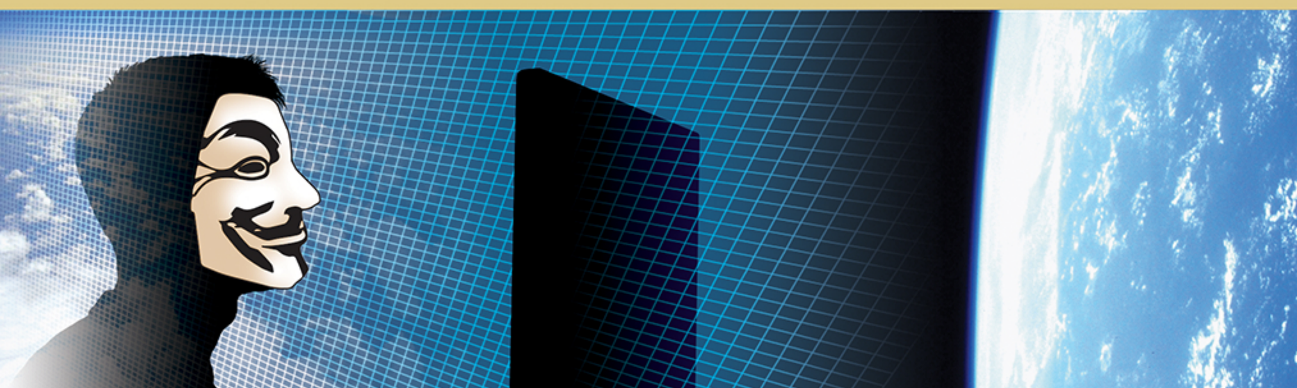
Perspectives on Cyber Power

CPP-1

Strategies for Resolving the Cyber Attribution Challenge

Panayotis A. Yannakogeorgos



Air Force Research Institute Papers

AIR UNIVERSITY

Air Force Research Institute
Perspectives on Cyber Power

Strategies for Resolving the Cyber Attribution Challenge

PANAYOTIS A. YANNAKOGEORGOS

CPP-1

Air University Press
Maxwell Air Force Base, Alabama 36112–6026

Library of Congress Cataloging-in-Publication Data

Yannakogeorgos, Panayotis A.
Strategies for resolving the cyber attribution challenge / Panayotis A. Yannakogeorgos.
pages cm. — (Air Force Research Institute perspectives on cyber power, ISSN 2329-5821 ; cp-1)
Includes bibliographical references.
ISBN 978-1-58566-226-5 (paper back : alk. paper)
1. Information warfare. 2. Cyberterrorism—Prevention. 3. Cyberspace—Security measures. 4. Computer security—Government policy—United States. 5. Computer crimes—Prevention—Government policy. I. Air University (U.S.). Air Force Research Institute. II. Title.
U163.Y36 2013
355.4—dc23

2013035305

First Printing December 2013
Second Printing February 2016
Third Printing May 2016

Air Force Research Institute Perspectives on Cyber Power

We live in a world where global efforts to provide access to cyber resources and the battles for control of cyberspace are intensifying. In this series, leading international experts explore key topics on cyber disputes and collaboration. Written by practitioners and renowned scholars who are leaders in their fields, the publications provide original and accessible overviews of subjects about cyber power, conflict, and cooperation.

As a venue for dialogue and study about cyber power and its relationship to national security, military operations, economic policy, and other strategic issues, this series aims to provide essential reading for senior military leaders, professional military education students, and interagency, academic, and private-sector partners. These intellectually rigorous studies draw on a range of contemporary examples and contextualize their subjects within the broader defense and diplomacy landscapes.

These and other Air Force Research Institute studies are available via the AU Press website at http://aupress.au.af.mil/papers.asp. Please submit comments to afri.public@maxwell.af.mil

This paper is dedicated to my parents

Everyone is to consider the same person a friend or enemy as the city-state does, and if someone should make peace or war with certain parties in private, apart from the community, the penalty is to be death. . . . If some part of the city-state should by itself make peace or war with certain parties, the Generals are to bring those responsible for this action into court, and the judicial penalty for someone who is convicted shall be death.

—Plato, *Laws*: Book I, 630e–631a

Contents

Illustrations

Figures

Tables

Foreword

Today's complex and interdependent global economy relies heavily on an Internet infrastructure that is fraught with risks, threats, and hazards the average computer user or small- and medium-sized enterprise is unaware of and unprepared for. Confidence in the ability to effectively, efficiently, and securely conduct commerce and business processes over the Internet and through emerging mobile device applications is vital and fundamental for vibrant and stable economies around the globe. The world faces unprecedented risks across the Internet in what has become known as "the twenty-first century's Wild West," where attacks on computer systems and networks are generally conducted with complete anonymity and immunity for those perpetrating these acts.

The generally insecure nature of our interconnected environment can be traced to several factors:

1. For over 40 years universities have taught courses on designing and writing computer coding. When these college-level courses were first established, we lived in a world where no one ever imagined the interconnectivity that would evolve and become so central to our lives today. Computer systems were stand-alone and not networked to third parties that performed various services or support. As the interconnectivity of the Internet evolved, few people realized the inherent flaws and lack of sound security measures in legacy systems or new systems that were developed utilizing legacy-style programming methodologies.

2. Legacy computer hardware, middleware, and network designers also overlooked or outright ignored building in security measures, as they were viewed as negatively affecting performance, output, or throughput and were generally deemed unnecessary.

3. Both software developers and hardware manufacturers established an environment from the beginning where they accepted no liability or responsibility for any loss, delay, disruption, or other action that might affect the purchaser/user community, whether caused directly or

indirectly by the systems, hardware, or software supplied. This "use at your own risk" disclaimer to liability has manifested itself into a patch management nightmare. Every new release of software or hardware is regularly followed with periodic security patches. These patches deal with flaws that the rush-to-market mentality of the manufacturers and producers created by failing to take a duty-of-care philosophy in product design and delivery. Early on in the evolution of software, hardware, and networks, people became accustomed to computer bugs and other design flaws that they simply accepted as the norm. Rarely has a single industry benefitted from such a desensitized consumer population, which has allowed the producers and manufacturers to skirt responsibility and liability for the flawed products and systems they produce.

4. Individuals, corporate executives, and elected officials have very little understanding of the scope of the risks and threats they face through computer systems and networks that are ultimately linked through the Internet today. To further highlight this point, a joint study on cyber-based crime conducted by Verizon and the US Secret Service indicated that in 65 percent of the data breach cases they reviewed, a third party notified unsuspecting victims that they had been subjected to a breach in their computer system or network. Additionally, a report issued by the White House in 2009 conservatively estimated the value of the loss of US intellectual property as a result of just cyber hacking at more than $1 trillion in 2008 alone.

When resourceful individuals, organized criminals, extremist groups, and ultimately nation-states started to exploit these inherent weaknesses in computer programs, networks, and hardware, a cottage industry was formed. These new companies focused on measures to counter computer attacks with firewalls and antivirus protection. Software developers also provide a continuous flow of patches to fix the flaws that contribute to these exploitations. It wasn't until the arrival of the twenty-first century that universities started to include preventative security measures into their coursework as a key basis of design for software and hardware.

A patchwork of state and federal laws and regulations has developed across the United States and around the globe to begin to deal with computer-related crime. Issues such as conflicting state laws and requirements to notify individuals if their personally identifiable information has been subjected to a computer breach have created confusion and excessive costs of compliance. The complexity of the privacy protection laws across the European Union, as well as individual countries in the EU having their own set of complex laws and regulations dealing with privacy and data breaches, has also created dramatic levels of difficulty in establishing compliance regimes.

To instill trust and order in the Internet as a key facilitator of global commerce, a number of things must be accomplished:

- Harmonizing of laws and regulations dealing with computer software, hardware, and networks to ensure that compliance is increased and that noncompliance can be easily identified and dealt with swiftly.
- Holding software producers, hardware manufacturers, and network providers liable for delivery of flawed products and services that contribute directly or indirectly to the loss, disruption, or denial of services of those using the systems, hardware, or networks. Liability exposure will force these producers, manufacturers, and providers to ensure that in-depth security is built into their products before they are delivered to market and is maintained after they are operational.
- Establishing treaties to ensure that no individual, organized criminal or extremist group, or nation-state can operate with anonymity or immunity on the Internet and that they be held accountable for their actions. Nation-states must be held responsible for rooting out, stopping, and bringing to justice any individual, group, or entity committing any illegal act over the Internet.

Instituting a robust system of monitoring, controls, and sanctions to ensure that the Internet functions as a trusted and heavily defended environment that fosters cooperation, collaboration, and commerce will have a dramatic effect on the stability, viability, and resilience of our interconnected global economy.

Lynn Mattice, President and Founder
National Economic Security Grid
lmattice@nesgusa.org

About the Author

Dr. Panayotis "Pano" A. Yannakogeorgos is a research professor of cyber policy and global affairs at the Air Force Research Institute. His expertise includes the intersection of cyberspace, national security and military operations, cyber international relations, cyber arms control, violent nonstate actors, and the Eastern Mediterranean. He has recently authored articles and chapters including "Internet Governance and National Security," *Strategic Studies Quarterly;* "Challenges in Monitoring Cyber Arms Control," *Journal of Information Warfare and Terrorism*; "Pitfalls of the Private-Public Partnership Model," *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice*; and "Cyberspace: The New Frontier and the Same Old Multilateralism" in *Global Norms: American Sponsorship and the Emerging Pattern of World Politics.* He has also published in the *Atlantic,* the *National Interest,* and the *Diplomat.* Prior to his current position, Dr. Yannakogeorgos taught graduate-level courses on globalization, security, and intelligence at Rutgers University's Division of Global Affairs, where he also served as senior program coordinator and led the Center for the Study of Emergent Threats in the Twenty-First Century. He has participated in the work of global cybersecurity bodies including the High Level Experts Group of the Global Cybersecurity Agenda of the International Telecommunications Union. In 2006 he served as an adviser within the United Nations Security Council on issues related to nuclear nonproliferation, the Middle East (including Iran), al-Qaeda, and Internet misuse. He holds a doctorate and a master of science in global affairs from Rutgers University and a bachelor of liberal arts in philosophy from Harvard University.

Acknowledgments

This project concludes research ongoing from January 2011. Several individuals helped refine my thinking and mature the ideas found herein. Grateful acknowledgement is extended to the following for their support in my fulfillment of this project. First, to the AFRI team: Gen John A. Shaud, USAF, retired, Dr. Dale Hayden, Mr. Steve Hagel, and Dr. Tony Gould. Second, there are the many individuals with whom I discussed and shared versions of this monograph, including Lt Gen Robert J. Elder Jr., USAF, retired, Dr. Simon Reich of Rutgers University, Mr. Jason Healey of the Atlantic Council, Dr. Roger Hurwitz of MIT, Ms. Judith Strotz of the Department of State, Ms. Jody Westby of Global Cyber Risk, Mr. Sean Kanuck of the Office of the Director of Naval Intelligence, Dr. Duncan Hollis of Temple University, Mr. Lynn Mattice of the National Economic Security Grid, Airmen of the Twenty-Fourth Air Force, and others serving silently. Finally, a heartfelt acknowledgment is extended to Ms. Jeanne Shamburger and Mr. Jim Howard at Air University Press, who helped prepare the final manuscript.

Executive Summary

Malicious cyber actors exploit gaps in technology and international cybersecurity cooperation to launch multistage, multijurisdictional attacks. Rather than consider technical attribution the challenge, a more accurate argument would be that "solutions to preventing the attacks of most concern, multistage multi-jurisdictional ones, will require not only technical methods, but legal/policy solutions as well."[1] Deep understanding of the social, cultural, economic, and political dynamics of the nation-states where cyber threat actors operate is currently lacking. This project aims to develop a qualitative framework to guide US policy responses to states that are either origin or transit countries of cyber attacks.

The current focus of attribution efforts within the national security context concentrates on law enforcement paradigms aiming to gather evidence to prosecute an individual attacker. This is usually dependent on technical means of attribution.[2] In malicious cyber actions, spoofing or obfuscation of an identity most often occurs. It is not easy to know who conducts malicious cyber activity. But private sector reports have proven that it is possible to determine the geographic reference of threat actors to varying degrees.[3] Based on these assumptions, nation-states, rather than individuals, should be held culpable for the malicious actions and other cyber threats that originate in or transit information systems within their borders or that are owned by their registered corporate entities. This work builds on other appealing arguments for state responsibility in cyberspace.[4] Engaging the global community to develop a global culture of cybersecurity is a requirement for beginning the mitigation of the risks of countries being used for transiting or originating of malicious cyber acts. The United States will need to build a framework based on the articulated norms of responsible state behavior in cyberspace to legitimize this global engagement.[5] I offer such a framework here as a starting point for discussion at this early stage in international cyber policy development.

Technical challenges are not a great hindrance to global cyber security cooperation; rather, a nation's lack of cybersecurity action plans that combine technology, management procedures, organizational structures, law, and human competencies into national security strategies are.[6] As concluded in the 2010 *Quadrennial Defense Review*, the 2010 *National Security Strategy, International Strategy for Cyberspace*, and the 2011 *Department of Defense Strategy for Operating in Cyberspace*, strengthening international partnerships to secure the cyber domain will require understanding the technical, legal, and defense challenges faced by our international partners.[7] The research project is also firmly within the scope of the administration's *Comprehensive National Cybersecurity Initiative* and *International Strategy for Cyberspace* and the *Department of Defense Strategy for Operating in Cyberspace*. These also tie in with the Office of Science and Technology Policy's research tasking to "provide knowledge in support of laws, regulations, and international agreements."[8]

Identifying the gaps in international cooperation and their socioeconomic and political bases will provide the knowledge required to support our partners' cybersecurity and contribute to building a cyber environment less hospitable to misuse. It will also help US policy makers to determine the appropriate escalation of diplomatic and defensive responses to irresponsible countries in cyberspace. Further research and discussion will likely enable the timely development of the response framework for US sponsorship of sound global norms to guide global cybersecurity.[9] This will also assist the US defense, diplomatic, and development communities in building consensus, leveraging resources to enhance global cybersecurity, and coordinating US global outreach to those countries most beset by cyber crime and conflict.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Clark and Landau, "The Problem Isn't Attribution," 1.

2. Technical attribution refers to "the ability to associate an attack with a responsible party through technical means based on information made available by the cyber operation itself—that is, technical attribution is based on clues available at the scene (or scenes) of the operation." Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," 49.

3. See, for example, Alperovitch, *Revealed*; Grey Logic, *Project Grey Goose Report on Critical Infrastructure*; and Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud*.

4. Healey, "The Spectrum of National Responsibility for Cyber Attacks"; Kanuck, "Sovereign Discourse on Cyber Conflict under International Law"; Yannakogeorgos and Mattice, *Essential Questions for Cyber Policy*.

5. Articulated global norms of behavior include UN General Assembly (UNGA), "Developments in the Field of Information and Telecommunications in the Context of International Security," preliminary para.7; and UNGA "Combating the Criminal Misuse of Information Technologies"; UNGA, "Creation of a Global Culture of Cybersecurity," A/RES/57/239, preliminary para. 5. For more on norms development and the norms lifecycle, see Finnemore and Sikkink, "International Norm Dynamics and Political Change"; and Reich and Yannakogeorgos, *Global Norms, American Sponsorship and the Emerging Pattern of World Politics*, 3.

6. Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture."

7. Department of Defense, "Operate Effectively in Cyberspace," in *Quadrennial Defense Review Report*, 37–39; National Security Council, *National Security Strategy*, 27–28; and White House, *International Strategy for Cyberspace*.

8. National Security Council, *Comprehensive National Cybersecurity Initiative; International Strategy for Cyberspace*; *Department of Defense, Department of Defense Strategy for Operating in Cyberspace*; and Executive Office of the President, National Science and Technology Council, *Trustworthy Cyberspace*, 12.

9. National Security Council, *Comprehensive National Cybersecurity Initiative*.

Chapter 1

Introduction

Cyber conflict activities constitute a critical form of coercive power. Effects can range from disruption to destruction. The loss of electrical power for extended periods of time, inability to conduct commerce due to networking failures, and incapacity of military organizations to command and control their forces are credible threats. In the past, the United States has faced adversarial states and violent nonstate actors organized in relatively hierarchical vertical structures. However, today the evolution of information and communication technology (ICT), such as those that make up the Internet, and the intensification of reliance on these vulnerable technologies provide US adversaries with the opportunity to organize themselves as horizontal networks with decentralized leadership and no clear evidence of state control.[1] More often than not, the framing of the question of who is responsible for an attack focuses on the individual actor. One expert notes:

> The question is who is responsible for these things, even if you trace it back to China, is if they are bored hackers or PLA [People's Liberation Army] members or criminals with ties to the PLA or PLA divisions acting criminally? We don't really know. I suspect that the majority of the attacks and espionage on the criminal side are by patriotic hackers that have some sort of connection, maybe financial, to the PLA or the State Security Ministry. In the cases of power grids and other cases like that, I suspect PLA affiliation, but there is no way to know.[2]

The question of attribution—what individual or group exploited US information systems?—ought to become, Which state did the group operate from, and What state did it filter its malicious digital traffic through?

There has been extensive press coverage regarding Chinese involvement in cyber espionage and Internet censorship. The United States' policies for responding to cyber events are still being developed. Experts have noted that "a big part of the [Chinese] strategy is the PLA civilian units—IT [information technology] engineers drawn from universities, institutes, and corporations."[3] O. Sami Saydjari, a former National Security

Agency executive, has stated that “the Chinese People’s Liberation Army, one of the world’s largest military forces, with an annual budget of $57 billion, has ‘tens of thousands’ of trainees launching attacks on U.S. computer networks.”[4]

This highlights the blurred lines between state and nonstate actors who may perpetrate cyber conflict. It is a line that states hide behind when confronted about attacks. Although these trainees might not be officially controlled by the Chinese government, allowing the PLA to plausibly deny its involvement in an attack, evidence of indirect control should be enough to hold China responsible for hackers without borders operating from within China. Several recent studies of cyber espionage and the publicized results of corporate investigations have traced several attacks against the United States’ commercial infrastructures to China after malicious data was pivoted through several servers around the world.[5] Denying its official involvement, the government of China bemoaned its fate as the greatest victim of cyber crime.[6]

A recent report to Congress by the United States–China Economic and Security Review Commission observed that China’s “professional state sponsored intelligence collection not only targets a nation’s sensitive national security and policymaking information, it increasingly is being used to collect economic and competitive data to aid foreign businesses competing for market share with their U.S. peers.” The same report noted that the Chinese are aware of the gaps in US cyber strategies and may be exploiting “U.S. policymaking and legal frameworks to create delays in U.S. command decision making.”[7] The major flaw in US policy is focusing on individual responsibility for an act of cyber espionage, crime, or conflict. The policy gaps that currently exist are those of formulating response frameworks to cyber events that do not rely on a law enforcement paradigm. Instead, I argue that we need to respond to states with our own mechanisms of statecraft and hold states responsible within varying degrees for attacks originating or transiting through their territory.

Attribution of cyber attacks is not an easy task. There are technical issues covered in chapter 2 which complicate identifying cyber attackers. Anonymization can occur when attacks transit through several countries and can even originate on infected computers without the knowledge of their owners. These are known as botnets in the popular press. A "bot" is malicious software that can infect and control a computer and interactively respond to remote commands to extract, corrupt, or insert data into each infected computer. Weak domestic-law-enforcement cybersecurity capabilities in both developed and developing nations create virtual safe havens from which perpetrators of cyber crime operate (either physically or virtually) to spoof their true identity and operate with near impunity. It is this "spoofing" that has come to dominate the discussions around response to cyber attack. Discussed in greater detail in chapter three, the attribution challenge arises from the vulnerabilities built into the transmission control protocol / Internet protocol (TCP/IP). The IP version 4 (IPv4), the Internet's backbone transport protocol, makes it possible for individuals to mask the true location of their persons and computers. Technical attribution is further complicated in the nature of an attacks. Distributed denial of service attacks present different challenges in determining their sources than attacks designed to "exfiltrate" or steal sensitive or proprietary data. Regardless of attack type, the trend today is for multistage and multijurisdictional attacks—attacks infecting a lot of computers in a lot of places worldwide.

