JUNE
2011

America's Cyber Future

Security and Prosperity in the Information Age

VOLUME II

Edited by Kristin M. Lord and Travis Sharp
Contributors: Robert E. Kahn, Mike McConnell, Joseph S. Nye, Jr. and Peter Schwartz (co-chairs); Nova J. Daly, Nathaniel Fick, Martha Finnemore, Richard Fontaine, Daniel E. Geer Jr., David A. Gross, Jason Healey, James A. Lewis, Kristin M. Lord, M. Ethan Lucarelli, Thomas G. Mahnken, Gary McGraw, Roger H. Miksad, Gregory J. Rattray, Will Rogers, Christopher M. Schroeder and Travis Sharp

Center for a New American Security

Acknowledgments

The authors would like to thank the more than 200 people who generously contributed their time and expertise to this project. We are especially indebted to our co-chairs Bob Kahn, Mike McConnell, Joe Nye and Peter Schwartz for their tremendous support and guidance over the past year. We also thank our contributing authors for producing such insightful essays.

We are particularly grateful to the many people who reviewed drafts of the papers included in this volume, including Irv Lachow, James Mulvenon, Charles Dunlap, Eric Rosenbach, Jeff Lord, Tom Gjelten, Greg Rattray, David Asher, Jeff Pryce, Andrew Lewman, Daniel Calingeart, David Gross, Nova Daly and several anonymous reviewers. In addition, we wish to thank the dozens of dedicated professionals in the U.S. government, armed services and private sector who candidly shared their perspectives. We also thank Global Business Network for hosting a workshop in San Francisco in February 2011, as well as the many technologists and other experts who attended. Peter Schwartz, David Babington and Audrey Plonk deserve special recognition for making the workshop a success.

We would like to recognize the valuable contributions made by our colleagues at CNAS, particularly Nate Fick, John Nagl, Tom Ricks, Richard Fontaine, Andrew Exum, Christine Parthemore, Brian Burton, Bill Uhlmeyer, Richard Weitz and Will Rogers. Nora Bensahel was a diligent and helpful editor. Liz Fontaine provided her usual high caliber of design expertise. Finally, we offer special thanks to our colleagues Abe Denmark, who played a key role in launching this project and participated in many of our working group sessions, and Jessica Glover and Jackie Koo, who provided scrupulous research and fact checking for this report.

Readers should note that the views expressed in each essay of Volumes I and II belong to the author(s) alone. They do not necessarily reflect the views of the editors, co-chairs or any of the other contributing authors, nor do they necessarily reflect the views of the authors' employers or any other organization.

A Note about Funding

This report was made possible, in part, through the generous support of the Markle Foundation. The opinions expressed in the report are those of the authors and do not necessarily reflect the views of the Markle Foundation.

Some organizations and companies that are mentioned in this report or have vested interests related to cyber security support CNAS financially. CNAS retains sole editorial control over its projects and maintains a broad and diverse group of more than one hundred funders including foundations, government agencies, corporations and private individuals. A complete list of CNAS' financial supporters can be found at http://www.cnas.org/support/our-supporters.

Cover Image

(ISTOCK)

JUNE 2011

America's Cyber Future

Security and Prosperity in the Information Age

VOLUME II

Edited by Kristin M. Lord and Travis Sharp

Contributors: Robert E. Kahn, Mike McConnell, Joseph S. Nye, Jr. and Peter Schwartz (co-chairs); Nova J. Daly, Nathaniel Fick, Martha Finnemore, Richard Fontaine, Daniel E. Geer Jr., David A. Gross, Jason Healey, James A. Lewis, Kristin M. Lord, M. Ethan Lucarelli, Thomas G. Mahnken, Gary McGraw, Roger H. Miksad, Gregory J. Rattray, Will Rogers, Christopher M. Schroeder and Travis Sharp

About the Contributors *(in order of appearance)*

Kristin M. Lord is Vice President and Director of Studies at the Center for a New American Security.

Travis Sharp is the Bacevich Fellow at the Center for a New American Security.

Joseph S. Nye, Jr. is University Distinguished Service Professor at the Kennedy School of Government at Harvard University.

Mike McConnell is Executive Vice President of Booz Allen Hamilton and former Director of National Intelligence and Director of the National Security Agency.

Gary McGraw is Chief Technology Officer of Cigital, Inc., a software security consultancy, and author of eight books on software security.

Nathaniel Fick is Chief Executive Officer of the Center for a New American Security.

Thomas G. Mahnken is Jerome E. Levy Chair of Economic Geography and National Security at the U.S. Naval War College and a Visiting Scholar at the Johns Hopkins School of Advanced International Studies.

Gregory J. Rattray is a Partner at Delta Risk LLC and Senior Vice President for Security at BITS, the technology policy division of The Financial Services Roundtable.

Jason Healey is Director of the Cyber Statecraft Initiative at the Atlantic Council and Executive Director of the Cyber Conflict Studies Association.

Martha Finnemore is Professor of Political Science and International Affairs at The George Washington University.

David A. Gross is a Partner at Wiley Rein LLP and a former Ambassador and Coordinator for International Communications and Information Policy at the State Department.

Nova J. Daly is a Public Policy Consultant at Wiley Rein LLP and former Deputy Assistant Secretary for Investment Security in the Office of International Affairs at the Treasury Department.

M. Ethan Lucarelli is an Associate at Wiley Rein LLP.

Roger H. Miksad is an Associate at Wiley Rein LLP.

James A. Lewis is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies.

Richard Fontaine is a Senior Fellow at the Center for a New American Security.

Will Rogers is a Research Associate at the Center for a New American Security.

Christopher M. Schroeder is an Internet entrepreneur, Chief Executive Officer of HealthCentral.com and a member of the Center for a New American Security's board of advisors.

Daniel E. Geer, Jr. is Chief Information Security Officer of In-Q-Tel, the independent investment firm that identifies innovative technologies in support of the missions of the U.S. intelligence community.

Robert E. Kahn is President and Chief Executive Officer of the Corporation for National Research Initiatives and co-inventor of the TCP/IP protocol that is the foundation of the modern Internet.

Peter Schwartz is Co-Founder and Chairman of Global Business Network and a member of the Center for a New American Security's board of directors.

Table of Contents

America's Cyber Future

Security and Prosperity in the Information Age

CHAPTER I:
POWER AND NATIONAL SECURITY IN CYBERSPACE

By Joseph S. Nye, Jr.

America's Cyber Future

Security and Prosperity in the Information Age

POWER AND NATIONAL SECURITY IN CYBERSPACE

By Joseph S. Nye, Jr.

The cyber domain is a new and a volatile man-made environment.* The characteristics of cyberspace often reduce power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century. The largest powers are unlikely to be able to dominate cyberspace as much as they have dominated other domains like sea or air. While powerful nations have greater resources, they also have greater vulnerabilities. So, at this stage in the development of the technology, offense dominates defense in cyberspace. That in turn leads to new and complex dimensions in national security policy.

The community of national security analysts is only beginning to grapple with the implications of the new technologies and what they mean for attack, deterrence, defense, negotiation, cooperation and non-state actors. In the words of the JASON advisory panel of defense scientists (an independent group of scientists that advises the government on technological and scientific issues), "People built all the pieces," but "the cyberuniverse is complex well beyond anyone's understanding and exhibits behavior that no one predicted, and sometimes can't even be explained well." The complexity goes beyond that of natural systems because it also involves human strategic interactions. Unlike atoms, human "adversaries are purposeful and intelligent."[1]

In some ways, current thinking about cyber security is analogous to the thinking about nuclear security in the 1950s, when the weapons were new and the concepts underlying adversarial interactions were still being developed. This paper is an effort to map some of the concepts that are necessary for the development of a national security strategy for cyberspace. The first section relates cyberspace to more traditional aspects of power and security in international relations theory. The

* This paper is adapted from Chapter Five of Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011): 113-151.

second section discusses cyber resources of governments and non-state actors. The third section puts forward the basic concepts of governance and security in cyberspace. The fourth section outlines the major cyber vulnerabilities for the United States and some responses to those threats and vulnerabilities. The fifth section discusses some of the prospects and problems for international cooperation.

Cyber Power

Power is the ability to influence others to obtain the outcomes one wants through hard power behavior (coercion and payments) and soft power behavior (framing agendas, attraction and persuasion). Different resources support power behavior in different contexts, and cyberspace is a new context.[2]

Power based on information resources is not new, but cyber power is. There are dozens of definitions of cyberspace but generally "cyber" is a prefix standing for electronic and computer related activities.[3] One can conceptualize cyberspace in terms of many layers of activities, but a simple first approximation portrays it as a unique hybrid regime of physical and virtual properties.[4] The physical infrastructure of cyberspace is a layer that relates well to existing economic laws regarding rival resources (for which the consumption of a good affects the experience of others using the same good) and increasing marginal costs, and to existing political laws of sovereign jurisdiction and control. The virtual or informational layer of cyberspace is characterized by economic traits of increasing returns to scale, and political traits that make jurisdictional control difficult.[5] Attacks from the informational realm where costs are low can be launched against the physical domain where resources are scarce and expensive. But conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer.

Defined behaviorally, cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. This includes the Internet of networked computers, but also intranets, cellular technologies, fiber optic cables and space-based communications. Cyber power can be used to produce preferred outcomes *within* cyberspace or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace.

By analogy, sea power refers to the use of resources in the oceans domain to win naval battles on the ocean, to control shipping chokepoints like straits, and to demonstrate an offshore presence, but it also includes the ability to use the oceans to influence battles, commerce and opinions on land. In 1890, Alfred Thayer Mahan popularized the importance of sea power in the context of new technologies of steam propulsion, armor and long-range guns. President Theodore Roosevelt responded by greatly expanding America's blue water navy and sending it around the world in 1907. After the introduction of aircraft in World War I, military men began to theorize about the domain of air power and the ability to strike directly at an enemy's urban center of gravity without armies having to first cross borders. President Franklin Roosevelt's investments in air power were vital in World War II. After the development of intercontinental missiles and surveillance and communications satellites in the 1960s, writers began to theorize about the particular domain of space power, and President John F. Kennedy launched a program to ensure an American lead in space and to put a man on the moon. In 2009, President Barack Obama called for a major new initiative in cyber power, and other governments have followed suit.[6] As technological change reshapes power domains, political leaders will soon follow.

The cyber domain is unique in that it is man-made, recent and subject to even more rapid

technological changes than other domains. As one observer put it, "the geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch."[7] Low barriers to entry contribute to the diffusion of power in the cyber domain. It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier task forces and submarine fleets create enormous barriers to entry and make it still possible to speak of American naval dominance. While piracy remains a local option for non-state actors in areas like Somalia or the Malacca Straits, sea control remains out of the reach of non-state actors. Similarly, while there are many private and governmental actors in the air domain, a country can still seek to achieve air superiority through costly investments in fifth-generation fighters and satellite support systems.

In contrast, the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at relatively low costs. Compared to sea, air and space, "cyber [space] shares three characteristics with land warfare – though in even greater dimensions: the number of players, ease of entry, and opportunity for concealment … On land, dominance is not a readily achievable criterion."[8] While a few states like the United States, Russia, Britain, France and China are reputed to have greater capacity than others, it makes little sense to speak of dominance in cyberspace as in sea power or air power. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors.

Cyber power affects many issues from war to commerce. We can distinguish "intra-cyberspace power" and "extra-cyberspace power." Just as with sea power, we can distinguish naval power on the oceans from naval power projection on land. For example, carrier-based aircraft can participate in land battles; trade and commerce may grow because of the efficiency of a new generation of container ships; and the soft power of a country may increase by the visit of naval hospital ships in humanitarian missions.

The cyber domain is unique in that it is man-made, recent and subject to even more rapid technological changes than other domains. As one observer put it, "the geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch."

Extreme conflict in the cyber domain or "cyber war" is different from past war.[9] The term "cyber war" is used very loosely for a wide range of behaviors. In this respect, it reflects definitions that range from armed conflict to any hostile contention ("war between the sexes"), but for this analysis I use a narrower definition of cyber actions that have effects outside cyberspace that amplify or are equivalent to kinetic violence.

TABLE 1: PHYSICAL AND VIRTUAL DIMENSIONS OF CYBER POWER

TARGETS OF CYBER POWER		
	WITHIN CYBERSPACE	**OUTSIDE CYBERSPACE**
Information instruments	**Hard:** Launch denial of service attacks. **Soft:** Set norms and standards.	**Hard:** Attack SCADA systems. **Soft:** Initiate public diplomacy campaign to sway opinion.
Physical instruments	**Hard:** Enforce governmental control over companies. **Soft:** Introduce software to help human rights activists.	**Hard:** Destroy routers or cut cables. **Soft:** Stage protests to name and shame cyber providers.

In the physical world, governments have a near monopoly on large-scale use of force, the defender has an intimate knowledge of the terrain, and attacks end because of attrition or exhaustion. Both resources and mobility are costly. In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial and a "single virtual offense is almost cost free."[10] Because the Internet was designed for ease of use rather than security, the offense currently has the advantage over the defense. This might not remain the case in the long term as technology evolves, including efforts at "re-engineering" some systems for greater security, but it remains the case at this stage. The larger party has limited ability to disarm or destroy the enemy, occupy territory or effectively use counterforce strategies.

As Table 1 illustrates, inside the cyber domain, information instruments can be used to produce soft power in cyberspace through agenda framing (the ability to influence what issues get attention and how they are portrayed), attraction or persuasion. For example, attracting the open source software community of programmers to adhere to a new standard is an example of soft power targeted within cyberspace. Cyber resources can also produce hard power inside cyberspace. For example, states or non-state actors can organize a distributed denial-of-service (DDoS) attack by using "botnets" of hundreds of thousands (or more) corrupted computers that swamp a company or country's Internet system and prevent from functioning, as happened to Georgia in 2008. Organizing a botnet by infiltrating a virus into unguarded computers is relatively inexpensive, and botnets can be illegally rented on the Internet for a few hundred dollars. Sometimes individual criminals do this for purposes of extortion.

Other cases may involve "hacktivists" or ideologically motivated intruders. For example, Taiwanese and Chinese hackers regularly deface each others' websites with electronic graffiti. In 2007, Estonia suffered a DDoS attack that was widely attributed to "patriotic hackers" in Russia who were offended by Estonia's movement of a World War II monument to Soviet soldiers. In 2008, shortly before Russian troops invaded, Georgia suffered a DDoS attack that shut down its Internet access. (In both

instances, however, the Russian government seems to have abetted the hackers while maintaining "plausible deniability.") Other forms of hard power within cyberspace include insertion of malicious code to disrupt systems or to steal intellectual property. Criminal groups do it for profit, and governments may do it as a way of increasing their economic resources. China, for example, has been accused of such activities by a number of other countries. Proving the origin or motive of such attacks is often very difficult as attackers can route their intrusions through servers in other countries to make attribution difficult. For example, many of the attacks on Estonian and Georgian targets were routed through American servers.[11]

Information can travel through cyberspace and create soft power by attracting citizens in another country. A public diplomacy campaign using the Internet is an example, as were Secretary of State Hillary Rodham Clinton's appeals for Internet freedom in China in 2010, and Egypt in 2011. In general, American officials have promoted a narrative about the Internet that "legitimizes their material practice of supporting anticensorship technologies."[12] But cyber information can also become a hard power resource that can do damage to physical targets in another country. For example, many modern industries and utilities have processes that are controlled by computers linked in SCADA (supervisory control and data acquisition) systems. Malicious software inserted into these systems could be instructed to shut down a process which would have very real physical effects, as the Stuxnet worm seems to have had on Iran's nuclear program last year.[13]

As Table 1 indicates, physical instruments can provide power resources that can be brought to bear on the cyber world. For instance, the physical routers and servers and the fiber optic cables that carry the electrons of the Internet have geographical locations within governmental jurisdictions, and companies running and using the Internet are subject to those governments' laws. Governments can bring physical coercion to bear against companies and individuals; what has been called "the hallmark of traditional legal systems." Legal prosecution made Yahoo restrict what it distributed in France to fit French laws, and Google removed hate speech from searches in Germany. Even though the messages were protected free speech in the United States – the companies' "home country" – the alternative to compliance was jail time, fines and loss of access to those important markets. Governments control behavior on the Internet through their traditional physical threats to such intermediaries as Internet service providers, browsers, search engines and financial intermediaries.[14]

As for investing in physical resources that create soft power, governments can set up special servers and software designed to help human rights activists propagate their messages despite the efforts of their own governments to create information firewalls to block such messages. For example, in the aftermath of the Iranian government's repression of protests following the election of 2009, the U.S. State Department invested in software and hardware that would enable protesters to disseminate their messages.[15]

Finally, as Table 1 illustrates, both hard and soft power resources can be used against the Internet. The cyber information layer rests upon a physical infrastructure that is vulnerable to direct military attack or sabotage both by governments and non-state actors such as terrorists or criminals. Servers can be blown up and cables can be cut. And in the domain of soft power, non-state actors and NGOs (non-governmental organizations) can organize physical demonstrations to name and shame companies (and governments) that they regard as abusing the Internet. For example, in 2006, protesters in Washington marched and demonstrated against Yahoo and other Internet companies that had provided the names of Chinese activists which led to their arrest by the Chinese government.

Potential Power Resources of Actors in the Cyber Domain

MAJOR GOVERNMENTS

- Development and support of infrastructure, education, intellectual property.
- Legal and physical coercion of individuals and intermediaries located within borders.
- Size of market and control of access; e.g. EU, China, United States.
- Resources for cyber attack and defense: bureaucracy, budgets, intelligence agencies.
- Provision of public goods; e.g. regulations necessary for commerce.
- Reputation for legitimacy, benignity, competence that produce soft power.

Key Vulnerabilities: High dependence on easily disrupted complex systems, political stability, reputational losses.

ORGANIZATIONS AND HIGHLY STRUCTURED NETWORKS

- Large budgets and human resources; economies of scale.
- Transnational flexibility.
- Control of code and product development, generativity of applications.
- Brands and reputation.

Key Vulnerabilities: Legal, intellectual property theft, systems disruption, reputational losses.

INDIVIDUALS AND LIGHTLY STRUCTURED NETWORKS

- Low cost of investment for entry.
- Virtual anonymity and ease of exit.
- Asymmetrical vulnerability compared to governments and large organizations.

Key Vulnerabilities: Legal and illegal coercion or retaliation by governments and organizations if caught.

Actors and Their Relative Power Resources

The diffusion of power in the cyber domain is evident in the vast number of actors and the relative reduction of power differentials among them. Anyone from a teenage hacker to a major modern government can do damage in cyberspace, and, as the famous *New Yorker* cartoon once put it, "on the Internet, no one knows you are a dog." The infamous "Love Bug" virus unleashed by a hacker in the Philippines is estimated to have caused 15 billion dollars in damage.[16] Computer networks essential to the American military are approached by outsiders "hundreds of thousands of times every day."[17] Cyber criminal groups are said to have stolen over 1 trillion dollars in data and intellectual property in 2008.[18] One cyber espionage network – GhostNet –infected 1,295 computers in 103 countries, of which 30 percent were high-value governmental targets.[19] Terrorist groups use the Web to recruit new members and plan campaigns. Political and environmental activists disrupt websites of companies and governments. What is distinctive about power in the cyber domain is not that governments are out of the picture as the early cyber libertarians predicted, but rather the different power resources that different actors possess, and the narrowing of the gap between state and non-state actors in many instances. But relative reduction of power differentials is not the same as equalization. Large governments still have more resources. On the Internet, all dogs are not equal.

As a rough approximation, we can divide actors in cyberspace into three broad categories: governments, organizations with highly structured networks and individuals and lightly structured networks. (Of course, there are many subcategories, and some governments have much more capacity than others, but this is a first approximation.)

Because the physical infrastructure of the Internet remains tied to geography and governments exercise sovereignty over geographic spaces, location still matters as a resource in the cyber domain. Governments can take steps to subsidize infrastructure, computer education and protection of intellectual property that will encourage (or discourage) the development of capabilities within their borders. The provision of public goods, including a legal and regulatory environment, can stimulate commercial growth of cyber capabilities. Geography also serves as a basis for governments to exercise legal coercion and control. If a market is large, a government can exert its power extraterritorially. Europe's tight privacy standards have had a global effect. Obviously, this is a power resource available to governments with jurisdiction over large markets, but not necessarily to all governments.

Governments also have the capacity to carry out offensive cyber attacks.[20] One should distinguish simple attacks, which use inexpensive toolkits that anyone can download from the Internet, from advanced attacks, which identify new vulnerabilities that have not yet been patched, involve new viruses and "zero day attacks" (first time use). These attacks require more skill than simple hacking. Little is publicly confirmed about cyber attacks or cyber exploitation or espionage, but most reports describe intrusions into computer systems as ubiquitous, and not limited to governments. Nonetheless, major governments have the greater economic and human resources.

There are reports of attacks as adjuncts to warfare in the cases of Iraq in 2003 and Georgia in 2008, and sabotage of electronic equipment in covert actions.[21] Israel is said to have used cyber means to defeat Syrian air defenses before bombing a secret nuclear reactor in September 2007, and the Stuxnet worm may have been a governmental effort to sabotage Iran's nuclear program.[22] Most experts see cyber attack as an important adjunct rather than an overwhelming weapon (unlike nuclear options) in inter-state wars. States intrude into each others' cyber systems in "preparation of the battlefield"

for what could be future conflicts. Both American and Chinese military theorists have discussed such steps but little is publicly stated about offensive cyber doctrines. A 2009 National Research Council report concluded: "Today's policy and legal framework for guiding and regulating the U.S. use of cyber attack is ill-formed, undeveloped and highly uncertain."[23]

Cyber attacks that deny service or disrupt systems are also carried out by non-state actors whether for ideological or criminal purposes, but such groups do not have the same capacities as large governments. Sophisticated attacks against high-value targets such as defense communications systems may require the involvement of large intelligence agencies that intrude physically (through supply chains or spies) and/or crack highly encrypted codes. A teenage hacker and a large government can both do considerable damage over the Internet, but that does not make them equally powerful in the cyber domain. Power diffusion is not the same as power equalization. Some government experts believe that concerted technological improvements in encryption and identity management could greatly reduce threats at the low end of the spectrum within five years.[24]

While governments derive power from greater resources, they lose power from greater vulnerability. In situations of reciprocal dependence, it is asymmetrical vulnerability that produces power, and in the cyber domain, individuals benefit from asymmetrical vulnerability compared to governments and large organizations. Such "super-empowered individuals" have very low investment and little to lose from exit and re-entry. Their major vulnerability is to legal and illegal coercion by governments and organizations if they are apprehended, but only a small percentage are actually caught. And in the case of WikiLeaks, the American government had difficulty in finding a way to prosecute its Australian leader, Julian Assange.[25] In contrast, corporations have important vulnerabilities because of large fixed investments in complex operating systems, intellectual property and reputation. Similarly, large governments depend on easily disrupted complex systems, political stability and reputational soft power. While hit-and-run cyber strikes by individuals are unlikely to bring governments or corporations to their knees, they can impose serious costs of disruption to operations and to reputations with a miniscule investment. Governments are top dogs on the Internet, but smaller dogs still bite.

Cyber Governance and National Security

Some see cyberspace as analogous to the ungoverned and lawless Wild West, but in practice there are many areas of private and public governance. Certain technical standards related to Internet protocol are set (or not set) by consensus among engineers involved in the non-governmental Internet Engineering Task Force (IETF). A non-governmental World Wide Web Consortium develops standards for the Web. The Internet Corporation for Assigned Names and Numbers (ICANN) has the legal status of a non-profit corporation under American law, though its procedures have evolved to include government voices (though not votes). In any event, its mandate is limited to domain names and routing management, not the full panoply of cyberspace governance. National governments control copyright and intellectual property laws, and try to manage problems of security, espionage and crime within national legal frameworks, though the technological volatility of the cyber domain means that laws and regulations are always chasing a moving target. And efforts by the International Telecommunications Union to establish new norms for cyberspace have been ineffectual, in part reflecting the wide range of governmental views about sovereignty and desirable norms for the Internet.

The cyberspace domain is often described as a public good or a global commons, but these terms are an imperfect fit. A public good is one

from which all can benefit and none can be excluded, and while this may describe some of the information protocols of the Internet, it does not describe the physical infrastructure which is a scarce proprietary resource located within the boundaries of sovereign states. And cyberspace is not a commons like the high seas because parts of it are under sovereign control. At best, it is an "imperfect commons" or a condominium of joint ownership without well-developed rules.[26] Cyberspace can be categorized as what the Nobel Laureate Elinor Ostrom terms a "common pool resource" from which exclusion is difficult and exploitation by one party can subtract value from other parties.[27] Government is not the sole solution to the problems of common pool resources. Ostrom says that community self-organization is possible under certain conditions such as limited number of users and a good understanding of system dynamics. However, some of the conditions that she associates with successful self-governance are weak in the cyber domain because of the large size of the resource, the large number of users and the poor understanding of how the system will evolve.

In its earliest days, the Internet was like a small village of known users – an authentication layer of code was not necessary and development of norms was simple. Security was not a major concern. All that changed with burgeoning growth. While the openness and accessibility of cyberspace as a medium of communication provide valuable benefits to all, free riding behavior in the form of crime, attacks and threats creates insecurity. The result is a demand for protection that can lead to fragmentation, "walled gardens," private networks and cyber equivalents to the 17th-century enclosures that were used to solve that era's "tragedy of the commons."[28]

Security is the absence or reduction of threat to key values. Absolute security is impossible, and providing security is usually a process of managing risks. The connectivity of the Internet provides benefits, but criminals, hackers and other governments constitute a threat to the preservation of the imperfect Internet commons. As more users feel threatened by such free riders, they may resort to inferior versions of cyber connectivity and trade off welfare in search of security. Jonathan Zittrain warns of the dangers of fencing off parts of the Internet, like fencing of the commons, limiting or destroying its generativity.[29]

But as important as it is to protect the key welfare benefits derived from cyber connectivity, some values such as life and liberty may be ranked as more important in national security, and connectivity that creates vulnerabilities that endanger those values may be sacrificed. People value freedom of movement and privacy of information in society, but in times of epidemics we limit them with vaccinations and quarantines to protect public health. Indeed, some analysts argue that we should think of cyber security as analogous to public health systems. Others think of law enforcement analogies, and still others use the analogy of fire departments with capabilities to install alarms, inspect, put out fires and carry out forensics. Indeed some responses to cyber intrusions, like the ad hoc group formed to combat the Conficker worm might be likened to a volunteer fire department.[30] No analogy is perfect, but these analogies help to remind us that cyber defense is not like military defense where one defends at national borders. Vulnerabilities are created by domestic practices and transnational attacks may come from surprising directions. Computer hygiene, redundancy and resilience are an important part of cyber security, and the incentives for private actors to pay for these public goods may mean that they will be under-produced from the perspective of national security.

Providing security is a classic function of government, and some observers believe that increasing insecurity will lead to an increased role for

> *"Terrorist groups today are ranked near the bottom of cyberwar capability. Criminal organizations are more sophisticated. There is a hierarchy. You go from nation states, which can destroy things, to criminals, who can steal things, to aggravating but sophisticated hackers … Sooner or later, terror groups will achieve cyber-sophistication. It's like nuclear proliferation, only far easier."*
>
> MIKE MCCONNELL,
> FORMER DIRECTOR
> OF NATIONAL INTELLIGENCE

governments in cyberspace. Many states desire to extend their sovereignty in cyberspace, and seek technological means to do so. As two experts have put it, "securing cyberspace has definitely entailed a 'return of the state' but not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty." [31] Efforts to secure the network help to facilitate its use by burgeoning non-state actors, and often entail devolution of responsibilities and authority to private actors. For example, banking and financial firms have developed their own elaborate systems of security and punishment through networks of connectedness, such as depriving repeat offenders of their trading rights, and by slowing speeds and raising transaction costs for addresses that are associated with suspect behavior. Governments want to protect the Internet so their societies can continue to benefit, but at the same time, they want to protect their societies from what comes through the Internet. China, for example, is described as developing its own companies behind its firewall, and planning to disconnect from the Internet if it is attacked.[32] Nonetheless, China – and other governments – still seek the economic benefits of connectivity. The tension leads to imperfect compromises, as one can see in the outcome of the dispute between China and Google in 2010.[33]

Cyber Threats and Responses

If one treats most hacktivism as mainly a nuisance, there are four major categories of cyber threats to national security, each with a different time horizon and with different (in principle) solutions: cyber war and economic espionage are largely associated with states, and cyber crime and cyber terrorism are mostly associated with non-state actors. For the United States, at the present time, the highest costs come from espionage and crime, but over the next decade or so, war and terrorism may become greater threats. Moreover, as alliances and tactics evolve among different actors, the categories may increasingly overlap. As described by former Director of National Intelligence Mike McConnell: "Terrorist groups today are ranked near the bottom of cyberwar capability. Criminal organizations are more sophisticated. There is a hierarchy. You go from nation states, which can destroy things, to criminals, who can steal things, to aggravating but sophisticated hackers … Sooner or later, terror groups will achieve cyber-sophistication. It's like nuclear proliferation, only far easier."[34]

According to President Obama's 2009 cyber review, theft of intellectual property by other states (and corporations) was the highest immediate cost. Not

only did it result in current economic losses, but by destroying competitive advantage, it jeopardized future hard power.[35] As we saw above, cyber criminals are also a significant burden on the economy. Looking further ahead, as other states develop their capacities for cyber attack on critical infrastructures and are able to deprive American military forces of their information advantages, the costs to American hard power could be significant. And as terrorist groups that wish to wreak destruction develop their capacity to do so, they could impose dramatic costs. The remedies for each threat are quite different.

