1, 2010).

United Nations General Assembly Resolution 37/92, Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting. 1983. www.un.org/documents/ga/res/37/a37r092.htm (accessed March 1, 2010).

United Nations Office of Legal Affairs, Division for Ocean Affairs and the Law of the Sea. *Digest of International Cases on the Law of the Sea*. 2007. New York, NY: UN Press, 2007.

United States Department of Defense. *Annual Report on the Military Power of the People's Republic of China 2002*. 2002.

http://www.defenselink.mil/news/Jul2002/d20020712china.pdf (accessed December 15, 2009).

United States Department of Defense. *Annual Report on the Military Power of the People's Republic of China 2009*. 2009. http://www.defense.gov (accessed December 15, 2009).

United States Department of State. "U.S. Outlines Priorities for World Summit on the Information Society." December 3, 2003. http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2003&m=December&x=20031203163730retropc0.0570032&t=usinfo/wf-latest.html (accessed August 13, 2009).

United States Senate Special Committee on the Year 2000 Technology Problem. "Investigating the Year 2000 Problem: The 100 Day Report." September 22, 1999.

United States Senate Special Committee on the Year 2000 Technology Problem. "Statement of Bruce W. McConnell, Director, International Y2K Cooperation Center." July 29, 1999.

United States Senate Special Committee on the Year 2000 Technology Problem. "Y2K Aftermath – Crisis Averted." Final Committee Report, February 29, 2000.

United States Strategic Command. "Space Control and Space Surveillance Fact Sheet." February 25, 2008. http://www.stratcom.mil/files/STRATCOM_Space_and%20Control_Fact_Sheet-25_Feb_08.doc (accessed July 2, 2009).

University of Minnesota. "International Y2K Cooperation Center Records (CBI 153)." *Charles Babbage Institute*. http://special.lib.umn.edu/findaid/xml/cbi00153.xml (accessed July 3, 2009).

"U.S. Military Grapples With Cyber Warfare Rules." *Reuters,* November 8, 1999. http://www.hartford-hwp.com/archives/27a/021.html, (accessed March 27, 2009).

"US Warned of China 'cyber-spying,'" *BBC*, November 20, 2008. http://news.bbc.co.uk/2/hi/asia-pacific/7740483.stm (accessed March 27, 2009).

Vamosi, Robert. "The Estonia cyberwar, One year later." *CNET News,* http://news.cnet.com/8301-10789_3-9948720-57.html (accessed July 12, 2009).

Vijayan, Jaikumar. "Internet Warfare: Is the focus on the wrong things?" April 27, 2009. http://www.networkworld.com/news/2009 (accessed December 14, 2009).

Waltz, Kenneth and Scott Sagan. *The Spread of Nuclear Weapons: A Debate.* New York: W.W. Norton, 2002.

Weiguang, Shen. "World War." In *The Third World War—Total Information Warfare.* Beijing: Xinhua Publishing House, January, 2000.

Wilkison, Roger. "Voice of America Correspondent Report," Federation of American Scientists, April 29, 1998. http://www.fas.org/news/china/1998/980429-prc.htm (accessed June 29, 2009).

Williams, Martyn. "UK, not North Korea, source of DDOS attacks, researcher says." *IDG News Service*, July 14, 2009. http://www.networkworld.com/news/2009/071409-uk-not-north-korea-source.html?ap1=rcb (accessed August 11, 2009).

World Trade Organization, "Building the Information Society: a global challenge in the new Millennium." *World Summit on the Information Society (WSIS) Declaration of Principles,* December 12, 2003. http://www.wto.org/english/docs_e/legal_e/28-dsu_e.htm#7 (accessed July 3, 2009).

Wozniak, Jeff and Samuel Liles. "Political and Technical Roadblocks to Cyber Attack Attribution." *IO Journal*, April, 2009.

Xiaoyan, Xu. "Establishing an Information Resource Mobilization Mechanism with Chinese Characteristics," *Zhongguo Junshi Kexue (China Military Science),* October 20, 2000.

Xuangqing, Li, Chai Yongzhong, and Bao Guojun. "Directly Facing the Roaring Tide of New Institutional Changes of the Military around the World—Dialogue with Experts and Scholars form the Academy of Military Sciences (Internet version)." July 16, 2003.

Yao Yunzhu. "Federal Republic of Yugoslavia Crisis Shows Need to Strenthen PLA: Discussion of the Kosovo Crisis Among Experts and Scholars," *Jiefangjun Bao*, April 13, 1999.

Yasman, Victor. "Monument Dispute with Estonia Gets Dirty." *Radio Free Europe Radio Liberty*, May 8, 2007. http://www.rferl.org/content/Article/1347550.html (accessed August 11, 2009).