The law enforcement paradigm of attribution has come to dominate early cyber policy dialogues about strategy and doctrine. Air Force doctrine for cyberspace operations describes the attribution problem in the following terms:

> Perhaps the most challenging aspect of attribution of actions in cyberspace is connecting a cyberspace actor or action to an actual, real-world agent (be it individual or state actor) with sufficient confidence and verifiability to inform decision- and policymakers. . . . The nature of cyberspace, government policies, and international laws and treaties make it very difficult to determine the origin of a cyberspace attack. The ability to hide the source of an attack makes it difficult to connect an attack with an attacker within the cyberspace domain. The design of the Internet lends itself to anonymity. . . . Nations can do little to combat the anonymity their adversaries exploit in cyberspace. . . . Nevertheless, nations have the advantage of law and the ability to modify the technological environment by regulation.[8]

The Air Force appears to be following the traditional attribution framework emphasizing knowing exactly who the perpetrator is. The result is that cyber operators are being asked to inform decision and policy makers with accurate and precise evidence for a serious response to cyber attack.[9] While these requirements for the collection of evidence might be appropriate in a law enforcement context, such standards of evidence are misapplied in military and strategic contexts. The statement of USAF doctrine relating to law and policy modifying the technological environment is more pertinent. However, laws and regulations take time and resources to accomplish. Consider the decades-long processes that led to the UN Convention on the Law of the Sea in 1982. Instead, I offer a paradigm of American sponsorship of already established, yet embryonic, global norms of cyber behavior to facilitate the formation of a global culture of cybersecurity. American sponsorship would enable enforcement of those norms and lessen the importance of knowing who the exact perpetrator of a cyber attack is, if the source of the attack can be traced to a specific nation-state.

Technologically, attribution works better than the dire picture presented in policy might suggest. Several attacks coming from within China over the past five years have been publicly traced to operators with Chinese characteristics.[10] Furthermore, several high-profile cyber crime cases, such as the FBI's multinational effort in Operation Takedown, illustrate the essentiality of international law enforcement cooperation to bring criminal justice into cyberspace.[11] Such cases offer evidence that individual perpetrators can be brought to justice when there is solid international cooperation. Countries and others not cooperating in cyber investigations alibi that because of anonymity on the Internet they cannot trace cyber attackers, while efforts of like-minded nations, the United States and the United Kingdom, have resulted in the dismantling of a global network of "anonymous" hackers. While attribution in cyberspace is complicated, it is not as impossible as the mainstream view portrays it to be.

As it stands, a nation-state cannot solely assure its security within cyberspace. The existence of vulnerabilities in the protocols, hardware, and software that make up the domain, the exploitation of these vulnerabilities, and the fact that malicious cyber events can come from anywhere over the Internet require international cooperation between states to create a global culture of cybersecurity.

Due to the vulnerabilities built into the Internet protocol, individuals can disguise their identities with relative ease. Attribution becomes even more complicated when the motivation of attacks is considered. Attack patterns, effects, and levels of ambiguity differ between criminal, terrorist, or state-sponsored cyber attacks. These challenges can be overcome with the establishment of global cybersecurity policy.

The current law enforcement paradigm for attribution does not offer a sound basis for attributing attacks. Rather, nation-states should be held culpable for the malicious actions and other cyber threats originating in or transiting information systems within their borders or owned by their registered corporate entities. This cannot be done without clear and accepted norms of responsible state behavior in cyberspace.

The process of establishing these norms has begun in forums associated with the United Nations and its International Telecommunications Union (ITU), but the United States is trying to lead the development of global cybersecurity initiatives within other forums. Instead, the majority of nation-states, including American allies and some American partners, prefer to follow the lead of Russia and China in support of the ITU frameworks. The United States should increase participation in the ITU and get behind the international efforts on behalf of cybersecurity. American sponsorship of the global norms coming out of the ITU would immediately increase cooperation between states to create a more secure cyber ecosystem and allay fears of a hegemonic United States.

In 2011, the White House released the *International Strategy for Cyberspace* emphasizing development, diplomacy, and defense in the US government's vision on how to secure cyberspace. The strategy highlights the US commitment to development through working to "play an active role in providing the knowledge and capacity to build and secure new and existing digital systems."[12] This element is important in helping reduce the numbers of safe havens in cyberspace through which malicious actors initiate or transit their attacks through. Secondly, through diplomacy, the United States will strive "to create incentives for, and build consensus around, an international environment in which states—recognizing the intrinsic value of an open, interoperable, secure, and reliable cyberspace—work together and act as responsible stakeholders."[13] The Department of State and the Federal Bureau of Investigation both have roles in developing relationships with foreign governments so that when a cyber attack originates in or transits through their territory, the mechanisms to respond and act responsibly are in place. These essential partnerships are in place to identify and prosecute cyber criminals and terrorists. Diplomacy also offers a channel through which the United States can voice its concerns to foreign governments implicated in malicious acts in cyberspace. If governments are not forthcoming, more coercive diplomatic measures can be employed to stem malicious cyber activities. Finally, when all else fails, the Department of Defense has a duty to "respond to hostile acts in cyberspace as we would to any other threat to our country."[14] The DOD's role is also diplomatic in that it is to build partnerships with foreign militaries and, as a last resort, defend the nation. Within DOD the Air Force in particular has an important role to play in military-to-military relations since the Air Force sustains its leading edge in cyber over the other services and its actions, in the view of the rest of the world matter.

In February 2013, the United States released the "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets" after reports of state-sponsored espionage against US corporations.[15] Thus, the United States is shifting toward embracing a paradigm of state responsibility. This publication aims to inform plausible directions for this emergent strategy. Success of the *International Strategy for Cyberspace* depends on the United States shifting from trying to *lead* the world toward *sponsoring* the existing global culture of cybersecurity that has been organized through the International Telecommunications Union. This will support the United States' global engagements to secure cyberspace while leading by example. Along these lines, specific recommendations for US cyberspace development, diplomacy, and defense will be presented.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Zanini and Edwards, "Networking of Terror in the Information Age."

2. Ungerleider, "The Chinese Way of Hacking."

3. Onley and Wait, "Red Storm Rising."

4. Grow, Epstein, and Tschang, "The New E-Spionage Threat."

5. Areddy, "People's Republic of Hacking."

6. This can be attributed to Chinese interpretations of what a cyber crime is. Their definition includes content, and, thus, using Facebook to mount jasmine revolutions would be considered a crime in China, whereas the United States considers such actions as social networking enabling the development of democracy (in most cases).

7. United States–China Economic and Security Review Commission, "Occupying the Information High Ground."

8. Air Force Doctrine Document 3-12, *Cyberspace Operations*, 10.

9. Lipson, *Tracking and Tracing Cyber-Attacks*, 3–5.

10. See Alperovitch, *Revealed: Operation Shady RAT*; Grey Logic, *Project Grey Goose Report on Critical Infrastructure*; and Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud*.

11. Federal Bureau of Investigation, "Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce Additional Arrests."

12. White House, *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*, 14.

13. Ibid., 11.

14. Ibid., 14.

15. Mandiant, *Advanced Persistent Threat*, 1.

Chapter 2

The Cyber Environment

Attribution of cyber events to people or machines is an overstated challenge. Every action in cyberspace has a source that can be identified if observers are looking. Experts have noted that "the very fact that one attempts to conduct cyber warfare means that some bit in some data stream is changed to reflect one's presence and actions."[1] All agents in the cyber world can be visible if a worldwide effort is in place to monitor malicious traffic and to punish behaviors that fall outside that which aims to use the Internet to communicate ideas freely, open pathways of commerce, or otherwise not infringe on the right to live free and secure.[2] Much of the discussion in doctrine and policy is focused on the issue of why—with current network topologies—there are no physical identifiers of cyber attack, like a missile flash observable from space or a radiological fingerprint indicating the origin of the attack. The conclusion reached is that ambiguity is the norm on the Internet and that attribution is an insoluble technical problem with current network protocols. In this vision of the cyber environment, individuals or groups can "spoof" their identities and the location of their computers on the network. Many experts argue that tracking cyber attackers in enough time to respond appropriately is nearly unachievable.[3] These views have come to dominate the policy debates shaping doctrine, but there are others who claim that cyber attribution is not a technical challenge—rather a policy challenge.[4]

The hunt for pedophiles and the arrest of members of the ad hoc conglomerate known as LulzSec offer evidence that individual perpetrators can be brought to justice when there is solid international cooperation. The arrests of members of the LulzSec group seem to have had a deterrent effect on other members of the group, and the entire project was disbanded after the high-profile arrests were made. The real problem in attribution is for nation-states to become cooperative and responsible for the actions of malicious actors within their sovereign cyberspace.

This work offers a framework for the creation of acceptable levels of attribution for national responsibility across the domain of conflict by shifting the paradigm from the individual to the state. Within the whole-of-government context, baseline standards of behavior and the framework suggested herein would allow decision makers to hold states accountable for actions undertaken within their sovereign cyberspace. While a necessary part of the whole-of-society response to cyber attacks, this is only a small part of the political reality of cyberspace. The framework provides suggestions for development of a global culture of cybersecurity, diplomatic responses, and—in incidents of national security significance—military action.

A Holistic View of Cyberspace

It is not the purpose of this work to elaborate on computer networking and the methods that individuals or groups may use to obfuscate their identity on the Internet. Cyberspace has been an influence on international relations for the final half of the last century and the first decade of the twenty-first century. As the consequences of events in cyberspace are felt throughout society, national security discussions will center on how to secure this new domain. However, these considerations tend to focus on the man-made elements of the cyber domain. While there is no argument against the man-made elements of cyberspace, focusing too much on technology creates conceptual hazards that cloud policy discussions.[5] The following discussion aims to bring clarity to the attribution problem by focusing on the physical, logical, information, and human elements of cyberspace rather than just computer code (fig. 1).

One reason for the current interest in technical attribution is emphasis on the logical versus the physical layers that compose cyberspace. For example, Air Force cyberspace operations doctrine states that "cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land and maritime."[6] This approach creates an aura of cyberspace as solely a virtual domain, divorcing it from the real world. Although the physical elements of cyberspace are noted within the Air Force's definition, they are largely secondary to the protocols and computer language through which digital communications occur.

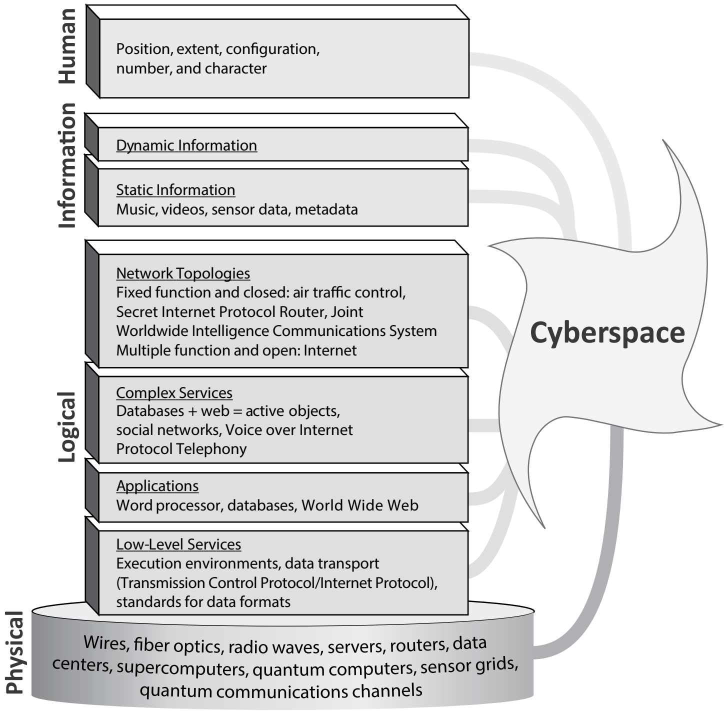


Figure 1. Characteristics-based model of cyberspace. (Based on David Clark, "Characterizing Cyberspace: Past, Present and Future," working paper, version 1.2, 12 March 2010, http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf.)

There are in fact no purposes for cyberspace but to serve human operators and to create effects in the physical world. Fixating on technology to the detriment of other characteristics that compose the cyber environment creates the impression that cyber is not that connected to the real world. Refining the conceptualization of cyberspace allows for its demystification and closer alignment within the physical world.[7] Achieving this goal requires looking at cyberspace as a complex ecosystem composed of human operators ranging from the casual Internet user to the information warrior; the actual information that is stored, transmitted, and transformed; the computer code and protocols; and the physical elements on which the logical elements reside.[8]

The human and physical aspects are just as important as the logical elements of cyberspace. Data and information are not transported in a virtual ether divorced from the laws of physics, space, and time. Rather, data and information travel through physical infrastructures, such as undersea cables, and reside on digital storage devices operated by people who are within the boundaries of a state's sovereign territory. The software and hardware companies, whose poorly coded or manufactured products are at the root of vulnerabilities, could be held responsible with regulations. People and computer systems responsible for cyber attacks could be made accountable to the laws of a state. And it could be possible to hold states liable for malicious cyber attacks based in their territory.[9] An unintended result of such an approach would be bringing clarity to the DOD discussions regarding the combatant command responsible for dealing with cyber attacks.

Modern Botnets

Botnets are good examples of multistage, multijurisdictional attacks. A "botnet" is a remotely controlled network. It can be used for sending spam, stealing money from bank accounts, denial of service attacks, and so forth. Botnets require a command and control (C2) server, hacker machine, and victim machines (drones). Botmasters target individuals specifically or randomly depending on the effect they wish to achieve. Malicious code is sent by e-mail or embedded in a website waiting for the victim to download an attachment or click a link. Once infected the victim's computer becomes a drone in the botmaster's network. The drone pings the C2 server and receives instructions. The botmaster on his end instructs the drone how to behave and maintains the software on the C2 server to keep it up to date so that he has the latest tools available. Botnets can include from tens to hundreds of thousands of bots.

All of the elements of cyberspace in the model have a role to play in resolution of the attribution challenge despite the Internet's ambiguity. The vulnerability of the data transport protocols, such as TCP/IP and media access control (MAC) addresses, to spoofing attacks is at the root of the attribution problem. While barriers to spoofing might be raised by the deployment of IP version 6 (IPv6), a determined adversary would not be deterred. Attributing information in a cyber attack within a particular nation-state could be found in other layers. At the logical level, metadata might exist within files used to execute an attack. The databases to which information is exfiltrated or the servers used to command a botnet might also provide clues and a trail back to the attacker's host country.

Multistage, Multijurisdictional Attacks

Understanding network behavior requires examining relations among network events (fig. 2). The technological issues related to TCP/IP outlined above are only part of the attribution problem. Attribution is typically thought of as the ability to trace attacks back to attackers.[10] Being able to do so allows an appropriate response to the attack via law enforcement or military action.[11] If attackers knew that their actions could be accurately traced, attacks could be deterred. Solving the technical attribution challenge by implementing new methodologies and techniques is widely seen as the way forward toward responding to cyber attacks. This can be seen in the pressure to deploy the upgraded IPv6 that has been in the works since 1998.[12]

Although strengthening network protocols is desirable, the respected cyber experts David Clark and Susan Landau have suggested that "better attribution techniques will neither solve nor prevent" the complex multistage, multijurisdictional nature of computer exploitations occurring today.[13] It is not the purpose here to delve into the intricacies of methods and techniques to technically attribute attacks. It is noteworthy that the multistage and cross-jurisdictional characteristics of cyber attacks determine the complexity of determining the sources of attacks. These factors highlight that gaps in international cooperation actually lie at the core of the attribution dilemma.

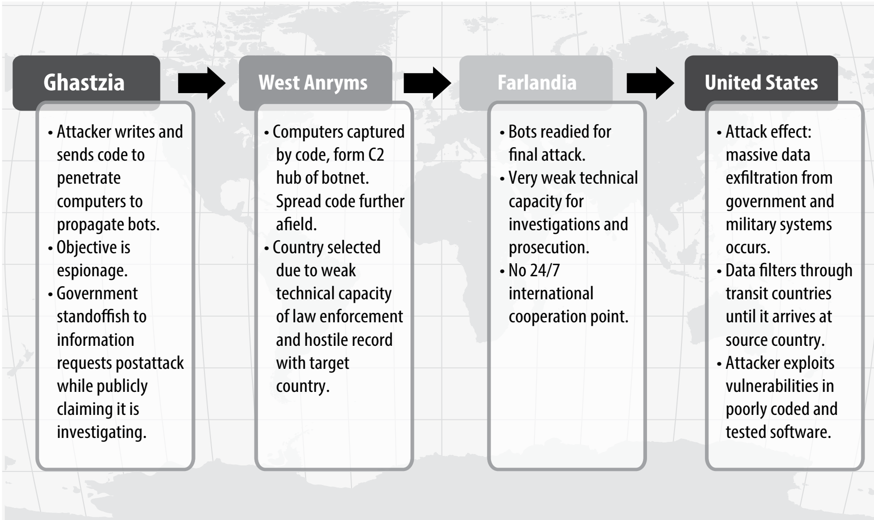


Figure 2. Outline of a hypothetical multistage, cross-jurisdictional attack launched for the purpose of data exfiltration

Spoofing Machines to Mask Geography

Very few people are capable of designing sophisticated Stuxnet-like targeted cyber weapons. However, the capabilities to mount less sophisticated exploits of vulnerabilities, such as spoofing a machine's location, have a much lower cost of entry. This is due to the inherent weakness of the network protocols and the availability of anonymizing tools. A brief description of Internet protocols as well as anonymizing tools is provided below.

Computer networks are dependent on the use of internationally standardized communications protocols, known as TCP/IP, to send and receive data packets and information.[14] TCP/IP allows for the flow of data packets and information across computer networks. For example, machines identify each other on the Internet through IP and MAC addresses. Designed and deployed for military and research purposes in the late 1960s, IP was not intended to function as the backbone of the global project that became the Internet. Approved in 1982 as the standard protocol for military computer network communications, the protocol was designed to allow for data packets to be sent across a computer network in the most efficient way the network deemed possible at a given time. The reasoning was that in the aftermath of a nuclear war, hierarchical networks would likely have had nodes critical to relaying data vaporized, and what was required was a nonhierarchical network structure that could reroute data-packets in an uncorrupted manner from point A to B via other pathways. The ability to track and trace user behavior in a high-threat computing environment was not built into communications protocols because they were intended for use within a trusted military environment.[15] Yet it is this foundational protocol that other networks began to build out from, eventually morphing into the National Science Foundation Network and the Internet.[16] According to Internet expert Tom Leighton, the Domain Name System (DNS), ports, and IP address systems are plagued by flaws that "imperil more than individuals and commercial institutions. Secure installations in the government and military can be compromised" as well.[17] Consequently, the current flaws in the network architecture of the Internet are a result of relying on protocols that were built 35 years ago when the Internet was not a global entity but a closed research network. When it did become global, there was no shift to create stronger security mechanisms.

To better understand the functioning of TCP/IP, a brief description of how information is sent across networks is necessary. Data packets are the basic units of network traffic. They are the standard way of dividing information into smaller units when sending information over a network. A significant component of the computer networks is the IP header, which contains information pertaining to the source and destination addresses. Machines require these strings of numbers to connect with other computers on the Internet or other networks.[18] All networked hardware must have a valid IP and MAC address to function on a network. Data packets are recreated by the receiving machine based on information within a header of each packet that tells the receiving computer how to recreate the information from the packet data. Without international standards, such as TCP/IP, there would be no assurance that packets could be read by a receiving machine.[19]

Manipulating TCP/IP to spoof identities has become very common in cyberspace. In the past, a significant understanding of networking was required to spoof one's IP address. Over the past 15 years, tools anonymizing Internet activities have proliferated. "Onion routing" of networks allows for the masking of a data packet's point of origin. Activists may enter the Internet from unsecured wireless or "Wi-Fi" networks and cybercafés or dial into Internet service providers (ISP) all over the planet to hide their identity from the prying eyes of government censors. Malicious actors can propagate bots to serve as proxies for cyber attacks. Actors might spoof IP addresses to inject malicious data into critical infrastructures, commit fraud, or bypass authorities.[20]

These kinds of spoofing attacks are the crux of the attribution challenge. Masking one's location on the Internet destroys trust in identity and security in cyberspace. An individual may manipulate various layers of the TCP/IP protocol to create a false appearance of a user, a device, or even a website. With the global nature of the Internet, it is possible for malicious actors to make their computers appear to be in others. This technique allows skilled attackers to thwart cyber crime investigations. Dorothy Denning aptly states that to "trace an intruder, the investigator must get the cooperation of every system administrator and network service provider on the path."[21] This is the basis of the attribution problem, but it would not be an impossible challenge with the appropriate global cyber policies holding states culpable for malicious cyber activities in place.