Cyber war, although only incipient at this stage, is the most dramatic of the potential threats. Major states with elaborate technical and human resources could, in principle, create massive disruption as well as physical destruction through cyber attacks on military as well as civilian targets. Responses to cyber war include a form of interstate deterrence (though different from classical nuclear deterrence), offensive capabilities, and designs for network and infrastructure resilience if deterrence fails. At some point in the future, it may be possible to reinforce these steps with certain rudimentary norms.[36]

In the case of war, fighting would be subject to the classic norms of discrimination and proportionality that are central to the existing laws of armed conflict, but cyber war raises new and difficult problems of how to distinguish civilian from military targets, and being sure about the extent of collateral damage. For example, an American general is quoted as saying that American planners did not use one particular cyber technique to disable the French-made Iraqi air defense network because they "were afraid we were going to take down all the automated banking machines in Paris." Moreover, because cyber defense is sometimes analogous to shooting the gun out of an outlaw's hand before he can shoot, and it must be handled by machines working at "netspeed" when an attack is first detected, offense and defense blur and rules of engagement that maintain civilian control become difficult to establish.[37]

Some observers argue that because of the difficulty of attribution of the source of an attack, deterrence does not work in cyberspace. However, this common view is too simple. While interstate deterrence is more difficult in the cyber domain, it is not impossible. Too often people think of deterrence in terms of the nuclear model that prevailed for the past half century, in which the threat of punitive retaliation is so catastrophic that it deters attack. But nuclear deterrence was never this simple. While a second strike capability and mutual assured destruction may have worked to prevent attacks on the homeland, they were never credible for issues at the low end of the spectrum of interests. Lying somewhere in between these extremes lay extended deterrence of attacks against allies and defense of vulnerable positions such as Berlin in the Cold War. Nuclear deterrence was supplemented by other measures (such as forward basing of conventional forces); a variety of signaling devices in the movement of forces; and a learning process that occurred over decades and led to areas of agreements ranging from non-proliferation to managing incidents at sea.

Cyber attacks lack the catastrophic dimensions of nuclear weapons attacks, and attribution is more difficult, but interstate deterrence through entanglement and denial still exists. Even when the source of an attack can be successfully disguised under a "false flag," other governments may find themselves sufficiently entangled in interdependent relationships that a major attack would be counterproductive. Unlike the single strand of military interdependence that linked the United States and the Soviet Union in the Cold War, the United States, China and other countries are entangled in multiple networks. China, for example, would itself lose from an attack that severely damaged the American economy, and vice versa.[38]

In addition, an unknown attacker may be deterred by denial. If firewalls are strong, or the prospect of a self-enforcing response seems possible ("an electric fence"), attack becomes less attractive. Offensive capabilities used to respond immediately to attacks can create an active defense that can serve as a deterrent even when the identity of the attacker is not fully known. Futility can also help deter an unknown attacker. If the target is well protected, or redundancy and resilience allow quick recovery, the risk to benefit ratio in attack is diminished. Finally, to the extent that false flags are imperfect, and rumors of the source of an attack are widely deemed credible (though not probative in a court of law), reputational damage to an attacker's soft power may contribute to deterrence.

Cyber terrorism and non-state actors are harder to deter. Thus far, cyber attacks have not been the most attractive route for terrorists, though they make extensive use of the Internet for recruitment and coordination for more conventional kinetic attacks. But as groups develop their cyber capacity to wreak great damage against infrastructure over the coming years, the temptation will grow. Since attribution will be difficult, improved defenses such as pre-emption and human intelligence become the most important responses. At a more fundamental level, many experts believe that the best long-term response is a program to re-engineer the Internet to make such attacks more difficult than under today's structure that emphasizes ease of use rather than security. One approach is to reduce the vulnerability of some sensitive aspects of the national infrastructure by reducing their connectivity to the Internet. Some suggest special "opt in" incentives for private owners of critical infrastructure (e.g., finance and electricity) to join secure systems rather than rely on the open Internet (which would continue to exist for those with lower stakes and willing to tolerate greater risks). But even systems disconnected from the Internet can be vulnerable to penetration by disloyal employees, compromised hardware and sabotaged software. Such threats will require better monitoring of personnel and systems, as well as greater redundancy in case of failures.

As for economic espionage via the Internet, which currently does the most damage, it is likely to continue unabated unless there are new responses. Spying is as old as human history, and does not violate any explicit provisions of international law. Nonetheless, at times governments have established rules of the road for limiting espionage, and engaged in patterns of tit for tat retaliation to create an incentive for cooperation. Experiments have shown that partners in prisoners' dilemma and public goods games can develop cooperation in repeated play over extended periods.[39] While it is difficult to envisage enforceable treaties in which governments agree not to engage in espionage, it is plausible to imagine a process of iterations (tit for tat) that develop rules of the road, which could limit damage in practical terms. For example, a country might threaten to filter and slow down communications from suspect addresses in another country if that government refuses to curtail the level of theft of intellectual property.

Governments often claim not to know the identity of those who attack and exfiltrate intellectual property. In the words of Howard Schmidt, the American cyber security chief, "one of the key things has been going back to the countries that it appears it's coming from and saying: 'If it's not you, you need to investigate this.'"[40] Failure to respond can be followed by measured retaliation. Under international legal doctrine, proportionate countermeasures can be taken in response to harm originating from a state even if the government is not behind it. While less than perfect, efforts can be made to deal with non-state actors by holding states responsible for actions that originate within their sovereign boundaries. To avoid escalation or "defection lock-in," it helps to offer assistance and to engage in discussions that can develop common

perceptions, if not fully agreed norms. Such "learning" is still at an early stage in the cyber domain, analogous to the nuclear era in the early 1950s.[41]

Cyber crime by non-state actors can also be reduced by responses that make access to some systems more difficult than they are today. Domestic hygiene, monitoring and resilience are all important. Steps could be taken to increase the use of reputation, markets and regulation to improve the robustness of systems. For example, to name but a few: a "cyber consumers report" that issued "do not buy" suggestions could change incentives for software providers; use of government purchasing power could create incentives for better software which is now purchased largely on price; and legislation or regulation could require all Internet service providers to warn and ultimately disconnect compromised computers.[42]

International Cooperation

While many of the most immediate and important steps toward increasing security involve domestic measures, the global nature of the Internet raises the issue of international cooperation. Some people call for cyber arms control negotiations and formal treaties, but differences in norms and the impossibility of verification makes such treaties difficult to negotiate or implement. Such efforts could actually reduce national security if asymmetrical implementation put legalistic cultures like the United States at a disadvantage compared to societies with a higher degree of governmental corruption. At the same time, it is not too early to explore international talks. The most promising early areas for international cooperation may not be bilateral conflicts, but problems posed by third parties.

For example, it may be possible to develop degrees of international cooperation to limit cyber crime analogous to efforts to discourage piracy at an earlier era. At one time, many governments found it convenient to tolerate some pirates and even charter privateers (until the Declaration of Paris in 1856), and today some governments have similar attitudes toward crime on the Internet. Russia and China, for example, have refused to sign the Council of Europe Convention on Cyber Crime, which has been signed by 46 countries and ratified by 30 as of June 2010. As scholars Abraham Sofaer, David Clark and Whitfield Diffie point out, adherence is diluted by inclusion of efforts to punish conduct based on content (such as fraud and child pornography) and its law enforcement framework operates on too long a time scale.[43] They suggest an agreement focused on punishing attacks that potentially damage the cyber infrastructure itself. Robert Knake argues that it should be possible to supplement the Council of Europe convention with more limited flexible and regional agreements.[44]

In the past, the lines between government and criminal activity sometimes blurred in countries with high levels of corruption, but attitudes may change over time if costs exceed benefits. For example, "Russian cybercriminals no longer follow hands-off rules when it comes to motherland targets, and Russian authorities are beginning to drop the laisser faire policy."[45] While the immediate prospects for Russia and China signing the Convention are not promising, it is possible to imagine coalitions of the willing that set a higher standard, and work together to raise the costs for those who violate an emergent norm, much as occurs with financial money laundering regulations or the Proliferation Security Initiative.

Among responses to the various cyber threats, large-scale formal treaties regulating cyberspace seem unlikely. Over the past decade, the U.N. General Assembly has passed a series of resolutions condemning criminal activity and drawing attention to defensive measures that governments can take. For more than a decade, Russia has sought a treaty for broader international oversight of the Internet, banning deception or the embedding of malicious code or circuitry that could be activated in the event of war. But Americans have argued

that arms control measures banning offense can damage defense against current attacks, and would be impossible to verify or enforce. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the Internet. Nonetheless, the United States has begun informal discussions with Russia, and one could envisage some limited agreements.[46] Even advocates for an international law for information operations are skeptical of a multilateral treaty akin to the Geneva Conventions that could contain precise and detailed rules given future technological volatility, but they argue that like-minded states could announce self-governing rules that could form norms for the future.[47]

Normative differences present a difficulty in reaching any broad agreements on regulating content on the Internet. As we saw earlier, the United States has called for the creation of "norms of behavior among states" that "encourage respect for the global networked commons." But as Jack Goldsmith has argued, "even if we could stop all cyber attacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense."[48] From the American point of view, Twitter and YouTube are matters of personal freedom; seen from Beijing or Teheran, they are instruments of attack.

The most promising areas for initial agreements may be issues that involve "environmental" effects and third parties. For example, little was accomplished in bilateral nuclear arms control in the 1950s. Much of what passed for nuclear knowledge rested on elaborate counterfactual abstractions, and the ambiguous structure of nuclear knowledge made it difficult to alter prior beliefs. However, when the United States and the Soviet Union turned to environmental effects of above-ground testing and to the dangers of proliferation to other countries in the 1960s, they were able to conclude a Limited Test Ban Treaty and the Non-Proliferation Treaty. The process of negotiation and communication advanced nuclear learning in the 1970s and 1980s with regard to command and control, inadvertent war, surveillance, verification and crisis communications. By 1985, President Ronald Reagan and Russian President Mikhail Gorbachev agreed that "nuclear war cannot be won and must never be fought" (in the words of their Geneva communiqué).[49]

Even if cyber processes are dynamic and our knowledge is limited given the fact that the Web is only two decades old, it may make sense to start intergovernmental communication and negotiation processes as a way of speeding up transnational learning. The place to start is not with ambitious arms control measures related to cyber war, but with the low hanging fruit discussed above. A treaty protecting the core working of the Internet suggested by Sofaer, Clark and Diffie is an example. Similarly, an improved approach to cyber crime may prove in the interests of many states. And governments such as China and the United States would have a common interest in not allowing a malign hacktivist to launch a cleverly routed attack designed to catalyze a conflict between them.

Conclusion

The cyber domain is both new and volatile. The characteristics of cyberspace reduce some of the power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century. But cyberspace also illustrates the point that diffusion of power does not mean equality of power or the replacement of governments as the most powerful actors in world politics. While cyberspace may create some power shifts among states by opening limited opportunities for leapfrogging by small states using asymmetrical warfare, it is unlikely to be a game changer in this century's power transitions among states. The United States, for example, has greater vulnerabilities, but also greater capabilities

for exploiting the vulnerabilities of other states. At some point, but not soon, states may progress far enough along a learning curve to design cooperative measures that limit such threats.

On the other hand, the cyber domain does give much more power to non-state actors than in the past, and the threats they pose are likely to increase. Some of the most important security responses must be national and unilateral, focused on hygiene, redundancy and resilience. It is likely, however, that governments will gradually discover that cooperation against the insecurity created by non-state actors will require greater priority in attention. We are a long distance from such response at this stage in the development of cyber technology. In an analogy to nuclear weapons, we are still in the period before the Limited Test Ban and Non-Proliferation Treaties, which dealt with environmental and third party problems rather than bilateral arms control. But those responses did not occur until we approached the third decade of the nuclear era. With the invention of the World Wide Web only two decades old, we may be approaching an analogous point in the political trajectory of cyber technology.

ENDNOTES

1. JASON, "Science of Cyber-Security Needs More Work," *Secrecy News* (14 December 2010), http://www.fas.org/irp/agency/dod/jason/cyber.pdf.

2. For more on the definitions of power resources and behaviors, see Joseph Nye, *The Future of Power* (New York: Basic Books, 2011) from which much of this paper is drawn.

3. Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin Kramer, Stuart Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington: National Defense Univerity Press, 2009): 26-28.

4. Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009): 12. Libicki distinguishes three layers of cyberspace: physical, syntactic and semantic. However, with applications added upon applications, the Internet can be conceived in multiple layers. See Marjory Blumenthal and David Clark, "The Future of the Internet and Cyberpower," in Franklin Kramer, Stuart Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington: National Defense University Press, 2009): 266.

5. I am indebted here to Jeffrey Cooper and his unpublished work on "New Approaches to Cyber-Deterrence".

6. Ellen Nakashima and Brian Krebs, "Obama Says He Will Name National Cybersecurity Advisor," *The Washington Post* (30 May 2009).

7. See Gregory Rattray, "An Environmental Approach to Understanding Cyberpower," in Franklin Kramer, Stuart Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington: National Defense University Press, 2009): 253-274 and especially 256.

8. Franklin Kramer, "Cyberpower and National Security," in Franklin Kramer, Stuart Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington: National Defense University Press, 2009): 12.

9. Paul Cornish, David Livingstone, Dave Clemente and Claire York, *On Cyber Warfare: A Chatham House Report* (London: Chatham House, 2010).

10. LTC David Johnson and Steve Pettit, "Principles of the Defense for Cyber Networks," *Defense Concepts* Vol. 4, No. 2 (Jan 2010): 17.

11. Author interviews with U.S. government officials (March 2010).

12. Daniel McCarthy, "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet," *Foreign Policy Analysis,* Vol. 7, No. 1 (January 2011): 89.

13. "A worm in the centrifuge," *The Economist* (2 October 2010): 63-64.

14. Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (Oxford: Oxford University Press, 2008): 180.

15. Some of these investments such as "Haystack" were counter productive. See Clay Shirky, "The Political Power of Social Media," *Foreign Affairs,* Vol. 90, No. 1 (January/February 2011): 31. See also Richard Fontaine and Will Rogers, "Internet Freedom and its Discontents: Navigating the Tensions with Cyber Security," in this volume.

16. Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (Oxford: Oxford University Press, 2008): 165.

17. General Keith Alexander, head of Cyber Command,quoted in, "Attacks on Military Computers Cited," *The New York Times* (16 April 2010).

18. McAfee Report, "Unsecured Economies: Protecting Vital Information," (Davos, 2009); Tim Weber, "Cybercrime threat rising sharply," BBC News (31 January 2009), http://news.bbc.co.uk/2/hi/business/davos/7862549.stm.

19. Munk Centre for International Studies, University of Toronto, "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor* (March 2009).

20. William Owens, Kenneth Dam and Herbert Lin, eds., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: The National Academies Press, 2009).

21. See for example, John Markoff, "Old Trick Threatens Newest Weapons," *The New York Times* (27 October 2009); and Shane Harris, "The Cyberwar Plan," *National Journal* (14 November 2009): 18.

22. Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco, 2010): Chapter 1. See also William Broad, John Markoff, and David Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times* (15 January 2011).

23. William Owens, Kenneth Dam and Herbert Lin, eds., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: The National Academies Press, 2009): 27.

24. Author interviews with U.S. government officials, March 2010.

25. Evgeny Morozov, "Wiki Rehab," *The New Republic* (7 January 2011).

26. The metaphor is from James Lewis. See also, "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" (Washington: Center for Strategic International Studies, 2008).

27. See Elinor Ostrom, Joanna Burger, Christopher Field, Richard Norgaard and David Policansky, "Revisiting the Commons: Local Lessons, Global Challenges," *Science* 284, 5412 (April 1999): 278 for a challenge to Garrett Hardin's 1968 formulation of "The Tragedy of the Commons," *Science* 162, 3859 (December 1968): 1243.

28. Elinor Ostrom, "A General Framework for Analyzing Sustainability of Social-Ecological Systems," *Science* 325 (July 2009): 421; Roger Hurwitz, "The Prospects for Regulating Cyberspace," unpublished paper (November 2009).

29. Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, CT: Yale University Press, 2008).

30. I am indebted to Deirdre Mulligan of University of California, Berkeley for the first insight, and Vint Cerf of Google for the second. Discussions at AAAS meeting (30 September 2010).

31. Ronald Deibert and Rafal Rohozinski, "Risking Security: The Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4 (March 2010).

32. Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco, 2010): 146.

33. See Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, CT: Yale University Press, 2008).

34. Quoted in Nathan Gardels, "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly*, 27 (April/ Spring 2010): 16.

35. Melissa Hathaway, "Strategic Advantage: Why America Should Care About Cybersecurity," Discussion Paper, Harvard Kennedy School (Cambridge: Belfer Center for Science and International Affairs, 2009); Ellen Nakashima and Brian Krebs, "Obama Says He Will Name National Cybersecurity Advisor," *The Washington Post* (30 May 2009).

36. See Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco, 2010) for a discussion of the limits of arms control and possible norms. See also Martha Finnemore, "Cultivating International Cyber Norms," in this volume.

37. Christopher Ford, "Cyber-Operations: Some Policy Challenges," posted report on Council for Strategic and International Studies meeting (3 June 2010).

38. A recent study by the National Research Council refers to this as "blowback, which refers to a bad consequence affecting the instigator of a particular action." National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks* (Washington: National Academies Press, 2010): 354.

39. Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984); David Rand, Anna Drebner, Tore Ellingsen, Drew Fudenberg and Martin Nowak, "Positive Interactions Promote Public Cooperation," *Science* 325 (September 2009): 1272.

40. Joseph Menn, "US cybercrime chief wary on provoking China and Russia," *Financial Times* (5 March 2010).

41. For a description of the gradual evolution of such learning in the nuclear area, see Joseph S. Nye, Jr., "Nuclear Learning and U.S.-Soviet Security Regimes," *International Organization* Vol. 41, No. 3 (Summer 1987).

42. For these and additional measures, see Joel Brenner, "Why Isn't Cyberspace More Secure?" *Communications of the ACM*, Vol. 53, No. 11 (November 2010): 33-35.

43. Abraham Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," In National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks* (Washington: National Academies Press, 2010).

44. Robert Knake, *Internet Governance in an Age of Cyber Insecurity* (New York, Council on Foreign Relations, 2010): 16-19.

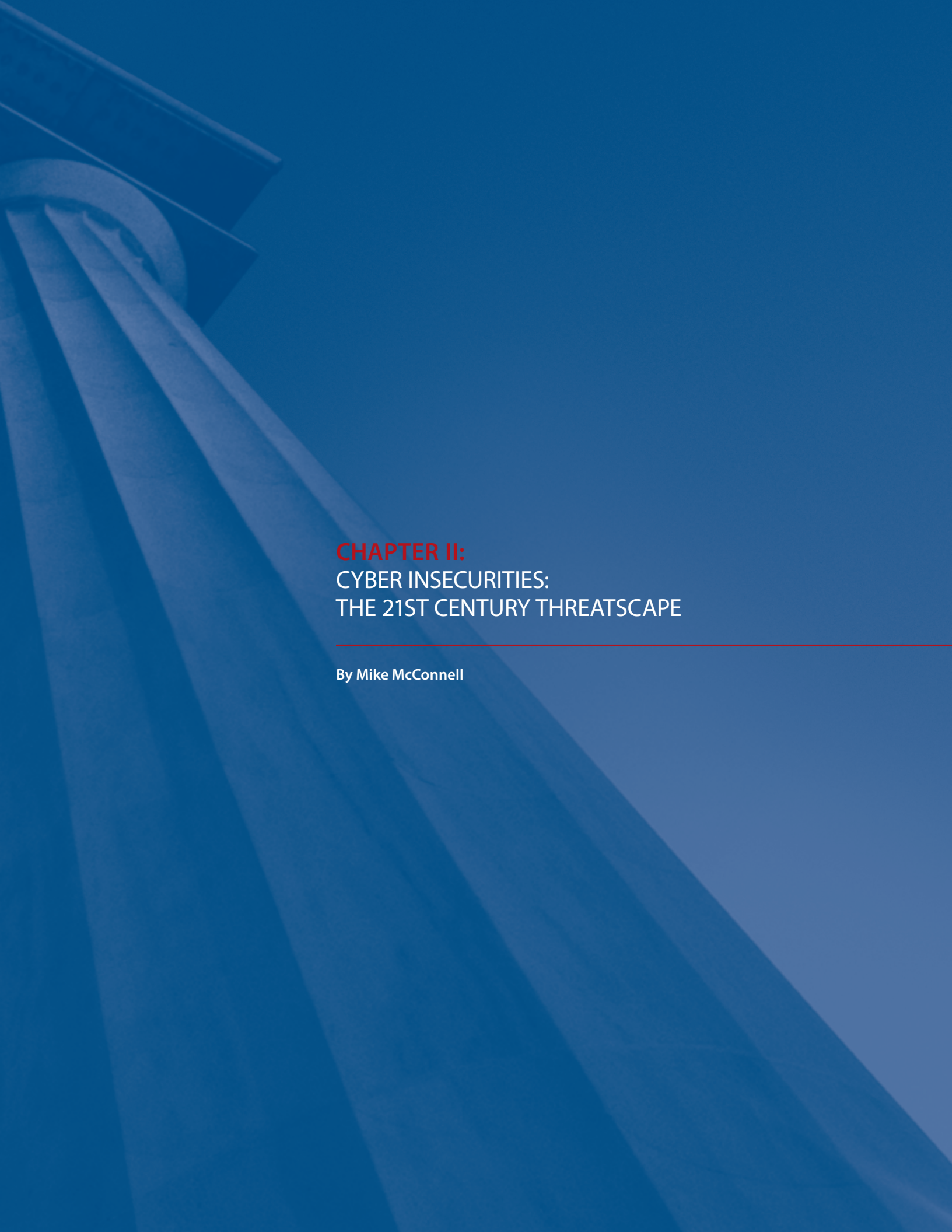
45. Don Jackson, quoted in Joseph Menn, "Moscow gets tough on cybercrime as ID theft escalates," *Financial Times* (22 March 2010).

46. John Markoff, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia," *The New York Times* (16 April 2010).

47. Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis and Clark Law Review* Vol. 11, No. 4 (2007): 1059.

48. Jack Goldsmith, "Can We Stop the Global Cyber Arms Race?," in Goldsmith and Wu, eds, *Who Controls the Internet?* (Oxford: Oxford University Press, 2008).

49. See Joesph S. Nye, Jr., "Nuclear Learning and U.S.-Soviet Security Regimes," *International Organization* Vol. 41, No. 3 (Summer 1987) for more examples and a detailed argument.



CHAPTER II:
CYBER INSECURITIES: THE 21ST CENTURY THREATSCAPE

By Mike McConnell

America's Cyber Future

Security and Prosperity in the Information Age

CYBER INSECURITIES: THE 21ST CENTURY THREATSCAPE

By Mike McConnell

Threats to U.S. national security in the 21st century are numerous. But the most critical threats of our time, with the lowest barriers to entry, are those to our cyber infrastructure. Until now, the primary focus has been on threats originating from online sources such as viruses, malicious code and distributed denial-of-service (DDoS) operations. This chapter, however, will discuss a broader national insecurity: threats to critical infrastructure in cyberspace from nation-state or extremist groups. It provides an assessment of cyber threats and the very real dangers to cyberspace that can originate from physical threats.

In the last 20 years, the actors posing the greatest threats to cyberspace have shifted from tactical actors whose impacts have ranged from operational nuisances (e.g., shutting down public-facing websites) and financial (e.g., credit card fraud and identity theft) to terrorist groups and nation-states whose strategic intent is to cause long-term harm to U.S. economic well being (e.g., stealing critical technology and intellectual property) and national security (e.g., attacks on the global financial system and national electric grid). As more and more of the U.S. economy and society move to the Internet through initiatives such as electronic medical records, telemedicine and "smart grids," the likelihood and severity of attacks in cyberspace will almost certainly increase.

In cyberspace, where the Internet provides global connectivity and access to a rich assortment of valuable assets of strategic importance, an enemy has the advantages of stealth, anonymity and unpredictability. The increasing levels of sophistication of computer-based attacks on civilian and military networks worldwide raise the cyber security bar each year, as does the exponential increase in information volume and the decrease of time-distance constraints.

Cyberspace is a domain, which has its own distinct features and challenges – just as the domains of

land, sea, air and space do. Industry, trade, finance, security, intellectual property, technology, culture, policy and diplomacy are some of the many areas in which the United States has become dependent on the cyber domain.

Cyberspace enables the creation, transmission, manipulation and utilization of digital information. Voice, video and data communications are transmitted through wired and wireless mediums to a range of connected devices that can include desktop and laptop computers, smart phones, mainframes, televisions, radios, SCADA (supervisory control and data acquisition) systems, sensor and navigation systems and communications satellites. Digitized content (e.g., television programs, music and books), digital devices and services, telecommunications and cable collectively form an increasingly interdependent and complex cyber domain that transcends traditional geographic boundaries.[1]

Fortunately, the United States and its allies are not standing still. Recent efforts to strengthen cyber security include the Comprehensive National Cybersecurity Initiative (CNCI), the appointment at the White House of a cyber security coordinator, and the establishment of U.S. Cyber Command. However, more sustained effort on several fronts is needed. First, the United States needs to work with its allies to develop a policy for cyberspace in the same manner as it developed norms, rules and standards for airspace and civilian aviation in the 1940s and 1950s. Second, the United States needs to craft a comprehensive cyber security strategy that links goals and objectives to budget and performance measures across the federal government to better integrate efforts and avoid duplicative investments. Third, the United States needs to streamline the interagency process and create a national cyber security center (modeled after similar efforts at the National Counterterrorism Center) that would serve as the "one stop shop" for cyber security operations both within the federal government and between government and the private sector, where the bulk of cyber assets are located and managed. This would improve information sharing and enhance the U.S. ability to respond to attacks with greater alacrity. Fourth, the United States needs a public-private research and development effort – modeled after SEMATECH[2] – to develop next generation cyber security technologies and ensure that the United States does not fall behind in this critical area. Lastly, the United States needs to rebuild the national human capital base in math, science, education and technology in areas like electrical engineering, computer science and cyber security.

This chapter is divided into four sections that outline cyber actors and their intentions; analyze the predominant vectors used to threaten the components of cyberspace; review the common targets; and assess the impacts produced by an attack.

Actors

The popular notion of threats to cyberspace still revolves around individual hackers seeking to prove their technical prowess, criminal elements whose goal is financial gain, or rogue agents who use cyber attacks to make a political statement. However, a wider range of actors can pose cyber threats, including nation-states, non-state actors, or a combination of both working together. Criminal networks, extremist groups, state-sponsored agents and nation-states now have the ability to conduct targeted and more sophisticated attacks.[3]

The United States' cyber adversaries share a common goal: to disrupt the nation's critical civilian and military infrastructures. Their motives may be distinct, but each uses the same vehicle – the cyber domain - as a vehicle through which to achieve exponential impact, including harming people and inflicting extensive economic damage. The main actors in cyberspace can be divided into three categories: states, organizations and individuals.[4]

STATES

States pose the most powerful and significant threats to cyberspace. These threats range from spreading disinformation to intelligence gathering to small- and large-scale attacks on critical infrastructures.

Roughly 140 countries were developing cyber weapons arsenals at the end of 2008. Within the next five years we will see countries and extremist groups jockeying for cyber supremacy.