Yinnina, Le, in Huang Youfu, Zhang Bibo, and Hang Song, "New subjects of Study Brought about by Infomration War—Summary of Army Command Academy Seminar on 'Confrontation of Command on Information Battlefield." *Jiefangjun Bao (Liberation Army Daily),* translated and reported in FBIS-CHI-97-354, November 11, 1997.

Yoshihara, Toshi. "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" *Strategic Studies Institute*, Carlisle Barracks: U.S. Army War College, November, 2001.

Youcai, Ye and Zhou Wenrui. "Building a High-quality Militia Information Technology Element," *Guofong*, September 15, 2003.

Young, Oran R. *Creating Regimes: Arctic Accords and International Governance*. Ithaca, NY: Cornell UP, 1998.

Young, Oran. "Regime dynamics: the rise and fall of international regimes." In *International Regimes,* edited by Stephen D. Krasner, Ithaca, NY: Cornell UP, 1991.

Young, Oran. *The Effectiveness of International Regimes: Causal Connections and Behavioral Mechanisms*. MIT. 1999.

Yuankui, Li, Wang Yanzheng and Yang Xiaoli. "On Defense in Modern Psychological Warfare." *Zhongguo Junshi Kexue (China Military Science)*, Number 6, 2000.

Zetter, Kim. "Lazy Hacker and Little Worm Set Off Cyberwar Frenzy." *Wired*, July 8, 2009. http://www.wired.com/threatlevel/2009/07/mydoom/, (accessed August 11, 2009).

Zetter, Kim. "Google Hack Attack Was Ultra Sophisticated, New Details Show." *Wired*, January 14, 2010. http://www.wired.com/threatlevel/2010/01/operation-aurora (accessed February 20, 2010).

APPENDIX A

ACRONYM LIST

Acronym	Definition
ACT	Allied Command Transformation
APC	Association for Progressive Communications
APCERT	Asia-Pacific CERT
ASAT	anti-satellite
BKIS	Bach Khoa Internetwork Security Centre
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CCDOE	Cooperative Cyber Defence Center of Excellence
ccTLD	country code top level domains
CERN	Centre Européen pour la Recherche Nucléaire
CERT	Computer Emergency Response Team
CERT/CC	CERT® Coordination Center
CERT-EE	Estonian CERT
CERT-FR	CERT France
CERT-PL	CERT Poland
COE	Council of Europe
CONOPS	Concept of Operations
CSIS	Center for Strategic and International Studies
CTNSP	Center for Technical and National Security Policy
DARPA	Defense Advanced Research Projects Agency
DDoS	distributed denial-of-service
DHS	Department of Homeland Security
DOD	Department of Defense
DoS	denial-of-service
DSB	Dispute Settlement Body
DSP	Defense Support Program
DSU	Dispute Settlement Understanding
ESCAPE	Electronically Secure Collaboration Application Platform for Experts
EW	electronic warfare
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FIRST	Forum of Incident Response and Security Teams

FMSO	Foreign Military Studies Office
FOIA	Freedom of Information Act
FP7	Seventh Framework Programme
FRY	Federal Republic of Yugoslavia
GAO	Government Accountability Office
GATT	General Agreement on Tariffs and Trade
GCA	Global Cyber Agenda
GEO	geosynchronous earth orbit
GISC	Global Innovation and Strategy Center
GRC	Global Response Centre
HAKR	Hacker Alias Knowledge Repository
HML	Hardware Markup Language
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board
ICAO	International Civil Aviation Organization
ICAN	International Commission for Air Navigation
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	information coordination center
ICJ	International Court of Justice
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IFF	Identification of Friend or Foe
IMF	International Monetary Fund
IMPACT	International Multilateral Partnership Against Cyber-Threats
INMARSAT	International Maritime Satellite
INSS	Institute for National Security Studies
INTELSAT	International Telecommunications Satellite Organization
INW	information-network warfare
IO/IW	information operations/information warfare
IP	Internet protocol
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Providers
IT	information technology
ITO	International Trade Organization
ITU	International Telecommunications Union
IW	information warfare
IWM	Information Warfare Monitor