While the ability to spoof one's location is a critical element of a cyber crime, cyber espionage, or cyber sabotage, the Department of State (DOS) is developing tools that utilize these same vulnerabilities in IP and network design to promote freedom of speech in closed regimes via the Internet. Such efforts complicate the attribution of cyber attacks since people are actively trained to anonymize their Internet activities. Prospects for international cooperation are also dampened because some closed regimes view breaching of censor systems as cyber warfare and might not be forthcoming with information during cyber attack investigations of interest to the United States.

The Onion Router (TOR) is one example of such a software (fig. 3). It is a distributed anonymous network of proxy servers connected by virtual encrypted tunnels that allows anonymous communications. A computer linked to a TOR network transmitting data sends the data through a series of randomly

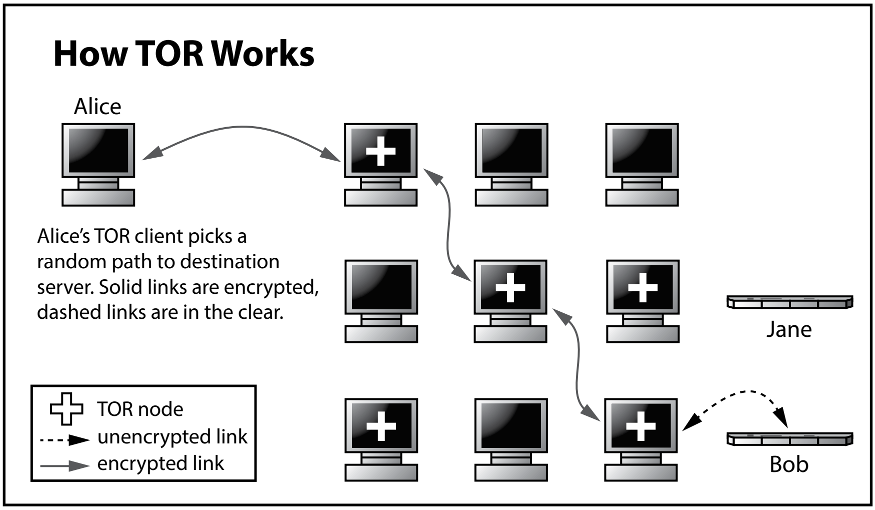


Figure 3. How TOR works

selected proxy servers that strip away one layer of encryption along with the IP identification information. The IP information is replaced and the data is sent off to another proxy server to repeat the same process before connecting to another server for final distribution of the information. The effect is that observers of the network traffic on any of the proxy servers will neither be able to discern the true location of the point of origin nor be able to tell what the destination of the data is, unless the observer can see the final transmission point. An observer at the destination point will not know where the data is really coming from as only the location of the last proxy server can be detected. In this way a network address is masked—there is no direct link between the data packet's point of origin and final destination. However, an observer operating the TOR server node prior to the final connection might be able to detect digital artifacts within the network traffic providing clues to the user's identity and location.[22] While TOR certainly complicates attribution efforts, weaknesses exist that can be exploited to identify machines or persons on the Internet.

Cyberspace is a dynamic environment where no defense will be perfect. Moreover, if targeting a specific network proves too difficult, indirect attacks taking out its supporting systems might prove just as effective.

Responding to any cyber incident requires knowing the answers, within acceptable levels, to the following questions: Who is the threat agent? What motivated the agent and what were his objectives? What methods and techniques were used? What were the causes of the effect? Which services were affected? What impact did the event have?[23]

The ecosystem where cyber attacks occur is not isolated from the real world. Real people are programming computers in specific places to send signals to other computers to cause effects in the "real" world. These signals can transit multiple countries to get to their target. Attacks occur only if there are attackers, facilitators, defenders, and targets. One could argue that certain cyber infrastructures, such as satellites or undersea cables through which Internet traffic flows, are not located within national jurisdictions. However, even these are operated by entities that are registered within the jurisdiction of a sovereign state. Understanding the actors involved in the progression of a multistage, multijurisdictional cyber attack highlights the importance of rapid international cooperation to resolve the cyber attribution challenge. Components of cyber attacks include the attackers, defenders, knowing or unwitting facilitators, and the targets.

While the exploitation of vulnerabilities within information systems poses a threat, not all of these attacks threaten national security. Mounting a complex attack with effects of national significance while preventing event attribution would require specialized capabilities (fig. 4). These would include (1) expert-level programming and cryptographic skills, (2) detailed knowledge of industrial control systems, (3) mastery of multiple open and closed operating systems, and (4) detailed knowledge of telecommunications and legal regimes.[24]

Attack Agents

Attack agents can be states, substate actors such as Chinese privateer hackers or Romanian computer criminals, regional or global organizations such as the Russian Business Network, ad hoc networks such as LulzSec or Anonymous, malicious individuals such as Kevin Mitnick before his reeducation, or a nefarious insider (fig. 5).

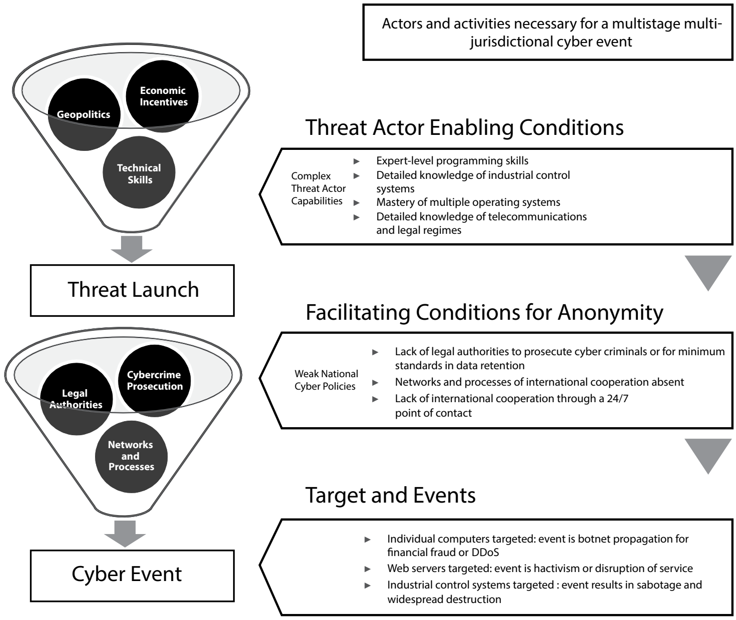


Figure 4. Some necessary conditions for cyber attacks: a holistic set of actors and activities required for an anonymized cyber attack

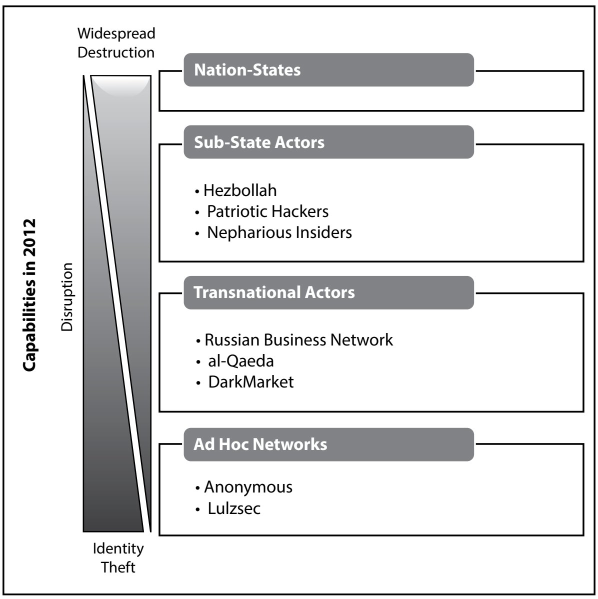


Figure 5. Attack agents and capabilities

Motivating factors for an attack are also important when gauging the attack agent's intention, be it identity theft, espionage, botnet propagation, extortion, sabotage, or widespread destruction (table 1). The first four of these often indicate economic incentives where the perpetrator of an attack judged that an investment of time and other resources would bring about a higher payoff. Such cyber events are possible on networks such as the Internet that are used for commercial purposes. The final two indicate more malicious intent. Sabotage and widespread damage would occur only if critical financial networks, industrial control systems (ICS), embedded systems, or military networks were targeted by malicious adversaries. The level of skill and financial resources required for such attacks is significant and, as of this writing, outside of the capabilities of violent nonstate actors. Cyber events of national significance are those that result in extensive damage to critical infrastructure or key assets.

Table 1. Motivating factors and targeted infrastructures

Motivating Factor	Targeted Cyber Infrastructure
Identity theft Espionage Zombie propagation Extortion	***Open, Multifunction Networks*** Internet, social media, mobile application markets, platforms as service, software as service
Sabotage Widespread destruction	***Closed, Fixed-Function Networks*** Industrial control systems, exchange trading system, Society for Worldwide Interbank Financial Telecommunication (SWIFT), military command, control, and logistics networks, embedded systems

The goals and objectives of an attack include information corruption, fabrication, destruction, disclosure, or discovery. System subversion or disruption can be additional goals. Cyber events occur by system or protocol compromise, resource exhaustion, hardware failure, or software crashes. The techniques for these objectives include the targeted exploitation of system, social, or protocol vulnerability. Overload of network or system resources and the autonomous self-propagation of malware are other techniques used. Figure 6 shows a spectrum of cyber conflict.

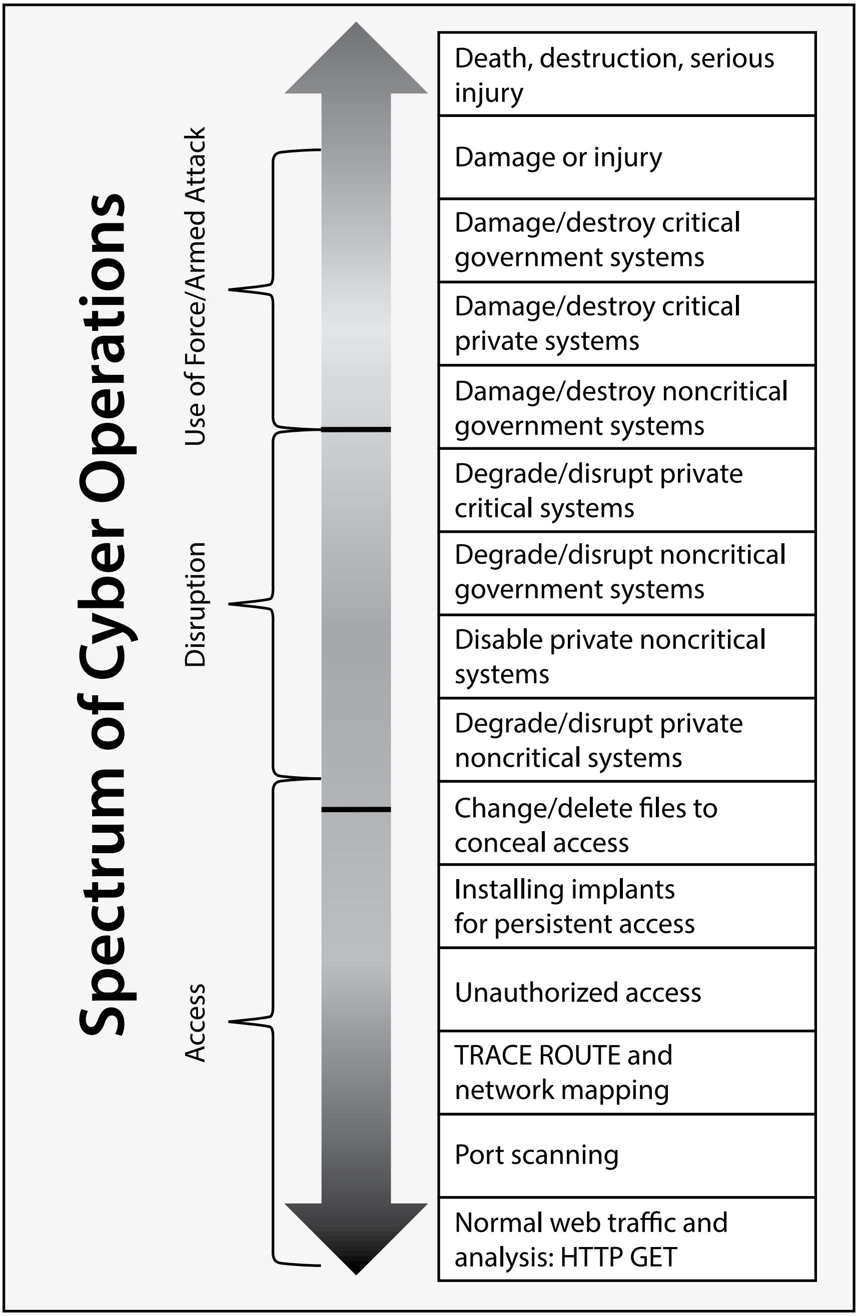


Figure 6. Spectrum of cyber conflict. (Courtesy of US Cyber Command, Judge Advocate)

Targets and Effects

Social engineering campaigns target people to exploit trust relationships among computer users. The recent data breach at the data security firm RSA is one example of how technically proficient and security-minded employees can be socially engineered with a malicious e-mail message. Other social engineering targets can include critical infrastructures and financial networks. The effects of a cyber-related event depend on the perpetrator's motivation for launching the attack. Consequences of cyber events can be either discrete and finite or advanced and persistent. An example of a discrete, finite event is an attempt to degrade the operation of critical infrastructure by attacking an ICS, a supervisory control and data acquisition (SCADA) system for example. Advanced, persistent threats are linked with espionage and criminal activities that aim to collect as much information about the functioning of a system as possible. Figure 7 is a spectrum of the kinds of operations that are possible and the effect they might have on targeted systems.

Effects are observed either as the result of a cyber disruption within a service or a cascading disruption of another service that the targeted system depends on. The services affected could include the sectors of energy, telecommunications, finance, water supply, health care, transportation, law enforcement, fire and emergency response, government administration, shipping, agriculture, commercial facilities, and critical manufacturing. The impact of the event could harm economies, populations, or even national security.

The motivating factors also play a role in the response. The severity of a cyber attack will determine whether a response will cross over the national defense threshold. Unlike criminal attacks, which usually involve widespread and indiscriminant targeting to obtain maximum profit from victims, cyber weapons are more focused. It has been noted that

> a cyberweapon might attack a particular country, a type of service (e.g., electrical grid or water system), or systems used by a certain political, ethnic or religious persuasion. Both the Georgia and Stuxnet attacks employed moderately focused targeting (insufficiently focused according to critics). However, potential vulnerabilities and attack vectors will not correlate much with targets and there must be significant testing. This complicates the job of the attacker and requires additional tools

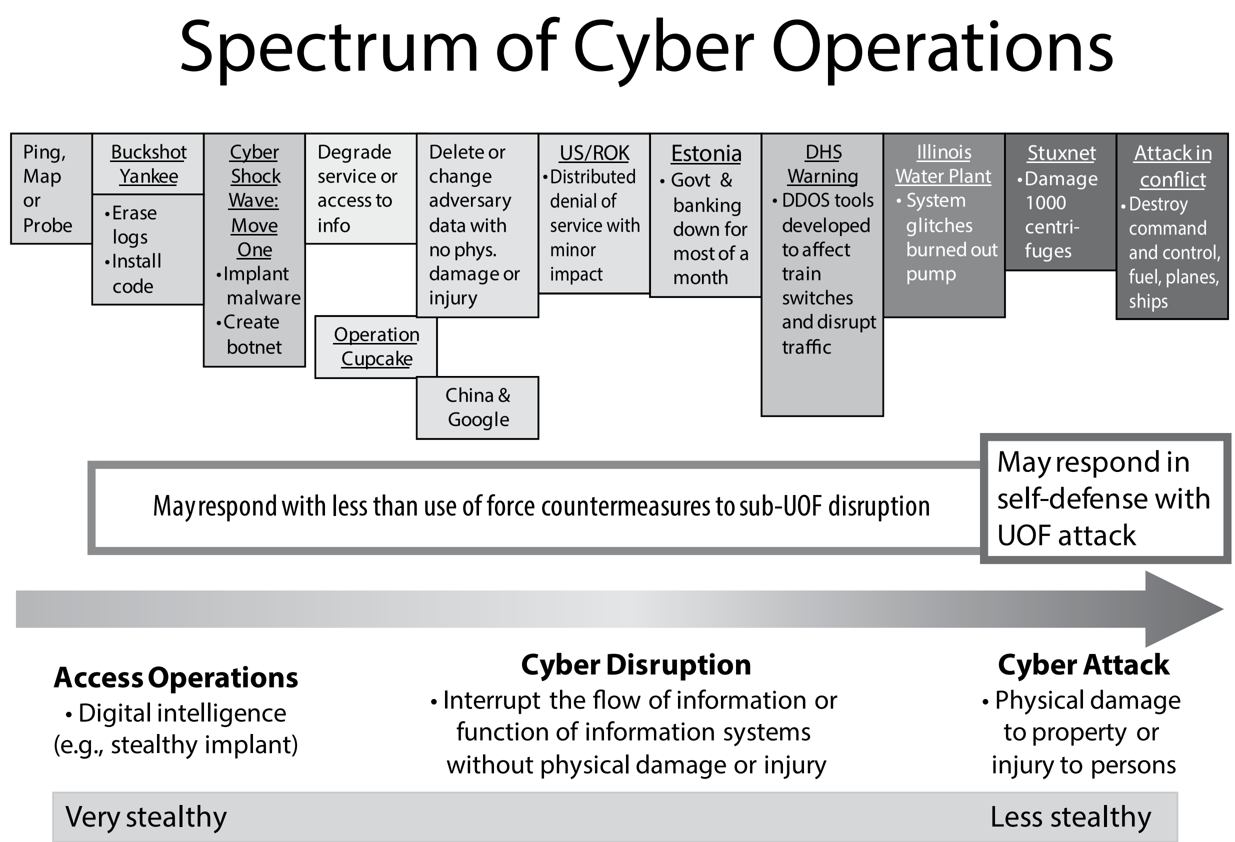


Figure 7. Spectrum of cyber operations. (Courtesy of US Cyber Command, Judge Advocate)

beyond those used in purely criminal endeavors. We can use this difference to our advantage in detecting cyberweapons development.[25]

For military purposes, tracing the source of cyber attacks might not be as difficult as often thought. Cyber-weapon testing activity may be spotted "in the wild" (on computers in day-to-day operations, outside of laboratories and research facilities) before an actual attack. Thus, observers can compile an attack signature database much like we have for identifying aircraft radar signatures.