Israel

The Israel Defense Forces (IDF) is reportedly honing its cyber warfare capabilities in preparation for future conflicts. According to one report, the IDF has already conducted a number of successful cyber warfare campaigns, including hacking into Syrian air-defense radars during an operation against the country's nascent nuclear weapons program.[5]

Press accounts of the 2006 Second Lebanon War suggest that Hezbollah hacked into Israeli communications systems. According to one report, Hezbollah members achieved "an unprecedented intelligence breakthrough that enabled them to thwart tank assaults by emplacing long-range armor-piercing munitions on pre-identified approach routes."[6] The Iranian Revolutionary Guard gave Hezbollah advanced frequency-hopping technology that enabled the group to track and analyze the IDF's radio communications. As a result, Hezbollah gained excellent situational awareness about Israel operations, tactics, and logistics. One former senior IDF official acknowledged that this capability had "disastrous" consequences for the offensive. The IDF has subsequently taken measures to improve operational security.[7]

Russia

Russia's cyber warfare doctrine uses offensive cyber weapons as a force multiplier, a military term that describes a weapon or tactic, which significantly increases combat potential when used alongside other military capabilities. Russia's cyber strategy emphasizes the ability to disrupt its adversaries' information infrastructure, military and civilian communications and critical infrastructure prior before traditional military operations commence.[8]

Russian cyber warfare doctrine states that all targets should be identified before an "information strike." Successful attacks should deny the enemy access to external information, disrupt credit and monetary circulation, and conduct psychological operations against the population – including disinformation and propaganda. Careful pre-strike planning and long-term investments in reconnaissance and covert penetration into enemy systems can help accomplish these objectives.

Perhaps the best known example of a Russian cyber operation occurred in Estonia in 2007, when an extensive DDoS attack severely disrupted many important websites, including those of parliament, newspapers and the central bank. Russia launched a similarly destructive attack against the Republic

Estonia 2007

Actor
Unknown, but the source is suspected to be either Russian government or an organized group of Russian individuals.

Vector
Multiple DDoS attacks.

Target
Estonian government, law enforcement, banking, media and Internet infrastructure. The attacks began on April 27 and continued for three weeks.

Impact
Estonia's two largest banks briefly lost all communications and international services were disrupted for days. Government communications were also disrupted.

of Georgia before their war in 2008.[9] States that feel threatened by Russia are prioritizing efforts to defend against such attacks.

China

China is currently building the technological capability to carry out a cyber attack anywhere in the world at any time. Nations around the world can no longer ignore the advanced threat China's cyber warfare capabilities present today and the one to which it aspires in the future.

China has significant cyber weapons and intelligence infrastructure in place today. As part of an integrated national plan, the People's Liberation Army (PLA), has adopted a formal cyber warfare doctrine and conducts cyber warfare exercised and simulations. One recent study concluded, "Beijing's intelligence services continue to collect science and technology information to support the government's goals, while Chinese industry gives priority to domestically manufactured products to meet its technology needs. The PLA maintains close ties with its Russian counterpart, but there is significant evidence that Beijing seeks to develop its own unique model for waging cyber warfare."[10]

China's cyber warfare doctrine seeks to attain global "electronic dominance" by 2050, which would include targeting its enemies' financial markets, military and civilian communications capabilities and critical infrastructure before traditional military operations begin. In 1999, the *PLA Daily* stated, "Internet warfare is of equal significance to land, sea and air power and requires its own military branch."[11]

The Chinese military is trying to coordinate cyber operations and kinetic strikes in order to disrupt an adversary's information and communications networks. Attacks on vital targets such as the enemy's computers, communications, command and control, intelligence, surveillance and reconnaissance (C4ISR), data nodes and networks would provide opportunities for exploiting enemy data and open an enemy's military to data exploitation and potentially crippling strikes.[12]

NON-STATE ORGANIZATIONS

Ideological or criminal non-state actors conduct cyber attacks to deny service or disrupt systems, but do not have the same capacities as large governments. In general, it is easy to mount low-cost DDoS attacks against low-value targets such as websites. Botnets of zombie computers are easy to infect, and websites are often vulnerable to such measures.

Sophisticated attacks against high-value targets such as defense communications systems require large intelligence agencies to intrude physically and crack highly encrypted codes. A teenage hacker, a group of criminals and a large government can all do considerable damage over the Internet, but they are not equally powerful in the cyber domain.

Organized criminal networks target both individuals and corporations in cyberspace. These attackers tend not to directly engage government entities and their operations in cyberspace.

Organized criminal networks typically target individual Americans in order to steal their identity. According to one estimate, cybercriminals create 57,000 fake websites each week that appear to be the websites of 375 high-profile brands, including eBay, Western Union, Visa, Amazon, Bank of America and PayPal.[13]

The greatest concern, however, comes from cyber criminals' data breaches and theft of intellectual property from corporations. The costs of cyber crime are hard to measure, but companies could be losing more than a trillion dollars a year.[14] Data breaches orchestrated by organized cyber criminals resulted in the loss of hundreds of millions of consumer records in 2008.[15]

According to one report, cyber criminal organizations "have taken on a Mafia-like structure that is a

According to one estimate, cybercriminals create 57,000 fake websites each week that appear to be the websites of 375 high-profile brands, including eBay, Western Union, Visa, Amazon, Bank of America and PayPal.

far cry from the early days of the lone-wolf hacker setting out to make a name for himself."[16]

Some criminal organizations are small and seek to profit quickly before they can be detected by governments and law enforcement. Others exist on a global scale and may receive protection from weak governments in exchange for bribes or other forms of payment. Black market forums such as Shadow Crew and DarkMarket have used underground economy computer servers for a variety of data brokering activities, including buying and selling stolen bank account details, government issued identity numbers, credit card details, personal identification numbers and email address lists. At its height, Darkmarket included more than 2500 global members who purchased and sold stolen passwords, credit cards and other financial information.[17]

Steven Chabinsky, deputy assistant director of the FBI's cyber division, recently identified ten different types of specialists involved in a typical cyber crime:

- Programmers who write malware and other codes needed to conduct the crime.
- Distributors or vendors who trade and sell stolen data.
- Technical experts who provide technical support.
- Hackers who identify and exploit vulnerabilities.
- Fraudsters who develop schemes like phishing and spamming.
- Hosters who provide safe and secure hosting.
- Cashers who control drop accounts and sell that information to other criminals.
- Money mules who are often controlled by cashers.
- Tellers who launder money.
- Organization leaders.[18]

INDIVIDUALS

Individuals who are potential cyber adversaries fall into four main groups: novices, hackers, hacktivists and cyber terrorists.

Novices

Novices possess limited programming skills. They conduct unsophisticated attacks using pre-written scripts called toolkits, such as NeoSploit, WebAttacker and IcePack. Novices usually seek adventure, thrills and acceptance into the hacker subculture. Their limited skills generally restrict the scope of their attacks. But as increasingly sophisticated toolkits are becoming available, their ability to conduct larger attacks is growing.[19]

Hackers

Hackers remotely access data, files and computer operating systems (usually without permission. The earliest hackers sought to learn more about how computers operated, not to conduct malicious activity. More recent hackers, however, deliberately seek to disrupt, damage, or disable computer networks through increasingly sophisticated and organized attacks.[20]

Hacktivists

Hacktivists are primarily motivated by a political cause rather than individual gain. They primarily conduct DDoS attacks, but they also use tools like

viruses and worms. Although they target specific organizations, these attacks can have broader consequences as well.[21] Perhaps the best-known recent example is the "Anonymous" group, which conducted a number of cyberattacks to protest the imprisonment of Private Bradley Manning, who allegedly gave classified material to WikiLeaks, and WikiLeaks founder Julian Assange.[22]

Cyber Terrorists

Cyber terrorists are similar to hacktivists in that their network intrusions are politically motivated, but the scope of their attacks is different. Unlike hacktivists, cyber terrorists seek to inflict damage to targets that are important to a society's economic and political functioning.

These groups may engage in state-sponsored cyber operations or facilitate organized criminal networks. They target the cyber assets and data of their adversaries. Cyber terrorists are usually very secretive, highly skilled, ideologically motivated, and well funded.[23]

The Internet has been described as a "virtual training camp" or "open university" for extremists. They can use it to gain new recruits (some of whom will be selected to attend physical training camps), and recruits can learn the skills needed to conduct terror attacks.[24]

Vectors

KINETIC

Threats to cyberspace can be kinetic (i.e. physical attacks). Kinetic attacks are instances of non-software-based attacks on targets critical to a state or organization's cyber networks.

Although most studies of threats to cyberspace focus on cyber attack vectors, physical attacks can profoundly impact cyberspace and should not be ignored.

A kinetic strike utilizes brute physical force against a chosen target using an explosive device, missile, bomb or even a blunt object to inflict severe damage or destroy the target that represents a critical node or component of a country or company's information, communications or command networks.

The successful Chinese anti-satellite missile test in 2007 is an example of this type of attack. The target in this incident was the FY-1C weather satellite. The test was carried out using an SC-19 ASAT missile with a kinetic kill warhead.[25] This incident demonstrated the impact a kinetic strike against a country's satellite communications network can have, causing international alarm, and prompting fears of an accelerated space arms race in Europe, the United States and Asia. This is critical to cyber security because the bulk of space-based assets either provides or transports information (e.g., global positioning satellites, communications satellites and reconnaissance satellites). As such, most satellites are simply cyber assets located in space.

Undersea Cable Cut, 2008

Actor
Iraqi-owned MV Hounslow and South Korean-owned MT Ann.

Vector
Anchors from the two ships were said to have caused Internet and telecommunications outages.

Target
SEA-ME-WE 4 and FLAG Telecom cables.

Impact
70 percent of Internet traffic in Egypt and 60 percent in India were reportedly disrupted. Problems also occurred in Afghanistan, Bahrain, Bangladesh, Kuwait, Maldives, Pakistan, Qatar, Saudi Arabia and United Arab Emirates.

GhostNet

Actor
GhostNet compromised proxy computers on Hainan Island. According to various reports, GhostNet is associated with the Chinese government.

Vector
GhostNet causes computers to download malware that allows attackers to gain complete control of a computer in real time.

Target and Impact
Up to 30 percent of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media and nongovernmental organizations.

The September 2007 Israeli air strike against a nuclear reactor target in Syria was reportedly accompanied by a simultaneous cyber attack against Syrian air defenses, which allowed Israeli aircraft to enter Syrian airspace without being detected. As one report noted, "More and more often, cyber attacks on government servers signal a physical attack in the offing."[26]

ELECTROMAGNETIC

Electromagnetic pulses (EMP) are large bursts of electricity in the atmosphere that can be caused by nuclear blasts or geomagnetic storms. Electromagnetic pulses can generate powerful ground currents that can cripple power lines and electrical grids across state lines.[27] They can also interfere with electrical systems. A strong EMP can physically destroy key computer components, including the motherboard.[28]

The United States and a few other countries have developed weapons that have the same effects as EMPs. Currently these weapons can operate effectively over distances as great as a kilometer, but they are not yet powerful enough to affect broad areas like a whole city.[29] However, nearly 30 countries (including North Korea) currently possess ballistic missile capabilities, which can create EMP effects.[30]

The Heritage Foundation identified several potential effects of an EMP-based attack on the cyber domain, including:

- Traffic lights would no longer function, so all roads would be gridlocked. The computer systems operating mass transit would be inoperative.
- After an EMP attack, transportation networks would grind to a halt and no food would be delivered.
- Satellites in low-earth orbit and many of the communication support systems would be disabled. Devices such as Blackberries and GPS would not work.
- Critical computers that direct the national electrical grid would be inoperative.[31]

CYBER

A majority of cyber threats are non-kinetic: malicious software programs, botnets and DDoS attacks. These forms of cyber attack also have transformed from the earliest days of cyber insecurity.

Malicious Software

Many industries and utilities use SCADA systems to control various processes. Cyber attackers could introduce malicious software into these systems and terminate any of these processes, which would have real physical consequences. A cyber attacker who disables the power grid in a cold-climate city during the winter, for example, can cause more damage than if he or she had conducted the attack with kinetic weapons. Generators would be able to provide some relief, but they would not be able to address the effects of a widespread regional blackout.[32]

The Conficker worm illustrates how sophisticated and resilient malicious software can be. It was introduced in November 2009 and rapidly spread around the world. Computer security experts soon created software that deleted the worm from millions of infected computers. Yet Conficker's authors continued to release new versions of the worm that included cutting-edge code. The attackers proved to be more agile than the security companies trying to counter the worm, which astounded many observers.[33]

Today, even novices can access free or low-cost toolkits that enable them to customize malicious computer code. According to Symantec, more than 90,000 different variants of the ZeuS toolkit existed during 2009 alone.[34]

Botnets

A botnet includes many compromised computers that are used to create and send spam or viruses, or inundate a network with messages in the form of a DDoS attack. There are several ways to gain access to the compromised devices. For instance, a hacker might exploit a security weakness in a Web browser, an Internet chat-relay program or the operating systems of the computers themselves. Upon gaining access, the hacker can run automated programs ("bots") on all the systems simultaneously.[35]

Botnets come in many shapes and sizes; they can involve a handful of computers or many thousands. While capable of inflicting the heaviest damage, the larger botnets are also the easiest to detect and destroy, as the enormous bandwidth they require may trigger an alert that leads one of more of the Internet Service Providers (ISPs) to the source.[36]

Distributed Denial-of-Service

Distributed denial-of-service attacks involve a hacker embedding malicious software on unsecured servers. The software allows an outside party to use the compromised servers to launch an overwhelming number of requests for a specific website. DDoS attacks make the target system inoperable, either by crashing it or making it so busy that it cannot operate normally. These operations can be used during military operations to flood networks, modify data, physically destroy hardware, or send electromagnetic pulses that interfere with signals and communications.[37]

During the 1999 Kosovo conflict, hackers tried to disrupt NATO military operations through hacking and achieved a few minor successes. Today, botnets that provide extensive DDoS capabilities are easily available and can be procured anonymously. Since defending against a DDoS attack is so difficult, attackers may conduct many diversionary attacks to distract from the main attacks. Identifying those responsible for DDoS attacks can be very challenging. Some investigations have lasted for years and yielded little progress.[38]

Hackers no longer simply scan cyberspace to find vulnerabilities. Instead, they have learned to create vulnerabilities in targets such as financial institutions, business competitors, political groups or hostile countries. Companies including Rolls-Royce, Royal Dutch Shell, Google and Adobe Systems have suffered from highly calculated and deliberate cyber attacks. In many cases, attackers seek to gain the intellectual property of companies, even when that information would only benefit a small number of the companies' competitors. Attackers are rarely punished because of difficulties in attributing and proving responsibility for their actions, as well as the reluctance of companies to publicly expose such breaches.[39]

Targets

Cyber attackers have expanded their targets beyond infrastructure to include assaults on applications as well. Web application attacks were responsible for 79 percent of records breached globally in 2009.[40] Yet a majority of spending in

cyber security is on infrastructure components, mostly because many companies lack the expertise to appreciate the reality of the problem. Companies that do want to focus on Web application attacks struggle to find people with the right skills to manage this risk.

According to McAfee, "Critical infrastructure owners and operators report that their networks and control systems are under repeated cyber attack, often from high-level adversaries like foreign nation-states."[41] Sixty percent of U.S. Internet technology and infrastructure executives surveyed for that report said that they expected to see a "major cyber incident" within two years.[42]

The targets of most interest to cyber adversaries comprise three groups:

- Federal – The White House, Congress, Department of Homeland Security and others are targeted because they symbolize our nation's domestic security.
- Military – The Pentagon and combatant commands are targeted to disrupt military operations such as in Iraq and Afghanistan.
- Civilian – Critical infrastructure (such as financial, power and telecommunications) is targeted because attacks can cause widespread damage and affect a large population.

Successful attacks on federal targets demonstrate adversaries' ability to exploit the vulnerabilities of those systems. To date, attackers have mainly targeted websites, which serve as the public face of the government. For example, on July 4, 2009, a series of coordinated cyber attacks was initiated against government, media and financial websites in both South Korea and the United States. Among the websites affected were the White House and the Pentagon. The perpetrators utilized a DDoS attack. The attacks themselves were relatively unsophisticated and deployed a botnet of roughly 50,000 to 65,000 computers, but because the attacks occurred in three distinct waves, each targeting different groups of websites, it is believed that this overall DDoS was launched as an organized and well-coordinated plan.[43]

Consequently, cyber attacks can compromise the functioning of critical infrastructures crucial to national security.[44] The U.S. government, for example, claims that, "The continued exploitation of information networks and the compromise of sensitive data, especially by nations, leave the United States vulnerable to the loss of economic competitiveness and the loss of the military's technological advantages."[45] So rather than existing as two distinguishable dimensions, economic well-being and national security are closely interconnected because critical information infrastructures are essential for both dimensions.

Impacts

A successful attack can have serious consequences for major economic and industrial sectors, infrastructure elements such as electrical power and the response and communication capabilities of first responders in crisis situations. The degrees of impact from cyber attacks range from network downtime of personal systems to life-threatening destruction of critical infrastructures.

Cyber attacks can have potentially enormous consequences. As one industry expert noted, "A security breach in the past meant that you had to respond quickly, keep law enforcement involved, deal with your affected customers, and ask their forgiveness. Today, a breach could mean that the engineering design you were betting your company's future on is in the hands of a competitor. A breach today could lead to the discovery of several other regulatory, legal, or policy violations, ultimately resulting in millions of dollars in fines and remediation costs."[46]

An attack on cyberspace can have profound impacts on multiple levels. This section will discuss

those impacts and use two case studies to highlight the critical nature of threats to cyberspace at different levels.

ORGANIZATIONAL EFFECTS

Cyber attacks at the organizational level range from operational disruptions and costs associated with recovering from an attack to serious economic damage in terms of lost revenue, fines and/or destruction of shareholder value.

For instance, on September 27, 2004, hackers compromised the computer systems of ChoicePoint Inc., one of the largest aggregators of U.S. consumers' personal and credit information. A security weakness in the ChoicePoint database enabled hackers to gain access to the personal information of over 163,000 ChoicePoint customers, leading to at least 5,000 cases of identity theft. However, ChoicePoint did not disclose the breach to the public until February 14, 2005 – more than four months later – when it sent letters of notifications to 35,000 Californians and 110,000 people across the country of an increased risk of identity theft.[47]

The Federal Trade Commission charged ChoicePoint with violating the Fair Credit Reporting Act by misrepresenting the security of their information database. ChoicePoint settled the case by paying 10 million dollars in civil penalties and 5 million dollars to customers whose identities had been stolen. The settlement also required ChoicePoint to conduct comprehensive background checks for every business requesting access to the database, to develop a stronger information security system and to hold annual audits of its systems (conducted by outside security professionals) until 2026.[48]

NATIONAL EFFECTS

National effects include those that transcend single organizations or localities whose effects are systemic and potentially catastrophic and includes most critical national infrastructure (e.g., energy, finance, transportation, etc). While no significant cyber attack on critical infrastructure has yet occurred, anecdotes provide evidence of the national effects that damages to infrastructure can have.

While it is true that 90 percent of cyberspace is in the private sector, securing cyberspace will require bipartisan leadership by the U.S. government, partnership with the private sector, and engagement with the American public.

One useful example is the blackout throughout the northeastern United States and southeastern Canada on August 14, 2003. A high-voltage power line in northern Ohio shut down after coming into contact with a tree. Usually this would have triggered an alarm, but a software bug (known as a race condition) in FirstEnergy's XA/21 SCADA caused the alarm system to fail. As a result, no one was alerted to the initial transmission line shutdown or the cascading system failures that occurred during the next two hours. The blackout killed 11 people and cost more than 6 billion dollars.[49]

The consequences of this monumental power failure demonstrate the interconnected nature of the nation's power grid and the inherent dangers it presents. One assessment of the damage reported that: "Sewage spilled into waterways. Train service in the Northeast Corridor, including those

provided by Amtrak, Long Island Railroad, and Metro-North, was shut down. Planes couldn't fly because passenger screening equipment was down, baggage couldn't be delivered, and electronic ticketing systems could not be accessed. Gas stations couldn't pump fuel. Oil refineries shut down. Cell phones and laptops quit working when their batteries ran out. Miners were marooned underground. The U.S./Canadian border shut down because of the lack of electronic border check systems. The backup diesel generator for the 1,900-room Marriott Hotel in New York wouldn't start even though it had been tested weekly. Guests had to walk down and sleep under the stars. It is thought that the Ontario government fell in October elections because of the blackout."[50]

Summary

The threat to cyberspace is real and will continue to grow as the world becomes more connected and as more critical functions (e.g., energy, health, transportation, commerce, etc.) migrate to digital platforms and networks. While it is true that 90 percent of cyberspace is in the private sector, securing cyberspace will require bipartisan leadership by the U.S. government, partnership with the private sector, and engagement with the American public. Specifically, this will require a clear cyber security policy to guide our international efforts; a comprehensive cyber security strategy to integrate the disparate efforts across the U.S. government; a streamlined and agile operating model that brings together the government and private sector to anticipate and respond to threats; a concerted and sustained R&D effort – again working with the private sector – to develop breakthrough cyber security technologies; and long-term investment in human capital. Cyberspace is critical to our economy, national security and society; our response must be commensurate with the challenge.

ENDNOTES

1. "Cyber 2020: Asserting Global Leadership in the Cyber Domain," Booz Allen Hamilton, Inc. (2010): 2, http://www.boozallen.com/media/file/cyber-vision-2020.pdf?utm_source=Twitter&utm_campaign=Cyber&utm_content=Cyber2020&utm_medium=bitly.

2. Semiconductor Manufacturing Technology, or SEMATECH, was a joint effort between the U.S. government and private industry to regain the manufacturing technology lead in semiconductors in the face of considerable Japanese dominance in this area in the 1980s.

3. Khalid Kark, "The New Threat Landscape: Proceed With Caution," Forrester Research for Security & Risk Professionals (13 August 2010): 2.

4. Joseph S. Nye, Jr., *The Future of Power* (New York: Public Affairs Press, 2011). See also Nye's chapter in this volume.

5. David Eshel, "Cyber-Attack Deploys in Israeli Forces," *Aviation Week* (15 September 2010), http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml.

6. "Arab and Israeli Cyber-War," *Day Press News* (22 September 2010), http://www.dp-news.com/pages/detail.aspx?l=2&articleid=55075.

7. Ibid.

8. Arie Schaap, "Cyber Warfare Operations: Development and Use under International Law," *Air Force Law Review* (Winter 2009): 133.

9. C. Myers, S. Powers and D. Faissol, "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches," Lawrence Livermore National Laboratory (April 2009): 10.

10. Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," Institute for Security Technology Studies at Dartmouth College (December 2004): 7-8.

11. Arie Schaap, "Cyber Warfare Operations: Development and Use under International Law," *Air Force Law Review* (Winter 2009): 132.

12. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corporation (9 October 2009): 6, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

13. "Cybercriminals Creating 57,000 Fake Websites every week," *Security Week* (9 September 2010), http://www.securityweek.com/cybercriminals-creating-57000-fake-web-sites-every-week.

14. Joseph S. Nye, Jr., "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010): 12.

15. Brian Krebs, "Organized Crime Behind Data Breaches," *The Washington Post* (15 April 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/04/15/AR2009041501196_3.html?sid=ST2009041501334.

16. Kenneth Corbin, "FBI Underboss Says Cyber Criminals the New Mafia," *eSecurity Planet* (23 March 2010), http://www.esecurityplanet.com/trends/article.php/3872326/FBI-Underboss-Says-Cyber-Criminals-the-New-Mafia.htm.

17. Joseph S. Nye, Jr., "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010): 12.

18. Steven R. Chabinsky, "The Cyber Threat: Who's Doing What to Whom?" GovSec/FOSE Conference (23 March 2010).

19. C. Myers, S. Powers and D. Faissol, "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches," Lawrence Livermore National Laboratory (April 2009): 7.

20. "Computer Hackers," World of Forensic Science, Enotes.com, http://www.enotes.com/forensic-science/computer-hackers.

21. C. Myers, S. Powers and D. Faissol, "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches," Lawrence Livermore National Laboratory (April 2009): 7.

22. See Volume I of this report.

23. C. Myers, S. Powers and D. Faissol, "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches," Lawrence Livermore National Laboratory (April 2009): 10.

24. Paul Cornish, Rex Hughes and David Livingstone, "Cyberspace and the National Security of the United Kingdom," Chatham House (March 2009): 6.

25. Shirley Kan, "China's Anti-Satellite Weapon Test," Congressional Research Service (23 April 2007): 1, http://www.fas.org/sgp/crs/row/RS22652.pdf.

26. Paul Cornish, Rex Hughes and David Livingstone, "Cyberspace and the National Security of the United Kingdom," Chatham House (March 2009): 4.

27. Dan Vergano, "One EMP Burst and the Whole World Goes Dark," *USA Today* (27 October 2010), http://www.usatoday.com/tech/science/2010-10-26-emp_N.htm.

28. C. Myers, S. Powers and D. Faissol, "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches," Lawrence Livermore National Laboratory (April 2009): 16.

29. Scott Stewart and Nate Hughes, "Electromagnetic Pulse Attack Debated – But Looms as a Real Threat," The Cutting Edge (13 September 2010).

30. Jean Baker McNeill and James Carafano, "Time for an EMP Recognition Day," The Heritage Foundation (23 March 2010), http://www.heritage.org/research/reports/2010/03/time-for-an-emp-recognition-day.

31. Ibid.

32. Joseph S. Nye, Jr., "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010): 6.

33. Khalid Kark, "The New Threat Landscape: Proceed With Caution," Forrester Research for Security & Risk Professionals (13 August 2010): 3.

34. Ibid.

35. The Tech Terms Computer Dictionary, "Botnet," http://www.techterms.com/definition/botnet.

36. Ibid.

37. Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Information Security Journal: A Global Perspective* 18 (2009): 4.

38. Ibid.

39. Khalid Kark, "The New Threat Landscape: Proceed With Caution," Forrester Research for Security & Risk Professionals (13 August 2010): 2-3.

40. "2009 Data Breach Investigations Report," Verizon Business (2009), http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

41. Stewart Baker, Shaun Waterman and George Ivanov, "In the Crossfire: Critical Infrastructure in the Age of Cyber War," McAfee (2009): 3.

42. Ibid.: 11.

43. "Governments Hit by Cyber Attack," BBC News (8 July 2009), http://news.bbc.co.uk/2/hi/technology/8139821.stm.

44. The White House, "Cyberspace Policy Review" (2009): 2; Estonian Ministry of Defense, "Cyber Security Strategy" (2008): 10; and NATO Parliamentary Assembly, "NATO and Cyber Defence" (2009).

45. "The White House, "Cyberspace Policy Review" (2009): 1.

46. Khalid Kark, "The New Threat Landscape: Proceed With Caution," Forrester Research for Security & Risk Professionals (13 August 2010): 3.

47. Quinn Bailey and Benjamin Gilfillan, "ChoicePoint: Personal Data and a Loss of Privacy (A)," Eugene D. Fanning Center for Business Communication, Mendoza College of Business, University of Notre Dame, 06-7 (2006): 1; and Joshua Pantesco, "FTC imposes record fine on ChoicePoint in data-loss case," Paper Chase (26 January 2006), http://jurist.org/paperchase/2006/01/ftc-imposes-record-fine-on-choicepoint.php.

48. Ibid.

49. JR Minkel, "The 2003 Northeast Blackout—Five Years Later," *The Scientific American* (13 August 2008): 1, http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later; and "The Great 2003 Northeast Blackout and the $6 Billion Software Bug," The Availability Digest (March 2007): 2-4, http://www.availabilitydigest.com/private/0203/northeast_blackout.pdf.

50. JR Minkel, "The 2003 Northeast Blackout – Five Years Later," *The Scientific American* (13 August 2008): 4, http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

America's Cyber Future

Security and Prosperity in the Information Age

CHAPTER III:

SEPARATING THREAT FROM THE HYPE: WHAT WASHINGTON NEEDS TO KNOW ABOUT CYBER SECURITY

By Gary McGraw and Nathaniel Fick

America's Cyber Future

Security and Prosperity in the Information Age

SEPARATING THREAT FROM THE HYPE: WHAT WASHINGTON NEEDS TO KNOW ABOUT CYBER SECURITY

By Gary McGraw and Nathaniel Fick

Washington has become transfixed by cyber security and with good reason. Cyber threats cost Americans billions of dollars each year and put U.S. troops at risk.[1] Yet, too much of the discussion about cyber security is ill informed, and even sophisticated policymakers struggle to sort hype from reality. As a result, Washington focuses on many of the wrong things. Offense overshadows defense. National security concerns dominate the discussion even though most costs of insecurity are borne by civilians. Meanwhile, effective but technical measures like security engineering and building secure software are overlooked.