IY2KCC	International Y2K Cooperation Center
JFCC-SPACE	USSTRATCOM Joint Functional Component Command for Space
JSpOC	Joint Space Operations Center
KrCERT	Korea Computer Emergency Response Team
LEO	low-earth orbit
LRTAP	Long-Range Transboundary Air Pollution
MDA	Maritime Domain Awareness
NAFTA	North American Free Trade Agreement
NEWS	Network Early Warning System
NORAD	North American Air Defense
NOTAMS	Notices to Airmen and Mariners
NRRC	Nuclear Risk Reduction Centers
NSC	National Security Council
NTBs	nontariff barriers
OECD	Organization for Economic Cooperation and Development
ONI	OpenNet Initiative
OSINT	open source intelligence
P2P	peer-to-peer
PICAO	Provisional International Civil Aviation Organization
PLA	People's Liberation Army
RBN	Russian Business Network
RHU	Red Hackers Union
ROE	rules of engagement
SQL	Structured Query Language
SSN	Space Surveillance Network
SSAC	ICANN Security and Stability Advisory Committee
TCP/IP	Transmission Control Protocol/Internetwork Protocol
UNCLOS	UN Convention on the Law of the Sea
UNESCO	United Nations Educational, Scientific and Cultural Organization
UPM	United Peoples Movement
URL	Universal Resource Locator
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command's
VNCERT	Vietnamese CERT
VoIP	voice over IP
VPN	virtual private network
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization

WSIS	World Summit on the Information Society
WTO	World Trade Organization
XML	Extensible Markup Language
Y2K	year 2000

APPENDIX B

GLOSSARY OF KEY TERMS

Term	Definition
botnet	Controlled network of hijacked computers
collective-action problem	Situation in which the uncoordinated actions of each player may not result in the best outcome each can achieve
computer confrontation operations	Chinese term translated as computer network attack in U.S. terminology
cyber espionage	The act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using illegal exploitation methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware
cyber riot	Form of virtual civil disorder characterized by disorganized groups lashing out in a sudden and intense rash of cyber attacks against people or property; typically chaotic, exhibiting herd behavior
cyber terrorism	1) The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives; or to intimidate any person in furtherance of such objectives; 2) Deployments of disruption attacks by known terrorist organizations against information systems for the primary purpose of creating alarm and panic
cyber warfare	The conduct of military operations by virtual means
cybercrime	The use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order
cyberspace	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers
cyberspace attack (cyber attack)	1) Malicious activity targeting the computer telecommunications networks of critical infrastructures, such as power systems traffic control systems or financial systems; 2) Computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it
decision-making procedures	Prevailing practices for making and implementing collective choice

deterrence	The persuasion of one's opponent that the costs or risks of a given course of action outweigh the benefits
denial of service attack	An attempt to make a computer resource unavailable to its intended users, generally consisting of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely
hybrid organization	Body that operates in both the public and private sectors, simultaneously fulfilling public duties and developing commercial market activities; deliberately mixing organizational forms in an attempt to blend the advantages of two or more different types or because the organization changing; e.g. including both decentralized aspects more attuned to the decentralized nature of cyberspace, as well as traditional centralized features that allow for the provision of security, authority, and accountability.
informationized force	Chinese term translated as net-enabled force in U.S. terminology
peer-to-peer command and control	Distributed command structure capable of spreading to computers around the world
norms	Standards of behavior defined in terms of rights and obligations
principles	Beliefs of fact, causation, and rectitude
regime	1)Implicit or explicit principles, norms, rules and decision-making procedures around which actor expectations converge in a given issue area; 2) Social institutions governing the actions of those interested in specifiable activities, (or accepted sets of activities); recognized patterns of behavior or practice around which expectations converge
rules	Specific prescriptions or proscriptions for action
thought experiment	Counterfactual analysis

VITA

Jeff McNeil
Graduate Programs in International Studies
Batten Arts and Letters Bldg., Room 7045
Old Dominion University
Norfolk, VA 23529

Jeff McNeil is a Principal Investigator with Scientific Research Corporation under contract to the Office of the Secretary of Defense, and a Lieutenant Colonel in the United States Marine Corps Reserve. He holds a Bachelor's Degree in Physics from the University of Nebraska-Lincoln, and a Master of Arts in International Studies from Old Dominion University.

Jeff previously developed targeting doctrine and curriculum as one of the original instructors for the Joint Targeting School in Dam Neck, Virginia, guest lectured at numerous service schools including the Joint Forces Staff College, and delivered the keynote address on behalf of the Joint Staff Director of Intelligence (J2) to the Aug 2002 DoD Military Sensing and Data Fusion Information Analysis Center (SENSIAC). He was the primary author of Joint Publication 3-60, Joint Targeting (1999) and the March 2001 OSD Net Assessment Study, "Predicting Intentions – Preventing Strategic and Operational Surprise: Behavior Moderating Factors."

Jeff's more recent assignments include Intelligence Plans and Operations Officer for U.S. Marine Forces Pacific and Central Commands, and Deputy Director for International Engagement at the U.S. Joint Futures Lab in Suffolk, Virginia. He is currently assigned to the U.S. Strategic Command Global Innovation and Strategy Center.