Criminals and cyber warriors will target institutions regardless of whether there is a way to do it in cyberspace. Many argue the cost of entry is low in cyberspace since it is relatively simple to digitally rob a bank; disrupt a hospital's heating, ventilation, and air conditioning system; or release the floodgates of a dam. The significantly fewer resources required for a cyber attack have less to do with the nature of the domain and more with its poor technological development, design, and implementation. Software developers, hardware manufacturers, and network providers face no liability or responsibility for the systems they produce or operate. As a result, there is no incentive to deliver secure products to the marketplace. This risk will be increasingly manifested as cloud computing takes hold and as the resulting breaches destroy multiple companies rather than single firms.[26] Thus, global policy responses are needed for international cooperation and to incentivize security in the private sector.[27]

Facilitators

Attack agents, especially those motivated by economic gains, will try to mask their identities and avoid prosecution. They will seek out places where governance and policy conditions facilitate masking their identities. Nation-states without technical capabilities for preventing attacks or not practicing due diligence in enforcing laws to prosecute attackers could be considered facilitators of cyber attacks. Complex attack agents will likely have thorough knowledge of telecommunications and legal jurisdictions, allowing them to route an attack through countries lacking abilities to prosecute cyber criminals or standards for internet service providers to retain data logs that could assist in law enforcement investigations. Countries without means of international cooperation, such as a 24/7 point of contact like a national computer emergency readiness team (CERT), described in detail as a defender of cyberspaces below, should also be considered as cyber attack facilitators. Inaction of national governments to organize their domestic resources to combat cyber crime results in havens for malicious cyber agents. Other facilitating actions would include a refusal to respond to requests for cooperation in responding to cyber attacks.

Facilitators can also include unwitting individual users whose computers have been infected with malicious code, allowing them to be remotely controlled by malicious agents. These situations often arise simply from users' lack of cyber threat awareness, training, and education.

Software companies, mobile application developers and distributors, and suppliers of hardware can become facilitators in the production of the physical and logical components of cyberspace. Hardware supply chains have been found to be infected with malicious logic from manufacturing sources outside of the United States. Software companies, concerned with their financial reports, push products onto the market before fully testing them for security. In fact, many of their programmers are not trained to write secure code. The continuing use of Java and C# to develop software weakens application security and contributes most of the vulnerabilities currently being exploited. More secure languages such as the Java Server Pages (JSP) or the Active Server Pages (ASP) and more secure coding practices must be encouraged. This might be done by automating secure coding practices and using more secure coding languages, requiring investments in secure technological development programs, and institutionalizing software security practices.

One example of vulnerabilities introduced by software companies can be seen in Microsoft's experience with China. In 2003 China received access to the source code for Microsoft Windows in a partnership between Microsoft and China to cooperate on the discovery and resolution of Windows security issues. The result was the China Information Technology Security Certification Center (CNITSEC). The CNITSEC Source Code Review Lab is described as "the only national certification center in China to adopt the international GB/T 18336 idt ISO 15408 standard to test, evaluate and certify information security products, systems and Web services."[28] Despite the ISO standards, Chinese computer scientists reverse engineered the code. This allowed them to discover zero-day exploits in the operating system. The fruits of their efforts resulted in the shutting down of the US Pacific Command Headquarters after a Chinese-based attack.[29]

When vulnerabilities are discovered in software, patches are issued to secure the computer from potential attack agents. People often do not keep their software up to date with the latest path or antivirus definitions. Most threat actors exploit vulnerabilities that are half a decade old in software that has not been updated by users. Current cyber policies and best practices, including those of the Department of Defense, place the burden on individual users to practice good cyber hygiene. The DOD's *Strategy for Operating in Cyberspace* concludes that "most vulnerabilities of and malicious acts against DoD systems can be addressed through good cyber hygiene. Cyber hygiene must be practiced by everyone at all times; it is just as important for individuals to be focused on protecting themselves as it is to keep security software and operating systems up to date."[30] While there is no argument against assuring that users of systems must remain aware and vigilant, current programs such as the yearly requirement of DOD Information Assurance Awareness training is not enough to assure that individuals are aware of the latest threats or understand the risks posed by information systems. Ultimately the burden for assuring good cyber hygiene should be placed on the service provider.

Vulnerabilities in the physical layer of cyberspace are often overlooked in discussions focusing on exploits at the logical, information layers. There are hardware supply chain risks to cybersecurity. For example, US original equipment manufacturers' (OEM) reliance on China, Singapore, Taiwan, and India for design and assembly of hardware components allows these countries to exploit their positions on the supply chain to implant malicious code and back doors into equipment used by US civilians, government, and industry that allow for escalated unauthorized privileges on a platform. Recent trends indicate that vulnerabilities in computer architecture can be exploited by anyone with an understanding of 16-bit assembly language using open source tools.[31] This lowers the threshold of expertise. To reduce the points of entry into a computer system, industry must be held accountable for supply chain risks at the manufacturing plant. Concurrently, the USAF, and other national security departments and agencies, should reform their acquisition policies to require hardware suppliers to deliver their products with physical mechanisms in place to avoid trivial backdooring of hardware.[32] Some progress has been made in standardizing supply-chain cybersecurity procedures by the National Industrial Security Program (NISP) for the defense industrial base to mitigate the risk of this threat.[33] Domestic production of all hardware used for national security purposes could be mandated to further mitigate the risk of supply-chain cyber attacks.

All of the above facilitating conditions have resulted in an ecosystem that highly favors attackers, relegating defenders to a postattack reactive posture. Industry software and hardware developers thus need to develop the cyber infrastructure with security in mind. Today, this seems to be an afterthought. In discussions with chief information security officers (CISO) from various sectors, as well as presentations on application security at technical conferences, the picture being painted is one and the same: no serious steps are being taken to mitigate the coding of vulnerabilities. One industry CISO noted that it is not the companies' fault. Rather, current university computer science programs are more interested in churning out the next Google or Facebook than training programmers to develop secure applications.[34] Reform of curricula is met with resistance from faculty.[35] Thus, companies may need to take it upon themselves to assure that their software and hardware engineers are trained to develop secure products. The national security community should use its purchasing power to buy software that has been coded with security in mind. These are just some steps to begin reducing the only reason why cyber attacks are possible: that is, vulnerabilities in software and hardware design and implementation. This will not resolve the problem, but at least it will raise the cost of attack.

Defenders of Cyberspaces

Defenders of cyberspaces include ISPs, law enforcement, corporate security branches, national computer emergency readiness teams, and computer security incident response teams (CSIRT) (fig. 8). CERTs in particular can serve an important function in

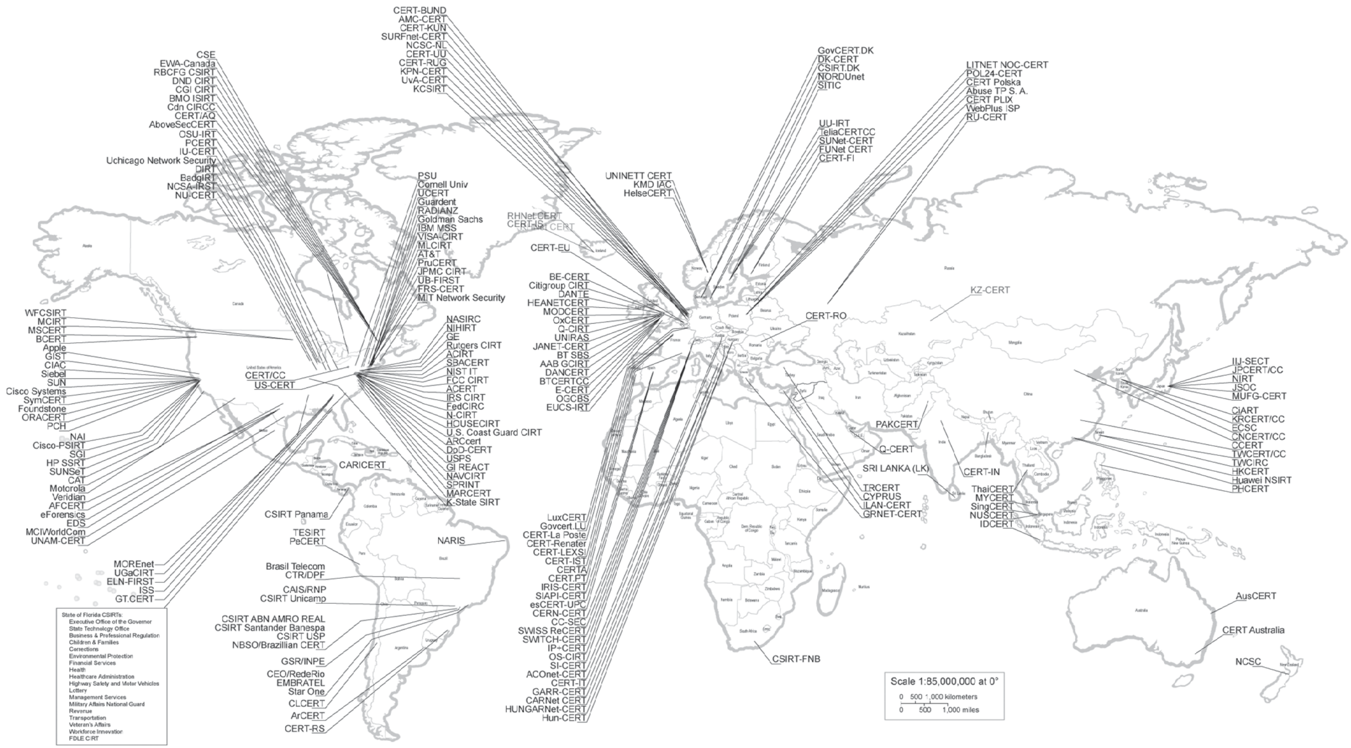


Figure 8. Incident response teams around the world: international cooperation speeds response to Internet security breaches. (Courtesy of Department of Homeland Security—US CERT)

global cybersecurity cooperation. When nations have national-level CERTs, these offer mechanisms for coordinating responses. Communities of trusted experts can provide insight into security incidents and vulnerabilities for local CERTs that may need the technical assistance. If a computer security incident becomes an event of national significance, CERTs can also serve in managing and coordinating responses.[36]

Although prevalent, CERT/CSIRT expertise is not uniform across national boundaries. Vulnerability and threat awareness, understanding the regulatory and legal requirements, determining constituencies and staffing requirements, funding, developing partnerships, and establishing situational awareness for critical infrastructures, security policies, and guidelines are necessary for a robust national CERT (fig. 9). It is estimated that developing these capabilities can take anywhere from 18 to 24 months.[37] The consensus is that governments are responsible for resourcing a CERT's stand up and coordinating domestic stakeholders to foster a national culture of cybersecurity. The ITU has been undertaking assessments of the abilities of developing nations to establish national CERTs.[38] These are steps in the right direction that should begin resulting in better national capabilities in the participating countries over the next 5–10 years.

Efforts toward a global culture of cybersecurity are starting to find an institutional home within the ITU's IMPACT program and are guiding global awareness as to the need to establish CERTs. The global culture of cybersecurity (GCC) will be discussed in greater detail in the next chapter. Not all countries have similar cyber defense capabilities. Many developing/democratizing countries are source countries for cyber attacks or are being used to pivot cyber attacks in order to mask their true origins.[39]

Internet service providers themselves are on the forefront of cyber defense. ISPs in the West are often reluctant to monitor their network traffic due to civil liberties concerns. The Stop Online Piracy Act (SOPA) and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP or PIPA) that would have authorized ISP monitoring of customers for copyright infringements illustrate how ISPs could participate in the effort to secure cyberspace.[40]

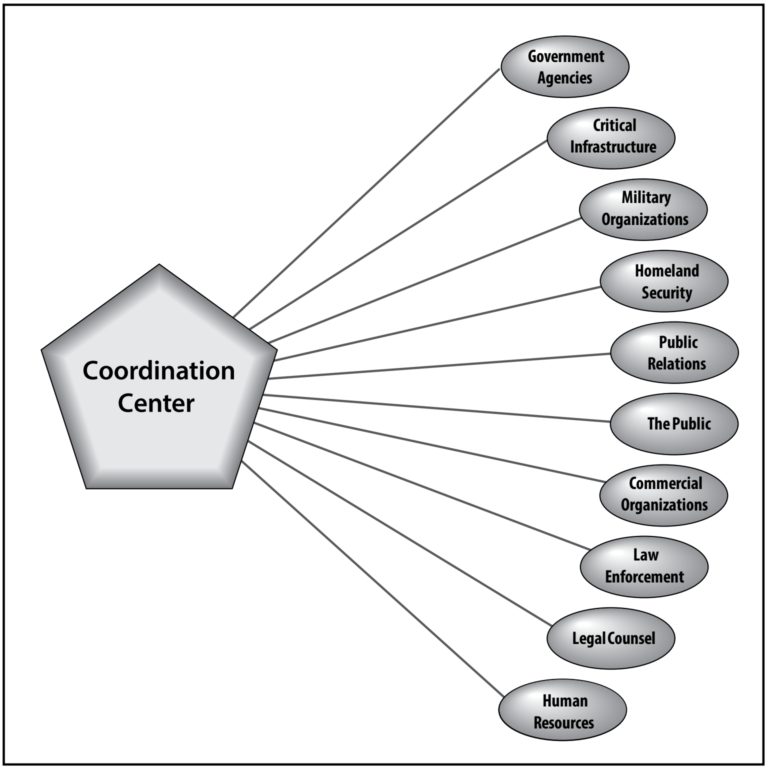


Figure 9. Necessary components of a CERT

Some ISPs abroad, such as TeliaSonera in Sweden, actually have monitoring systems in place to lift the cyber hygiene burden off of customers (fig. 10).

Upon notice, the customer's machine is isolated from the network until the infection is removed. The customer is then returned onto the network. This "cycle of protection" for users has been successful in stopping infections on computers and reducing the number of computers on TeliaSonera's networks that are victims of botnet propagation. The company's cooperation with the Finnish national CERT and Microsoft is indicative of the complex relationships that were required in order to take down the Rustock Botnet, which was responsible for high levels of spam e-mails. According to Arttu Lehmuskallio, security manager of the CSIRT at TeliaSonera, "The benefits of an ISP monitoring their network are so great, and the costs are so

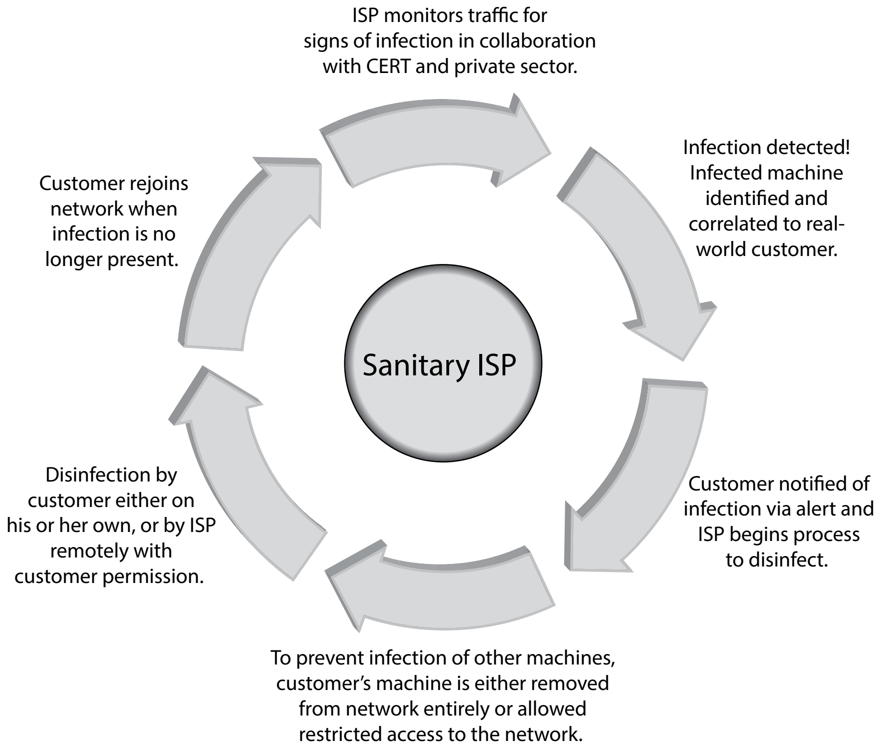


Figure 10. Sanitary ISP

small, that I'm surprised more ISPs have not already implemented a similar solution."[41] In the United States, such concepts apply in principle, with reports issued by the Department of Commerce lauding the benefits of adopting automation protocols such as the Security Content Automation Protocol (SCAP), continuous monitoring, and the Department of Homeland Security (DHS) models for automated continuous security.[42] ISPs in the United States tend to push back, arguing that they can apply best practices voluntarily without the heavy hand of the law forcing compliance.[43] In response to recent legislative efforts in 2012, Jason Livingood, vice president for Internet systems engineering at Comcast said that "attempting to impose uniform cybersecurity solutions could actually be counterproductive, by enabling an attacker that cracks a single solution to compromise multiple systems, and by slowing down or constraining our ability to rapidly develop innovative cybersecurity solutions."[44] However, the facts of TeliaSonera's success invalidate this claim since the Swedish company was able to effectively implement a course of action that has allowed Finland to claim the lowest infection rates.

The underlying technology that allows TeliaSonera, however, is the controversial method of deep packet inspection (DPI). Privacy advocates in the West are concerned about issues of using DPI methods to read e-mail and other content on these systems. TeliaSonera uses DPI "as a statistical tool to gather information about the usage of the networks and as an analyzing tool whenever abnormal traffic or fault situations occur."[45]

Although employment of this system has reduced the amount of cyber crime, civil libertarians may protest the use of DPI and stall its implementation. Internet service provider Comcast's Web Notification System Design concept is one innovation that does not rely on deep-packet inspection. It provides critical end-user notifications to web browsers. Such a notification system is being used to provide near-immediate notifications to customers, such as to warn them that their traffic exhibits patterns that are indicative of malware or virus infection.[46] It would seem that such a system might address privacy concerns using open tools and standards to allow for transparency in the functioning of non-DPI critical notification systems. These and other such efforts will help create a cyber environment that does not put the burden of "cyber hygiene" on the user who lacks the technical expertise or does not analyze his or her network traffic looking for irregular patterns in the data.

The remainder of this work offers a framework for the creation of acceptable levels of attribution for national responsibility across the domain of conflict by shifting the paradigm from the individual to the state. Within the whole-of-government context, adherence to baseline standards of behavior and the offered framework would allow holding states accountable for actions within their sovereign cyberspace. While a necessary part of the whole-of-society response to cyber attacks, this is only a small part of the political reality of cyberspace. The framework provides suggestions for development of a global culture of cybersecurity, diplomatic responses, and—in incidents of national security significance—military action.

Notes

1. Parks and Duggan, "Principles of Cyber-Warfare."

2. One might argue that it is difficult to assess whether or not an activity is malicious until it's too late. However, for the purpose of holding states responsible, the model assumes that there are preventative efforts in place that would reduce the noise, thereby mitigating the risk of legitimate network activity being used to disguise an attack.

3. Libicki, *Cyberdeterrence and Cyberwar*, 44.

4. Healey, "The Spectrum of National Responsibility for Cyber Attacks"; Kanuck, "Sovereign Discourse on Cyber Conflict under International Law"; and Yannakogeorgos and Mattice, *Strategically Using Global Norms to Resolve the Cyber Attribution Challenge*.

5. A separate but related question is whether cyber is a domain at all or whether the electromagnetic spectrum is the domain and cyber is simply a means for enhancing the ability to exploit it. A similar parallel is how airspace is the domain and aircraft allow its exploitation. However, air traffic control corridors and other man-made elements for the exploitation of airspace are not domains.

6. Air Force Doctrine Document 3-12, *Cyberspace Operations*, 2–3.

7. Clark, *Characterizing Cyberspace*.

8. Ibid., 1. Note that the definition of *cyberspace* the Joint Chiefs of Staff provide in the *National Military Strategy for Cyberspace Operations* is parsimonious with Clark's character-driven versus purpose-driven definition. The USAF should consider embedding the JCS definition within its doctrine.

9. Healey, "Spectrum of National Responsibility for Cyber Attacks."

10. Clark and Landau, "Untangling Attribution," 25.

11. Libicki, *Cyberdeterrence and Cyberwar*, 41–52, 99–100.

12. A note of caution with the hope latched onto IPv6—while it works well on a small scale, it will still contain vulnerabilities that may not be known until deployed on a vast scale. New security vulnerabilities will be discovered and exploited, and the learning curve will be just as steep as for the deployment of IPv4.

13. Clark and Landau, "The Problem Isn't Attribution," 1.

14. TCP/IP is standardized by the International Organization for Standardization (ISO) for the open systems interconnection (OSI) model as the basis of Internet and other networking.