The conceptual conflation of cyber war, cyber espionage and cyber crime into a monolithic and dangerous "cyber menace" perpetuates fear, uncertainty and doubt. This has made the already gaping policy vacuum on cyber security more obvious than ever before. But as Washington grapples with the challenge of cyber security, the risks – which range from failing to act, to acting poorly to overreacting – are real and have far-ranging consequences.

When it comes to cyber security, it is hard even for experts to understand what is real and what is a cyber chimera. How much of what we are hearing about cyber war is driven by hype? How much of it is something that we need to worry about, and who should do the worrying? More to the point, if the hype and fear engines ran out of fuel for a day, leaving only even-handed and well-reasoned analysis, how would we describe the current situation and begin to create an approach for improvement? Our aim in this chapter is to help policymakers find their way through the fog and set guidelines to protect the best of the Internet and cyberspace, both from those who seek to harm it, and from those who seek to protect it but risk doing more harm than good.

Cyber Hype and Cyber Reality

Any discussion of cyber security must begin by separating hype from reality. It is true that cyber war, cyber espionage and cyber crime all share the same root cause – dependence on insecure cyber systems. The bad news about U.S. cyber dependency is that cyber war appears to be dominating the conversation among policymakers even though cyber crime is a much larger and more pervasive problem. When pundits and policymakers focus only on the dangers of cyber war, the most pressing threats emanating from cyber espionage and cyber crime are relegated to the background.

WHAT IS CYBER WAR?

Whether online, on television or in print, hyperbolic discussion of cyber war has become widespread. The most hyped of these "cyber war" stories are worth reviewing:

- Hyped Story #1 – In 2007, a number of distributed denial-of-service (DDoS) attacks, in which many coordinated computers overwhelm a target computer with messages and thereby block legitimate traffic, were directed against Estonia. This happened during a political dust-up with Russia over the removal of a statue. While the complexity of modern conflict makes it difficult to draw perfect distinctions, the DDoS attack against Estonia had no warlike impact. Most importantly, the technical sophistication of the attacks was very low. In 2009, similar cyber attacks targeted the Republic of Georgia during the Russian armed invasion. However, from a technical standpoint, attacks like these would fail utterly if launched against popular U.S. e-commerce websites such as Amazon or Google, possibly to the point of not even being noticed.[2]
- Hyped Story #2 – In 2009, CBS aired a segment on its show *60 Minutes* that attributed several blackouts in Brazil to unidentified cyber attackers. Brazil's top cyber security officer denied the allegations.[3] A few days after the show aired, a major blackout in Brazil prompted renewed speculation of cyber attacks. The subsequent discovery of some very minor implementation bugs involving databases in the power company's website provided feeble evidence in support of the claim.[4] Nonetheless, speculation about a cyber attack surged. Ultimately, an investigation revealed the blackout was the much more pedestrian result of a combination of operational and procedural failures from one electric power supplier company.[5]
- Hyped Story #3 – In 2010, a mistake made when managing one of the protocols at the heart of the Internet called Border Gateway Protocol (BGP) was incorrectly characterized as a malicious "hijacking" of 15 percent of U.S.-based Internet traffic by Chinese attackers.[6] The mistake led to a temporary and short-lived diversion of traffic on some segments of the Internet through servers in China. Much of the spin characterized the mistake, which is unfortunately very easy to make due to the poor design of BGP, as an intentional and malicious act. Though the actual traffic numbers in question were inflated, even members of the U.S. Congress appear to have regarded this incident as a deliberately orchestrated cyber attack.[7]

It is a bad idea to intermingle hyped stories such as these with more severe attacks. Doing so obscures understanding of the seriousness of cyber warfare and its implications. Though computer geeks and policy wonks must work together to solve cyber security problems, continuing to use a loose definition of cyber war risks alienating experts who see through computer security jargon and hype. Distributed denial-of-service attacks with no physical impact should not be used as an example of cyber war. Doing so will only widen the chasm between computer security specialists and Washington decision makers.[8]

Compounding the misinformation spread by these kinds of stories is the lack of a clear definition of cyber war. Definitions vary widely. The "war" part is relatively straightforward: Violent conflict between groups for political, economic or philosophical reasons. The less straightforward part is determining whether an action with no real world impact constitutes cyber war. For example, is simply taking down a website or infecting a computer with a malicious virus an act of cyber war? Although sometimes framed as such, this definition seems far too sweeping.

When pundits and policymakers focus only on the dangers of cyber war, the most pressing threats emanating from cyber espionage and cyber crime are relegated to the background.

Cyber war requires a consequential impact in the physical world, or what military experts call a "kinetic" (or physical) impact. Infecting an adversary's command and control system with malicious software yielding the attacker complete control, thereby allowing the attacker to command the adversary's Predator drones to shoot at the wrong targets would, for example, count as an act of cyber war. In the end, war is the application of force to achieve a desired end. Or, as Prussian military theorist Carl von Clausewitz famously put it, war is the continuation of politics by other means. To qualify as cyber war, the means may be virtual, but the impact should be real.

To be sure, some cyber attacks do transcend the confines of cyberspace and qualify as cyber war. In their recent book, *Cyber War*, Richard Clarke and Robert Knake include a number of case studies that illustrate the notion of kinetic impact.[9] Perhaps the most interesting example involves Israeli cyber war maneuvers during the bombing of a suspected Syrian nuclear facility in 2007.[10] Syria's formidable air defense system could not track inbound Israeli fighter jets because it was taken over by Israeli cyber warriors who incapacitated or otherwise blinded it before the raid. This meets the definition of cyber war; the tie to a kinetic impact is clear – a completely destroyed Syrian facility.

There are a number of additional examples of real cyber attacks going back decades that are worth mentioning. In 1982, Canadian computer code, modified by the CIA before it was stolen by the Soviets, caused a Soviet gas pipeline to explode. Last year and perhaps earlier, the Stuxnet worm was used to attack uranium enrichment facilities in Iran. While analysis of Stuxnet continues to this day, it appears to be a real offensive cyber weapon with a clear kinetic impact, namely, non-functioning centrifuges.[11] Stuxnet is a fascinating study in the future of malicious software or "malware." Not only did its delivery vehicle reveal at least four previously unknown exploits in Microsoft software, its payload clearly demonstrated that systems of the sort that control power plants and safety-critical industrial processes are rife with vulnerabilities.[12]

Another real and serious instance of a cyber attack occurred in 2008, when a USB drive in the Middle East was used to infect U.S. Department of Defense command and control systems, prompting Deputy Secretary of Defense William Lynn to write in *Foreign Affairs*, "This previously classified incident was the most significant breach of U.S. military computers ever, and it served as an important wake-up call."[13] However, the impact of this attack appears to have remained limited to cyberspace.

War has both defensive and offensive aspects, and understanding this fundamental dynamic is central to understanding cyber war. Overconcentrating on offense can be very dangerous and destabilizing as it encourages actors to attack first and ferociously, before an adversary can since no effective defense is available. On the other hand, when defenses are equal or even superior to offensive forces, actors have less incentive to strike first because the expected advantages of doing so are far less. The United States is supposedly very good at cyber offense today, but from a cyber defense perspective it lives in the same glass houses as everyone else. The root of the problem is that the systems we depend on – the lifeblood of the modern world – are not built to be secure.

This notion of offense and defense in cyber security is worth teasing out now and returning to later. In our view, *offense* involves exploiting systems, penetrating systems with cyber attacks and generally leveraging broken software to compromise entire systems and systems of systems.[14] On the other hand, *defense* means building secure software, designing and engineering systems to be secure in the first place and creating incentives and rewards for systems that are built to be secure.[15]

Unlike physical reality, cyberspace has a completely different makeup that affects the mix of offense and defense. It is impossible to "take and hold" cyberspace, to invoke a term traditionally used in military operations. Cyberspace more closely resembles the naval or space domains where powerful countries are able to monitor, patrol, exert influence and deter aggression, but they do not exercise control in the way it is traditionally conceived of during ground conflicts. Cyber sharpshooters cannot control a section of cyberspace and should not be asked to do so.

Indeed, cyberspace is a dynamic system in constant motion where clocks run at superhuman tempo close to the speed of light. Time and space are different in cyberspace. There is no "there" there, and humans are intolerably slow.

There is also no isolated battlefield on the Internet. In the case of cyber war, the battlefield will, by necessity, involve civilian systems of every stripe.

In the final analysis, the threat of cyber war is real but overstated. Even acts amounting to cyber war have thus far never led to military conflict in the real world.

WHAT IS CYBER ESPIONAGE?

Cyber espionage is another prominent cyber security problem that captivates the imagination. Cyber espionage is much more common than cyber war. The highly distributed, massively interconnected nature of modern information systems makes keeping secrets difficult. When almost one million U.S. citizens have security clearances and information system managers are told that "connecting the dots" should be their top method for stopping terrorism, it should come as little surprise that classified information often leaks. It is easier than ever before to transfer, store and hide information. A pen drive the size of a little finger can store more information than the super computers of a decade ago.

WikiLeaks is not an anomaly. That is, the WikiLeaks commotion that grabbed headlines is not just the result of a lone information terrorist; it also resulted from flawed policy on the part of the U.S. government. Other than perhaps some minor deterrent effects, prosecuting the leadership of WikiLeaks does absolutely nothing to fix the root cause of cyber espionage. The better solution is reasonable information system policy and proper technology enforcement, including the proper engineering of systems so that they are secure.

Civilian and corporate espionage is also a factor in cyber security. Look no further than the so-called "Operation Aurora" attacks by Chinese hackers against technology companies such as Google.

Laissez-faire information stances combined with overly lax cyber security policy means that cyber espionage and intellectual property infringement are easier to pull off than they should be. The target environment is ripe for the picking, and the Aurora episode, in which the Chinese spirited away vast quantities of intellectual property, is something to expect more of and to prepare for now.

Why did Willie Sutton, the notorious Depression-era gangster, rob banks? As he famously (and perhaps apocryphally) put it, "That's where the money is." Criminals flock to the Internet for the same reason.

Unfortunately, the theft of intellectual property and company secrets appears not to be alarming enough for some who hype cyber threats. Some of the most shrill hypemongers misconstrue espionage as war, in effect arguing, "We may call it espionage, but it's really warfare because they're planting logic bombs," while offering little actual evidence of such activity.

WHY NOT CYBER CRIME?

Among the three major cyber security concerns in the public eye, cyber crime is far more pervasive than cyber war and cyber espionage, yet is the least commonly discussed. By every measure and according to every public report, cyber crime is growing and already commonplace. Indeed, 285 million digital records were breached in 2008 alone, with 79 percent of those breaches resulting from attacks against programs that run on the Web through Internet browsers.[16] Cyber crime and data loss are estimated to cost the global economy at least 1 trillion dollars each year.[17] Perhaps because it is so common, cyber crime is easy to overlook. The fact is, as consumers flock to the Internet, so do criminals. Why did Willie Sutton, the notorious Depression-era gangster, rob banks? As he famously (and perhaps apocryphally) put it, "That's where the money is." Criminals flock to the Internet for the same reason.

It is abundantly clear to most computer security professionals that cyber crime is a major and very real concern that needs to be addressed. Cyber crime is orders of magnitude more prevalent than cyber war and cyber espionage.

Interestingly, building systems properly from a security perspective will address the cyber crime problem just as well as it will address cyber espionage and cyber war. We can kill all three birds with one stone.

Washington's Distorted Focus

Because of the hype surrounding cyber war, Washington's focus has become distorted. Developing offensive capabilities has taken precedence over strengthening cyber defenses. Meanwhile, concern about military vulnerabilities and the concentration of resources there has led the national security establishment to dominate cyber security policy.

CYBER DEFENSES IGNORED

For years, computer security professionals have been attempting to protect systems riddled with security defects from potential attackers by placing a barrier between the broken stuff and the bad people. That is what firewalls are all about. But this endeavor has failed. Instead of continuing to sink resources into this flawed approach, we need to fix the broken stuff so that attacking it successfully takes far more resources and skill than is currently the case.[18] Concentrating on

the improving offensive cyber capabilities simply will not alleviate dependence on vulnerable cyber systems. Concentrating on improving defense through proper engineering is a much better route.

The United States has reportedly developed formidable cyber offenses. Yet America's cyber defenses remain weak. What passes for cyber defense today – actively watching for intrusions, blocking attacks with network technologies such as firewalls, law enforcement activities and protecting against malicious software with anti-virus technology – is little more than a cardboard shield.

It is much catchier to talk about cyber offense and its impacts than to focus on defense and building things right in the first place.

What we identify as "the NASCAR effect" applies, causing shortsighted pundits to focus on offense, which is sexy, to the detriment of defense, which is engineering.[19] Nobody watches NASCAR racing to see cars driving around in circles. They watch for the crashes. People prefer to see, film and talk about crashes more than building safer cars. There is a reason why there is no Volvo car safety channel on television even when there are so many NASCAR channels.

This same phenomenon happens in cyber security. In our experience, people would rather talk about cyber war, software exploit, digital catastrophe and shadowy cyber warriors than talk about security engineering, proper coding, protecting supply chains and building security in.[20] It is much catchier to talk about cyber offense and its impacts than to focus on defense and building things right in the first place.

Simply put, America has neglected its cyber defenses because strengthening them is a painstaking and unglamorous task. Because of the NASCAR effect, emphasizing cyber offense attracts more attention and funding than a more prosaic focus on defense and building security into software at the outset. Ultimately, a balanced approach to cyber security requires offense and defense in more equal measures.

NATIONAL SECURITY DOMINATES CYBER SECURITY

Thus far, the national security establishment has taken the lead on cyber security. The Pentagon established U.S. Cyber Command in 2009 to defend military networks against hacker attacks and consolidate cyber capabilities and personnel under a single authority.[21] To the extent that Cyber Command focuses on defense, so far it has been more reactive than proactive, concentrating on how to protect networks that are already vulnerable and seeking out malware already propagating on the network. Cyber Command also appears to be developing an impressive array of offensive capabilities, though these remain highly classified and the subject of media speculation.

Meanwhile, the civilian networks that account for at least 90 percent of America's cyber exposure go largely unappreciated. No agency inside the U.S. government has line responsibility for securing them. Insofar as civilian networks receive any attention from policymakers, the focus, once again, is on reacting rather than on building in security from the beginning.

Discussions outside government tend to underscore that cyber security is chiefly the purview of the national security establishment. The media emphasizes the U.S. defense industry, the U.S. intelligence community and the burgeoning cyber

security industry. What the civilian high-technology sector and civilian agencies within the U.S. government can contribute to cyber security goes overlooked.

The real and perceived dominance of the U.S. national security establishment in setting cyber security policy is problematic in several respects. First, cyber security is neither solely nor primarily a military problem but rather a confluence of economic, cultural, diplomatic and social issues. Ignoring these dimensions and devoting singular focus to the military aspects of cyber security – the inevitable result of putting national security agencies in the lead – will result in a flawed approach.

Second, cyber security is a global problem. The Internet recognizes no geographical boundaries and does not follow the contours of national borders. This point is particularly salient when we consider a few facts: fewer than 15 percent of Internet users are American citizens; a large portion of the U.S. information technology and security workforce is composed of foreign nationals; and the supply chain for the global information technology market is not actually a chain but rather a complicated web involving many non-American actors. National security agencies within the U.S. government are ill-suited for managing such a domain by themselves. Indeed, their dominance of cyber security policy will render cooperation with international actors more difficult.

Toward a Balanced Cyber Security Policy

The United States needs a more balanced cyber security policy. Such an approach should include the following:

Focus on defense by building security in. A good offense is not a good defense. Instead a good defense is the best defense. A proper cyber defense involves building security into systems from the outset. The United States should invest greater resources in software security and solid security engineering. The U.S. government has an integral role to play in building more secure systems. Specifically, it should develop incentives for companies to engineer security into software rather than rely on endless patches after vulnerabilities become apparent. The U.S. government should consider granting tax credits to companies that develop more secure software. It should also publicize security failures to boost the situational awareness of companies and individual consumers.

There are literally thousands of ways in which better security engineering can help mitigate cyber risk. Border Gateway Protocol, one of the building block protocols of the Internet, is deeply broken and needs to be fixed. The vulnerabilities inherent to BGP illustrate our view that improved defenses through better security engineering is essential to attaining cyber security and keeping the cyber peace. If BGP were better designed, it would be more difficult to exploit and more difficult to mismanage accidentally.

People know how to build secure software. The commercial world, led by independent software vendors (think Microsoft, SAP, Adobe and Intuit) and financial services companies (think Bank of America, Wells Fargo and Goldman Sachs), has made great strides in software security over the last decade. The Building Security In Maturity Model (BSIMM) is designed to help understand, measure and plan a software security initiative.[22] The BSIMM carefully describes the work of 33 firms – all household names – responsible for building a majority of software in common use today.[23] The BSIMM was created by observing and analyzing real-world data and is designed to help a firm (or government agency) determine how its organization compares to other real-world software security initiatives and what steps can be taken to make its approach more effective. The most important use of the BSIMM is as a measuring stick to determine where a particular approach to software security currently stands relative to others.

Unfortunately, the U.S. government is drastically behind in software security. Not even the most advanced government agencies or contractors are ready for participation in the BSIMM project – mostly because there is nothing to measure.

Building more secure software is an important option because it kills three birds with one stone. Building security in will not only deter cyber crime and cyber espionage but it will also keep the cyber peace. Working to promote software security and security engineering is a considerably more viable response to cyber threat than blithely developing new offensive capabilities. In fact, shiny new cyber weaponry can be repurposed for crime and espionage – reason enough to pause before investing too much in offense.

Throwing a better, more accurate rock in a glass house is still throwing a rock. U. S. systems are so permeated with problems that even a relative amateur can exploit them – as a quick trip to the Black Hat hacker conference will show. To stretch the analogy a bit, if a cyber peashooter in the hands of a teenager is sufficient to wreak havoc on today's vulnerable systems, why bother to even work on a cyber rock?

Reorient Public-Private Partnerships. As it turns out, security is only partially a game of operations centers, information sharing and reacting when the flawed systems get exploited. (This is the cardboard shield defense.) Similarly, a focus on forensics assumes that an exploit has already happened and there is a mess to clean up.

Unfortunately, today's public-private partnerships focus overwhelmingly on information sharing and reacting collectively to cyber threats. There is nothing wrong with this approach, but it does little to help create fundamentally more secure systems. Public-private partnership discussions should be reoriented toward software security and building on the collective wisdom of many (as the BSIMM project does).

Focus on Information Users Instead of Plumbing. Civilian, government and military systems are deeply entangled. As the WikiLeaks episode demonstrates in no uncertain terms, the nature of the entanglement is the people who interact with the systems, not the technology, sets of wires or physical infrastructure. Although the U.S. government adopted some new security measures after WikiLeaks, there are still hundreds of thousands of users of classified government networks who also use the open Internet and carry around pen drives. Just as military and civilian social groups mix in complex and unpredictable ways in the physical world, so too do the information systems that these people use. The notion of building a "walled garden" to protect critical systems or classified information is thus misguided.

Instead of trying to construct new networks that exist in isolation, the U.S. government would do better to focus on the users. Thinking about who should access what information, when, where and why, and how much information should be accessed at once, are far superior to trying (and failing) to wall things off artificially.

Of course, the military has already attempted to separate certain networks with the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet), systems of interconnected computer networks used to transmit classified information securely. The proposed "dot secure" network, which U.S. government officials have floated as a separate, secure computer network to protect civilian government agencies and critical industries, is basically the same notion, but intended to be used by critical infrastructure providers. However, there is an essential difference in purpose that we must point out.

The secret networks are for protecting state secrets, whereas "dot secure" is meant to protect against active attack. The current design of the SIPRNet and

JWICS allows information to transfer from low-to-high (from the open Internet "up" to SIPRNet, for example). Because of this feature – a feature that is accounts for most of the utility of the secret networks – the secret networks are susceptible to a malicious code infection that rides its way "up" on data. Deputy Secretary of Defense William Lynn's *Foreign Affairs* article shows that not only is this possible, but it has actually happened. The problem that this raises has everything to do with the different purpose that "dot secure" is intended for. A command and control system meant to stay up during an active attack has a completely different threat model and risk profile than a network to store and manipulate secrets.

Any Internet pundit familiar with Facebook knows that the value of a network is directly proportional to the number of people connected to it. By imposing limitations and constraints on a network, one degrades its value and utility. Make a network useless enough and users will go elsewhere or, worse yet, they will hack their way around security controls.[24]

Even if substantial taxpayer money and collective expertise is dedicated to the task of building better, more secure systems, successful attacks are still inevitable. Cyber security policy should be assume that risk cannot be completely avoided and systems must continue to function even in suboptimal conditions.

Let civilian agencies lead. The American government should not allow the National Security Agency (NSA) or another part of the intelligence community to dominate U.S. cyber security policy, for two reasons. The first has to do with separation of duties. Spycraft is facilitated by vulnerabilities in software that can be exploited in order to turn electronic devices into eavesdropping platforms. Consequently, an agency charged with spycraft understandably has mixed incentives to promote better software security.

The balance that the United States struck during the Cold War on nuclear policy may prove instructive here. Duties were separated between the Department of Energy – charged with building nuclear weapons – and the Department of Defense – charged with delivering them. This division has endured until today, and suggests that civilian agencies should take the lead on building cyber defenses while the national security establishment should focus on military dimensions.

An additional reason the intelligence community should not dominate cyber security is that important cultural differences exist between the national security community and the rest of civilian government and corporate America. There is a clearer command and control structure within the former than within the latter two. Though some ambiguity persists within the national security community, it is clearer who has to do what, and where the chain of command goes next. The same sort of clarity does not exist elsewhere. Put more colloquially, what seems to work for the NSA is very unlikely to work for Duke Energy, JP Morgan Chase or Microsoft.

Conclusion

In our view, cyber security policy must focus on solving the software security problem – fixing the broken stuff. We must refocus our energy on fixing the glass house problem instead of on building faster, more accurate rocks to throw. We must identify, understand and mitigate computer-related risks.[25] We must begin to solve the software security problem.

To date, when it comes to software, newly-minted Apple Chief Information Security Officer David Rice said it best in his book *Geekonomics*, "Unfortunately, the blunders of government are matched almost equally by the blunders of the market itself, if not more."[26] We believe that the government can and should play a role in building more secure systems. The U.S. government should

develop incentives for vendors to build security in and break the endless loop of feature creep and bloatware. The government should publicize security failures so that we know what is really happening and we can learn from our mistakes. Perhaps the government should even grant tax credits for creating better, more secure software.

Equally important is what the government should not do. The government should not legislate cyber security excessively. The U.S. Computer Fraud and Abuse Act has done little to deter the explosive growth of cyber crime. Frankly, the target-rich environment filled with broken software makes it far too easy and too tempting to misbehave criminally. The government should not pretend that its buying power can single-handedly move the software market. It cannot. The government should not build any more overly bureaucratic taxonomies for security evaluation such as the Common Criteria or the Trusted Computer System Evaluation Criteria (TCSEC), a Pentagon standard that sets basic requirements for assessing a computer system's security control effectiveness. The market does not care.

When bits are money, the invisible hand will move to protect the bits. Of course, the invisible hand must be guided by the sentient mind and slapped hard to correct the grab reflex if and when it occurs. There is an active role for government in all of this, not just through regulation, but also through monitoring and enforcing due process and providing the right incentives and disincentives. In the end, somebody must pay for broken security and somebody must reward good security. Only then will things start to improve. Washington can and should play an important role in this process.

ENDNOTES

1. President Obama addressed cyber risk in an important address on cyber security and the national infrastructure. President Barack Obama, "Remarks By The President on Securing Our Nation's Cyber Infrastructure" (29 May 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

2. That standard issue distributed denial-of-service attacks are considered a bad joke among those in the technical know does little to frame or even inform the seriousness with which politicians approach the issue.

3. Brian Krebs, "Brazilian Govt: Soot, not hackers, caused '07 blackouts," *The Washington Post* (11 November 2009).

4. That is, injection bugs in Structured Query Language (SQL), a computer database language.

5. Agencia Nacional De Energia Eletrica, "Monitoring of the Blackout on November 10th, 2009" (26 March 2010), http://www.aneel.gov.br/aplicacoes/noticias_area/dsp_detalheNoticia.cfm?idNoticia=3338&idAreaNoticia=347.

6. For one of the worst offenders, see "Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic," *National Defense* (12 November 2010), http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249.

7. For the real numbers, see Craig Labovitz, "China Hijacks 15 Percent of Internet Traffic?" *Arbor Networks Security* (19 November 2010), http://asert.arbornetworks.com/2010/11/china-hijacks-15-of-internet-traffic/.

8. When pressed on the issue of mixing hyped stories with more severe attacks, Richard Clarke responds that he merely wants to put all the data on the table and let people decide for themselves. Gary McGraw discusses that point with Richard Clarke on *Silver Bullet Security Podcast* episode 50, http://www.cigital.com/silverbullet/show-050/.

9. Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco, 2010).

10. Uzi Mahnaimi, Sarah Baxter and Michael Sheridan, "Israelis 'blew apart Syrian nuclear cache,'" *The Sunday Times* (London) (16 September 2007).

11. Gary McGraw, "How to p0wn a Control System with Stuxnet," *informIT* (23 September 2010), http://www.informit.com/articles/article.aspx?p=1636983.

12. For more on Stuxnet, listen to Gary McGraw interviewing Ralph Langner on *Silver Bullet Security Podcast* episode 59, http://www.cigital.com/silverbullet/show-059/. Note that there are millions of control systems currently vulnerable to Stuxnet-like attacks spread throughout the industrialized world.

13. William Lynn, "Defending a New Domain," *Foreign Affairs* (September/October 2010).

14. Greg Hoglund and Gary McGraw, *Exploiting Software* (Reading, MA: Addison-Wesley Professional, 2004).

15. Gary McGraw, *Software Security* (Reading, MA: Addison-Wesley Professional, 2006).

16. Verizon Business RISK Team, *2009 Data Breach Investigations Report*, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

17. David DeWalt, "Unsecured Economies – A Trillion Dollar Headwind," *McAfee Blog Central* (29 January 2009).

18. Ross Anderson, *Security Engineerin*g, 2nd ed. (Hoboken, NJ: Wiley, 2008).

19. Gary McGraw, "If You Build It, They'll Crash It," *Dark Reading* (7 July 2006), http://www.darkreading.com/security/application-security/208803559/index.html.

20. Note that software security is a relatively recent field in computer security with the first book published a little less than a decade ago. See John Viega and Gary McGraw, *Building Secure Software* (Reading, MA: Addison-Wesley Professional, 2001).

21. Siobhan Gorman and Yochi Dreazen, "Military Command is Created For Cyber Security," *The Wall Street Journal* (24 June 2009).

22. The Building Security In Maturity Model itself is available for free under the creative commons at http://bsimm.com.

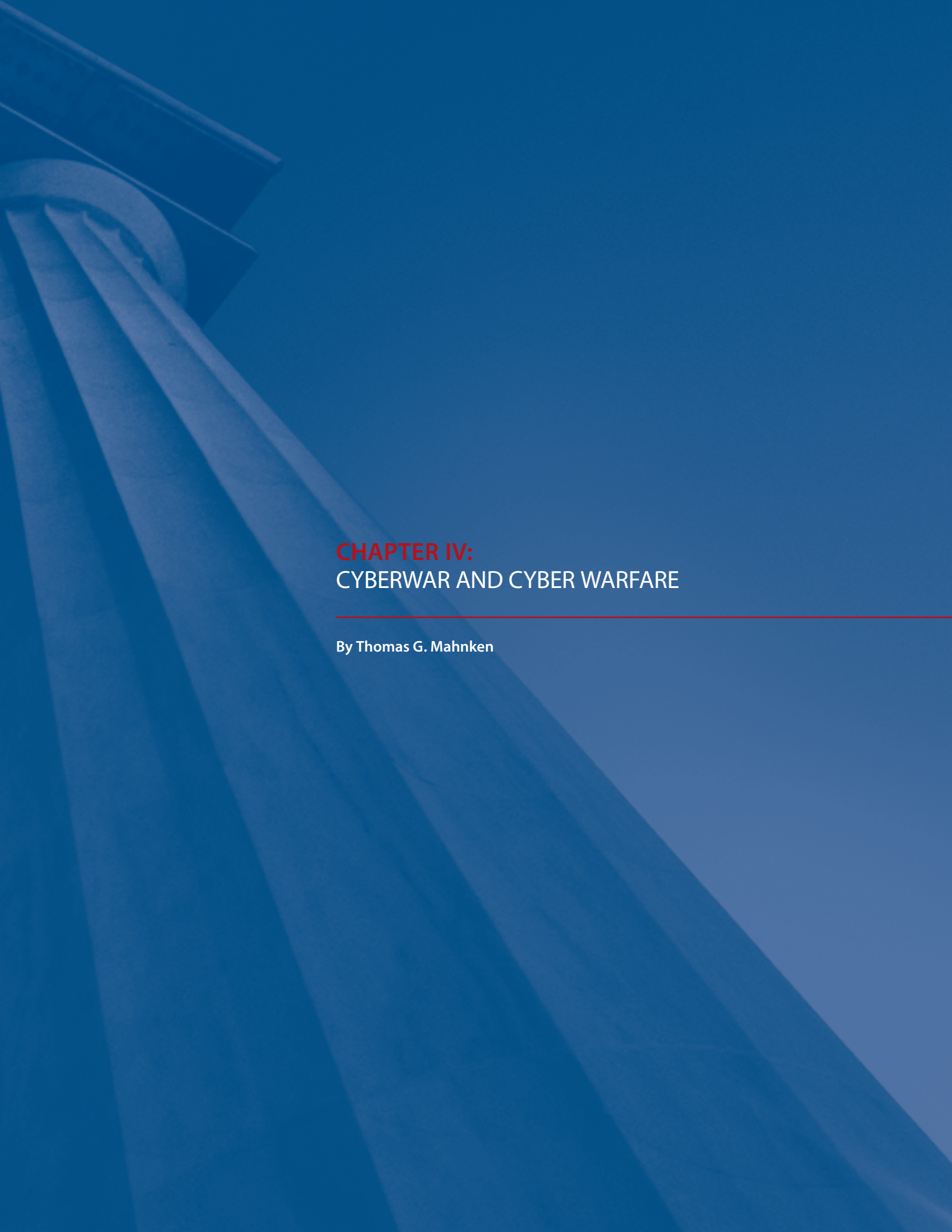
23. Building Security In Maturity Model (BSIMM) companies who graciously agreed to be identified include: Adobe, Aon, Bank of America, Capital One, The Depository Trust & Clearing Corporation (DTCC), EMC, Google, Intel, Intuit, McKesson, Microsoft, Nokia, QUALCOMM, Sallie Mae, SAP, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, VMware and Wells Fargo.

24. For real-world examples of this phenomenon, see Gary McGraw and Jim Routh, "Lifestyle Hackers," *CSO Online* (2 November 2009), http://www.csoonline.com/article/506309/lifestyle-hackers.

25. Peter Neumann, *Computer Related Risks* (Reading, MA: Addison-Wesley Professional, 1994).

26. David Rice, *Geekonomics: The Real Cost of Insecure Software* (Reading, MA: Addison-Wesley Professional, 2007): 286.

Acknowledgment: Portions of this article are based on an earlier work by Gary McGraw and Ivan Arce, "Cyber Warmongering and Influence Peddling," *informIT* (24 November 2010).



CHAPTER IV:
CYBERWAR AND CYBER WARFARE

By Thomas G. Mahnken

America's Cyber Future

Security and Prosperity in the Information Age

CYBER WAR AND CYBER WARFARE

By Thomas G. Mahnken

Although the history of the use of information as an instrument of war and statecraft is quite long, the idea of waging non-violent warfare against an adversary's information networks and infrastructure is relatively new.[1] Still, for nearly two decades now, military affairs experts have discussed and debated the prospective use of the cyber instrument of warfare. Prior to the September 11, 2001 terrorist attacks, a number of analysts and policymakers viewed the prospect of a cyber attack on U.S. infrastructure as one of the most significant contingencies facing the United States. Similarly, both scholars and soldiers have argued that cyber warfare offers a promising strategic option for the United States.[2]

Discussions of the strategic use of the cyber instrument of warfare have tended toward the simplistic or the alarming. Former National Security Council staffer Richard Clarke, for example, has argued that what states "are capable of doing in a cyber war could devastate a modern nation."[3] Former Director of National Intelligence ADM Mike McConnell has argued, "The cyber war mirrors the nuclear challenge in terms of the potential economic and psychological effects."[4] However, what has been lacking is an understanding of the circumstances under which the cyber instrument of warfare is likely to prove important or even decisive. This paper is an attempt to address that shortfall.

Despite sweeping pronouncements, the use of cyber means to achieve political aims remains an abstract and underdeveloped topic. In fact, cyber means can be put to a variety of uses. At the highest level, the cyber instrument is a tool of national power, akin to political warfare. As the introduction of the Stuxnet virus into Iran's nuclear infrastructure demonstrates, cyber means can also be used as a tool of covert action. Cyber means have also been used for espionage. China, for example, has reportedly conducted extensive spying against U.S. government agencies, including the Office of the Secretary of Defense, National

Defense University and Naval War College.[5] It has also used cyber means to infiltrate Tibetan nationalist groups.[6]

Although cyber means can be used for a variety of purposes, this paper confines itself to use in war. This is not to say that other cyber activities, such as espionage and crime, are not important. Indeed, they may be the most important venues of cyber activity. However, the topic of the use of cyber means in warfare is both distinct and important enough to demand individual attention. Specifically, this chapter explores both the independent use of the cyber instrument of warfare, which I term "cyber war," as well as the use of the cyber instrument as a dimension of a larger military conflict, which I term "cyber warfare."[7]

To date, cyber warfare has consisted of a tool that has been used in support of other military operations, as Russia did in its 2008 war with Georgia, or to achieve a modest political outcome, as Russia sought in intimidating Estonia in 2007. There are a few key questions strategists and policymakers must contemplate: First, is this experience indicative of future possibilities? Second, does the potential exist for cyber means to be used to achieve more decisive outcomes in conjunction with other military instruments? Finally, can cyber means achieve such outcomes independently? Fortunately, strategic theory, particularly insights into the enduring nature of war contained in the writings of Carl von Clausewitz and Sun Tzu, offers a lens through which we can assess the prospective effectiveness of cyber war and cyber warfare. Indeed, the theory of war is as valuable for understanding cyber power as it is for every other military instrument. The basic nature of war has survived numerous changes in its character due to the advent of new instruments of warfare. Just as it had with nuclear weapons, it is my assumption that it will survive the advent of cyber conflict. Were it not so, we would be left adrift when trying to forecast future events.[8]

This chapter attempts to describe the circumstances under which a state or non-state actor may be able to use cyber means – either independently, or in combination with other military instruments – to compel an adversary. This essay is, of necessity, speculative, and its tone is skeptical but not dismissive. It begins with a discussion of the enduring nature of warfare as well as an assessment of the strategic effects of the cyber instrument of warfare. It goes on to explore the utility of cyber war and cyber warfare across three dimensions:

- The power relationship between the belligerents.
- Their aims.
- The value that they attach to achieving those aims.

Its conclusions counter much of the received wisdom about cyber war and cyber warfare. Specifically, it argues that the cyber instrument of war is most likely to be effective in wars pitting the strong against the weak, fought for limited aims, and to gain something that the target of a cyber attack does not hold dear. Whereas cyber war is unlikely to be decisive, cyber warfare in support of other military instruments is likely to be an increasingly prevalent form of combat.

Understanding Cyber Warfare

Strategic thought regarding cyber power is noticeable by its paucity. This is understandable, given the unique features of the cyber realm as well as the fact that there has yet to be a cyber war. Because the world has yet to witness cyber war, and the cases of cyber warfare are few and indeterminate, analysts have tended to reason by analogy. In particular, cyber enthusiasts have drawn analogies between cyber war and other forms of "strategic" warfare, in particular strategic air bombardment and nuclear warfare. As Jean-Loup Samaan has pointed out, however, these analogies are inapt at best, misleading at worst.[9] It is, for example, difficult to imagine a situation in which cyber war could cause the level

of devastation that either conventional or nuclear bombardment can. On the night of March 9, 1945, for example, bombers from GEN Curtis LeMay's 21st Bomber Command dropped 1,665 tons of incendiary bombs on Tokyo, killing 80,000 Japanese people, damaging 250,000 buildings and destroying 22 major industrial facilities.[10] Five months later, an atomic bomb killed 40,000 and destroyed half of the city of Hiroshima in a matter of seconds.[11] It is inconceivable that cyber means alone could inflict similar damage over a comparable span of time.

In order to assess the prospective effectiveness of cyber war and cyber warfare, it is first necessary to define the context in which it would be used: that is, war. As Colin Gray has observed, "Even if cyber combat has some stand-alone qualities, still it must occur in the political and strategic context of warfare."[12] In Clausewitz's famous formulation, "War is thus an act of force to compel our enemy to do our will."[13] Three aspects of this definition are notable. First, the fact that war involves force separates it from other types of political, economic and military competition. War involves, or at least has involved, violence, bloodshed and killing. Second, the fact that war is not senseless slaughter, but rather an instrument that is used to achieve a political purpose, differentiates it from other types of violence, such as criminal activity. Third, war is interactive. It is not the use of force against an inanimate object, but rather against an organization that possesses its own values and objectives and responds to attack with reciprocal action.

Some have argued that Clausewitz's identification of war with violence is outdated. Rather, they argue, the advent of cyber war may permit the achievement of Sun Tzu's ideal in warfare: "To subdue the enemy without fighting."[14] Phillip Meilinger, for example, has termed cyber attack "A…bloodless yet potentially devastating new method of warfare."[15] The first adjective is true by definition; the second, however, is eminently contestable.

History is not on the side of those who herald the advent of bloodless battles. History contains far more instances of politicians and soldiers seeking quick victories over their adversaries than actual cases of decisive battles. This is particularly true in a war against a determined opponent who is fighting for something he holds dear. As Clausewitz cautioned:

> Kind-hearted people might of course think that there was some ingenious way to disarm or defeat an enemy without too much bloodshed, and might imagine this is the true goal of the art of war. Pleasant as it sounds, it is a fallacy that must be exposed: war is such a dangerous business that the mistakes which come from kindness are the very worst.[16]

The serious student of military history must look long and hard to find cases where one belligerent defeated another in a dispute over serious matters without resorting to the use of force. Perhaps the only modern example is the 1954 Guatemalan coup, which saw the government of Jacobo Árbenz Guzmán relinquish power in the face of what it believed was a massive uprising. In fact, the insurgency (Operation PBSUCCESS) was largely the creation of the Central Intelligence Agency and the insurgent army tiny. By contrast, even though the Cold War did not see large-scale combat between the United States and Soviet Union, it nevertheless was a war in the classic, Clausewitzian sense of the word. The U.S.-Soviet competition spawned wars, including those in Korea and Vietnam, which cost millions of lives. Moreover, we now know that American and Soviet pilots faced each other in combat in the skies over Korea and Vietnam, as well as in the airspace adjacent to the Soviet Union. Between 1950 and 1959, for example, the Air Force and Navy lost at least 16 aircraft with 164 crewmen killed on reconnaissance missions against the Soviet Union.[17] I am therefore skeptical that cyber warfare will usher in an era of bloodless victories.

The cyber instrument may have its own grammar, but its logic is that of war as a whole. In other words the cyber instrument is, like land, sea and air power, a means to achieve a political aim. Moreover, different military instruments are capable of producing different strategic effects that circumscribe their utility. For example, ground forces are not only able to inflict damage on an adversary's military, but also to seize and hold territory. Naval forces are able to control, or deny an adversary control of, the seas; to project power overseas; and to attack commerce. Air forces are capable of supporting ground and naval operations as well as inflicting damage upon an adversary independently.

The cyber instrument of warfare has a number of unique attributes. Unlike other military instruments, for example, its effects can be both instant and global. In addition, cyber means are available both to state and non-state actors. As a relatively new military instrument, it is also surrounded by a great deal of uncertainty. Attributing cyber actions to actors may be difficult, though this difficulty is likely to be less in wartime than in peacetime. Finally, the novelty of cyber conflict makes it unclear what actions may constitute an act of war and which actions may lead to escalation.

Cyber warfare can be thought of as producing two strategic effects: punishment and denial. Of these, the former, the ability to inflict punishment, is likely to be far less significant. The cyber instrument's power to inflict punishment on an adversary is but a fraction of that of other instruments of warfare. Cyber attacks do not produce any direct lethal effects and have a limited ability to inflict damage more broadly. Even in the case of attacks on a state's economic infrastructure, it is doubtful that a cyber attack would be capable of producing more damage than a strategic air campaign. Other military means are far better at killing people and inflicting damage than cyber attacks. The cyber instrument's limited ability to cause direct damage, in turn, means that it will possess a constrained ability to compel an adversary. It may equally be ignored or lead to escalation. Also, because cyber war has yet to be demonstrated, the prospect of a cyber attack is unlikely to provide an effective deterrent.

It is possible to imagine cyber attacks exposing American forces to attack by an adversary's land, sea or air units. It is this role, with cyber means being used to enhance the effectiveness of other military instruments, that holds the greatest promise.

It is denial, rather than punishment, that represents the comparative advantage of cyber warfare. Unlike other instruments of war, cyber offers the ability to block the adversary from using information systems and networks. This is a significant capability, one that could have a considerable effect on military operations. It is possible, for example, to imagine an adversary using cyber means to disrupt U.S. command and logistical networks in order to delay an American response to an act of aggression. It is also possible to imagine cyber attacks exposing American forces to attack by an adversary's land, sea or air units. It is this role, with cyber means being used to enhance the effectiveness of other military instruments, that holds the greatest promise.

War is a diverse phenomenon. First, wars are fought by a broad spectrum of actors, ranging from

non-state actors such as insurgents and terrorist groups to states of different sizes and capabilities. Second, actors wage war to achieve a variety of objectives, from compelling their adversary to cease objectionable behavior, to the seizure of territory and resources, to the overthrow of their foe. Third, belligerents place different values upon achieving their objectives. In some cases, wars are, or are seen to be, existential struggles. In other cases, they involve secondary interests. By exploring these dimensions of warfare, we can assess the circumstances under which cyber war and cyber warfare may prove effective.

Actors

A number of authors have argued that cyber war is a weapon that favors the weak against the strong. They characterize the cost of achieving a cyber capability as relatively low, well within the reach of a sophisticated non-state actor or a small power. They also argue that advanced states such as the United States are highly vulnerable to attacks on their information networks and infrastructure because they are more reliant on those systems than less advanced states and non-state actors.

It is true that a growing number of actors – both state and non-state – are likely to be able to develop cyber means of warfare. They may also be tempted to use cyber means against their stronger adversaries, particularly given the confusion over what constitutes an act of war in cyberspace. However, cyber means cannot compensate for weakness in other instruments of power. In other words, if a cyber attack by a weaker power on a stronger one fails to achieve its aim, the attacker is likely to face retaliation. In such a situation, the stronger power will possess more, and more lethal, options to retaliate. The stronger belligerent possesses, in nuclear deterrence terminology, escalation dominance. The weaker power might be able to cause a stronger power some annoyance through cyber attack, but in seeking to compel an adversary through cyber war, it would run the very real risk of devastating retaliation. Moreover, that response need not be confined to the cyber realm; it could include kinetic strikes.

In addition to escalation dominance, stronger powers, particularly stronger states, are likely to possess a greater ability to combine cyber means with other military instruments to conduct a combined-arms campaign: that is, to wage cyber warfare. As a result, it may very well be that although weak powers may attempt to wage cyber war, they are likely to face cyber warfare wielded by the strong.

Aims

A second way to assess the prospects of cyber war and cyber warfare is by examining the aims for which they cyber instrument might be used. Wars can be fought for a wide range of objectives, from the quest for land and resources to the utter destruction of the enemy. In a note for the revision of his book *On War*, Clausewitz drew a distinction between wars fought for limited aims and those fought for unlimited aims. As he wrote:

> War can be of two kinds, in the sense that either the objective is to *overthrow the enemy* – to render him politically helpless or militarily impotent, thus forcing him to sign whatever peace we please; or *merely to occupy some of his frontier-districts* so that we can annex them or use them for bargaining at the peace negotiations. Transitions from one type to the other will of course recur in my treatment; but the fact that the aims of the two types are quite different must be clear at all times, and their points of irreconcilability brought out.[18]

This distinction affects the way that wars are fought and how they end. In wars for limited aims, soldiers and statesmen must translate battlefield success into political leverage over the adversary. As a result, they must continually reassess how far to go militarily and what to demand politically. Such wars end through formal or tacit negotiation and agreement between

the warring parties. Wars for unlimited aims are fought to overthrow the adversary's regime or achieve unconditional surrender. They end in a peace settlement that is imposed rather than negotiated.[19]

Cyber advocates have failed to offer a theory of victory for cyber war, a chain of causal logic linking the use of cyber means to the achievement of political ends. It is unclear, for example, how a state or non-state actor could use a cyber attack upon a nation's financial system to achieve a political aim. Despite the apocalyptic language that frequently accompanies discussions of cyber war, it is hard to conceive of it leading to the achievement of unlimited aims: that is, to the overthrow of a government. Indeed, it is unclear whether cyber means alone would be sufficient to achieve even more limited aims. One coerces an adversary by raising the cost of resistance beyond that which he is willing to pay. Moreover, such a calculation is prospective rather than retrospective. History has shown that the loser in war concedes not because of the damage that he has sustained, but rather because of the damage he may sustain in the future.[20] That is, a leader capitulates when he believes that things will get worse – for him, his government or his country – if he does not. However, the limited ability of the cyber instrument to inflict costs upon an adversary translates into a limited ability to coerce.

Of course, when paired with other military instruments, cyber means may enhance the ability to achieve either limited or unlimited aims. As Colin Gray has noted, because all warfare is about shaping or overcoming the will of the adversary, at a minimum future warfare will be waged both on land and in cyberspace.[21]

Value of the Object

A final way to assess the prospects of strategic cyber warfare is through an understanding of the value that belligerents place on achieving their objectives. The outcome of war depends not only on the aims of the two sides, but also the value they attach to them. One of Clausewitz's key insights is the notion that there should be a correlation between the value a state attaches to its ends and the means it uses to achieve them. As he wrote:

> Since war is not an act of senseless passion but is controlled by its political object, the value of this object must determine the sacrifices to be made for it in *magnitude* and also in *duration*. Once the expenditure of effort exceeds the value of the political object, the object must be renounced and peace must follow.[22]

States should thus be willing to fight longer and harder to secure or defend vital interests than peripheral ones. It helps explain, for example, why the U.S. government chose to withdraw from Somalia after the death of 18 soldiers in a single battle but remained in Korea despite suffering 33,000 deaths over three years.

The notion of a rational calculus of war would appear to be one area in which strategy most resembles a science. However, although the notion makes sense in theory, it is far more problematic to apply in practice. It is often difficult, for example, for decision makers to determine the costs and benefits of military action beforehand. Furthermore, estimates of the political, social and economic costs change as war unfolds. As Clausewitz notes, "the original political objects can greatly alter during the course of the war and many finally change entirely *since they are influenced by events and their probable consequence*."[23] States may continue fighting beyond the "rational" point of surrender when their leaders' prestige becomes invested in the war or the passions of the people become aroused. Alternatively, heavy losses may lead to escalation of a conflict, changing its character.

One would thus expect cyber means to be most effective in trying to achieve an objective that the adversary does not value highly. By contrast, one would expect an adversary to be unimpressed with

by a cyber attack aimed at something that he holds dear. Indeed, in such a situation the object of attack could see the use of cyber rather than kinetic means as a sign of weakness. Moreover, such an attack would raise the very real prospect of escalation. As Lawrence Freedman has written, "Even if a successful strategic information campaign could be designed and mounted, there could be no guarantee that a victim would respond in kind, rather than with whatever means happened to be available."[24]

Conclusion

Considerable uncertainty surrounds the strategic impact of the cyber instrument of warfare. In overestimating the prospective impact of cyber war, we run the risk of self-deterrence, much as the British government during the second half of the 1930s deterred itself from taking action against Hitler because it believed a strategic air campaign would have horrific results.[25]

Groups that seek to use cyber war and cyber warfare face the challenge of trying to predict how an adversary will respond. As Clausewitz notes, in contemplating the use of force, the commander must essentially guess:

> Guess whether the first shock of battle will steel the enemy's resolve and stiffen his resistance, or whether, like a Bologna flask, it will shatter as soon as its surface is scratched; guess the extent of debilitation and paralysis that the drying up of particular sources of supply and the severing of certain lines of communication will cause the enemy; guess whether the burning pain of the injury he has been dealt will make the enemy collapse or, like a wounded bull, arouse his rage; guess whether the other powers will be frightened or indignant, and whether and which political alliances will be dissolved or formed.[26]

Neither cyber war, nor cyber warfare alone, is likely to deliver victory or defeat in future conflicts. However, the cyber instrument of warfare is likely to play an increasingly important role as an enabler of lethal forms of warfare. The cyber instrument of war is most likely to be effective when wielded by the strong against the weak in wars for limited aims. By recognizing what cyber means can – and cannot – do, we can better prepare ourselves for a more realistic range of scenarios.

ENDNOTES

1. Emily O. Goldman, "Introduction: Information Resources and Military Performance," *Journal of Strategic Studies* Vol. 27, No. 2 (2004): 195-219.

2. John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy,* Vol. 12, No. 2 (Spring 1993): 141-165.

3. Richard Clarke and Robert Knake, *Cyberwar: The Next Threat to National Security and What to Do About it* (New York: HarperCollins, 2010): 31.

4. Mike McConnell, "How to Win the Cyberwar We're Losing," *The Washington Post* (28 February 2010).

5. Timothy L. Thomas, "Google Confronts China's 'Three Warfares'," *Parameters* (Summer 2010).

6. "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor* (Toronto: Munk Center for International Studies, 2009); Shishir Nagaraja and Ross Anderson, *The Snooping Dragon: Social-Malware Surveillance of the Tibetan Movement*, Technical Report 746 (Cambridge: University of Cambridge Computer Laboratory, 2009).

7. Colin S. Gray, *Another Bloody Century* (London: Weidenfeld & Nicolson, 2005): 319.

8. Those who argue that the emergence of cyber means of warfare presage a fundamental transformation of warfare are welcome to put forward an alternative framework providing greater explanatory power.

9. Jean-Loup Samaan, "Cyber Command: The Rift in U.S. Military Cyber-Strategy," *RUSI Journal* Vol. 155, No. 6 (December 2010): 16-21.

10. Williamson Murray and Allan R. Millett, *A War to be Won: Fighting the Second World War* (Cambridge: Harvard University Press, 2000): 506-507.

11. Richard Overy, *Why the Allies Won* (New York: Norton, 1995): 127.

12. Colin S. Gray, *Another Bloody Century* (London: Weidenfeld & Nicolson, 2005): 293-294.

13. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989): 75. Original in italics.

14. Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (Oxford: Oxford University Press, 1963): 77.

15. Col Phillip S. Meilinger, USAF (Ret.), "The Mutable Nature of War," *Air and Space Power Journal* (Winter 2010): 26.

16. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989): 75.

17. William E. Burrows, *By Any Means Necessary: America's Secret Air War in the Cold War* (New York: Farrar, Straus and Giroux, 2001).

18. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989): 69. Emphasis in the original.

19. The 1991 Gulf War and 2003 Iraq War illustrate the difference between the two types of wars. In 1991, the U.S.-led coalition fought to liberate Kuwait from Iraqi occupation, restore Kuwait's government to power, ensure the safety of U.S. citizens in the region and ensure the security and stability of the gulf region. In 2003, the United States and its allies fought to overthrow Saddam Hussein's Ba'athist regime.

20. Robert McQuie, "Battle Outcomes: Casualty Rates as a Measure of Defeat," *Army* (December 1987): 30-34.

21. Colin S. Gray, *Another Bloody Century* (London: Weidenfeld & Nicolson, 2005): 327.

22. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989): 92. Emphasis in the original.

23. Ibid. Emphasis in the original.

24. Lawrence Freedman, *The Revolution in Strategic Affairs* (London: International Institute for Strategic Studies, 1998): 57.

25. Wesley K. Wark, *The Ultimate Enemy: British Intelligence and Nazi Germany, 1933-1939* (Ithaca, NY: Cornell University Press, 1985).

26. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989): 572-573.

CHAPTER V:
NON-STATE ACTORS AND CYBER CONFLICT

By Gregory J. Rattray and Jason Healey

America's Cyber Future

Security and Prosperity in the Information Age

NON-STATE ACTORS AND CYBER CONFLICT

By Gregory J. Rattray and Jason Healey

Conflict in cyberspace engages a wider range of actors and activities than conflict in other environments or domains. Though consideration of cyber conflict at the political level often focuses solely on governmental actors,[1] this chapter outlines how conflicts in cyberspace are dominated by the actions of non-state actors. Early attention has focused on the malicious intent and capability of hackers or cyber criminals, with little analysis on the potential for non-state attackers to achieve significant, even strategic, effects. Even more importantly, non-state actors play a fundamental role in cyber defense at all levels and we suggest ways they can nurture collaboration and defensive capability. As the United States considers its own role in achieving national security objectives in the cyber domain, the fundamental role of non-state actors must remain at the forefront.

The other domains of land, sea, air and space are generally dominated by empty "space." The broad ocean, airspace and outer space are wide-open domains where conflict is dominated by high-tech forces with a high degree of freedom of action. Land combat often occurs in relatively open spaces but increasingly involves situations where civilians are at risk, especially in urban environments. However, non-state actors are generally non-combatants and seek to flee any fighting, even in urban areas.[2]

In cyberspace, there is no analogous empty "space" and the activities of civil and military users are intertwined together. Non-state actors cannot flee the domain since cyberspace is composed of technologies, software and hardware overwhelmingly created, owned and operated by non-state commercial actors with their own capital and for their own reasons.[3] Global fiber optic networks, tier I Internet service providers[4] (ISPs) and large commercial web hosting companies will be the battlespace for many or most conflicts, and they cannot evacuate the battlefield except by unplugging and dismantling part of cyberspace itself. Crucially, the actions of

the United States and other governments in cyberspace will largely depend on systems and networks owned and operated by private sector actors.

To address the challenges and opportunities presented by the dominance of non-state activity in cyber conflict, it is essential to approach the cyber domain as an ecosystem of competing and collaborating actors. Each actor seeks a wide range of interdependent objectives within a global commons. In order to continue reaping the benefits of a vibrant, globally interconnected cyber ecosystem, the United States needs to improve its ability to control malicious non-state actors. This requires collaborating with the appropriate non-state actors to improve the health and resilience of this ecosystem. Effective policy approaches also must address problems such as insecure systems that facilitate the spread of malicious software.

This chapter will discuss the roles that non-state actors play in cyber conflicts. We examine the roles that they have played in past conflicts: Non-state actors have taken offensive action in cyber conflicts but they have also played defense, improving the overall cyber ecosystem. We also examine several approaches that can be used to identify opportunities to defeat or remove non-state actors who choose to attack, while empowering those who choose to defend. These approaches include traditional ones, like crime and warfare, as well as new approaches, like public health and environmentalism. These approaches are not mutually exclusive, but each highlights different aspects of the problem. Taken together, they can help identify promising policy mechanisms and operational capabilities that the United States can use to achieve its cyber security objectives.

The Roles of Non-State Actors

Non-state actors[5] wield more influence and pose greater national security risks in the cyber domain than in other domains for many reasons, starting with low barriers to entry.[6] Technical tools that enable both malicious and benevolent actions can be downloaded or captured on the Internet. Software can be adapted to malicious purposes with the proper expertise – and that expertise is generally available for hire. However, the low barriers of entry should not be overblown. Though even advanced capabilities can be obtained, it is difficult for non-state actors to master other tasks – such as gathering intelligence and analyzing centers of gravity for attack and defense – that are likely needed to have lasting strategic effects. In cyber conflict, it is easier to attack than to defend due to many factors, including the relatively low cost of sophisticated attack tools and the weaknesses in operating systems and networks that create large numbers of significant, vulnerable targets.[7] Moreover, stopping attacks even from small groups often requires coordinated actions by defenders in both state and non-state organizations who may have little trust and few incentives to cooperate.

Cyber attack capabilities are also useful to malicious non-state actors pursuing diverse motives because they can be modulated to achieve a wide range of effects quickly, including worldwide Internet disruptions, quiet theft of industrial secrets or mass theft and sale of personal information. Furthermore, even though cyberspace is not as borderless as is often assumed,[8] the ever-increasing degree of connectivity and speed of access and transmission worldwide certainly challenges traditional concepts of national sovereignty, making it more difficult to attribute cyber attacks and investigate and prosecute cyber crime.