15. Lipson, *Tracking and Tracing Cyber-Attacks*, 5.

16. Waldrop, "DARPA and the Internet Revolution." See also Leighton, "The Net's Real Security Problem," 44.

17. Ibid.

18. Molyneux, *The Internet under the Hood*, 85–86.

19. Ibid., 27.

20. Indeed, as part of its Internet freedom agenda, the US Department of State, in cooperation with Internet companies, is distributing tools for and running seminars on how to mask one's identity in cyberspace. While the goal is the free flow of information, these tools and tactics can be used to attack US-based information systems as well. This does not contribute to a safe cyber ecosystem.

21. Denning and Denning, eds., *Internet Besieged*, 35.

22. Zetter, "Rogue Nodes Turn Tor Anonymizer into Eavesdropper's Paradise."

23. Harrison and White, "A Taxonomy of Cyber Events Affecting Communities," 1–9. This work included natural events; however, for the purpose of this paper, chipmunks chewing through fiber-optic cables is not deemed to be relevant to state responsibility for cyber attacks.

24. Nelson et al., *Cyberterror*, 90.

25. Rowe et al., "Steps towards Monitoring Cyberarms Compliance."

26. I am grateful to Mr. Lynn Mattice, president and founder, National Economic Security Grid, for this observation.

27. Yannakogeorgos, "Promises and Pitfalls of the Private Public Partnership Model," 259.

28. Microsoft Corporation, "China Information Technology Security Certification Center Source Code Review Lab Opened."

29. Barrett, "Information Warfare: China's Response to U.S. Technological Advantages."

30. DOD, *Department of Defense Strategy for Operating in Cyberspace*, 7.

31. Brossard and Demetrescu, "Hardware Backdooring Is Practical."

32. One such option, as mentioned in Brossard, is to "offer a physical switch which needs to be manually auctioned to allow the flashing of the firmware." Such a solution would certainly resolve the issue of kernel-level infections.

33. DOD Instruction 5205.13, *Defense Industrial Base (DIB) Cyber Security/ Information Assurance (CS/IA) Activities*.

34. Personal interview with CISO from a Fortune 500 company in mid 2012.

35. Personal interview with professor of computer science at a US top-100 school.

36. Killcrece, *Steps for Creating National CSIRTs*, 8.

37. Ibid, 17.

38. International Telecommunications Union (ITU), *ITU/IMPACT Country Readiness Assessment to Establish a National CIRT*. ITU-IMPACT has, to date, completed CIRT workshops for 29 countries to assist them in setting up an implementation plan.

39. UN Department of Economic and Social Affairs, *Cybersecurity*.

40. Sandoval, "Top ISPs Agree to Become Copyright Cops."

41. Microsoft Corporation, *European Telecom Uses Microsoft Security Data to Remove Botnet Devices from Network*.

42. Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation and the Internet Economy*, 18; and Department of Homeland Security, *Enabling Distributed Security in Cyberspace*.

43. Federal Communications Commission, Reliability and Interoperability Council, Working Group 8, Communications Security, *Final Report*.

44. Gross, "ISPs."

45. TeliaSonera, *TeliaSonera's Response to the European Commission Consultation on Net Neutrality and the Open Internet*.

46. C. Chung et al., "Comcast's Web Notification System Design."

Chapter 3

American Sponsorship of Embryonic Global Norms

Global norms, institutions, and patterns of cooperation among state and private sector stakeholders can serve as a foundation for solving the attribution problem in cyberspace. Norms of state responsibility in cyberspace must be institutionalized at the international level, and they must be enforced by relevant US government departments, including defense, state, justice, and commerce, and by other appropriate federal, national, state, and tribal agencies.

More than one American expert has noted that "although numerous multinational organizations are working on various aspects of cyber crime and/or cyber conflict, only ITU has taken a global view and put forth an agenda intended to address major problem areas, while leveraging the efforts of other organizations."[1] In this section, I aim to describe a process that might be used to modify the policy actions of states and hold them responsible for their actions. I argue that ineffective US attempts at multilateralism will result if the United States continues its path to pick alternative forums and tries to lead the world into them. Instead, I use the lens of US "sponsorship" of global norms as the suggested way forward to achieving US objectives of securing cyberspace.

It is without question that the United States has the most superior military in the world. This does not equate with being able to influence processes to achieve policy objectives.[2] The logic of the current US position is that the United States should be able to both make and break norms at will to achieve policy goals. As Finnemore and Sikkink state, "Sometimes these platforms are constructed specifically for the purpose of promoting the norm, as are many nongovernmental organizations (NGO) (such as Greenpeace, the Red Cross, and Transafrica) and the larger transnational advocacy networks of which these NGOs become a part (such as those promoting human rights, environmental norms, and a ban on land mines or those that opposed apartheid in South Africa)."[3]

International organizations, as conduits, play a crucial role in diffusing norms. For example, Finnemore and Sikkink suggest, "The structure of the World Bank has been amply documented to effect the kinds of development norms promulgated from that institution; its organizational structure, the professions from which it recruits, and its relationship with member states and private finance all filter the kinds of norms emerging from it. The UN, similarly, has distinctive structural features that influence the kinds of norms it promulgates about such matters as decolonization, sovereignty, and humanitarian relief."[4] Professionals, with legitimacy born of their expertise and access to information, influence the behavior of other actors, including states.

The concept of American sponsorship of global norms has emerged within the global affairs community as one way to address complex transnational policy issues. Global affairs expert Simon F. Reich suggests this as a way to merge hard and soft power to effect change on certain transnational policy issues. This concept entails an American "willingness to enforce or underwrite the costs of enforcing a policy without necessarily taking the lead in placing it on the agenda. . . . Sponsorship entails the selective enforcement, by the United States, of policy initiatives promoted by NGOs and codified by global organizations. Where such conditions exist, global norms take root and influence behavior."[5] The process of norm development and articulation by private entities, norm codification, and norm institutionalization is a critical formula for American sponsorship to be effective. When these conditions are not met, US sponsorship is observed as unilateral, imperialistic, or ineffectively multilateral. It does not result in the desired outcome of behavioral management in accordance with the norm. According to Reich, three conditions must be met for the creation of a global norm: broad-based support of private entities, global institutional codification, and American sponsorship through enforcement.[6] As outlined in the previous chapter, the first sequence—that is, the articulation of norms and their (attempted) institutionalization—has been met. What remains to be done is for the United States to sponsor norms with soft- and hard-power mechanisms. One way forward is outlined below; however, it remains for policy makers to work toward the formulation of effective US international cyber policy that takes these academic theories and applies their lessons to practice. Table 2 represents the various variables involved in norm lifecycles.

Table 2. Norm lifecycles and American support

	Yes	No	Outcome
Entrepreneurial support	X		Articulation, consolidation, and implementation of global norm
Institutionalization	X		
American support	X		
Entrepreneurial support		X	Articulation and implementation of imperialist policies lacking global legitimacy
Institutionalization	X		
American support	X		
Entrepreneurial support	X		Weak multilateralism
Institutionalization		X	
American support	X		
Entrepreneurial support	X		Norms articulated and consolidated but weakly implemented
Institutionalization	X		
American support		X	
Entrepreneurial support	X		Norms articulated but not consolidated or implemented
Institutionalization		X	
American support		X	
Entrepreneurial support		X	US unilateralism or bilateralism
Institutionalization		X	
American support	X		
Entrepreneurial support		X	Empty cell
Institutionalization		X	
American support		X	
Entrepreneurial support		X	International regime in decline. Very weakly implemented
Institutionalization	X		
American support		X	

Reprinted from Simon Reich with Panayotis A. Yannakogeorgos, *Global Norms American Sponsorship and the Emerging Patters of World Politics* (New York: Palgrave Macmillan, 2010), 17.

Beyond possible bilateral measures, a global policy framework for holding all states responsible for cyber attacks originating or transiting through their territory is required. The retaliation framework introduced in the previous chapter would help guide these efforts. It is argued that a toolbox for responding to attacks needs to be further developed to address appropriate responses to states that fall within the spectrum of responsibility. Elsewhere, I have recommended that the DOD and USAF create a resource similar to the State Department's annual *Trafficking in Persons [TIP] Report* as a first step toward developing global norms that will help identify what degree of responsibility a state must bear in a cyber attack.[7] It has taken almost a century for antitrafficking initiatives to evolve from an area of nongovernmental concern to criminalized activity under international law. However, perhaps as a result of information and communication technology (ICT), cybersecurity efforts within institutions of diplomacy have been catalyzed. What remains is for the US government to clean up the country's cyber environment and take the global lead to establish the coercive mechanisms that will solidify global norms of behavior for cyberspace.

American Sponsorship of Global Norms

The United States generally uses diplomatic pressure to engender domestic reforms and stimulate enforcement of minimum standards for the elimination of trafficking in persons by governments in individual countries. Antitrafficking initiatives have a long history, with early efforts beginning in the mid-nineteenth century and resulting in various treaties. The UN has been dealing with this issue since the inception of the organization, largely as the result of pressure from nongovernment organizations. However, during the Cold War, nuclear and other security issues did not allow for the United States to focus on trafficking issues. In the mid-nineties, as a result of US-based NGO pressure on the US government, antitrafficking became an important item on the US policy agenda, leading up to the Trafficking Victims Protection Act (TVPA) of 2000.

I suggest that one way forward is to look at the success of the United States as the world leader in stemming the scourge of human trafficking as a model for international engagement in cyberspace. Hence, the antitrafficking agenda has many parallels to the global cybersecurity agenda. The following draws on these commonalities to illustrate that policy tools exist to hold states accountable for the actions of transnational elements operating on their soil.

The Anti-Trafficking-in-Persons Initiative

The TVPA added a coercive capacity to US government efforts to curb the transnational problem of modern-day slavery.[8] Like cyber crime, human trafficking relies on actions not directly attributable to a state government. Nevertheless, states could still be held responsible for not doing enough to end its menace. To gauge progress on implementing the minimum standards for the elimination of trafficking applicable to the government of a country of origin, transit, or destination for victims of severe forms of trafficking, the TVPA mandated that the *Trafficking in Persons Report* be issued annually by the DOS Office to Monitor and Combat Trafficking in Persons. On the basis of these minimum standards, the *TIP Report* is designed to grade the efforts of individual countries with the intent of "naming and shaming" (and potentially sanctioning) states adjudged to be wavering in their efforts.[9]

Based on a three-tier scale, the TIP process's intent is to coerce the worst transgressors (Tier 3 countries) through the threat of a variety of sanctions. Tier 1 countries are those whose governments are complying with the minimum standards. Tier 2 countries are not complying but are making significant efforts to do so. Tier 2 watch list countries are those in which there are a significant or increasing number of trafficking victims as well as an increasing failure to show evidence of taking additional steps to combat that situation, in contrast to the commitments the country made in the prior year. Once a country is placed on the Tier 2 watch list in the annual *TIP Report*, it is liable to automatic downgrading to Tier 3 status. Tier 3 countries face sanctions.

To further enhance the TVPA, Congress enacted and Pres. George W. Bush signed, the Trafficking Victims Protection Reauthorization Act, which refined and expanded the "minimum standards" for foreign governments, increased their responsibility for provision of data, created a new "watch list" category, and, again, substantially increased funding. Furthermore, to demonstrate his commitment of prosecuting US citizens, President Bush signed the PROTECT (Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today) Act into law, granting the United States extraterritoriality in the prosecution of US citizens engaged in child sex tourism.[10] Furthermore, section

7202 of the Intelligence Reform and Terrorism Prevention Act of 2004 established the Human Smuggling and Trafficking Center "to improve the effectiveness of ongoing interagency efforts, particularly in supporting the conversion of intelligence into appropriate enforcement and other response actions [and] to achieve greater integration and overall effectiveness in US government enforcement and other response efforts and to promote intensified efforts by foreign governments and international organizations to combat these problems."[11] In addition to the TIP program's potential sanctions, the Department of Justice provides training and logistical support to other states in conjunction with the FBI's International Criminal Investigative Training and Assistance Program, while the Department of Labor holds prevention and awareness-raising programs abroad.[12]

Naming and shaming are not enough to cause governments to change their behavior. To give antitrafficking initiatives a coercive capacity, the United States uses its annual *TIP Report* and UN initiatives to go beyond naming and shaming. Tier 3 countries can be subject to sanctions on "nonhumanitarian, nontrade related foreign assistance."[13] Similarly, the United States has threatened to withdraw its support for loans from international financial institutions, such as the International Monetary Fund (IMF) and the World Bank, for countries that either do not pass requisite laws or do not enforce them.[14] Nations face potential loss of US military and economic assistance as well as World Bank and IMF support.[15] The United States is the largest depositor at the World Bank and the IMF and US support has substantial implications for countries seeking loans. The United States has been just as aggressive on a regional level in organizations such as the Organization for Security and Cooperation in Europe (OSCE) and the Southeast European Cooperative Initiative (SECI).

This is a good model on which to begin shaping US policies toward malicious cyber behavior. In the following section, I provide a brief tracing of the fundamental international agreements where cyber norms are being articulated and developed. The broad ideas have been echoed in US policy. However, when the global community attempts to institutionalize the norms within existing forums, such as the International Telecommunication Union, there is US backlash. This, I believe, is a misguided approach and will lead the world away from coherent cybersecurity cooperation. Indeed, one Pew survey of international perceptions of America's effort to lead the world concluded that "on average, only one in four agrees that the United States is an important leader in promoting international laws and sets a good example by following them, while two-thirds say the United States tries to promote international laws for other countries, but is hypocritical because it does not follow these rules itself."[16] Such perceptions of US "leadership" just as easily extend to the cyber domain where the United States may be trying to lead the world in developing global norms of behavior for cyberspace, while concurrently it leads the world in infected machines and as a source of cyber attacks.

The Global Culture of Cybersecurity and Embryonic Norms for State Responsibility in Cyberspace

What are the prospects of resolving the cyber attribution challenge given our present knowledge of politics, government, and law? Global cybersecurity is hindered by a lack of cybersecurity action plans for organized defense at the national level. Such plans would employ the technological, managerial, organizational, legal, and human competencies in national security strategies for defense.[17] Criminals, privateer-hacker networks, and information warriors exploit countries lacking these structures for cyber attacks of national and global significance. Indeed, the vitality of American social, economic, and governmental institutions is at great risk from cyber vulnerabilities present in less developed countries.[18] Reducing the threats to the United States from cyber attack depends on support for already articulated international norms of behavior, enforced by local authorities, to secure the global cyber ecosystem.[19] Specifically, the global culture of cybersecurity, which is a broad normative framework, has already been accepted over the past decade. The norms therein may serve as bases for discerning a state's wrongful acts in cyberspace.

Cyber norms guiding responsible nation-state behavior have been articulated in various forums. The Council of Europe's (COE) Convention on Cybercrime, November 2001, seeks the alignment of European Union (EU) member states' laws for evidence gathering and prosecution and increasing international collaboration and investigative capabilities to deal with cyber crimes. Ratified by the United States in 2007, elements of the COE convention are considered a model text for international cooperation.[20] The World Summit on the Information Society's Declaration of Principles committed to building a global culture of cybersecurity promoted, developed, and implemented in cooperation with all stakeholders and international bodies of experts.[21]

The Global Cybersecurity Behavioral Baseline

There is currently broad international consensus on what the behavioral baseline should be for cybersecurity. The global culture of cybersecurity grew from a series of United Nations General Assembly (UNGA) resolutions. The 2002 UNGA Resolution 56/19, "Developments in the Field of Information and Telecommunications in the Context of International Security," established several embryonic norms. The UNGA recognized the global characteristics of ICT, such as the Internet and World Wide Web (WWW), as the bases for the information society and determined that international cooperation is required to assure the peaceful use of ICT.[22] Further, it was acknowledged that ICT could be misused in ways that "adversely affect the security of states in both civil and military fields."[23] Member states were encouraged to prevent the use of information technology by criminals or terrorists while concurrently promoting its peaceful use, though guidelines for how to do so were not offered. In the operational paragraphs of Resolution 56/19, the UNGA calls on member states to support and contribute to multilateral efforts tasked with identifying present and future threats to international security resulting from the misuse of information technology and to develop countermeasures to these threats. Cybersecurity solutions must be "consistent with the need to preserve the free flow of information."[24] These elements planted the seeds of embryonic norms that continue to serve as the behavioral baseline for good behavior in cyberspace.

In 2002 the UNGA also passed Resolution 56/121, "Combating the Criminal Misuse of Information Technologies," and strengthened the language of Resolution 56/19, saying that the "misuse of information technologies may have a grave impact on all States" and encouraging the utilization of ICT to enhance international cooperation and coordination.[25] A limiting factor to securing cyberspace was identified. "Gaps in the access to and use of information technologies by states can diminish the effectiveness of international cooperation in combating the criminal misuse of information technologies."[26] The UNGA called for "cooperation between States and the private sector in combating the criminal misuse of information technologies . . . [and] for effective law enforcement."[27] To preserve the utility of cyberspace, all states must have access to and use ICT and establish mechanisms to deter the criminal misuse of telecommunications technologies. The UNGA provided a framework for international cyberspace development in Resolution 56/121 by calling for transfer of information technology to developing countries and the training of their people to use it, thereby enhancing international cooperation in combating the criminal misuse of information technology.

In 2004 the concept of a "global culture of cybersecurity" (GCC) was articulated in UNGA Resolution 57/239.[28] Member states recognized that "effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society."[29] "Technology alone cannot ensure cybersecurity. . . . In a manner appropriate to their [respective] roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for, and take steps to enhance the security of these information technologies."[30] The resolution is not binding, but the basic tenets of the global culture of cybersecurity are summarized in table 3.

Table 3. Foundations of the global culture of cybersecurity

Element	Intended outcome
Awareness	All information society stakeholders, including individuals, should sustain a level of awareness regarding the importance of having secure information systems.
Responsibility	Stakeholders are responsible for securing their own information systems and reviewing the policies, practices, measures, and procedures pertaining to their own cyberspace.
Response	Timely and cooperative response is achieved with stakeholders sharing information about threats, vulnerabilities, and security incidents to facilitate the detection of and response to the misuse of information systems. Cross-border information sharing may be required.
Ethics	The ethical basis of the GCC is founded on utilitarian grounds in that each participant is expected to respect the interests of others and to act or avoid inaction that will harm others.
Democracy	Cybersecurity regimes are guided by democratic principles, identified as the freedom of thoughts and ideas, free flow of information, confidentiality of information and communication, protection of personal information, openness, and transparency.
Risk assessment	Periodic broad-based risk assessments of the security implications of technological, physical, and human factors, policies, and services should be conducted to determine what an appropriate level of risk is and how best to manage the risk of potential harm to information systems according to a scale based on the importance of information to the information system being assessed.
Security design and implementation	Security should be incorporated during the planning, design, technological development, operation, and use of an information system.
Security management	It is on the basis of dynamic risk assessment that security management occurs.
Reassessment	Given the dynamic nature of the information insecurity, in order to assure that all the above elements remain relevant, a periodic reassessment of security protocols and procedures is required.

Adapted from UN General Assembly, "Creation of a Global Culture of Cybersecurity," Resolution A/RES/57/239, 31 Jan 2003, 2–3, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

In 2003 the UNGA addressed cyber threats to critical information infrastructures.[31] Critical infrastructures are identified as "those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations."[32] It is urged that emergency warning networks should be established to identify and warn of cyber vulnerabilities, threats, and incidents.

- General awareness should be raised about the importance of critical infrastructures as well as the roles that stakeholders have in infrastructure protection.
- The formation of partnerships between private and public stakeholders to prevent, investigate, and respond to threats to critical information infrastructures should be encouraged.
- Communications networks should be in place and regularly tested to assure their effective operation during a crisis situation.
- States should develop adequate domestic laws and policies to allow the investigation and prosecution of cyber crime. States should also assure adequate trained personnel to accomplish investigation and prosecution.
- States are responsible for identifying the perpetrators of attacks against critical information infrastructure and sharing of this information with affected states.
- Appropriate international cooperation should take place in accord with properly crafted domestic laws assuring that critical information infrastructures are secure.