Non-state actors – with their own benevolent or malicious intent and capability – may engage in different roles in cyberspace. They may be thought of as forming interconnected webs – an ecosystem – just as these actors' internetworked devices form another ecosystem, and the interconnected chips and components inside those devices yet one more. As other recent works[9] have discussed those

technical ecosystems, we will focus on the ecosystem of non-state actors, including the following:

- **User:** The actor uses cyberspace for legal or illegal purposes to gain information, communicate with others or procure goods and services. Users may range from individuals, to educational institutions, to large, global enterprises such as FedEx or Sony.
- **Attacker:** The actor intentionally initiates malicious activity against other actors in the ecosystem. "Attacks" may not always mean disruptive activities, but can also include subtler actions such as intruding into computers to steal data.
- **Target:** The actor is the object of intentional malicious activity by other actors in the cyber ecosystem.
- **Unwitting Host:** The actor has computers that have been compromised without his or her knowledge and used by attackers against targets.
- **Responder:** The actor helps to identify, understand and/or respond to malicious activity against other actors (such as Computer Security and Incident Response Teams [CSIRTs][10] or McAfee).
- **Provider:** The actor provides secure information technology and/or services that are kept secure through periodic updates (such as Microsoft, Cisco, AT&T or Google).
- **Improver:** The actor helps to improve the health and resilience of the cyber ecosystem against malicious activity or other failures (such as helping to engineer a stronger Internet), or educates other actors on these issues.

A given actor may have many roles. For example, Microsoft, Google or Nokia might play several roles at any one time, including user, target, source of the malicious activity, responder or improver. Even an individual with a home computer may act as user, target and source of malicious activity. Government activities may also span all roles. In general, the more organized and well funded an actor is, the more capable it will be on either offense or defense.

Table 1 depicts the wide range of roles that individual actors can play in cyberspace (from individual citizens at the top to national governments at the bottom).[11]

The Evolution of Non-State Involvement in Cyber Conflict

Non-state actors have conducted significant intrusions and malicious activity of national significance for decades. The 1988 Morris Worm was released by a young man (the son of a senior researcher at the U.S. National Security Agency) who wanted to demonstrate security vulnerabilities and accidentally took down thousands of computers instead.[12] Around the same time, Cliff Stoll – an astronomer turned system administrator at Lawrence Berkeley National Laboratory – was working with technical and law enforcement partners worldwide to find a German hacker who sold information to the Soviet KGB.[13] During the run up to the 1991 Gulf War, Dutch hackers intruded into dozens of U.S. Department of Defense (DOD) computer systems, searching for any information on nuclear weapons or Operation Desert Shield.[14] In 1994, Russian hacker Vladimir Levin was able to steal 10 million dollars from Citibank.[15] Intrusions suspected to come from Saddam Hussein's Iraq in 1998 turned out to be California teenagers with an Israeli mentor.[16] In 2000, a major virus called "ILOVEYOU" affected perhaps one-tenth of all computers connected to the Internet and caused billions of dollars in damage – and had been created by a lone Filipino youth.[17] That same year, a disgruntled Australian used his privileged systems access to a former employer's sewage control system to release 800,000 liters of raw sewage.[18]

These early intrusions tended to be individuals working alone or in small groups, and were more about teenage curiosity or hooliganism than about

TABLE 1: THE PREDOMINANT ROLES OF MAJOR ACTORS IN THE CYBERSPACE ECOSYSTEM

Protective roles are colored green and marked with an "O," while malicious roles are colored red with an "X."

MAJOR ACTOR	USER	ATTACKER	TARGET	SOURCE	RESPONDER	PROVIDER	IMPROVER
Individuals	O		X	X			
Individual Hackers	X	X					
Hacker Groups	X	X					
Hacktivists	X	X					
Volunteer Security Groups	O				O	O	O
Non-governmental Organizations	O		X	X			
Universities	O		X	X	O	O	O
Internet Companies and Carriers	O	?	X		O		O
Critical Infrastructure Companies	O	?	X	X	O		
Security Companies	O	?	X	X	O	O	O
Other Companies	O	X	X	X		O	
Terrorists	X	X					
Massed Patriot Hackers	X	X					
Organized Criminal Groups	X	X					
International Organizations	O		X		O		O
Nation States	O	X	X	X	O	O	O

warfare (although some did have specific criminal or political roots). Since then, the intent of malicious actors has shifted. For example, individuals in many countries have formed nationalistic groups to respond with malicious cyber activity to perceived slights. Some of these first "patriotic hackers" were Chinese hackers responding to the accidental bombing of the Chinese embassy in Belgrade in 1999 and a collision between Chinese and U.S. military aircraft in 2001. The earliest patriotic hacker campaigns were tracked by Attrition.org, a website that archived defaced web pages from 1995 to 2001.[19] Even though Attrition.org was a non-state actor, both military and civilian cyber defenders relied on it to track malicious activity.[20]

Patriotic hacking has become a regular feature of the conflicts between Israel and the Palestinians as well as Indian-Pakistani disputes. More recently, Chinese hackers increased their activities after the Nobel peace prize was awarded to a Chinese dissident in 2010, and websites hosting leaked WikiLeaks cables suffered denial-of-service attacks that many suspected were conducted by U.S. patriotic hackers. In each of these cases, non-state actors were both conducting these malicious activities and being targeted. The last 10 years have seen a "rise of the professional" – a drastic increase in the capability of non-state actors – in which recent incidents have become increasingly organized and sophisticated, and have sometimes involved ties to national governments.

Criminal activity in cyberspace has exploded because, as Misha Glenny argues, "No other sector of organized crime can match the growth rates of cyber crime" since "the profit levels are astronomical."[21] How much is astronomical? In Brazil, police cracked down on a ring that netted 33 million dollars from online banking accounts[22] with an earlier fraud yielding 125 million dollars.[23] Intrusions into retailer TJX Companies, Inc., and other companies in 2007 yielded tens of millions of credit card details.[24] One hacker received a 13-year prison sentence for credit card scams that cost U.S. banks approximately 86 million dollars.[25] Overall, according to one British estimate, worldwide online fraud generated 52 billion pounds in illegal gains in 2007 (roughly 78 billion dollars).[26]

Cyber crime yields money, not just through selling stolen identity information or credit details, but also through extortion. If a company makes 10,000 dollars a day from its website, it may be willing to pay many times that amount to forego or stop a lengthy disruption campaign. According to Jose Nazario of Arbor Networks, "Cyber extortionists are able to demand huge sums of money to cease the attack, yet these amounts are small in comparison with the financial impact of a sustained assault."[27] In 2008, online casinos were threatened with just such an attack timed to disrupt their accepting wagers for the Super Bowl unless the attackers were paid 40,000 dollars.[28] This cost, like in the costs of some other white-collar crimes, may even be reimbursed to the victim. Joined by many other insurers, American International Group, Inc., has been offering cyber-extortion insurance coverage for nearly 10 years that "provides reimbursement of investigation costs, and sometimes the extortion demand itself, in the event of a covered cyber-extortion threat."[29]

Cyber criminals are also able to exploit gaps in existing laws. One network, named Koobface, stole more than 2 million dollars a year. However, the money was derived from thousands of individual criminal micro-transactions. It cost victims spread across dozens of national jurisdictions only a fraction of a penny each. While the criminal payoff accumulated, finding a complaining victim would be difficult, and so it was difficult for the police force to justify spending resources on investigating the case. It was equally difficult for prosecutors to pinpoint a perpetrator.[30]

Even more significantly, some of the financial gains from cyber crime nets have been used to develop a major Internet underground of sophisticated

technologists, such as the group formerly known as the Russian Business Network, who constantly seek to overcome any improvements in cyber defenses.[31] These technologists also make available extremely large botnets that can be used for spam, massive denial-of-service attacks and similar criminal purposes.[32] The operational sophistication necessary to maintain and control these botnets suggests that governments are no longer the only actors that can conduct significant cyber attacks.

With all of this malicious activity, one type of non-state actor has been noticeably absent: terrorist groups. They do, however, remain interested in cyber capabilities to fund their activities through crime, reach supporters and disseminate their message. For example, Ibrahim Samudra was executed by Indonesia as he testified to raising 200,000 dollars to fund the bombings in Bali[33] while the United Kingdom convicted Younis Tsouli (aka "Irhabi [Terrorist] 007") of inciting to commit terrorism by posting extremist websites and for conducting at least 2.5 million pounds of fraudulent activity including credit card fraud.[34]

One of the few examples of cyber terrorism is a case of malicious cyber activity linked to al Qaeda. Court records show that Mohamedou Ould Slahi told his detainers at Guantanamo Bay that the group "used the Internet to launch relatively low-level computer attacks" and "also sabotaged other websites by launching denial-of-service attacks, such as one targeting the Israeli prime minister's computer server."[35] Such low-level, non-disruptive activity highlights that cyber terrorism to date has been a much less significant concern than cyber crime or espionage. However, more recent developments indicate that it may only be a few short years before terrorist groups are able to grow or purchase significant capabilities, such as reports from Israel that a distributed denial-of-service (DDoS) attack from a half million infected computers "may have been carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah."[36]

Non-state actors can cause strategic effects in two critical ways. First, they can make advanced capabilities available for sale or through cooperation with state or via the Internet underground non-states actors. One of the most important pieces of malicious software for stealing credentials for online banking and other commerce is named Zeus and can be bought for as little as 700 dollars online.[37] Zeus yielded criminal gains of 70 million dollars to just one of the many groups using it.[38] According to the security company Symantec:

> Zeus provides a ready-to-deploy package for hackers to distribute their own botnet. The botnet is easily purchased and also freely traded online and continues to be updated to provide new features and functionality. The ease-of-use of Zeus means the Zeus bot is used widely and is highly prevalent, allowing the most novice hackers to easily steal online banking credentials and other online credentials for financial gain.[39]

There are already reports that the Stuxnet worm, which focused on the rarefied software and control systems of nuclear facilities, could be hijacked and redirected to other targets.[40] For example, the "hacktivist" group known as "Anonymous" has posted a decompiled version of Stuxnet (having stolen it from the files of a security company) on the Internet, and at least one security researcher believes that the more dangerous binary version is "widely available."[41] As advanced capabilities continue to be made available online, non-state actors will be able to acquire increasingly powerful capabilities to disrupt or destroy cyber systems and the actual physical infrastructure connected to them.

The second way in which non-state actors can cause strategic effects is by forming unholy alliances, where states provide advanced capabilities

One of the most important pieces of malicious software for stealing credentials for online banking and other commerce is named Zeus and can be bought for as little as 700 dollars online. Zeus yielded criminal gains of 70 million dollars to just one of the many groups using it.

(whether targeting details, money or actual intrusion tools and countermeasures) directly to non-state actors to use while retaining plausible deniability. Recent examples include the large-scale malicious activities against Estonia in 2007 and Georgia in 2008.

In Estonia, there were no direct links to the Russian government, though malicious activity was linked to nationalist groups "following instructions provided on Russian language Internet forums and websites,"[42] and was conducted by at least one group linked to the Kremlin.[43] The primary targets included both state institutions and non-state organizations, such as major Internet service providers, e-banking services and news organizations,[44] while the defenders were largely non-state actors. Fortunately, the peak of the attacks occurred while the European network operators group, Réseaux IP Européens, was meeting in Tallinn, so the quick global collaboration between these ISPs and network operators helped to rapidly mitigate the attacks. Estonia also informally requested NATO assistance, which generated discussions about the alliance's role in cyber defense but at the time led to little more than limited pledges of help.[45]

As in Estonia, the malicious activity in Georgia the following year also targeted both state and non-state targets but with more fingerprints of the Russian government. Russian organized crime was implicated and the attackers, according to one assessment, "were tipped off about the timing of the Russian military operations while these operations were being carried out" so that "any direct Russian military involvement was simply unnecessary."[46] Another group of analysts assessed "with high confidence" that "Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions."[47]

Future unholy alliances could develop between Iran and Hezbollah, other Islamist extremist groups supported by splinter elements of like-minded governments, or extremist groups supported by Pakistan or India against the other. Such alliances need not be formal or bilateral, and may simply include a loose coalition of actors with shared interests. The United States and other governments may face real strategic threats when state adversaries cooperate with non-state actors – if they cooperate, for example, to launch cyber guerilla or terror campaigns to cause political and economic disruption over months or years.

An often-overlooked strategy to better respond to threats by non-state adversaries is to put non-state actors at the center of the defense, such as during the Conficker worm in 2008 and 2009. This worm, estimated to have infected 2 million to 10 million computers in a period of a few months, was frequently updated to defeat responses to it. However, in February 2009 – five months into the spread – a collaboration of responders formed the Conficker Working Group,[48] bringing together governments, Internet organizations,

companies, service providers, security experts and academics. This group developed detection and eradication tools and coordinated operations globally to include domain system operators in places as diverse as the United States, China and Iran.[49] Because the private sector was in the lead, there was little of the red tape or diplomatic mistrust that would have existed if it had been a government-to-government response.

Non-state actors had the lead role in the working group and many participants felt, "It was the first truly successful effort they were involved in after a decade of attempts to collaborate."[50] For all of their benevolent intent, though, such ad hoc, voluntary projects often lack the capability or staying power over long periods of time as new threats appear, the costs to volunteering companies rise and the adversaries unleash harder-to-defeat malicious software.

Non-state actors fortunately have found many other avenues to bring collaborative capability to the defense and resilience of the ecosystem. Importantly, they have become trusted sources of security information, often able to disseminate information faster and more openly than governments. For example, the Information Warfare Monitor has helped pioneer an "open source" or "crowd source" analysis of cyber intrusions, which has revealed extensive cyber espionage intrusions into computers associated with the Dalai Lama's Tibetan government-in-exile and hundreds of other computers – many associated with foreign ministries and embassies – across many dozens of countries.[51] Similarly, journalists and companies have released previously unknown information on key security events that might have been expected to come from government. In only one month (February, 2011) information was shared about intrusions into oil and gas companies (revealed by McAfee[52]) and an intrusion into a NASDAQ network (revealed by *The Wall Street Journal*).[53] There are also numerous informal collaboration mechanisms, such as the North American Network Operators Group (NANOG) or ShadowServer, where network operators identify and analyze emerging threats, crack encrypted communication channels, provide information to affected parties and orchestrate collaborative responses.[54]

As some nations engage with nationalistic, malicious non-state cyber actors to create unholy alliances, the United States and other like-minded governments must work more closely with non-state actors to build counterbalancing alliances for defensive purposes; to reduce the risks of cyber attacks; to improve resiliency; and to enable free speech, privacy and commerce in cyberspace.

Approaches to Better Engage Non-State Actors

To date, governments and non-state actors have thought about cyberspace, cyber security and cyber conflicts using three traditional approaches: the Technical Approach, the Criminal Approach and the Warfare Approach. This chapter will spend a short amount of time on each traditional approach before going into detail into three newer approaches: Environmental, Public Health and Irregular Warfare. Each of these offers fresh insights that are particularly helpful in understanding the roles of non-state actors.

TRADITIONAL APPROACHES

Technical Approach

The Technical Approach has two branches, the first of which argues that the technical community can either invent a new, more secure cyberspace[55] or that cyberspace would be more secure if users chose secure technologies or would just read the manual to the tools they already have. This approach is typified by the open source software movement and standards and coordination bodies (such as the Internet Engineering Task Force and Internet Society). This branch can perhaps best be characterized by one of the true believers, John

Barlow of the Electronic Frontier Foundation:

> Governments of the Industrial World … I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. … Where there are real conflicts, where there are wrongs, we will identify them and address them by our means.[56]

Such thinking has unleashed innovation but has not (yet) significantly advanced cyber security by, for example, making it easier to defend than to attack.[57]

The second branch of the Technical Approach involves responding to incidents after they occur. The technical community has a long and generally successful history of coordinating incident responses and analysis of likely attackers. However, these efforts are often not fully trusted by governments, are poorly funded and tend to be ad hoc, created for each new outbreak of malicious software. They do not effectively conduct sustained efforts, such as eradicating botnets, nor do they share lessons learned about technical methods and processes for information sharing and collaboration.

This is the only traditional approach that is not inherently governmental and is the one that most embraces non-state actors, as the norms are meritocratic. Generally, anyone with technical prowess can participate, regardless of organizational affiliation. However, while technical solutions can serve as a foundation for other approaches they so far have not and likely cannot solve the challenges facing the health and resilience of the cyber ecosystem on their own.

Criminal Approach

States have used their traditional law enforcement powers to bring criminal or civil cases against non-state actors acting maliciously in cyberspace. This has generally been an effective approach, especially since all malicious activity is a crime. Although there may be disagreements about particular laws, sanctions and prohibited actions, the Criminal Approach has strong and widely understood domestic and international norms and formal legal regimes. There are long-standing traditions of states cooperating to reduce crime and bring criminals to justice. However, it is very difficult to solve cyber crimes due to cross-jurisdictional difficulties; lack of trained police, prosecutors and judges; problems with digital forensics and evidence; and other issues.

A key disadvantage of the Criminal Approach is that it is inherently governmental and also inherently slow. While some corporations assist in investigations and may alert the government when attacks occur, the formal investigation and possible prosecution of crimes are governmental activities. Non-state actors can prevent crime by taking preventive actions (such as not clicking on attachments from unknown people) and they can report crimes and give evidence, but otherwise there is little scope for non-state actors in the Criminal Approach.

Warfare Approach

Since the beginning of malicious cyber activity, some actions have been considered not merely criminal but actual "cyber warfare," and indeed *Time* magazine featured a cover article with that phrase back in 1995. A Warfare Approach does not depend on any specific definition of "cyber warfare" since the defining approach is a military approach to cyber conflict. For example, in the United States cyberspace has become a top tier national security concern prompting the formation of a U.S. Cyber Command and frequent public statements by the Deputy Secretary of Defense and other senior leaders.[58]

One advantage of the Warfare Approach is that it enables militaries to recognize the threat of cyber attacks as an offensive threat … and a possible offensive opportunity. Another advantage is that it leverages existing norms and regimes. For example, even if adherents to the Technical or Criminal Approaches will not understand it, other national

TABLE 2: APPROACHES TO ENGAGE NON-STATE ACTORS IN CYBER SECURITY

TRADITIONAL APPROACHES			
	TECHNICAL	**CRIMINAL**	**WARFARE**
Viewpoint	Non-state actors should improve technology and response for the best defenses	States should improve defenses by using law enforcement to stop non-state criminals	States should improve defenses for defeating states and non-state actors
Relationship to Non-State Actors	Enables benevolent non-state defenders	Stops malicious non-state attackers	Stops malicious non-state attackers
Primary Role Belongs to Whom	Non-state actors who are extremely active in all aspects of this approach	Governments as law enforcers	Governments as warfighters
Role of Non-State Actors	Researchers, coordinators or inventors	Criminals, victims or witnesses	Attackers or non-combatants
Generally How?	Enables non-state actors on defense	States lock up non-state cyber criminals	Improves state defenses and offenses
Specifically How?	Non-state actors lead in many kinds of cyber incident coordination, improved and secure technology, standards	States undertake forensics, improve laws; train cyber smart police, prosecutors and judges	States treat warfare in cyberspace as analogous to warfare in other domains
Enables International Norms?	Weakly	Strongly	Strongly
Possible Norms	"New standards and technologies should be secure from the start"	"Don't be a victim; practice safe clicking"	"International humanitarian law applies to cyber attacks"
"Natural" Lead Government Agency	Commerce	Justice	Defense

NEWER APPROACHES			
	PUBLIC HEALTH	**ENVIRONMENTAL**	**IRREGULAR WARFARE**
Viewpoint	State and non-state actors improve defenses as if confronting pandemic threat	State and non-state actors could improve defenses if cyberspace is seen as polluted domain	Militaries could improve defenses if cyber conflict is seen as irregular warfare
Relationship to Non-State Actors	Primarily to enable non-state defenders but also to stop non-state attackers	Both enable non-state defenders and stop non-state attackers	Stop malicious non-state attackers
Primary Role Belongs to Whom	Governments as cyber public health coordinators (e.g. cyber World Health Organization or Centers for Disease Control)	Both government (as lawmaker and regulator) and non-state actors (as non-governmental organizations, individuals)	Governments as warfighters
Role of Non-State Actors	Important supporting roles equivalent to care providers, drug companies, etc.	Individuals who decide not to pollute or are regulated or incentivized	Irregular adversaries to be defeated
Generally How?	Improving defenses in both states and non-states	Enrolling non-states and states to improve defenses	Improving state defenses against non-state offense
Specifically How?	International agreements to measure and share data, respond to incidents, enroll non-state actors	Creating norms of behavior and legal regimes based on "pollution" of cyberspace	Change of mindset based on tenets and tactics of irregular warfare
Enables International Norms?	Strongly	Strongly	Weakly
Possible Norms	"Practice safe cyber hygiene"	"ISPs should not allow traffic polluted with botnets to pass their systems"	"We must patch our systems to fight on a more favorable terrain"
"Natural" Lead Government Agency	White House or Homeland Security	Homeland Security	Defense

militaries will have a good idea what is meant by the statement, "The U.S. has affirmed that the international Law of Armed Conflict, which we apply to the prosecution of kinetic warfare, will also apply to actions in cyberspace."[59]

One downside of the Warfare Approach is that the use of overly militaristic language frames this issue in competitive terms, which undermines efforts to build international cooperation on cyber security measures. Similarly, a Warfare Approach mindset leads many observers into a mistaken view of many malicious actions as "cyber war" rather than what they usually are: crimes (or even petty nuisances). A wide range of crimes from patriotic hacking[60] to WikiLeaks hacktivism[61] have mistakenly been called "war," as has Chinese espionage,[62] even though warfare and espionage are distinct activities. Using the term "warfare" will always be inappropriate for non-state malicious activity that causes no casualties, no physical damage or loss of information or services that can be set right in only a few days.[63]

Another disadvantage is that, like the Criminal Approach, there is only a very limited role for non-state actors. In its traditional sense, war is an activity for militaries – non-state actors can assist, but these actors are generally considered victims or are mandated or expected to support their government.[64] The military conducts most of the action, while non-state actors are limited to helping on "the home front." Cyberspace has flipped this traditional arrangement around, with non-state actors conducting most of the protection, response and defense activities. Of course, non-state actors can take a more direct role as combatants in the Irregular Warfare Approach, which is considered below.

Some militaries actively seek to bridge the gaps between their uniformed forces and non-state actors. The United States only has limited programs so far, such as assigning some National Guard and Reserve units to cyber defense or offense missions, and a new information technology exchange program to exchange cyber personnel between the Department of Defense and the private sector. Other nations have gone much further. Estonia is creating a Cyber Defense League as part of its all-volunteer paramilitary force,[65] while one of Iran's responses to the Stuxnet worm has been to develop cyber units for their Basij paramilitary, subordinate to the Iranian Revolutionary Guard Corps.[66]

NEW APPROACHES

These traditional approaches have been useful but are inadequate to identify ways to leverage non-state actors for cyber defense. We identify three new approaches that provide new ways to better nurture the benevolent intent and capability of non-state actors. These approaches could be used within governments, between governments, by governments to engage with non-state actors or by non-state actors on their own.

Public Health Approach

The Public Health Approach uses the spread of biological diseases as an analogy for malicious cyber activities, and focuses on ways to stop them from spreading.[67] Though non-state actors – such as hospitals, researchers and pharmaceutical companies – have important roles, governments remain at center stage, particularly through the World Health Organization (WHO) and at the national level through organizations such as the Centers for Disease Control (CDC).

The Public Health Approach – which emphasizes collaboration, measurement and transparency – has several advantages. First, public health authorities strongly emphasize mandatory reporting and measurement to enable early warning, a transparency lacking in cyberspace. Second, public health and epidemiology focus on practical intervention to stop diseases from spreading– including inoculation, quarantine and isolation,

and protecting against harm and against transmission – all of which have direct correlations in cyber security.

Third, public health may provide a useful framework for organizing the resources of cooperative state and non-state actors in response to an outbreak of malicious software – similar to how public health authorities work with universities, researchers and pharmaceutical companies to deal with biological outbreaks. Though the idea of a cyber equivalent for the CDC dates back at least to a 1996 study by RAND[68] the idea has recently been refreshed and championed by Microsoft. Senior Microsoft executive Craig Mundie told the World Economic Forum in 2010 that "we need a kind of World Health Organization for the Internet,"[69] an idea better defined in a follow-up concept paper, "Applying Public Health Models to the Internet" by Scott Charney, another senior executive.[70] In a similar vein, the Department of Homeland Security (DHS) has recently released a parallel white paper by Deputy Undersecretary Philip Reitinger on the cyber "ecosystem," which covers similar ground as the public health model, such as analogizing on cyber security based on the human immune system.[71]

A fourth advantage is that the Public Health Approach may identify useful ways for ordinary Internet users to take preventive measures. During cold and flu season (and especially during a pandemic), people increasingly understand that they should take basic hygiene actions for their own safety and others'. "Cyber hygiene" may be another way to highlight similar preventive measures in cyberspace.

At the global level, a potentially significant downside is that the WHO is a United Nations organization. If a U.N. organization runs the cyber equivalent of WHO, repressive regimes may be able to shape the organization's efforts in ways that would raise concerns about Internet censorship.

Environmental Approach

Environmental awareness has grown during the past decade, in large part because of the activities of grassroots organizations, non-profits, think tanks and motivated individuals. This same concern can be directly applied to the "environment" of a polluted cyberspace, full of viruses, malware and other malicious code. In the cyber environment as much as in the "real" environment, the actions of one person can have serious and unintended negative downstream consequences. This call for individual and collective actions enables one of the main strengths of this approach: it includes all kinds of non-state actors, not just governments. Where the other approaches focus on scaring non-state actors ("Don't be a victim!") the Environmental Approach might better motivate people and organizations to become involved in ensuring a healthy, clean future for the Internet.

Translating concerns about pollution in the *physical* environment to the *cyber* environment may be relatively simple with the right messages to the correct communities. Individuals and corporations that think it is unjust to throw a can from a window of a car or fail to recycle their trash may be willing to take positive and even intrusive actions to ensure their own computers are not launching spam or participating in DDoS attacks. Major telecommunication providers might be more willing (or under more pressure) to avoid passing polluted traffic downstream: According a survey by Arbor Networks, 27 percent of network operators do not attempt to detect outbound or cross-bound attacks,[72] and of those that do, nearly half take no actions to mitigate such attacks.[73]

Further, problems with pollution and cross-border emissions may also apply to cyber pollution. In the physical world, for example, there is a legal principle that the "polluter pays." In the 1930s, the United States complained to Canada about sulfur dioxide emissions from a smelter of zinc and lead in Trail, British Columbia that were poisoning crops across the border. The international arbitration panel in

this "Trail Smelter" case ruled that Canada should pay a hefty penalty and the smelter should refrain from causing further damage and measure its impact on the local environment.[74] This principle has been extended in more recent decades through the United States Superfund law.[75] It could potentially be used to hold individuals or organizations accountable for activities that "pollute" cyberspace, whether by omission or commission.

The Environmental Approach also facilitates productive ties with the development and sustainability communities. Concepts such as "clean food, clean water, clean Internet" or building a "sustainable" Internet are more likely than language from Warfare or Criminal Approaches to resonate with international elites at non-profits, the World Bank and donor nations, and developing nations.

An Environmental Approach may be more palatable to international state and non-state actors than an overt national security approach (such as Warfare or Criminal), even though it directly and intentionally enhances national security. This approach may offer a more effective way to reduce overall levels of malicious activity.

Irregular Warfare Approach

The Irregular Warfare Approach involves malicious and persistent non-state actors who purposefully seek to blur traditional distinctions such as combatant and non-combatant.[76] Not all non-state actors engage in irregular warfare in cyberspace (though some indeed may be) but governments may profitably borrow insights and methods from irregular warfare and counterinsurgency.

Succeeding in an irregular war is, at root, a problem of "winning the hearts and minds of the people." Governments often have no more legitimacy or credibility about cyber security issues than any other group with a loud voice – and the Internet comes fully equipped with a multitude of loud voices.

Governments need to recognize the limits of their own credibility and partner with non-state actors who are often more trusted by Internet users.

Political legitimacy to deal with cyber security requires convincing individuals that the government's cause is the right one and they personally need to take steps to help – that is, nurturing both their intent to be helpful (or at least not harmful) and their capability to do so. However, none of the U.S. government actions to date (from cyber security awareness month to speeches, bulletins and warnings) have sufficiently won the hearts and minds of people, perhaps because of the perceived difficulty of securing home systems, mistrust of government intentions and perceived threats to privacy and free speech. Governments are also limited by political and ideological debates over the degree of their involvement in securing cyberspace, where government action is proper (if it is proper at all), and what activities, norms and goals support government involvement. As a result, governments need to recognize the limits of their own credibility and partner with non-state actors who are often more trusted by Internet users.