The statement of the role of the government in dealing with the critical information infrastructure is clearer than in previous resolutions. Constant testing of the protection systems and education of personnel are deemed essential for the success of such measures.

In 2009 the UNGA mandated a UN Group of Governmental Experts on Cybersecurity: "On the basis of equitable geographical distribution, a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems."[33] Based on the results of this work, the group prepared a report for the UN

Secretary General in 2010.[34] The group recognized a need for enhanced dialogue among states to develop measures that would reduce collective risk to national and global cyber infrastructures. It also stated that "existing agreements include norms relevant to the use of ICTs by states. Given the unique attributes of ICTs, additional norms could be developed over time."[35] The existing agreements are not specified, though these would include current international laws, such as the UN Charter in addition to UNGA resolutions and the World Summit on the Information Society (WSIS) outcome documents. One may extend this to say that the norms of good cyber behavior actually do exist. However, as in all matters of international law, the elaborations, perceptions, and interpretations of the elements in existing agreements and UNGA resolutions need global recognition and acceptance.

In March 2010, the UNGA adopted Resolution 64/211 on the "creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures." The resolution included an annex to serve as a self-assessment tool for national efforts to protect critical information infrastructures. It addressed assessment of cybersecurity needs and strategies, stakeholder roles and responsibilities, policy processes and participation, public/private cooperation, incident management and recovery, and legal frameworks. However, "this is a voluntary tool that may be used by Member States, in part or in its entirety, if and when they deem appropriate, in order to assist in their efforts to protect their critical information infrastructures and strengthen their cybersecurity."[36] These UN efforts should be the framework for the criteria for determining a state's responsibility. Without American sponsorship, enforcement of the global culture of cybersecurity will not work.

The WSIS and Global Cybersecurity

The global community finalized the *Declaration of Principles* and *Plan of Action* for the information society at two convenings of the WSIS. These proceedings were unique because they included state and nonstate actors. Global norms of behavior for the information society were developed in the lengthy negotiations leading up to and during the summits.

States are predominant in the negotiations in the Internet government and cybersecurity forums being held by the UN. The foundational work was carried out in the preparatory committees and the regional and other conferences related to the WSIS.[37] The preparatory phases were the most important since this is where nation-states voted on items for the summits' agendas, the processes and procedures of the summit, and the wording of the final-outcome documents presented and finalized at the actual summits. The states also interacted with global civil-society actors. Regional meetings were held to supplement this work to assure that each region could voice its own needs and expectations regarding the information society. By these means, the global community has established generally accepted norms of behavior and indicators of appropriate state behavior in cyberspace.

Figure 11 illustrates the broad participation in the WSIS processes held under the auspices of the United Nations and the ITU. Originally founded in the mid-nineteenth century to regulate international telegraphy, the ITU has brought government and private telecommunications interests together to negotiate standards, development, and other issues pertaining to ICT. Private ICT corporations have built trust over time as active contributors to the ITU's program of work. Although business entities do not have voting rights at the ITU, they do serve as norm entrepreneurs who articulate standards of behavior and provide agenda items.

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

During the lead-up to the WSIS, the United Nations Economic Commission for Europe reported on challenges to the WSIS process. It noted that complexities and controversies arising from the process were due not only to development issues, but also to political questions including the issue of security.[38] Furthermore, the commission noted (in 2002) that "there is a growing sense of fatigue with global conferences and processes, and that there is no global architecture for international dialogue on knowledge of information technologies."[39]

As of 2012, the appropriate global architecture for international dialogue continues to be a hotly contested agenda issue. As an increasing number of track-two diplomatic initiatives ramp up (e.g., EastWest Institute's Worldwide Cybersecurity Initiative), conference fatigue remains a key concern.

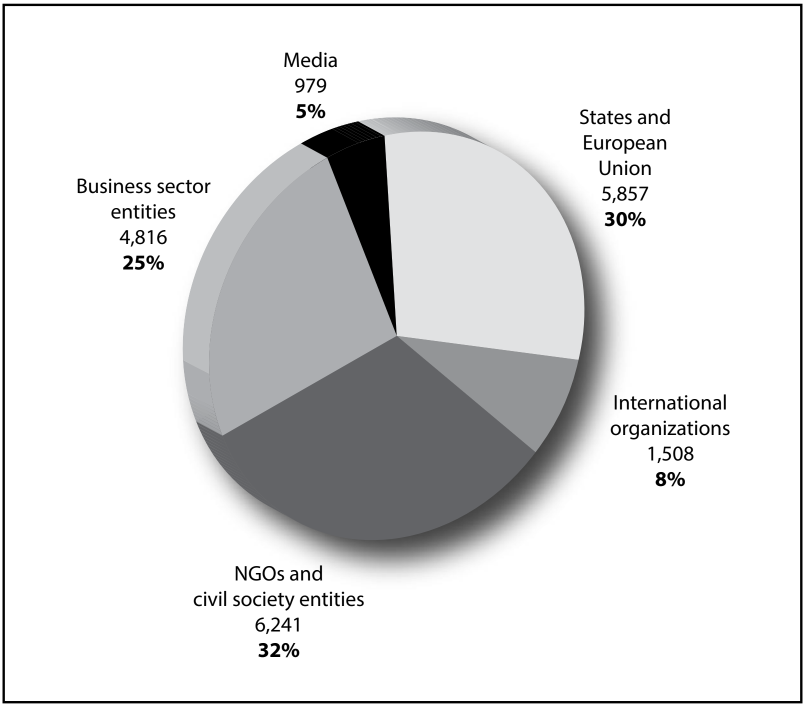


Figure 11. Number of participants at WSIS as of 18 November 2005. (Adapted from: "Number of participants recorded by the World Summit for the Information Society," *About WSIS*, http://www.itu.int/wsis/tunis/newsroom/index.html.)

The outcome documents of the WSIS established that security is the foundation of the information society. Paragraph five of the Geneva *Declaration of Principles* states that users must have confidence in the information society. A framework of trust that includes "information security and network security, authentication, privacy and consumer protection" must be established to assure that data, privacy, access, and trade are protected.[40] The WSIS also recommended that appropriate actions at the national and international levels should be taken to secure cyberspace so that ICT is not used "for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within states."[41] In this regard, the *Declaration of Principles* called for all interested stakeholders to have a strong commitment to "digital solidarity" with governments at the national and international level and recognized that new forms of partnership will be required in order to meet the goals set out in the declaration.

Participants in the first phase of the WSIS in Geneva also negotiated and agreed on a *Plan of Action*. In section C5.12, the WSIS laid out the actions needed to reach the objectives contained in paragraph five of the *Declaration of Principles*.[42] Reiterating the importance of security and its role in developing users' confidence with ICT, the *Plan of Action* recommended private/public partnerships for the prevention, detection, and response to cyber crime and ICT misuse. Governments are encouraged to develop guidelines to support the ongoing efforts in these areas.

The *Plan of Action* emphasized the "need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues."[43]

The work at the UNGA and WSIS has established a global behavioral baseline of responsible activities in cyberspace. It sets forth the criteria for the national responsibilities to secure domestic cyberspace and cooperating in a community to prevent the use of cyberspace by malicious actors.

In 2011 the White House released the US *International Strategy for Cyberspace*. This document echoes much of the UNGA and WSIS processes. The United States will

> expand and regularize initiatives focused on cybersecurity capacity building—with enhanced focus on awareness-raising, legal and technical training, and support for policy development. Such programs must address more than purely technology issues; we will work with states to recognize the breadth of the cybersecurity challenge, assist them in developing their own strategies, and build capacity across the whole range of sectors—from network security and the establishment of

> Computer Emergency Readiness Teams (CERTs), to international law enforcement and defense collaboration, to productive relationships with the domestic and international private sector and civil society.[44]

This conforms to the tenets of the global culture of cybersecurity and indeed echoes the work already being done by IMPACT, the global culture of cybersecurity's operational arm, although the United States does not currently support it.[45] The IMPACT Global Response Centre, based in Cyberjaya, Malaysia, was set up in 2009 to serve the international community by proactively tracking and defending against cyber threats. Its alert and response capabilities include an early warning system that enables IMPACT members to identify and head off potential and imminent attacks. Although norms of cyber behavior have been established, what is missing is American sponsorship of those norms. The United States should more actively support these efforts as, in the words of John Grimes, former chief information officer of DOD, IMPACT "is something that is sorely needed. . . . [It's] filled an important international gap in cyber response and cooperation."[46]

Internationally Wrongful Acts in Cyberspace

The law of state responsibility is very complicated and took three decades to develop. In August 2001 the International Law Commission adopted the *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, which have established the principle of state responsibility in international law. State responsibility can be extended if the nature of a cyber attack is such that malicious data packets are traced back to national territory. Chapter 2, article 4, states that "the conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other function, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State."[47] State responsibility might be extended to cyber attacks from national territory as an accepted principle of due diligence under the global culture of cybersecurity. That is, state responsibility could be inferred, maybe, in an act of omission (as opposed to an act of commission).

Furthermore, article 5 states that "the conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of the State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance."[48]

How can we hold a state responsible for activities in cyberspace? Some arguments focus on tests for the degree of control the state might have had over nonstate actors within their territory to establish overall and effective control.[49] Past precedent within the United Nations suggests that nonstate actors function as de facto agents of the state if the state is harboring them. After 9/11, NATO attacked al-Qaeda and the Taliban. No one thought that the Taliban had control over al-Qaeda, but they were not preventing it the use of Afghan territory. The international community accepted intervention against a state for the actions of nonstate actors in part because the UN Security Council had voted on Resolution 1267 in 1999 that placed sanctions on both al-Qaeda and the Taliban in Afghanistan.

Sponsorship of "illegal" acts and actual control over the nonstate actors within national territory are important here. For example, if a state provides hacker tools online and encourages hackers to use those tools to perpetrate attacks, then the state is culpable for the hackers' actions. However, the level of official involvement is most often difficult to discern—much less prove. This is why the responsibility to respond, as stated in UNGA resolutions, is an important norm to sponsor and enforce. In the Estonia cyber attack case of 2007, patriotic hackers in Russia were launching attacks against Estonia; however, since the Russian government was not openly encouraging the hackers, Russia could not be held responsible under the law of state responsibility. At the same time, it was not responding to requests for assistance, contrary to its support of the tenets of the global culture of cybersecurity in UNGA and the ITU.

Global norms articulated in the UNGA can serve to establish levels of state responsibility in a cyber attack. Although present international law does not explicitly address malicious cyber incidents, an argument can be made that the UNGA and other UN efforts related to global cybersecurity establish the baselines for state responsibilities in cyberspace.

Notes

1. Westby, "Conclusion."

2. For an important critique of the contemporary realist approach on the grounds that it fails to link power to influence, see Lebow, "Power, Persuasion and Justice."

3. Finnemore and Sikkink, "International Norm Dynamics and Political Change," 899.

4. Ibid.

5. Reich and Yannakogeorgos, *Global Norms, American Sponsorship, and the Emerging Pattern of World Politics*, 3.

6. Ibid., 4.

7. While there are suggestions to use models based on counterterrorism efforts, such models should be avoided. Based on discussions in international forums, such as the EastWest Institute's Worldwide Cybersecurity Initiative in London in June 2011 (which the author attended), equating cyber crime with terrorism is a controversial approach that will not promote cooperation.

8. For a more comprehensive account of the Trafficking Victims Protection Act, see Reich and Yannakogerogos, "George Bush and the Sponsoring of the Anti-Trafficking Norm."

9. Note that if a similar mechanism were created, there is a contrast in cyberspace. Although the Department of State (DOS) is uniquely positioned to collect information from nongovernmental organizations (NGO) on human trafficking, the technical nature of cyberspace makes the DOD the more suitable element of national power to collect information on cyber compliance.

10. Further, in January 2006, President Bush signed H.R. 972, the Trafficking Victims Protection Reauthorization Act. This amended the original Trafficking Victims Protection Act further by increasing assistance to foreign victims trafficked to the United States, increasing focus on children, and directing relevant US agencies to develop antitrafficking strategies for postconflict and humanitarian crisis areas. It also extended US extraterritoriality for US government workers and contractors who are involved in "acts of trafficking," addressing the problems of peacekeeper and aid personnel who are "complicit" in trafficking. See Department of Justice, *Assessment of U.S. Government Efforts to Combat Trafficking in Persons in Fiscal Year 2004*, 13–14.

11. DOS, *Charter and Amendments*.

12. Concurrent with these legal efforts, the United States aggressively pursues regional and multilateral initiatives. It was an instrumental force in the UN Commission on the Status of Women's adoption of the trafficking resolution. See UN Commission on the Status of Women, "Eliminating Demand for Trafficked Women and Girls for All Forms of Exploitation."

13. DOS, *Working for Women*. The document was prepared for the 10th anniversary of the Beijing Declaration of the UN Commission on the Status of Women.

14. Miko, *Trafficking in Persons*, 8–14.

15. "America Will Not Tolerate Slave Traders, Bush Says," *America in Context*, 9, 6.

16. See "Though Obama Viewed Positively, Still Much Criticism of US Foreign Policy," *World Public Opinion.org.*

17. Ghernouti-Helie, *A National Strategy for an Effective Cybersecurity Approach and Culture.*

18. Gady, "Africa's Cyber WMD [Weapons of Mass Destruction]."

19. US Secretary of State Hillary Clinton gave a speech on Internet freedom in which she stated,

> The spread of information networks is forming a new nervous system for our planet. . . . States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among States and encourage respect for the global networked commons.
>
> Clinton, "Remarks on Internet Freedom."

20. Council of Europe, *Convention on Cybercrime.*

21. World Summit for the Information Society (WSIS), *Declaration of Principles.*

22. UN General Assembly (UNGA), "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/56/19, preliminary para. 7.

23. Ibid., preliminary paras. 7 and 8.

24. Ibid., operation para. 1.

25. UNGA, "Combating the Criminal Misuse of Information Technologies," preliminary para. 5.

26. Ibid., preliminary para. 6.

27. Ibid., preliminary paras. 8 and 11.

28. UNGA, "Creation of a Global Culture of Cybersecurity."

29. Ibid., preliminary para. 5.

30. Ibid., preliminary paras. 7 and 8.

31. UNGA, "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures."

32. Ibid., "Annex: Elements for Protecting Critical Information Infrastructures," preliminary para.3.

33. UNGA, "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/60/45.

34. Indicative of the broad representation are the 15 nation-states from which representatives were appointed from Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom, and the United States.

35. UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 8.

36. UNGA, "Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures."

37. Yannakogeorgos, "Cyberspace."

38. UN Economic Commission for Europe (UNECE), *Information Society in Europe and North America*, 3.

39. Ibid.

40. Ibid., para. 5.35.

41. Ibid., para. 5.36.

42. WSIS, *Plan of Action*, section C5.12.

43. WSIS, *Tunis Agenda for the Information Society*, para. 69.

44. The White House, *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*, 15.

45. Westby, "US Administration's Reckless Cyber Policy Puts Nation at Risk."

46. Ibid.

47. UN, *Responsibility of States for Internationally Wrongful Acts, 2001*, pt. 1, chap. 2, art. 4.

48. Ibid., art. 5.

49. Shackelford, "State Responsibility for Cyber Attacks."

Chapter 4

A Framework for Development, Diplomacy, and Defense

The subject of this chapter is a possible framework to guide US statecraft in cyberspace based on the antitrafficking initiatives the United States sponsored in the past decade. As has been noted throughout this work, nation-states are not currently held culpable for the actions of malicious agents in cyberspace. The United States–China Economic and Security Review Commission recently stated that "even if circumstantial evidence points to China as the culprit, no legislation or policy currently exists to easily determine appropriate response options to attacks on U.S. military or civilian networks in which definitive attribution is lacking. Beijing, understanding this, could easily exploit such gray areas in U.S. policymaking and legal frameworks to create delays in U.S. command decision making."[1] A framework for responding to a range of state activity in cyberspace is required—not only going after the people committing wrongful acts in cyberspace, but acting against the state that is responsible for either promoting or allowing malicious cyber activities.

Cyber statecraft specialist Jason Healey developed a taxonomy of a range of actions for state responsibility.[2] It provides a useful framework for categorizing state actions regarding cyber attacks. I have used it as a starting point for developing a broader response framework for actions or inactions in responding to a range of cyber incidents. Table 4 combines the Healy taxonomy with a framework for development, diplomacy, and defense.

In the range of state activities above, there are three phases of response within the categorization of state action that could potentially guide cyber statecraft responses by the US.

State-prohibited cyber attacks are those which a state has laws against and for which it has enforcement mechanisms in place but which may occur anyway. If cyber attacks occur despite prohibition, the state is nevertheless in violation of its responsibility to prevent use of its territory against other states,

Table 4. US cyber retaliation framework

		Development	Diplomacy	Defense
Range of State Activity	State prohibited	X		
	State prohibited but inadequate	X		
	State ignored	X	X	
	State encouraged		X	
	State shaped		X	
	State coordinated		X	
	State ordered			X
	State-rogue conducted			X
	State executed			X
	State integrated			X

Adapted from Jason Healey, "Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks" (Vienna, VA: Cyber Conflict Studies Association, 2010). The cyber retaliation framework is Dr. Yannakogeorgos's addition to a taxonomy for nation-state actions adapted from categories of nation-states in "Beyond Attribution."

but the state could be eligible for US aid in combating cyber crime. Refusing aid would then place the state in a subsequent category for response.

This second range for response options is one in which sanctions are either authorized bilaterally or pursued multilaterally and diplomatically. If there is some state involvement, then US countermeasures could be justified as well.

The standards of overall and effective control of cyber activity within and emanating from a sovereign territory are currently used to attribute state behavior. While useful guides, these standards do not completely resolve the attribution problem since there is no established case law where states have been held responsible for cyber attacks. The effective control standard requires proof of state involvement without any reasonable doubt.[3] The problem is that this standard relies on a world where perfect attribution exists—a world in which states have perfect evidence to attribute the attack. This world does not exist. On the other hand, the world where the overall control standard allows victims to hold states responsible for damages does exist and governments must be made aware of their obligations and the implications of failure to comply with their responsibilities under international law.

Development, Diplomacy, and Defense Responses

This section introduces a framework based on sponsored global norms.[4] The development, diplomacy, and defense structure articulated within the White House's recent *International Cyber Strategy* is a positive step toward American sponsorship of global norms. As has been noted, embarking on a path that diverges from the accepted global culture of cybersecurity established within the ITU will result in noncooperation and the United States being perceived as imperialist.[5] Indeed, this already seems to be the case. Closed forums such as the Organization for Economic Cooperation and Development (OECD), which is being pursued as a vehicle to forward US Internet policy, will not promote global cooperation for the security of the cyber commons except among already like-minded developed states. A way forward would be for like-minded states to use the OECD and other regional councils to develop common positions from which they can negotiate at the ITU. In this way, the United States could begin to manage the cyber behaviors of states with broad support and cooperation with the international community. Development, diplomacy, and defense could then be within US sponsorship of global policy initiatives.

Development

Not all countries have an equal capacity for investigating cyber events. They need assistance to help stem the flow of malicious activities through their borders. The ITU issues a Toolkit for Cybercrime Legislation that countries may use.[6] This is one way to provide technical assistance and education to all aspects of society, especially to government and law enforcement officials.

The White House's *International Strategy for Cyberspace* states that the United States

> will expand and regularize initiatives focused on cybersecurity capacity building—with enhanced focus on awareness-raising, legal and technical training, and support for policy development. Such programs must address more than purely technology issues; we will work with states to recognize the breadth of the cybersecurity challenge, assist them in developing their own strategies, and build capacity across the whole range of sectors—from network security and the establishment of Computer Emergency Readiness Teams (CERTs), to international law

enforcement and defense collaboration, to productive relationships with the domestic and international private sector and civil society.[7]

This echoes several of the elements of the global culture of cybersecurity, as well as the work being done within the ITU's IMPACT. With US sponsorship these endeavors could be undertaken within existing multilateral institutions. The existing institutional frameworks, such as those being developed at IMPACT, could be used to avoid duplicating efforts within frameworks accepted by other countries. This would also avoid the risk of the United States appearing imperialistic.