In irregular warfare, the underlying conditions might include a corrupt government, poverty and malnutrition, or perceived slights or tit-for-tat violence from other groups. In cyber conflict, the most important underlying condition is un-patched computers and insecure protocols. Militaries seeking to reduce these underlying conditions may be more effective using an argument based on irregular warfare than one of "cyber hygiene" or "reducing pollution."

In both irregular and cyber conflicts, adversaries may be able to hide in the terrain, whether at rest (in villages or in infected computers) or in motion (on the jungle trail or traversing networks). Removing the cyber adversary's ability to hide could involve rapidly isolating or fixing home computers, preventing DDoS attacks out of the main networks, cleaning the environment and enabling network operators and defenders to identify sophisticated malicious activity. This would involve Tier 1 ISPs having the legal authority and sufficient public support to shut down computers and networks that are proliferating DDoS attacks and botnets. Martin Van Creveld has pointed out, "To remain hidden, insurgents must disperse – the more of them there are at any one place, the more easily found they are. They must also avoid movement as much as possible."[77] In the cyber domain the insurgents are not very dispersed, nor do they avoid movement; in fact, successful attacks require transiting through tier 1 networks. This means that it may be easier to deal with cyber "insurgents" than with the physical kind.

Sanctuaries in irregular warfare can include neighboring countries where the adversary is able to move, equip and rest with impunity, or similar domestic places. In cyberspace, sanctuaries are where nations do not have the ability to stop all malicious activity from their national territory or are unwilling to do so.

These mindsets and methods of the Irregular Warfare Approach may help governments to improve their security *as if* they were really engaged in an irregular conflict in cyberspace. Of course, there may be conflicts between non-state actors and governments, between governments, between government-sponsored proxies, or even between non-state actors who allow competition to spill over, violently, into cyberspace.

Selecting the Right Approach

The approaches that policymakers, practitioners and researchers use to think about cyber conflict greatly affect how they diagnose problems and develop solutions. According to computer security specialist Bruce Schneier:

> If we frame this discussion as a war discussion, then what you do when there's a threat of war is you call in the military and you get military solutions. You get lockdown; you get an enemy that needs to be subdued. If you think about these threats in terms of crime, you get police solutions. And as we have this debate … the way we frame it, the way we talk about it; the way the headlines read, determine what sort of solutions we want.[78]

Yet the issues posed by non-state actors in cyberspace are so complex and multidimensional that no single approach can ever be sufficient. Instead, an integrated strategy must incorporate insights from different approaches to address different aspects of the problem such as the 2003 *National Strategy to Secure Cyberspace* did when clearly differentiating between approaches. It declared that:

> When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner.[79]

So when is each approach most helpful? The traditional approaches (Criminal, Warfare and Technical) remain extremely useful but only with respect to their own area of expertise: the Technical Approach will always be needed to improve and expand the domain of cyberspace, while the Criminal Approach is most appropriate to specifically defeating criminals. The Warfare Approach is understood by warriors and can effectively address national security conflicts, especially but not exclusively between nations, in cyberspace.

However, these traditional approaches will remain insufficient singularly and collectively. Even with better technology, more prosecutions and more users deciding to "Stop, Think, Connect" (in the words of a current public cyber safety campaign[80]) many non-state adversaries will continue to exploit the massive global population of insecure machines for criminal and other purposes.

Each of the three new approaches provides useful insights on how to counter malicious activity by non-state actors. The Public Health Approach emphasizes global cooperation among governments and non-governmental organizations, based on lessons learned from epidemiology and related fields. This approach can be especially effective at stopping, detecting and responding to rapidly spreading malicious outbreaks like the Conficker worm.

The Environmental Approach may be most helpful to enroll young people, corporations, foundations and think tanks to clean the cyber environment and stopping sources of pollution emissions that cause significant downstream effects (like botnets). These communities are more likely to engage in an Environmental project than one built on a Criminal or Warfare Approach. A main strength here is that, along with Public Health, this approach embraces non-state actors as a critical part of the solution – not just part of the problem, as happens with the Criminal and Warfare Approaches.

The Irregular Warfare Approach is best for helping the Department of Defense understand how to address cyber conflict with non-state adversaries. For example, DOD personnel are much more likely to understand their role in cyber conflict if they are told to eliminate safe havens and reduce places where adversaries can hide than if they are told to "improve cyber hygiene." Winning the hearts and minds of the denizens of cyberspace will be just as important to military success as it is in the sands of Iraq or mountains of Afghanistan.

Recommendations for the United States

First, the United States must recognize that the threats posed by malicious non-state actors are just as significant as those posed by potential state adversaries in cyberspace and ensure that intelligence collection and analysis, and contingency and operational planning focus on both types of threats. In particular, the United States must prepare for the possibility of a long-term cyber guerilla campaign targeting U.S. economic activities and public confidence.

Second, the White House should use the Public Health and Environmental Approaches to root a new national strategy for improving the "health and resilience of cyberspace." The Department of Homeland Security should lead this effort in collaboration with the Department of Commerce, DOD, Department of Justice and the FBI. To encourage benevolent intent and strengthen capabilities of non-state actors, this strategy should:

- Engage the private sector operators of the cyber commons – such as ISPs, companies that register web domains and web hosting firms – to establish norms for appropriate user behavior and operator obligations in enforcing these norms. The government should act as an enabler, by explicitly permitting activities such as quarantining infected machines from the Internet, rather than through top-down regulation.
- Collaborate with the private sector in educating users at all levels about cyber hygiene and contributing to a healthy Internet environment.
- Establish funding sources for innovation and effective private sector competition to further cyber health. The government should consider stimulating these efforts by high-profile challenge competitions such as those conducted by the Defense Advanced Research Projects Agency.

Third, the United States should lead a global cyber security engagement strategy led from the White House with the following priorities:

- Ensuring that U.S. cyber security initiatives are consistent with a global approach that explicitly seeks to engage nongovernmental stakeholders worldwide.
- Engaging global multi-stakeholder bodies[81] and leveraging the strong technical capabilities and collaborative relationships of the global incident response community to clean the cyber environment. These organizations could form the basis of a new Cyber Risk Reduction Center that would develop metrics and reporting standards, improve transparency about malicious activities and establish crisis communications mechanisms that bridge public and private sector organizations globally.

Fourth, the United States should pursue a concept of "advanced persistent national cyber defense" that includes a role for non-state actors. The Department of Defense should lead this effort, supported by the Department of State, DHS, the Department of Justice and FBI. This concept should:

- Encourage private sector operators of cyber infrastructure to proactively identify and remove malicious code as well as filter and block large-scale disruptive attacks.
- Support the establishment of a private sector foundation that identifies lessons from ad hoc technical and operational collaboration by network operators in response to cyber threats.

Fifth, DOD should analyze the dynamics of "irregular cyber warfare" as a major aspect of the development of cyber war doctrine and operational concepts. This might drive internal procedures based on familiar concepts of irregular war, rather than the arcane and poorly understood jargon of computer security.

Sixth, the Department of Justice, DOD and DHS should continue to pursue counterterrorism, counterintelligence and traditional Warfare Approaches in appropriate areas. These traditional approaches already fit the existing missions of the Departments of Justice, Defense and Homeland Security, so they should continue improving and adapting these approaches to address cyber issues as well.

And **last**, the U.S. government – especially DOD and the new U.S. Cyber Command – must use caution when describing cyber security in terms of warfare and terrorism when alternative approaches will prove more effective. As noted earlier, the militaristic language of the Warfare Approach frames this issue in competitive terms, which are not likely to be as effective as the other approaches in engaging other nations and global multi-stakeholder groups in cooperative projects.

The United States and other governments are still learning how to establish a more secure, resilient cyberspace and manage conflicts in this realm. The new approaches introduced here should be studied in more detail, especially in understanding the utility and limits of specific organizational approaches, the alignments of state and non-state actors and the most promising strategies and negotiating forums for promoting operational collaboration and new norms. Focusing more on the role of the private sector and other non-state actors will help improve U.S. cyber defense efforts.

ENDNOTES

1. See, for example, Martin Libicki's *Cyberdeterrence and Cyberwar* (Santa Monica, CA: Rand Publishing, October 2009); or Timothy Thomas's in-depth examinations of Chinese writing and operations, including *Dragon Bytes: Chinese Information-war Theory and Practice from 1995-2003* (Fort Leavenworth, Kansas: Foreign Military Studies Office, 2004), and *Cyber Silhouettes: Shadows Over Information Operations* (Fort Leavenworth, Kansas: Foreign Military Studies Office, 2006).

2. Insurgencies and other kinds of irregular warfare are obvious exceptions to non-state actors as non-combatants, and will be examined later in this work. We do recognize the increasing significance of armed groups and other non-state actors in 21st century conflicts.

3. Even in the areas of cyberspace dominated by states, such as military communication satellites, the underlying technology is still often civilian. Lockheed Martin, not the U.S. military, produced the Defense Satellite Communications System. Boeing built the Wideband Global SATCOM (satellite communications) system.

4. The tier 1 ISPs are generally those companies that are the largest providers of network access and that "peer" with other similarly major providers.

5. There is no single definition of a non-state actor. See, for example, Karl Rauscher and Andrey Korotkov, *Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace* (New York: East-West Institute, 2011). For example, the International Law Association's Committee on Non-State Actors excluded the Mafia, al Qaeda and pirates because of their criminal nature. As criminal groups are important non-state actors in cyberspace. this chapter necessarily must diverge from the definition from the International Law Association committee.

6. For other iterations of this point see especially, Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown and Company, 1993); and John Arquilla and David Ronfeldt, "Cyberwar is Coming!," in John Arquilla and David Ronfeldt, eds., *Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997).

7. Perhaps best described in the Committee on Offensive Information Warfare, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Research Council, 2009).

8. For a good overview, see *The Economist*, "A virtual counter revolution" (2 September 2010); for a more detailed discussion see, Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press USA, 2006).

9. For example, see the Department of Homeland Security's white paper on the technical ecosystem, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action" (23 March 2011), http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

10. Computer Security Incident Response Teams (CSIRTs), also known as Computer Emergency Response Teams (CERTs), respond to computer and network failures, typically those by a malicious actor. They are typically part of a larger organization (such as the US-CERT that performs these functions for the U.S. government).

11. Some areas are marked with a question mark, as they represent industrial espionage or other schemes where one company may conduct malicious cyber activity against others. This activity may occur but is not a major focus of the current papers.

12. United States versus Morris, judgment (7 March 1991), http://morrisworm.larrymcelhiney.com/morris_appeal.txt.

13. Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday, 1989).

14. Jack Brock Jr., "GAO Testimony Before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs," United States Senate (20 November 1991), http://www.net-security.org/article.php?id=30.

15. PowerPoint presentation from the FBI's Los Angeles Field Office Computer Crime Squad (2001), http://media.ais.ucla.edu/BTseminars/fbi_slides.pdf.

16. Kevin Poulson, "Solar Sunrise hacker 'Analyzer' escapes jail," *The Register* (15 June 2001), http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/.

17. See Wayne Arnold, "Philippines to Drop Charges on E-Mail Virus," *The New York Times* (22 August 2000), http://www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html; and "The Love Bug: A Retrospective," http://rixstep.com/1/20040504,00.shtml.

18. Marshall Abrams and Joe Weiss, "Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia," MITRE presentation (2008), http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_briefing.pdf.

19. Robert Lemos, "Defaced-site archive retires" (21 May 2001), CNET News, http://news.cnet.com/2100-1001-258006.html. Brian Martin of Attrition.org explained why Attrition.org was no longer able to track online vandalism. The excuse,"Because the volunteer staff can no longer keep up with the volume of defacements," is an example of a lack of staying power compared to government organizations. It is a common theme explored in further depth later in the chapter.

20. As with many other intelligence analysts, one of the authors (Jason Healey) relied on Attrition.org data for current and predictive warning while at the first cyber warfighting organization, the Joint Task Force - Computer Network Defense from 1999-2001.

21. Misha Glenny, *McMafia: Seriously Organized Crime* (London: Vintage, 2009): 313.

22. Lester Haines, "Brazil cuffs 85 in online bank hack dragnet," *The Register* (29 August 2005), http://www.theregister.co.uk/2005/08/29/brazil_hack_arrests/.

23. Misha Glenny, *McMafia: Seriously Organized Crime* (Vintage, 2009): 308.

24. Department of Justice Press Release, "Major International Hacker Pleads Guilty For Massive Attack On U.S. Retail And Banking Network" (29 December 2009), http://www.justice.gov/criminal/cybercrime/gonzalezPlea.pdf.

25. John Leyden, "CardersMarket hacking kingpin jailed for 13 years," *The Register* (15 February 2010), http://www.theregister.co.uk/2010/02/15/max_vision_cybercrook_jailed/.

26. Original estimate from the UK Association of Chief Police Officers and quoted in the Cabinet Office's "Cyber Security Strategy of the United Kingdom" (2009): 13.

27. Jose Nazario, "Cyber Extortion Is Now A Very Real Threat – Is Your Business At Risk?" Continuity Central (28 March 2006), http://www.continuitycentral.com/feature0322.htm.

28. Kelly O'Connell, "Online Casinos Will Experience Cyber-Extortion During SuperBowl Betting," Internet Business Law Services (28 January 2008), http://www.ibls.com/internet_law_news_portal_view.aspx?id=1967&s=latestnews.

29. Robert Hammesfahr and Ty Sagalow, et al., "@Risk version 2.0: The definitive guide to legal issues of insurance and reinsurance of internet, e-commerce and cyber perils," (London: Reactions Publishing Group, 2002).

30. Information Warfare Monitor, *Koobface* (2010): II.

31. See, "The Russian Business Network: The Rise and Fall of a Criminal ISP," in James Graham, ed., *Cyber Fraud: Tactics, Techniques and Procedures* (New York: CRC Press, 2009): 171-207.

32. Botnets are "networks of compromised computers used for nefarious means." See Jose Nazario, "Botnet Tracking: Tools, Techniques and Lessons Learned" Arbor Networks (2007), http://www.blackhat.com/presentations/bh-dc-07/Nazario/Paper/bh-dc-07-Nazario-WP.pdf.

33. Daniel Fowler, "U.S. Cybersecurity Efforts Likened to the Maginot Line," CQ Homeland Security (2008), http://www.coresecurity.com/content/us-cybersecurity-efforts/.

34. Gordon Corera, "The world's most wanted cyber-jihadist," BBC News (16 January 2008), http://news.bbc.co.uk/2/hi/americas/7191248.stm.

35. Alex Kingsbury, "Documents Reveal Al Qaeda Cyberattacks" *U.S. News and World Report*, (14 April 2010), http://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks.

36. Anshel Pfeffer, "Israel suffered massive cyber attack during Gaza offensive," Haaretz (15 June 2009), http://www.haaretz.com/news/israel-suffered-massive-cyber-attack-during-gaza-offensive-1.278094.

37. Nicolas Falliere and Eric Chien,"Zeus, King of Bots," (Cupertino, CA: Symantec Corporation, 2009): 1.

38. *BBC News*, "More than 100 arrests, as FBI uncovers cyber crime ring" (1 October 2010), http://www.bbc.co.uk/news/world-us-canada-11457611.

39. Falliere and Chien (2009): 13.

40. Mark Clayton, "Son of Stuxnet? Variants of the cyberweapon likely, senators told," The Christian Science Monitor (17 November 2010), http://www.csmonitor.com/USA/2010/1117/Son-of-Stuxnet-Variants-of-the-cyberweapon-likely-senators-told.

41. Jeremy Kaplan, "Anonymous Hackers Release Stuxnet Worm Online," FoxNews.com (15 February 2011), http://www.foxnews.com/scitech/2011/02/15/anonymous-hackers-offer-stuxnet-worm-online/.

42. Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2010): 33.

43. One person claiming to have organized the attack is a leader of the Kremlin-backed Nashi ("Ours") youth nationalism group and also an assistant of a member of the Duma (parliament). See Charles Clover, "Kremlin-backed group behind Estonia cyber blitz," *The Financial Times (*11 March 2009), http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac. html#axzz1F0wNeeJX; and "Behind The Estonia Cyberattacks," Radio Free Europe (6 May 2009), http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html. Nashi had attacked the Estonian ambassador to Moscow and barricaded the embassy over the same incident that led to the cyber attacks. See "Protest at Estonian Embassy Called Off," *The Moscow Times* (4 May 2007), http://www.themoscowtimes.com/news/article/protest-at-estonian-embassy-calledoff/197288.html; and Peter Finn, "Protesters in Moscow Harass Estonian Envoy Over Statue," *The Washington Post* (3 May 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/02/AR2007050202547.html.

44. Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2009): 22.

45. Wyatt Kash, "Lessons from the Cyberattacks on Estonia" *Government Computer News* (13 June 2008), http://gcn.com/articles/2008/06/13/lauri-almann--lessons-from-the-cyberattacks-on-estonia.aspx.

46. U.S. Cyber Consequences Unit, "Overview of the US-CCU of the Cyber Campaign Against Georgia in August of 2008" *US-CCU Special Report* (August 2009): 3.47. Project Grey Goose, "Russia/Georgia Cyber War – Findings and Analysis" (17 October 2008).

48. Microsoft, "Microsoft Collaborates With Industry to Disrupt Conficker Worm" (26 March 2009), http://www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.mspx.

49. Conficker Working Group, "FAQ – Announcement of Working Group," http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/FAQ.

50. The Rendon Group, "Conficker Working Group: Lessons Learned" (January 2011): 33, http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf. This working group report was supported by the Department of Homeland Security.

51. Other examples of open source or crowd source analysis include SANS Internet Storm Center, Shadow Server Foundation, Project Grey Goose and the Honeynet Project.

52. McAfee Foundstone Professional Services and McAfee Labs, "Global Energy Cyberattacks: 'Night Dragon'" (10 February 2011).

53. Devlin Barrett, "Hackers Penetrate Nasdaq Computers," *The Wall Street Journal* (5 February 2011), http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html.

54. See the websites for NANOG at http://www.nanog.org/ and the Shadowserver Foundation at http://www.shadowserver.org/wiki/.

55. In the past, any number of technologies were often promised to make the Internet and computing safe from trusted computing, public key cryptography, firewalls, intrusion detection devices, intrusion prevention devices and more.

56. John Perry Barlow, "A Declaration of the Independence of Cyberspace" (8 February 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

57. For example, according to Arbor Networks, despite a massive 1000 percent increase in the size of the single largest distributed denial-of-service attacks over five years, only 53 percent of network operators tried to mitigate the effects of outbound distributed denial-of-service attacks and 66 percent did not proactively block sites associated with botnet command and control, malware drop sites and phishing servers.

58. For example, see William J. Lynn III, "Defending a New Domain" in *Foreign Affairs,* Vol. 89, Number 5 (September/October 2010).

59. General Keith Alexander, Statement before the House Armed Services Committee (23 September 2010): 7, http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf.

60. For example, see Ellen Messmer's *CNN* story from 1999, "Kosovo cyberwar intensifies Chinese hackers targeting U.S. sites, government says" (12 May 1999), http://articles.cnn.com/1999-05-12/tech/9905_12_cyberwar.idg_1_hackers-webservers-web-sites?_s=PM:TECH.

61. Mark Townsend, et al., "WikiLeaks backlash: The first global cyber war has begun, claim hackers," *The Guardian* (11 December 2010), http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war.62. Michael Evans and Giles Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets," *The Times* (8 March 2010), http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053254.ece.

63. As a giveaway that CNN did not consider their story on the Kosovo "cyberwar" as *real* war (see footnote above), the story was in the Technology section.

64. While a somewhat dated example, AT&T was placed under federal government control during both World Wars. See Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001): 311-313.

65. Tom Gjelten, "Volunteer Cyber Army Emerges In Estonia," National Public Radio (4 January 2001), http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation.

66. Kevin Fogarty, "Iran responds to Stuxnet by expanding cyberwar militia," ITWorld (12 January 2011), http://www.itworld.com/security/133469/iran-responds-stuxnet-expanding-cyberwar-militia.

67. For a more detailed treatment of cyber implications of a public health model, see Rattray, Chris Evans and Healey, "American Security in the Cyber Commons," in Abraham M. Denmark and Dr. James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World* (Washington: Center for a New American Security, 2010).

68. Robert Anderson and Anthony Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: The Day After in Cyberspace II* (Santa Monica, CA: RAND Corporation, 1996).

69. *Agence France Press*, "At Davos, ITU Chief Calls for Anti-Cyberwar Treaty" (2 February 2010), http://planetrussell.posterous.com/un-chief-calls-for-treaty-to-prevent-cyber-wa-0.

70. Scott Charney, "Collective Defense: Applying Public Health Models To The Internet" (Microsoft, 2011).

71. Department of Homeland Security, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automat ed Collective Action" (23 March 2011), http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf. For an even more extensive analogy of the immune system, see Martin Libicki's "Postcards from the Immune System" in *Defending Cyberspace and Other Metaphors* (Washington: National Defense University, 1997).

72. That is, attacks that originate from within their own network against either a target within their own network (cross-bound) or in another provider's network (outbound). This would compare with in-bound attacks, originating from another provider.

73. Arbor Networks, "Worldwide Infrastructure Security Report: 2010 Report," Vol. 6: 15-16.

74. "Trail Smelter," case summary from the University of Montreal's Center of International Studies and Research, www.cerium.ca/IMG/doc/7-Trail_Smelter_Case.1937.doc.

75. The Comprehensive Environmental Response, Compensation, and Liability Act of 1980, section 107(a).

76. Irregular warfare is comprised of a wide range of operations, from insurgency and counterinsurgency, to terrorism and counterterrorism and stability and reconstruction tasks. Key authors who have written on the role of non-state actors in irregular warfare include: Mao Zedong, *On Guerilla Warfare,* Samuel B. Griffith trans. (Urbana, IL: University of Illinois Press, 2001); Richard H. Schulz, Douglas Farah and Itamara V. Lochard, *Armed Groups: A Tier One Security Priority,* INSS Occasional Paper, no. 57 (Colorado Springs, CO: USAF Institute for National Security Studies, September 2004); David Kilcullen, *The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press USA, 2009); General Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred A. Knopf, 2007); and John Nagl *Learning to Eat Soup With a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Westport, CA: Praeger, 2002).

77. Martin Van Creveld, "War in Complex Environments: The Technological Domain," *Prism*, The Center for Complex Operations, Vol. 1, No. 3 (June 2010): 125.

78. Bruce Schneier, "Me on Cybersecurity," (1 October 2010), http://www.schneier.com/blog/archives/2010/10/me_on_cyberwar.html.

79. The White House, *National Strategy to Secure Cyberspace* (2003): 50, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

80. See www.staysafeonline.org.

81. See, for example, the Internet Society, Internet Engineering Task Force, the Internet Center for Assigned Names and Numbers and the World Wide Web Consortium.

CHAPTER VI:
CULTIVATING INTERNATIONAL CYBER NORMS

By Martha Finnemore

America's Cyber Future

Security and Prosperity in the Information Age

CULTIVATING INTERNATIONAL CYBER NORMS

Martha Finnemore

Coordinating activity in cyberspace has become a crucial challenge. Virtually every sector of society in a wide array of countries now relies on Internet communication to carry out the most basic functions of modern life. Businesses, militaries, government at all levels and citizen groups of every imaginable kind now depend heavily on, and indeed cannot function without, an efficient and secure Internet.

This varied array of stakeholders holds a varied set of ideas about how cyberspace should be used and governed. Military and security professionals envision using the Internet to coordinate counter-terrorist activities and combat organized crime. They want rules to allow these actions. However, this alarms many privacy advocates who, in turn, want rules to protect against precisely this kind of surveillance. Meanwhile, various national governments hold different views about the legitimate uses of the Internet and are pushing hard for rules that reflect their preferred vision. For example, governments in Russia and China see internal dissent and anti-government writings disseminated on the Internet as a threat. Both have curtailed free speech and access to the Internet as part of their vision of "cyber security" – a view the United States is not likely to embrace. Without some basic "rules of the road," conflict between these competing values and visions will intensify. The essential resource of cyberspace cannot reliably perform the functions that we all depend on without agreed upon Internet norms.

This chapter analyzes the tasks involved in cultivating new norms and rules for cyberspace. Drawing on efforts to develop norms on other issues, we can see broad patterns in the kinds of norms that are likely to succeed and the strategies that are likely to prevail. Findings of this chapter include:

- Successful norms are likely to be simple and clear, obviously useful and relatively easy to follow. Overly complex and technical prescriptions

are unlikely to reach the very broad audience needed to ensure some of the most basic elements of a safe and secure cyberspace.[1]

- "Grafting" cyber norms onto existing, well-established normative frameworks, for example human rights norms or laws of war, may increase chances of success. Building on existing norms can help to make the new cyber norms seem intuitive and sensible to diverse audiences and enhances compliance.
- Multipronged and multilevel approaches to norm dissemination also seem particularly suited to cyber security. Pushing for new norms in multiple venues, among diverse audiences simultaneously will probably yield more timely progress than concentrating on some single norm-building enterprise, like a single treaty negotiation.
- Where possible, norms can and should be buttressed by appropriate laws at national, local and even international levels. Norms and formal laws should be treated as complementary tools, and a judicious use of both will yield the best results.
- Technical assistance and funding to help key actors "do the right thing" in cyberspace will greatly increase compliance.

These strategies may seem intuitive and obvious, but are difficult to implement. The cyber realm presents some unique challenges for norm development. Few issue areas penetrate every aspect of society as thoroughly as the Internet. Coordinating such diverse stakeholders with such varied values will not happen quickly or easily. To illustrate some of the challenges, this chapter briefly analyses norm promotion issues in two areas: developing norms around civilian protection and Internet freedom. Cultivating cyber norms may best be viewed a continuing challenge rather than a discrete task. Cyber insecurity is likely to be a chronic condition that must be constantly managed rather than a single problem to be solved and put to rest. As a consequence, cyber norms must continually evolve, and mechanisms to promulgate new norms must be developed.

Norms and Law

One common reaction to coordination problems, particularly in the international sphere, is to negotiate a treaty and make binding or "hard" law on the topic. There are obvious advantages to this. Treaties have the force of law. Theoretically, there should be enforcement by governments of their provisions. Treaties also offer at least an illusion of clarity since they usually spell out details of the agreement and explain rules in great detail. But negotiating treaties can be a slow and cumbersome process, ill-suited to fast-changing issues like cyber security and Internet governance. Governments may also not be the best or only actors to be making rules in this area since so much of the technology is in private hands.

Norms offer another tool to coordinate action. Norms may be defined most simply as shared expectations of proper behavior.[2] Shared expectations among actors can be dynamic and change quickly to suit the needs of those relying on them. As expectations rather than legal obligations, they invite broad participation. Actors who may feel nervous about being bound by formal laws may be willing to engage with groups governed by norms. Over time, these initially reluctant states, firms and individuals may become socialized into deeper acceptance of the norms. Compliance becomes internalized as people get used to the expectations, see their utility and come to share them more fully than they did when they joined the group.

Characteristics of a Successful Norm

As we develop new norms for cyberspace, it will be important to pay attention to both the form and content of a proposed norm. The successful spread of new norms is greatly facilitated if the norm, itself, is *clear*, *useful* and *do-able*.

Clarity. Norms are easier to spread, and more likely to spread successfully, if they are organized around clear principles. Absolute prohibition norms often have a leg up on this dimension, but other norms can also be simply stated. "Do not litter" and "clean up after yourself" are norm formulations that are simple, straightforward, and easy to remember and understand. They also might have clear applications to cyberspace. Establishing norms of responsibility for maintaining secure networks would build on these general, well-established norms of social life. "Clean up your networks" would thus be a clear, simple and potentially useful cyber norm.

Few issue areas penetrate every aspect of society as thoroughly as the Internet. Coordinating such diverse stakeholders with such varied values will not happen quickly or easily.

One potential pitfall of these simple imperatives could be the lack of specific responsibility. Who is responsible for maintaining clean networks? States? Businesses? Individuals? The usual answer is everyone is responsible – just as no one is allowed to litter, no one is allowed to have insecure networks. But saying everyone is responsible may mean that no one actually takes responsibility, creating a classic collective action problem.