Diplomacy

To offer technical assistance and development, partnerships with countries need to be established on the basis of trust and confidence. The White House strategy notes, "As countries develop a stake in cyberspace issues, we intend our dialogues to mature from capacity-building to active economic, technical, law enforcement, defense and diplomatic collaboration on issues of mutual concern."[8] The strategy also clearly articulates that the White House will take steps to "facilitate relationships among countries developing cybersecurity capacity—using both regional fora and technical bodies possessing specialized expertise—and will continue to promote the sharing of best practices, lessons learned, and international technical exchanges."[9] While these are positive words, the United States should abandon the practice of forum picking. Despite the shortcomings of the ITU, the United States must lead within this institution to assure that others follow.

The DOD and the Air Force with its global mission also have roles to play in this diplomacy. The 2011 *National Military Strategy* maintained that the DOD is essential in fostering regional and international cooperation in response to transnational threats. For example, cooperative security could be further developed by funneling transnational threats through combatant commanders who can leverage their resources "tailor[ed] to their region and coordinate[d] across regional seams."[10] The Air Force conducts an array of diplomatic missions established in the Air Force Security Cooperation Strategy and offers many additional irregular and ad hoc diplomatic missions.[11] Given its cyber technical expertise, the Air Force would be optimally positioned to assist nations in their development—with foreign officer cybersecurity training within its Air University—and in building international partnerships for exchanging technical information on cyber attacks. Since the Air Force was the first to stand up a cyber command, Air Force experience would be useful in assisting friends and allies in standing up their own cyber commands.

More rigorous diplomatic initiatives could also be directed toward states that choose to continue down the path of ignoring, encouraging, shaping, and/or coordinating cyber attacks. The US policy community could explore a framework for invoking chapter 7 of the UN Charter to authorize sanctions against countries that fail to abide by global norms of behavior in cyberspace. Proposals for new legal mechanisms to combat cybercrime and global cyber attacks have also been suggested.[12] However, these will be long-term legal efforts similar to the UN Convention on the Law of the Sea and International Court of Justice processes; the same controversy surrounding the latter would likely exist with the formation of cyber legal mechanisms.

Both soft and coercive diplomacy thus could serve to strengthen the role of capacity-building initiatives. They also provide institutional frameworks for cooperation among like-minded countries wishing to benefit from a trustworthy cyber environment. States can be held responsible for their actions by eliminating the option of plausible deniability.

Defense

Inevitably, the United States will face adversaries who are ordering, executing, and integrating attacks or cooperating with rogue entities. The US military leadership has purposed to "be prepared to demonstrate the will and commit the resources needed to oppose any nation's actions that jeopardize access to and use of the global commons and cyberspace, or that threaten the security of our allies."[13] Defensive options in the face of cyber attack could include

- throttling Internet traffic,

- blocking Internet traffic,
- offensive computer operations in hot pursuit, or
- kinetic attacks in response to cyber events of national significance.

It is important to note that responses one and two above are not easy given that the private sector controls the infrastructure of the Internet. Additionally, since an argument could be made that such measures are contrary to the free flow of information across the global networks, a proper policy framework is needed to establish the conditions in which throttling or blocking Internet traffic could be justified. Sanctions, blocking, throttling of traffic, and other actions short of war could all be taken. Conflict in cyberspace that escalates into kinetic attacks could occur if the effects of cyber attack are consequential enough—attacks against critical infrastructures that create effects of national significance. Richard Clarke in his book *Cyber War* offers many such hypothetical scenarios.[14] Response to cyber attack would be a policy decision, not an automatic response. States engaged in cyber warfare might not even mask their activities, thereby obviating the attribution challenge altogether.[15]

A Need for Norms on Cyber Weapons

While global norms have been articulated regarding criminal and terrorist cyber activities, none have been devised regarding the design and use of cyber weapons. Stuxnet was a proof of concept attack against SCADA and ICS. Just because the United States was not the apparent target does not mean that it will not be in the future. Rumors aside, it is still unclear who launched Stuxnet—the malicious worm software that caused Iranian nuclear centrifuges to spin out of control.[16] However, it was a well-designed cyber weapon that did not cause global effects. Indeed, if Iranian claims are to be believed, its effects were reversed and Iran's nuclear program is back on track.[17]

The United States could begin advocating norms of responsible cyber weapon development. If properly designed, the effect of a cyber weapon can be reversed. For instance, according to Geneva Convention discussions on cyberspace, the effects produced in ball bearing factories could be such that they could be reversed upon war termination. Neil Rowe's framework for ethical cyber weapon design, below, is one good place to start. He describes several reversible ways that attackers attempt to foil their victims, including

1. encrypting key software and data so that victims are unable to decrypt it;
2. obfuscating systems via data manipulations that are hard to understand yet algorithmic and reversible;
3. withholding key information that is important to the victim; [and]
4. deceiving victims to make them think their systems are not operational when they actually are.[18]

As Rowe describes, "In the first two cases, reversal can be achieved by software operations by the attacker; in the third case, the attacker can restore missing data; and in the fourth case, the attacker can reveal the deception."[19] The DOD could begin promoting this sort of norm of cyber weapons development by adopting some of these measures if it chooses to conduct an offensive cyber operation. Such a norm would make attacks directly traceable to an attacker and make for more responsible cyber weapons.

Adequate international norms of cyber behavior exist, and the United States has a role to play in the sponsorship of these norms. I have described a taxonomy for state responsibility and the possible role of the United States in cyber warfare policy development, diplomacy, and defense. The objects of all of this are to create a framework for state responsibility and to reduce the gaps in international cooperation and domestic laws that undermine global cybersecurity. The time is at hand to disallow plausible deniability and to promote the global norms of cyber behavior.

Language for "Victims of Trafficking in Malicious Code" Legislation

What is required for US government sponsorship is US legislation to mandate international engagement on cyber crime. Current draft legislation, such as the Cybersecurity Act of

2012, is indicative of movement in Congress toward this. Sections of the bill include provisions for the coordination of international cyber issues with the US government, consideration of cyber crime in foreign policy, and foreign assistance programs.[20] Overall, what is needed is engagement in multilateral and bilateral diplomacy to develop international cooperation and development to enhance foreign nation capabilities to combat cyber threats.

One difference between the TVPA model and a potential adaptation of it for cyber attacks is that the DOD should be mandated to serve as the clearinghouse for data pertaining to state behavior and cyber attacks. Current draft legislation places the overarching international engagement strategy within the US Department of State. With human trafficking, the sources of information are NGOs with whom the DOS maintains close affiliations by its diplomatic work. The DOD has the technical capacity and relationships with private entities to report on state cyber behaviors and investigation capacities. The DOD should provide annual reports modeled on the TIP reports to describe the compliance with relevant global policies in the UNGA's global culture of cybersecurity. The US Air Force in particular is the most suited to provide its best practices and lessons learned to nations requiring developmental assistance.

Further steps need to be taken in legislation drafted by Congress similar to the TVPA to guide the government's efforts to name and shame countries misbehaving in cyberspace. The following elements should be included as minimum standards of making serious and sustained efforts to eliminate cyber crime (see also fig. 12):

- Review and update legislation and regulations for the investigation and prosecution of cyber crime, including extradition measures that may be outdated or obsolete.
- Determine key cybersecurity stakeholders in national and local governments, industry, civil society, and academia for the development of networks and processes of international cooperation to enhance incident response and contingency planning.
- Assure that prosecutors, judges, and legislators have an adequate level of understanding of cyber issues.

- Create government points of contact to monitor data patterns for evidence of malicious cyber activities.
- Create 24/7 international cyber crime contacts (CERT/CSIRT) to cooperate with international counterparts for investigating transnational and international malicious cyber events.
- Prescribe punishment commensurate with that for grave crimes, such as criminal behavior or armed attacks, for any cyber attack involving government officials.
- Prescribe punishment that is sufficiently stringent to deter and that adequately reflects the reality of the offense for individuals engaged in malicious cyber behavior within sovereign territory.

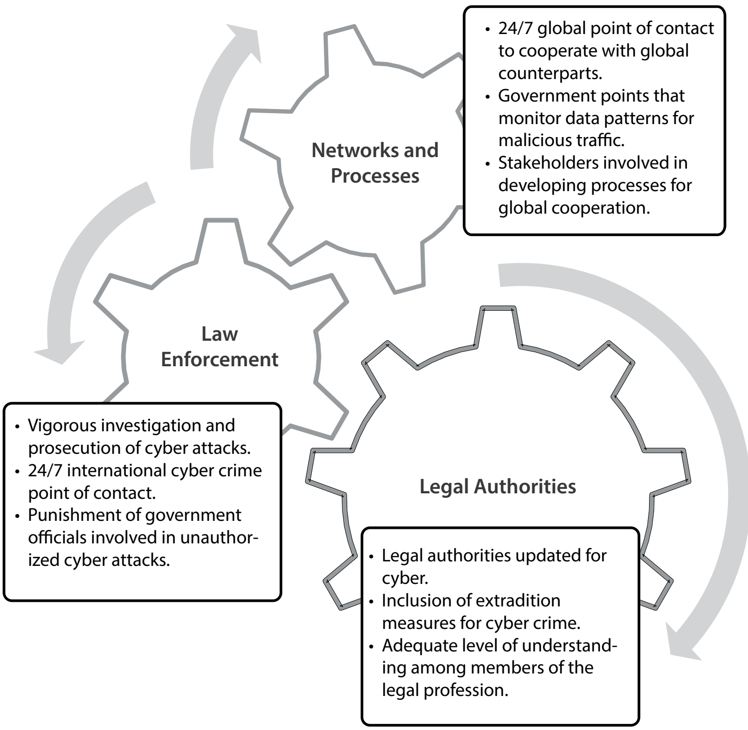


Figure 12. Model of a Tier-One country

Additionally, the following should be considered as indications of serious and sustained efforts to eliminate cyber crime and cyber attacks from a country:

- Monitoring of data patterns for evidence of malicious cyber activities.
- Effective response of law enforcement agencies to evidence of cyber crime.
- Vigorous investigation and prosecution of acts of cyber crime within the sovereign territory.
- Vigorous investigation, prosecution, conviction, and sentencing of all public officials who participate in or facilitate cyber attacks.
- Provision of data regarding cyber crime investigations, prosecutions, convictions, and sentences on request.
- Cooperation with other governments in the investigation and prosecution of cyber crime.
- Extradition of persons charged with malicious cyber acts.
- Informing and educating the public, including potential victims, about the causes and consequences of cyber crime.
- Equal cyber crime protection for all within sovereign territory.

As reported in the DOD's 2010 *Quadrennial Defense Review Report*, the 2011 *Department of Defense Strategy for Operating in Cyberspace*, and the White House's 2011 *International Strategy for Cyberspace* and 2010 *National Security Strategy*, strengthening international partnerships to secure the cyber domain requires an understanding of what gaps exist in the capabilities of our international partners within the technical, legal, and organizational domains.[21] Identifying these gaps and their root causes will provide the US policy community with the knowledge required to support our partners to strengthen their national cybersecurity, thereby contributing to a cyber environment less hospitable to attempts to misuse cyberspace.

Leading by Example: US-Based Entities' Responsibility

In addition to holding countries responsible, the US government needs to understand that it has its own role to play in securing the global commons. Industry is likely to vigorously push back against regulatory efforts. With the potential power of destructive activities, both in the economic sense and the military sense, it is high time that reliance on industrial volunteerism be scrapped and replaced with a regulation providing incentives and punishments to encourage standards for cybersecurity. Regulations must be crafted on the basis of policies informed by technical realities to assure a positive impact. Doing so will legitimize the United States as a leader in the fight to hold other states responsible for cybersecurity while providing greater cybersecurity for the American public.

US-Based Internet Intermediaries

Germany, Japan, and other countries have developed partnerships to encourage ISPs to voluntarily notify subscribers whose computers are suspected of being infected by malware. But security experts caution that imposing such policies could impact competition and favor large, established firms. They also indicate that additional security risks could be generated in building surveillance and control systems that might also invite abuse.[22]

Nevertheless, ISPs should be held responsible for malicious activities that occur within their systems. Table 5 shows that most network attacks originate in the United States. US-based entities also own a large percentage of the Internet backbone. But US Internet businesses appear reluctant to invest in implementing initiatives that could significantly curb malicious activities originating in US networks. An exception is Comcast's Web notification system "used to provide near-immediate notifications to customers, such as to warn them that their traffic exhibits patterns that are indicative of malware or virus infection."[23] While such systems are good indicators that the industry is moving forward on cybersecurity, more proactive efforts are needed to assure that malicious software does not infest their customers' computers.

Table 5. Malicious activity by source: network attack origins, 2010–11

	2011		2010		Change
Source	**Overall Rank**	**Percentage**	**Overall Rank**	**Percentage**	
United States	1	21.1	1	19.3	+1.8
China	2	9.2	2	16.2	-7.0
India	3	6.2	6	3.9	+2.3
Brazil	4	4.1	4	4.4	-0.3
Germany	5	3.9	3	5.2	-1.3
Russia	6	3.2	10	2.3	+0.9
United Kingdom	7	3.2	5	4.3	-1.2
Taiwan	8	3.0	9	2.6	+0.5
Italy	9	2.7	8	3.0	-0.3
Indonesia	10	2.4	28	0.7	+1.7

Adapted from "Threat Activity Trends," Symantec, http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=malicious_activity_by_source.

Secure Design and Implementation

Secure design and implementation of computer technology are perhaps the most critical factors in securing the cyber commons. Efforts in this direction are being made with the redesign of future networking protocols and the proper implementation of IPv6. Design of software and hardware for security is crucial to dealing with existing vulnerabilities that have resulted from poor computer programming. But there is a heavy bias against regulatory regimes that would require rigorous testing to assure securely designed and coded products. According to reports, "technology and telecommunications companies lobbied hard against regulation, arguing that the private sector is better qualified to develop the most effective security . . . [and] White House advisers held fast to their philosophical reluctance to regulate free markets or to impose industry standards that might favor one sector over another."[24] Operators of critical infrastructure systems balk at sharing vulnerability and security incident information with the government, fearing disclosure of proprietary information through Freedom of Information Act requests.[25]

US-based software entities, hardware manufacturers, and Web service providers who deliver consumer products must be held responsible for dealing with vulnerabilities in the cyber ecosystem. Likewise, DOD-contracted commercial hardware and software providers must provide adequate protections against compromise of their products. A requirement to deliver uncompromised classified and unclassified systems, services, or products to the government would save the government money and the lives of war fighters.[26]

Notes

1. Krekel, Adams, and Bakos, *Occupying the Information High Ground*, 33.
2. Healey, *Beyond Attribution*, 4.
3. Shackelford, "State Responsibility for Cyber Attacks."
4. It should be noted that the stages of covert activity could also be classified in the category of "short of war"; however, covert action requires a presidential finding. The processes and political risks involved in the planning and execution of covert activity are beyond the scope of this paper.
5. Reich and Yannakogeorgos, *Global Norms, American Sponsorship, and the Emerging Pattern of World Politics*.
6. International Telecommunications Union (ITU), *ITU Toolkit for Cybercrime Legislation*, 2010, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf.
7. The White House, *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*, 14.
8. Ibid.
9. Ibid.
10. Joint Chiefs of Staff (JCS), *National Military Strategy of the United States of America*, 15.
11. Shaud, *Air Force Strategy Study 2020–2030*, 15.
12. Schjolberg, "Proposals for New Legal Mechanisms on Combating Cybercrime and Global Cyberattacks."
13. JCS, *National Military Strategy of the United States of America*, 14.
14. Clarke and Knake, *Cyber War*. Of course, these are just hypothetical scenarios. Should the air traffic control system suffer systemic failure, Clarke will automatically be considered a hero. Ringing the warning bell of catastrophe when disaster strikes is a surefire way to gain hero status.
15. Libicki, *Cyberdeterrence and Cyberwar*.
16. For an example of a counteranalysis to the typical accusations of Israeli or US involvements, see Yannakogeorgos, "Was Russia behind Stuxnet?"
17. Associated Press, "Iranian Leader Orders Creation of Internet Oversight Agency in Bid to Control Web."
18. Rowe et al., "Challenges in Monitoring Cyberarms Compliance."
19. Ibid.

20. Senate, *Bill to Enhance the Security and Resiliency of the Cyber and Communications Infrastructure of the United States*.

21. DOD, *Quadrennial Defense Review Report*, 12 February 2010, 37–39. See also National Security Council, *National Security Strategy 2010*, 28.

22. Organization for Economic Co-operation and Development, *Role of Internet Intermediaries in Advancing Public Policy Objectives*.

23. C. Chung et al., "Comcast's Web Notification System Design."

24. Krim, "Cyber-Security Strategy Depends on Power of Suggestion."

25. Yannakogeorgos, "Privatized Cybersecurity and the Challenges of Securing the Digital Environment."

26. I am grateful to Mr. Lynn Mattice for this observation.

Chapter 5

Conclusion

The only way forward in creating a robust network of global processes and policies to found a formal international agreement is to begin by holding states accountable for malicious activities that originate in or transit their territories. The United States should not shy away from sponsoring existing international frameworks and the emerging institutions such as IMPACT.

Where Do We Go from Here?

Attributing a cyber attack to a state requires a rapid response to the event. Unlike law enforcement, different standards and technical evidence are required to hold states accountable. Experts have suggested that the high standard of evidence for criminal prosecution is not required from a purely legal standpoint.[1] Increasingly the technical community does not view attribution as a technical problem.

State and nonstate actors exploit the lack of international cooperation and laws by routing their multistage attacks via multiple jurisdictions to camouflage their activities and identities.[2] The White House strategy recognizes this and, in its clearest statement of a norm of state responsibility, states that such international cooperation "is a responsibility and duty that every nation, and its people, all share."[3] This statement implies that state governments should be held responsible for actions their citizens take within cyberspace. What is required is that the United States begin documenting and issuing reports on each nation's efforts to both create and enforce legal mechanisms within their countries to prosecute cyber crime and to measure the extent of cooperation in cyber crime investigations. This would require a framework of metrics and methodologies that will produce reliable reporting. A bevy of recent cyber policy has documented that the strengthening of international partnerships for cybersecurity requires knowledge of existing gaps in the technical, legal, and organizational capabilities of our international partners.[4] Identifying these gaps and their root causes will provide the US policy community with the knowledge required to support our partners in strengthening their national cybersecurity, thereby invigorating international cooperation and shaping a cyber environment that is less hospitable for malicious actors. An Air Force effort is needed to utilize its cyber skill sets to provide an empirically based approach by drilling into the social and technical fabrics of society. This will be useful in targeting the development, diplomacy, and defense strategies already suggested.

The United States has recently pursued international cyber policies aimed at promoting international cooperation within a politico/military context. Cyber crime attribution is often considered to be a complex technical problem, and too often the focus is on the technical components of cyberspace. Instead, the emphasis should be on the attributable physical layer of cyberspace tied to a state's territory. Once a malicious cyber incident or event is discovered, states should be responsible to identify the perpetrators and cooperate in investigations. If not, then the government should be held culpable for damages. A policy tool kit modelled on the antitrafficking-in-humans processes should determine responsibilities and responses. With the large number of victims of cyber crime worldwide, the United States has an opportunity to deal directly with individual governments on the issue—and be met with little criticism. This sort of engagement will have two benefits. First, it will help create legitimate enforcement mechanisms for the global culture of cybersecurity. Second, through bilateral engagements, the United States would be leading the effort in creating a bilateral treaty-based entity. This is much like the International Civil Aviation Authority is today.

Linking It All Together

David Clark and Susan Landau, in "The Problem Isn't Attribution," state that "solutions to preventing the attacks of most concern, multi-stage multi-jurisdictional ones, will require not only technical methods, but legal/policy solutions as well."[5] Treaties that specify state cyberspace accountability and obligations to assist corollaries have been suggested.[6] These would be most desirable. Multistage and multijurisdictional attacks are increasing, and negotiating such agreements will take years if not decades. An alternative approach might be to shift toward policy tools that would allow the United States to hold states responsible for malicious actions within their sovereign cyberspace.

Cybersecurity based on the creation of global norms of cyber behavior has been proposed without specifying what the norms should look like. The UN and the COE have been promulgating the groundwork of international norms with cooperation from private parties within multilateral processes such as the World Summit on the Information Society and the Internet Governance Forum. The United States has been active in venues such as the Organization for Economic Cooperation and Development in developing behavioral norms rather than the ITU/UN forums. Although the institutionalization of global norms progresses, the United States has been missing in promoting and enforcing the ITU/UN norms of cyber behavior. The purpose of this study was to determine what, if any, benefit could be accrued from the US engagement with the UN/ITU in cybersecurity. A United States hesitant and reluctant to engage with the global bodies has frustrated the realization of global norms of cyber behavior. Securing cyberspace is a long journey that has only just begun and will not end soon. With malicious activities in cyberspace heightening geopolitical tensions, it seems that these tensions will prompt new ideas and strategies on how to engage great powers in cyberspace, while shaping the behavior of smaller powers to assure a more trusted cyber ecosystem.

Notes

1. Clark and Landau, "The Problem Isn't Attribution," 4. Criminal investigations where cyber evidence would not be permissible in court provide law enforcement authorities other leads, such as money trails, that eventually allow for the apprehension and prosecution of a suspect.

2. Ibid., 39.

3. The White House, *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*, 8.

4. Department of Defense, "Operate Effectively in Cyberspace," 37–39. See also National Security Council, *National Security Strategy, 2010*, 28.

5. Clark and Landau, "The Problem Isn't Attribution," 1.

6. Clarke and Knake, *Cyber War*, 251–53. See also Healey, "The Spectrum of National Responsibility for Cyberattacks."

Abbreviations

AFDD	Air Force doctrine document
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
ASP	Active Server Pages
AU	African Union
C2	command and control
CERT	computer emergency response team
CISO	chief information security officer
CNITSEC	China Information Technology Security Certification Center
COE	Council of Europe
CSIRT	computer security incident readiness team
DHS	Department of Homeland Security
DNS	Domain Name System
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DPI	deep packet inspection
EU	European Union
G-8	Group of Eight
GCC	global culture of cybersecurity
ICS	industrial control system
ICT	information and communication technology
IEEE	Institute of Electrical and Electronic Engineers
IGF	Internet Governance Forum
IMF	International Monetary Fund
IMPACT	International Multilateral Partnership against Cyber Threats
IRC	internet relay chat
ISO	International Organization for Standardization
ISP	Internet service provider
IT	information technology
ITU	International Telecommunications Union
JCS	Joint Chiefs of Staff
JSP	Java Server Pages

MAC	media access control
NGO	nongovernmental organization
NISP	National Industrial Security Program
NSC	National Security Council
OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
OEM	original equipment manufacturer
OSCE	Organization for Security and Cooperation in Europe
OSI	open systems interconnection
PLA	People's Liberation Army
PROTECT Act	Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act
PROTECT IP or PIPA	Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act
SCADA	supervisory control and data acquisition
SCAP	Security Content Automation Protocol
SECI	Southeast European Cooperative Initiative
SOPA	Stop Online Piracy Act
TCP/IP	transmission control protocol / Internet protocol
TIP Report	*Trafficking in Persons Report*
TOR	the Onion Router
TVPA	Trafficking Victims Protection Act
UN	United Nations
UNGA	United Nations General Assembly
UOF	use of force
WiFi	wireless fidelity
WSIS	World Summit on the Information Society
WWW	World Wide Web

Bibliography

Air Force Doctrine Document 3-12. *Cyberspace Operations*, 2010.

Alperovitch, Dimitri. *Revealed: Operation Shady RAT*, White Paper version 1.1. McAfee, 2011. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

"America Will Not Tolerate Slave Traders, Bush Says." *America in Context*. http://usinfo.org/wf-archive/2004/040716/epf507.htm.

Areddy, James. "People's Republic of Hacking." *Wall Street Journal*, 20 Feb 2010, A1.

Associated Press. "Iranian Leader Orders Creation of Internet Oversight Agency in Bid to Control Web." *Washington Post*, 7 March 2012. http://www.washingtonpost.com/world/middle_east/iranian-leader-orders-creation-of-internet-oversight-agency-in-bid-to-control-web/2012/03/07/gIQAlpYawR_story.html.

Barrett, Barrington M., Jr. "Information Warfare: China's Response to U.S. Technological Advantages." *International Journal of Intelligence and Counterintelligence* 18, no. 4 (21 August 2006): 682–706.

Brossard, Jonathan, and Florentin Demetrescu. "Hardware Backdooring Is Practical." *Hackito Ergo Sum*, 7 March 2012. http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-jbrossard_fdemetrescu-Hardware-Backdooring-is-pratical.pdf.

Chung, C., A. Kasyanov, J. Livingood, N. Mody, and B. Van Lieu. "Comcast's Web Notification System Design." The Internet Engineering Task Force, February 2011. http://tools.ietf.org/html/rfc6108.

Clark, David. *Characterizing Cyberspace: Past, Present and Future*, Version 1.2. MIT Computer Science and Artificial Intelligence Laboratory, 12 March 2010. http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf.

Clark, David D., and Susan Landau. "The Problem Isn't Attribution; It's Multi-Stage Attacks." MIT Computer Science and Artificial Intelligence Laboratory, Advanced Network Architecture, 30 November 2010. http://groups.csail.mit.edu/ana/ANA%20PUBLICATIONS/The_Problem_isnt_Attribution.pdf.

———. "Untangling Attribution." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, DC: National Research Council, The National Academies Press, 2010. http://www.nap.edu/openbook.php?record_id=12997&page=25.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do about It.* New York: HarperCollins Publishers, 2010.

Clinton, Hillary Rodham. "Remarks on Internet Freedom." Department of State (DOS), 21 Jan 2010. http://www.state.gov/secretary/rm/2010/01/135519.htm.

Council of Europe. *Convention on Cybercrime*, 2001. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Denning, Dorothy E., and Peter J. Denning, eds. *Internet Besieged: Countering Cyberspace Scofflaws.* New York: ACM Press, 1998.

Department of Commerce, Internet Policy Task Force. *Cyber-security, Innovation and the Internet Economy*, June 2011. http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

Department of Defense (DOD) Instruction 5205.13. *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*, 29 January 2010. http://www.dtic.mil/whs/directives/corres/pdf/520513p.pdf.

———. *Department of Defense Strategy for Operating in Cyberspace, July 2011.* http://www.defense.gov/news/d20110714cyber.pdf.

———. "Operate Effectively in Cyberspace." In *Quadrennial Defense Review Report*, February 2010, 37–39. https://acc.dau.mil/adl/en-US/346631/file/48786/QDR%20Report%20Feb%202010.pdf.

———. *Quadrennial Defense Review Report*, 12 February 2010. http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

Department of Homeland Security. *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*, 23 Mar 2011. http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

Department of Justice. *Assessment of U.S. Government Efforts to Combat Trafficking in Persons in Fiscal Year 2004*, 2005. http://www.justice.gov/archive/ag/annualreports/tr2005/assessmentofustipactivities.pdf.

DOS. *Charter and Amendments: Human Smuggling and Trafficking Center*, 9 July 2004. http://www.state.gov/m/ds/hstcenter/41444.htm.

———. *Working for Women, Worldwide: The U.S. Commitment*, 2005. http://usinfo.state.gov/products/pubs/women/combat.htm.

Executive Office of the President, National Science and Technology Council. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, December 2011. http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.

Federal Bureau of Investigation. "Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce Additional Arrests as Part of International Cyber Crime Takedown," 11 July 2012. http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-additional-arrests-as-part-of-international-cyber-crime-takedown/.

Federal Communications Commission, Reliability and Interoperability Council, Working Group 8, Communications Security. *Final Report: Internet Service Provider (ISP) Network Protection Practices*, December 2010. http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52 (Autumn, 1998): 887–917.

Gady, Franz-Stefan. "Africa's Cyber WMD [weapons of mass destruction]." *Foreign Policy.com*, 24 Mar 2010. http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd.

Ghernouti-Helie, Solange. *A National Strategy for an Effective Cybersecurity Approach and Culture*. Presentation at the International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010. http://www.computer.org/portal/web/csdl/doi/10.1109/ARES.2010.119.

Grey Logic. *Project Grey Goose Report on Critical Infrastructure: Attacks, Actors and Emerging Threats*, 21 January 2010. http://dataclonelabs.com/security_talkworkshop/papers/25550091-Proj-Grey-Goose-report-on-Critical-Infrastructure-Attacks-Actors-and-Emerging-Threats.pdf.

Gross, Grant. "ISPs: No New Cybersecurity Regulations Needed." *IT World*, 7 Mar 2012. http://www.itworld.com/networking/256662/isps-no-new-cybersecurity-regulations-needed.

Grow, Brian, Keith Epstein, and Chi-Chu Tschang. "The New E-Spionage Threat: A *Business Week* Probe of Rising Attacks on America's Most Sensitive Computer Networks Uncovers Startling Security Gaps." *Business Week*, 21 Apr 2008. http://www.businessweek.com/stories/2008-04-09/the-new-e-spionage-threat.

Harrison, Keith, and Gregory White. "A Taxonomy of Cyber Events Affecting Communities." In *Proceedings of the 2011 44th Hawaii International Conference on System Sciences*, 1–9. Washington, DC: IEEE Computer Society Conference Publishing Services, 2011.

Healey, Jason. *Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks*. Vienna, VA: Cyber Conflict Studies Association, 2010.

———. "The Spectrum of National Responsibility for Cyber Attacks." *Brown Journal of World Affairs* 18, no. 1, (Fall/Winter 2011): 57–70.

Information Warfare Monitor and Shadowserver Foundation. *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, April 2010. http://shadows-in-the-cloud.net/.

International Telecommunications Union (ITU). *ITU/IMPACT Country Readiness Assessment to Establish a National CIRT*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/CIRT_%20Assessment041011-final.pdf.

———. *ITU Toolkit for Cybercrime Legislation*, 2010. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf.
Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations*. Washington, DC: DOD, 2006. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.
———. *The National Military Strategy of the United States of America: 2011, Redefining America's Military Leadership*, 8 February 2011.http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.
Kanuck, Sean. "Sovereign Discourse on Cyber Conflict under International Law." *Texas Law Review* 88 (June 2010): 1571–97.
Killcrece, Georgia. *Steps for Creating National CSIRTs*. Pittsburg, PA: Carnegie Mellon Software Engineering Institute, 2004. http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.
Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Northrop Grumman Corp., 7 March 2012. http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.
Krim, Jonathan. "Cyber-Security Strategy Depends on Power of Suggestion." *Washington Post*, 15 Feb 2003, E01. http://www.washingtonpost.com/ac2/wp-dyn/A10274-2003Feb14?language=printer.
Lebow, Richard Ned. "Power, Persuasion and Justice." *Millennium: Journal of International Studies* 33, no. 3 (1 June 2005): 551–81.
Leighton, Tom. "The Net's Real Security Problem." *Scientific American*. https://www.scientificamerican.com/article.cfm?id=the-nets-real-security-pr.
Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009.
Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6 no. 3 (Fall 2012): 46–70.

Lipson, Howard F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, special report no. CMU/SEI-2002-SR-009. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002.

Mandiant. "Advanced Persistant Threat 1: Exposing One of China's Cyber Espionage Units," February 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Microsoft Corporation. "China Information Technology Security Certification Center Source Code Review Lab Opened," 26 Sept 2003. http://www.microsoft.com/presspass/press/2003/sep03/09-26gspchpr.mspx.

———. *European Telecom Uses Microsoft Security Data to Remove Botnet Devices from Network*, 13 Mar 2012. http://www.microsoft.com/casestudies/Microsoft-Lync-Server/TeliaSonera/European-Telecom-Uses-Microsoft-Security-Data-to-Remove-Botnet-Devices-from-Network/710000000132.

Miko, Francis T. *Trafficking in Persons: The U.S. and International Response*. Washington, DC: Congressional Research Service, 19 January 2006.

Molyneux, Robert E. *The Internet under the Hood: An Introduction to Network Technologies for Information Professionals*. Westport, CT: Libraries Unlimited, 2003.

National Security Council. *Comprehensive National Cybersecurity Initiative*. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

———. *National Security Strategy, 2010*, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

Nelson, Bill, Rodney Choi, Michael Iacobucci, Mark Mitchell, and Greg Gagnon. *Cyberterror: Prospects and Implications*. Monterey, CA: Center for the Study of Terrorism and Irregular Warfare, US Naval Postgraduate School, 1999. http://www.nps.edu/Academics/Centers/CTIW/files/Cyberterror%20Prospects%20and%20Implications.pdf.

Onley, Dawn S., and Patience Wait. "Red Storm Rising: DOD's Efforts to Stave Off Nation-State Cyberattacks Begin with China." *Government Computer News*, 21 Aug 2006.

Organization for Economic Co-operation and Development (OECD). *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. Paris: OECD Publishing, 2011. http://www.oecd-ilibrary.org/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_5kgdp5mpxgxqpdf;jsessionid=57i4941o6ebe6.delta?contentType=/ns/Book&itemId=/content/book/9789264115644-en&containerItemId=/content/book/9789264115644-en&accessItemIds=&mimeType=application/pdf.

Parks, Raymond C., and David P. Duggan. "Principles of Cyber-Warfare." In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY, 5–6 June 2001, 122–25. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.1478&rep=rep1&type=pdf.

Reich, Simon, and Panayotis Yannakogeorgos. "George Bush and the Sponsoring of the Anti-Trafficking Norm: A Rare Success Story." In *Global Norms: American Sponsorship and the Emerging Pattern of World Politics*, edited by Simon Reich and Panayotis Yannakogeorgos, 178–205. New York: Palgrave 2010.

———. *Global Norms: American Sponsorship, and the Emerging Pattern of World Politics*. New York: Palgrave 2010.

Rowe, Neil C., Simson L. Garfinkel, Robert Beverly, and Panayotis Yannakogeorgos. "Challenges in Monitoring Cyberarms Compliance." *International Journal of Cyber Warfare and Terrorism* 1 (2011): 2–14.

———. "Steps towards Monitoring Cyberarms Compliance." In *Proceedings of the 10th European Conference on Information Warfare and Security*. Tallinn, Estonia: Tallinn University of Technology, July 2011, 221–27. http://faculty.nps.edu/ncrowe/rowe_eciw11.htm.

Sandoval, Greg. "Top ISPs Agree to Become Copyright Cops." *CNET News.com*, 7 July 2011. http://news.cnet.com/8301-31001_3-20077492-261/top-isps-agree-to-become-copyright-cops.

Schjolberg, Stein. "Proposals for New Legal Mechanisms on Combating Cybercrime and Global Cyberattacks: An International Criminal Court or Tribunal for Cyberspace (ICTC)." A paper for the EastWest Institute Cybercrime Legal Working Group, May 2011. http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC).pdf.

Senate. *A Bill to Enhance the Security and Resiliency of the Cyber and Communications Infrastructure of the United States*. 112th Congress, 2nd sess., 2012, S 3414.

Shackelford, Scott J. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." Department of Politics and International Studies, University of Cambridge. http://irps.ucsd.edu/assets/001/501281.pdf.

Shaud, John A. *Air Force Strategy Study 2020–2030*. Maxwell AFB, AL: Air University Press, 2010.

TeliaSonera. *TeliaSonera's Response to the European Commission Consultation on Net Neutrality and the Open Internet*, 30 September 2010.

"Though Obama Viewed Positively, Still Much Criticism of US Foreign Policy: Global Poll." *World Public Opinion.org*, 7 July 2009. http://www.worldpublicopinion.org/pipa/articles/views_on_countriesregions_bt/623.php?nid=&id=&pnt=623&lb=.

United Nations (UN). *Responsibility of States for Internationally Wrongful Acts, 2001*. http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf.

UN Commission on the Status of Women. "Eliminating Demand for Trafficked Women and Girls for All Forms of Exploitation," Resolution 49/2, March 2008. http://www.humantrafficking.org/uploads/updates/csw_tip_res_adopted_031105.doc.

UN Department of Economic and Social Affairs. *Cybersecurity: A Global Issue Demanding a Global Approach*, 12 December 2011. http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html.

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

UN General Assembly. "Combating the Criminal Misuse of Information Technologies," A/RES/56/121, 23 January 2002. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf.
———. "Creation of a Global Culture of Cybersecurity," A/RES/57/239, 31 January 2003. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57 _239.pdf.
———. "Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures," A/RES/64/211, 17 Mar 2010. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/64/211&Lang=E.
———. "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures," A/RES/58/199, 30 January 2004. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.
———. "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/56/19, 29 November 2001. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/60/45&Lang=E.
———. "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/60/45, 6 January 2006. http://www.worldlii.org/int/other/UNGARsn/2001/81.pdf.
———. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 30 July 2010. http://www.unidir.org/pdf/activites/pdf5-act483.pdf.
Ungerleider, Nearl. "The Chinese Way of Hacking." *Fast Company*, 13 July 2011. http://www.fastcompany.com/1766812/chinese-way-hacking.
United States–China Economic and Security Review Commission. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage." http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.
Waldrop, Mitch. "DARPA and the Internet Revolution." Defense Advanced Research Projects Agency. www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554.

Westby, Jody R. “Conclusion.” In The Quest for Cyber Peace, edited by Hamadoun I. Touré. ITU, January 2011, 112–113. http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E .pdf.

———. “US Administration’s Reckless Cyber Policy Puts Nation at Risk.” *Forbes*, 6 June 2012. http://www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk/.

White House. Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, 20 February 2013. http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

———. *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

World Summit for the Information Society (WSIS). *Declaration of Principles*. December 2003, http://www.itu.int/wsis/docs/geneva/official/dop.html.

WSIS. *Plan of Action*, December 2003. http://www.itu.int/wsis/docs/geneva/official/poa.html.

———. *Tunis Agenda for the Information Society*, November 2005. http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

Yannakogeorgos, Panayotis. “Cyberspace: The New Frontier and the Same Old Multilateralism.” In *Global Norms: American Sponsorship and the Emerging Pattern of World Politics*, edited by Simon Reich and Panayotis Yannakogeorgos, 147–77. New York: Palgrave 2010.

———. “Privatized Cybersecurity and the Challenges of Securing the Digital Environment.” In *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice*, edited by Leslie W. Kennedy and Edmund F. McGarrell, 255–67. New York: Routledge, 2011.

———. “Promises and Pitfalls of the Private Public Partnership Model.” In *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice*, edited by Leslie W. Kennedy and Edmund F. McGarrell, 255–67. New York: Routledge, 2011.

———. “Was Russia behind Stuxnet?” *The Diplomat*, 10 December 2011. http://the-diplomat.com/2011/12/10/was-russia-behind-stuxnet/.

Yannakogeorgos, Panayotis, and Lynn Mattice. *Essential Questions for Cyber Policy: Strategically Using Global Norms to Resolve the Cyber Attribution Challenge*. Maxwell AFB, AL: Air University Press, 2011.

Zanini, Michele, and Sean J. A. Edwards. "The Networking of Terror in the Information Age." In *Networks and Netwars*, edited by John Arquilla and David Ronfeldt, 29–60. Santa Monica, CA: RAND Corporation, 2001.

Zetter, Kim. "Rogue Nodes Turn Tor Anonymizer into Eavesdropper's Paradise." *Wired*, 10 September 2007. http://www.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=1.

Strategies for Resolving the Cyber
Attribution Challenge

Commander and President, Air University
Lt Gen David S. Fadok

Director, Air Force Research Institute
Lt Gen Allen G. Peck, USAF, Retired

Air University Press Team

Chief Editor
James S. Howard

Copy Editor
Carolyn Burns

Cover Art and Book Design
Daniel Armstrong

Illustrations
Daniel Armstrong

Composition and Prepress Production
Nedra O. Looney

Print Preparation and Distribution
Diane Clark

AIR FORCE RESEARCH INSTITUTE

AFRI AU PRESS
AIR FORCE RESEARCH INSTITUTE
http://aupress.au.af.mil

ISBN 978-1-58566-226-5
ISSN 2329-5821