Again, the parallels with similar norms may help in cyberspace. In other realms, norms like these create overlapping and therefore redundant responsibility. There may also be overlapping and redundant pressures to comply. If one litters, one expects nasty looks and comments from others, so the norm has some social enforcement thanks to social pressures and expectations to conform. Dirty behavior is embarrassing and hurts reputations of both individuals and business. The social norm also has a legal backstop: One can be fined individually for littering. But ultimately government clean-up crews pick up trash when no one else does. Change in littering behavior thus started at the social level with social norms; enforcement is a backstop, not the driving force behind less litter. A similar configuration of norms and laws might be helpful in cyberspace.

A complex and technical problem like cyber security might not obviously lend itself to simple norms, but that is the challenge. Simplicity and clarity must be manufactured by the norm promoters. One way to do this is to distill a few core principles about cyber security, each of which is relatively simple. This has worked in other complex issues. Trade is probably one of the messiest and most complex bodies of international rules and law, but buried within it are still some rather simple, clear norms about "most favored nation" status and "national treatment." The laws of war have similarly become enormously detailed and elaborated. However, while only a few lawyers know all the rules, every soldier knows the basic norms of noncombatant immunity, and targeting norms about discrimination and proportionality. Cyber norms would certainly benefit if a few basic expectations could be clearly and simply articulated.

Utility. People are more likely to adopt norms if they can see clear connections between norm-following and desired outcomes. Adopting new norms is usually not costless for adopters. At a minimum, adoption by apex actors (governments, CEOs, heads of organizations) usually commits them to elaborate persuasion and enforcement efforts downstream in their country, business or organization. If government officials sign a treaty or endorse a multilateral effort committing the

United States to carbon reduction, child literacy or weapons build-downs, they still face domestic political battles internally to get a wide array of other national actors (governors, local officials, companies, Congress) to sign on. This would certainly be true of cyber norms, which would likely require broad cooperation inside states, societies and the private sector.

One powerful tool for persuading actors to incur these costs is a strong argument or narrative about how adopting the norm will produce desired results. Such an argument or narrative would have at least two components. First, it would need to convince people that cyber security is really important to their well-being in some meaningful and immediate way. Some audiences may be harder to convince than others. Cyber professionals will probably be easy to persuade on this score, although they may disagree about the right "fix" or best norms to address the problem. To the extent that broader groups whose concerns are less immediately or obviously linked to cyber security need to cooperate, this narrative will be crucial. People need to be motivated to incur costs to adopt these norms. They need to be convinced that the threats are real and the costs of non-adoption are high.

Second, this narrative would need to convince people that complying with the proposed norm would actually produce the desired result. Climate change efforts stalled on failures of this kind. There were direct and active challenges to the causal factual connections norm promoters were claiming. The counter-narrative by norm opponents disputed the link between human activity and climate change. If human activity is not causing climate change, why adopt carbon restrictions? In the case of cyber security, people would need to believe that complying with the new norms would actually reduce vulnerabilities. To the extent there is uncertainty about whether the norm with work or result in advertised benefits, selling the norm will be harder.

Cyber hygiene norms look particularly ripe for this kind of narrative. Under such norms, users would recognize the broad negative impact of their own failure to take simple steps to ensure cyber security by preventing their own computers from becoming hosts for malware. Implementing cyber hygiene norms will require broad cooperation by a great many diverse social actors. Part of the norm promotion process will have to be some kind of public education about the dangers of botnets and insecure networks more generally. Just telling people there are abstract threats to unnamed others if they do not clean up networks may not do the trick. A narrative that links this to real damage to themselves and others they know will be more effective.

Do-ablility. New norms are more likely to be respected and change behavior if people see clear and easy ways to comply. People are more likely to comply with a "do not litter" norm if trash and recycling receptacles are easy to find in public spaces. Countries are more likely to implement childhood vaccination programs if they have funding and public health professionals to carry it out. Making it easy for people to "do the right thing" is an important ingredient in any norm cultivation effort.

Of course, in many situations, "doing the right thing" may be quite difficult. If it were easy, the desired norm would probably have arisen naturally and one would not need a big norm cultivation effort. Difficulties in implementing a norm, even when it is clear and its utility is understood, can come from several sources. Often there are *political* problems in compliance. Responsible government officials who adopt a norm may not be able to persuade legislatures to enact needed laws. If the law is unpopular politically, government officials who adopt a norm may not get reelected. And, of course, getting parties to agree on a common norm in the first place may also face serious political challenges.

There may be *economic or financial* problems with compliance if it is expensive and money is scarce (which it usually is). Securing networks domestically will cost money. Questions of who will bear those costs – business, government or individuals – may be a bone of contention. Securing networks abroad may also involve serious economic costs. Many of the states that are big sources of cyber crime, like Moldova and Belarus, are relatively poor. Persuading them to adopt new cyber norms may not be enough; they may need financial assistance.

Compliance may also be complicated if the *technology or basic knowledge* required to comply is missing. Again, this may be a problem both domestically and abroad. However, technical assistance programs may also be an opportunity. These efforts do more than disseminate technical knowledge. They can also be powerful socializing tools and opportunities to spread "best practices" on the Internet. These socialization effects have been amply documented in other policy areas. The International Monetary Fund, World Bank and bilateral state aid all involve massive technical assistance designed to socialize people into new best practices in finance, development, human rights and the environment, as well as delivering technology. While never 100 percent effective, these efforts do have demonstrable effects and shift expectations in desired directions.

Those cultivating cyber norms will encounter difficulties of all three types. Politically, there are likely to be roadblocks. Any clear formulation of cyber norms is likely to prompt objections from somewhere. Implementing these norms is bound to cost money, which always opens avenues for objection and fights. National, state and local governments may not want to appropriate money for this purpose, particularly when change is expensive. Businesses are likely to raise similar objections. At all levels of government, there is likely to be some shortage of expertise, and the usual measure of technical and bureaucratic foul-up in implementing whatever norms are crafted. Although this list of obstacles may sound daunting, it is normal. Most norm promotion efforts face similar problems, and a great many of these efforts succeed.

Stages of Norm Cultivation

Creating successful new norms usually involves at least three sequenced tasks or stages: 1. norm articulation and promulgation; 2. norm dissemination; and 3. norm internalization, institutionalization and enforcement.

Norm promulgation. One of the most common, and commonly successful, strategies for promulgating new norms is to build on existing, widely accepted norms. "Grafting" or piggybacking on existing robust normative frameworks could help legitimate new norms for cyberspace. It makes them seem familiar and intuitive, thus increasing prospects for compliance. Promoters of a norm that states "access to the Internet is a basic human right," for example, might try to graft this new norm onto existing human rights norms. Promoters could argue that, in the contemporary world, Internet access is an essential component of and prerequisite for securing many of the core rights in the U.N.'s Universal Declaration of Human Rights and the U.N.'s International Covenant of Civil and Political Rights. Norms about conflict or war in cyberspace will be easier to promote if they build on and fit with existing norms about discrimination, proportionality and non-combatant immunity.

Many potential cyber norms might be complementary – they might deal with different types of cyberspace problems and thus might rarely conflict. For example, cyber norms about warfare are not likely to conflict with cyber hygiene norms. In some situations, though, we should expect stakeholders to propose opposed or conflicting norms that reflect their different values and goals. For example, Western states have generally promoted Internet freedom norms that require unfettered access to

online information and freedom of expression. Such norms conflict with many of the "information security" norms being proposed by authoritarian states like Russia and China. Information security, for authoritarian states, often means restricting both freedom of expression on the Internet, and access to information emanating from sources considered hostile, such as political dissident groups. To authoritarian states, Internet freedom, as the West understands it, is a threat and may constitute an act of ideological aggression against other states' core interests. Western states, by contrast, object to efforts to "secure" or restrict information in this way as a violation of basic rights.

Simply articulating new norms is not enough to change behavior. Norms need adherents, and actors will lobby hard for their preferred norms, looking for support. The process might be thought of as a "norm marketplace" in which U.S. cyber norms compete with Chinese and Russian ones, or military cyber norms compete with norms that focus on commercial and free speech.

Like products in a market, new cyber norms will compete, both with other norms and for time and attention of stakeholders whose support is required to change behavior. Changing expectations, attitudes and ultimately behavior takes work. Norms often fail, not because anyone particularly dislikes them, but for lack of enthusiasm. The size and power of the norm promoter will also influence its success. The United States clearly has advantages here. American power means people will pay attention to U.S. norm preferences and may allow the United States to induce or coerce others into following. Of course, the content of the norm, itself, may influence its success. Norms that make technical sense in addition to promoting popular values should have an advantage. Thus, which norms are adopted by which actors depends on a variety of factors – the content of the norms, the power or politics of their sponsors and the characteristics and needs of adopters.

One can imagine several possible outcomes to a competition and selection process. Clear winners might emerge; perhaps some variant of "national responsibility" for all cyber activity on one's soil would be widely accepted. Several winners might emerge. We could get "norm blocs" if large groups of countries or companies cluster, each focused on a different norm. Some of the related norms onto which cyber norms could be grafted have this "bloc" character. Different European Union (EU) and U.S. norms about privacy, for example, are two such competing norm frameworks. This creates some conflict, as indicated by debates post-9/11 over sharing airline passenger information, and the result may not be entirely stable. Norm cultivation processes also often get stuck at suboptimal equilibria. Think about the United States' continued adherence to non-metric systems of measurement. Perhaps there are no winners, which could leave us with no "shared expectations of appropriate behavior" at all. Thus, the norm cultivation process may never leave this promulgation stage.

One way to intervene in this process might be to devise forums in which to negotiate norm definitions. Again, this could unfold in more and less centralized ways. A centralized apex process to negotiate wide-ranging cyber norms would have the virtue of broad participation and, theoretically, the ability to harmonize norms across different cyber issues. It would probably also be extremely slow and have trouble keeping up with the dynamic cyber environment. Negotiations over the U.N.'s Law of the Sea Treaty might be an example of this kind of centralized norm promulgation process. It had broad participation and scope, but the process took years (or decades, depending on how you count) – something that makes no sense for cyber issues.[3] It would probably also be a largely intergovernmental endeavor, which may raise hackles in a policy domain with a tradition of minimal government interference.[4]

A more decentralized approach might involve different forums for different kinds of actors (e.g. states) or different forums to negotiate different kinds of cyber norms (e.g. commercial vs. military). Again, using existing institutions and structures might be useful in this regard. Already we can see groups of actors beginning to negotiate new cyber norms. For example, NATO has provided a forum for discussing these issues among its members. Getting cyber norms on the agendas of other regional and functional bodies might also be useful. These smaller bodies might move more quickly both because of smaller numbers but also because the members often share concerns and are more likely to reach some agreement. Of course, the risk is that decentralized promulgation might produce conflicting norms, which may cause trouble down the road.

The normative architecture of some existing forums may be especially attractive for promoting particular cyber norms. For example, Internet freedom advocates have put forth clever proposals to tie the free flow of, and access to, online information with international trade regimes (making Internet repression a non-tariff trade barrier), allowing democratic states to use the World Trade Organization's dispute arbitration mechanism to deter authoritarian governments from censoring online information.[5]

One thing to note: complete agreement or some flagship formal treaty may not be required for big multilateral negotiations to have an impact. Multilateral negotiations can influence norms even without unanimity. Simply publicizing preponderant agreement among important parties can create focal points around which other actors begin to organize. The negotiation process can also have benefits if it forces actors to improve clarity on at least some components of the norm where there is substantial, if not complete, agreement. The 1997 Ottawa Treaty, banning certain landmines, did not obtain signatures from key states (the United States, China and Russia) but clarified the norm, spelled out obligations, and disseminated it widely, shaping public opinion on the issue. Faced with a new, clear norm, U.S. procurement policies and behavior on this issue started to change, even if its signatory status has not. Similarly, the International Criminal Court has enjoyed cooperation from non-signatories like the United States, which found it a useful tool for handling atrocities in Sudan and Sierra Leone.[6] Big multilateral negotiations can also inspire productive track two efforts among non-governmental experts that can then facilitate broader agreement. An example of this kind of synergy may be the recent U.S.-Russian negotiations sponsored by the East-West Center that applied the Geneva and Hague conventions to cyber conflicts, prompted in part by Russia's efforts at cyber arms control at the U.N.[7] The norm negotiation process may thus have value in and of itself, regardless of the outcome.

Norm dissemination. Once promulgated, norm cultivators need to think about ways to spread the new cyber norms globally. The task at this stage would be to persuade (or coerce) more actors to adopt the norm. One can think of this task as having two dimensions – breadth and depth.

One goal of norm dissemination is usually to attract adherents and broaden the norm's reach. For cyberspace, this would seem to be particularly important. A constant worry is that networks are often only as robust as their weakest nodes. Getting all nodes in the network on board with new cyber norms would seem an obvious priority. If the norms apply to states, one would want to attract Nigeria, Ukraine, China and Russia – countries that may be skeptical of new cyber norms and may be sources of cyber problems – as well as the Organisation for Economic Co-operation and Development (OECD) countries. There may be a private sector analog to this. Big, well-heeled corporate actors with reputations to defend may be quicker to see benefits in adopting "good cyber citizen" norms (or may have more to lose from a crackdown and active enforcement). Smaller, fly-by-night enterprises may be harder to attract.

One persistent problem with norm dissemination is that the actors least in need of the norm are the first to adopt; actors who most need to adopt are often the recalcitrants. This is not surprising. Adopting a norm is easy if its requirements mostly line up with your preferences and current practices. Costs of adoption may be relatively low and desire to comply may be relatively high. The reverse would be true for actors whose current behavior most flagrantly violates the proposed norm. One advantage to the large group negotiation as a means of developing and promulgating a norm may be that the norm has wide adherence and dissemination at the time it is promulgated. (Indeed, it is being promulgated precisely because many actors have signed on.)

Another goal of cyber norm dissemination will almost certainly have to be expanding the depth of the norm's reach and its penetration into state and corporate actors. Getting national governments to adopt the norm may not be enough. State, provincial and municipal governments will also have a role to play if cyber norms are to be successful. So, too, will national companies, nongovernmental organizations and all other civil society actors. Similarly, getting corporate CEOs to agree with these norms may be easier than getting all the subsidiaries and suppliers to implement them.

Adherence from these smaller and more local actors may be less of a problem if national governments legislate norm compliance for all subsidiary governments in their jurisdiction. This happy outcome would require that national governments have both the power and the will to legislate. They may not. If they do legislate, however, the norm cultivation problem becomes a law enforcement problem, which lies more in the realm of implementation.

Norm institutionalization and implementation. Even after broad rhetorical and policy acceptance of new cyber norms at all levels, promoters of new norms will have to think about ways to ensure compliance. This is notoriously difficult and implementing major new norms is almost always an incomplete and continuous process. One should expect cyber norms to be no different.

One persistent problem with norm dissemination is that the actors least in need of the norm are the first to adopt; actors who most need to adopt are often the recalcitrants.

One source of potential lessons for cyber norm promotion might be efforts at "mainstreaming" new norms about gender, environment, corruption and other social goals at big international institutions. For gender concerns, the U.N. defines "gender mainstreaming" as: "Ensuring that gender perspectives and attention to the goal of gender equality are central to all activities…"[8] What we want in cyberspace is presumably something like cyber mainstreaming. We want awareness of cyber security issues and organizational rules mandating appropriate preventive measures (that presumably involve compliance with the new norms) to penetrate all levels of adhering organizations, be they states, corporations or civil society groups.

Big international organizations like the U.N. or U.S. government agencies often are given new jobs or are assigned new normative concerns. The common result of these dictates from the top tends to be superficial adherence. Organizations adopt the rhetoric or even the rules of compliance with the norm, but do not change the way they behave or actually implement the rules on the ground. Often this is not the result of active resistance or evil intent. Bureaucrats are busy. They have many other

things to do besides implement new directives, which may not come with clear guidance, additional funds or technical support, to say nothing of additional hours in the day. The result is not surprising: new norms often get lip service, sometimes extensive lip service, from organizations but little meaningful implementation.[9]

Strategies to avoid this problem, at least in part, might flow from an understanding of these problems facing bureaucrats. Funding and technical assistance will almost certainly have to be part of this effort for global cyber norms. This is true on both the breadth and depth dimensions, discussed earlier. Many of the countries the United States worries about as potential sources of cyber crime or cyber attack lack the laws but also lack the basic infrastructure – personnel, equipment and expertise – to ensure basic cyber hygiene. Figuring out the best way to help them help themselves (and the United States), both technically and financially, will be important. One obvious question is whether this assistance is best organized bilaterally, which would give the United States control over the funds it gives and the uses to which these are put, or multilaterally, which could spread out the costs and make assistance acceptable in more places.

Inside norm-adhering states, similar assistance may be needed. Apex actors, for example federal government bureaucracies centrally involved in cyberspace issues like the Department of Defense (DOD), may be able to implement new cyber norms on their own, but this is unlikely to be true at state and local levels, nor will it be true of the vast array of civil society and business actors using networks in the United States. Enforcement through well-formulated laws can help. Indeed, effective laws will be essential to a broad and deep norm implementation strategy. But even laws will be ignored if people do not know how to comply with them or do not have the funds to comply. Even when they have both knowledge and means, there will still be a non-trivial group of distracted, lazy or obstructionist citizens. Reducing the size of this group would improve norm success. Making it easier for people to "do the right thing" does not guarantee good outcomes. However, good outcomes seem almost impossible if compliance is difficult.

Relevant Features of Cyberspace

Every norm cultivation process is unique and the content of the norm being proposed matters to its success. So, too, do characteristics of the issue area that the norm is supposed to influence. Two issues are worth considering. Both flow from the ubiquitous nature of the Internet.

One distinctive feature of this policy arena is the diversity of stakeholders. Since the Internet touches almost everyone, almost everyone has an interest in, and views about, how cyberspace is governed, especially the military, businesses and civil society groups. Normative frames likely to be developed by these three sectors (which are not homogeneous) are very different and they are likely to champion very different kinds of cyber norms. The United States Cyber Command may think about cyber security norms as a "laws of war" issue. Economic actors are likely to think about cyber security norms as a crime issue. Civil society groups may be vocal about privacy and Internet freedom issues. These broad orientations will conflict at times and norm promoters will have to figure out how to handle this.

If norm development follows a decentralized path, these different actors may be able to promulgate their own norms inside different forums. But this, too, may create problems. Some of these stakeholders will find it easier to organize and promote their norms than others. DOD is out in front on this issue and is likely to develop, articulate and institutionalize its cyber norms internally long before civilians get organized.

This may matter because path dependence looms large in norm development; there are big "first mover" advantages. Once one set of norms is in

place, in this case military laws-of-war norms, they tend to color and in some ways perhaps constrain subsequent norm development by civilian actors. How, exactly, will DOD operationalize the details of discrimination, proportionality and non-combatant immunity in cyber conflicts? Will these be norms that the human rights community share or prefer? How might espionage be operationalized by the military in cyberspace? Would those be the norms preferred by business? Or by citizens' groups? These may not be a big problem, depending on one's goals and concerns, but it is worth some thought. The alternative – telling the military to hold off on cyber norm development until civilians get their acts together – seems politically unlikely and possibly dangerous given the rate at which civilians move on these things. External cyber attackers are not likely wait for our norm cultivation process to bear fruit.

The pervasiveness of the Internet and cyber issues, themselves, may shape the norm cultivation possibilities and prospects in other ways as well. Most norms govern domains that are more bounded. There is some discrete and usually limited population of stakeholders who care about the issue, whom the issue effects, and who are essential to change. These limits make the norm cultivation process more manageable. With cyberspace, by contrast, it may be hard to figure out who is not relevant to the process or essential to change.

This need for very broad involvement in solving cyber problems is challenging, but not unique. Other analysts have explored the policy effects of this pervasiveness of cyber concerns with a very good and helpful analogy to public health.[10] They point out that cyber attacks are like pandemics and can be averted by using similar methods. This is useful. It focuses our attention on crucial features of the problem – cyber's penetration deep into all aspects of society, the importance of prevention and good cyber hygiene, the deeply interconnected nature of the cyber world and dependence of each actor on good behavior by all others. This is a very happy analogy since no one is in favor of illness.[11] Yet a different analogy might give more caution.

Getting people to care about threats that seem abstract and distant to most of us (like climate change) is extraordinarily difficult.

Promoting cyber security and good cyber norms may also be like combating climate change. In important ways, cyberspace may be like carbon. Both are foundations for nearly all aspects of contemporary life. Modern militaries, business and social interactions depend on functioning networks and cheap carbon. You cannot fight a war, protect the nation from threats or run an economy without both. Yet both are associated with huge threats. Predictions about the potential damage from cyber attacks are catastrophic, as are predictions about the consequences of unabated carbon release.

Unfortunately, the fate of norms to prevent climate change is not encouraging. Formulating norms that command broad support by even a small numbers of apex actors (i.e., national governments) has been difficult. Achieving any kind of deep norm adoption or compliance inside societies is not faring much better. Getting people to care about threats that seem abstract and distant to most of us (like climate change) is extraordinarily difficult. Getting people to accept even modest short-term costs (higher gas prices, fuel efficient cars) to prevent long-term catastrophe is difficult. If those things are required for cyber norms, we should be worried.

Neither of these comparisons (cyberspace and health, cyberspace and climate change) are exact. It may be that the greater military concern with cyberspace will help put it on a different path from climate change. But the climate change analogy does suggest just how hard it may be to formulate and implement new norms that require cooperation of such a broad swathe of society.

Prospects for Norm Development: Two Examples

The foregoing analysis does not let us predict which norms will succeed or fail, but it does focus our attention on likely problems that norm promoters may encounter. Diverse stakeholders have proposed a variety of cyber norms. Each will face different challenges, as the following examples illustrate.

Civilian protection and minimization of collateral damage are widely accepted by all states as foundational norms of war. Following the grafting logic, outlined above, a number of analysts have explored ways to translate these norms into the cyber domain. The norms themselves are fairly clear – no harm to civilians, minimize collateral damage – and their rationale or utility would be the same as in kinetic, physical combat ("I don't kill your civilians, you don't kill mine.") Much of the debate here surrounds "do-ability" and technical obstacles to controlling effects of different cyber attacks (for example, cascading network failures). While attackers certainly have obligations to be concerned about these, the laws of war have always involved cooperation from potential victims to minimize damage as well. Hospitals and medical personnel must identify themselves if they want non-combatant immunity, for example. Promoters of cyber norms in this area might improve their prospects, then, with a multipronged approach: They could focus both on ensuring military targeting plans with an eye to ensuring civilian safety, but also on civilian planning to minimize entanglement with potential military targets. Protocols to share information about civilian systems and reduce opacity about them might also enhance compliance and, again, would very much conform to extant norms in physical space.[12]

Norms supporting Internet freedom will also present obstacles. At a basic level, efforts to secure the Internet are likely to involve some kind of regulations, limits and control. How national governments define "cyber security" and how they implement those understandings could thus place limits on online freedom of expression, and so create conflict over basic Internet norms. Opposing interpretations of cyber security by the United States and authoritarian governments such as Russia and China, mentioned earlier, are just one example. Disagreements will also surface between the American vision and that of our closest allies who exercise greater limits on free speech.[13] The United States, for example, did not sign the Additional Protocol to the European Convention on Cybercrime even though it ratified the convention. The Additional Protocol sought to harmonize domestic laws by making online racist and xenophobic acts a criminal offense, which the United States found to be contradictory to U.S. constitutional guarantees of free speech.[14] Such differences may make it difficult for norm promoters to achieve clarity about cyber security norms. Successful efforts to disseminate norms that comport with U.S. values must clearly distinguish efforts to secure basic infrastructure and networks from efforts to censor or control access to Internet content (to which the United States objects).

Attempts to align norms about Internet freedom with corporate business practices will be difficult as well, given the potential economic tradeoffs involved. Asking information technology companies to ignore foreign government requests for Internet user data could result in suspension or revocation of those companies' licenses, cutting off their access to those markets. "Do-ability" could thus be a big challenge for Internet freedom norms in an authoritarian state such as China,

which has eclipsed the United States as the world's largest Internet market with more Internet users than there are U.S. citizens. Some companies have already taken it upon themselves to articulate codes of conduct for responding to information requests and protecting their users, but these efforts need to be broadened and include more corporate stakeholders. Proactive steps from the private sector could also help give them some flexibility and leverage when negotiating with foreign governments. The fact that these companies are employing these practices on their own, for business reasons and not at the request of the U.S. government, could help insulate them from claims by authoritarian regimes that these companies are merely agents of U.S. statecraft. A private sector-led negotiation about business norms in cyberspace would therefore be a logical track to pursue.

ENDNOTES

1. Greg Rattray, Chris Evans, Jason Healey, "American Security in the Cyber Commons" in Abraham M. Denmark et al, eds., "Contested Commons: The Future of American Power in a Multipolar World, " Center for a New American Security (January 2010).

2. Definitions in social science often add a clause: Norms are collective expectations of proper behavior *for an actor with a given identity.* This amendment might be important if we want different cyber norms to apply to different types of actors. For example, the cyber norms one wants to cultivate for governments may differ from the norms one wants to cultivate for business or individuals. To the extent that what is normatively appropriate for one type of actor may not be appropriate for another, this extended definition could be useful.

3. The first U.N. Conference on the Law of the Sea (UNCLOS I) began in 1956. UNCLOS III produced a convention in 1982 that came into force in 1994.

4. Of course, creating a bigger role for government may be precisely the goal of some actors. For those suspicious of U.S. dominance in cyberspace, intergovernmental negotiations in a one-state, one-vote system like the U.N. might be very attractive. This kind of "forum-shopping" is common in norm promulgation processes.

5. "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information," Google, Inc. (15 November 2010): 8, http://googlepublicpolicy.blogspot.com/2010/11/promoting-free-trade-for-internet.html.

6. Vijay Padmanabhan, *From Kampala to Rome: The U.S. Approach to the 2010 International Criminal Court Review Conference*, Council on Foreign Relations Special Report No. 55 (April 2010).

7. Karl Frederick Rauscher and Andrey Korotkov, *Working Toward Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace,* East-West Institute (January 2011), http://www.ewi.info/working-towards-rules-governing-cyber-conflict.

8. U.N. Women, "Gender Mainstreaming," http://www.un.org/womenwatch/osagi/gendermainstreaming.htm.

9. For an excellent analysis of this kind of "organizational hypocrisy," see Catherine Weaver's study of the World Bank's efforts to implement reforms. Note that one of the ironic but often validated predictions of the theoretical work on organizational hypocrisy is that rhetoric about norm compliance may be inversely related to actually implementation. Talk becomes a substitute for action and a strategy (often a successful one) for obfuscating non-compliance. Catherine Weaver, *Hypocrisy Trap: The World Bank and the Poverty of Reform* (Princeton, N.J.: Princeton University Press, 2008); Nils Brunsson, *The Organization of Hypocrisy*: *Talk, Decisions, and Action in Organizations* (New York: Wiley, 1989).

10. Greg Rattray, Chris Evans, Jason Healey, "American Security in the Cyber Commons" in Abraham M. Denmark et al, eds., "Contested Commons: The Future of American Power in a Multipolar World, " Center for a New American Security (January 2010).

11. Biowarfare is, of course, a concern, but most pandemics to date have not been purposefully instigated by humans as a tool of either statecraft or terror, or as a criminal effort for financial gain.

12. Martin Libicki, "Pulling Punches in Cyberspace," in Committee on Deterring Cyberattacks, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academies Press, 2010): 123-147.

13. While the United States has some limits on free speech (speech involving child pornography, slander, perjury and "fighting words" is illegal online or off) its free speech laws are generally stronger than those of other major countries. Germany, for instance, prohibits Holocaust denial online and France does not allow the sale of Nazi paraphernalia online. The United States does not exercise these kinds of restrictions. For a more detailed discussion of this issue, see Richard Fontaine and Will Rogers, "Internet Freedom and It's Discontents: Navigating the Tensions with Cyber Security" in this volume.

14. See "Council of Europe Convention on Cyber Crime: Frequently Asked Questions and Answers," U.S. Department of Justice, http://www.justice.gov/criminal/cybercrime/COEFAQs.htm#QA8.

CHAPTER VII:
CYBER SECURITY GOVERNANCE: EXISTING STRUCTURES, INTERNATIONAL APPROACHES AND THE PRIVATE SECTOR

By David A. Gross, Nova J. Daly, M. Ethan Lucarelli and Roger H. Miksad

America's Cyber Future

Security and Prosperity in the Information Age

CYBER SECURITY GOVERNANCE: EXISTING STRUCTURES, INTERNATIONAL APPROACHES AND THE PRIVATE SECTOR

By David A. Gross, Nova J. Daly, M. Ethan Lucarelli and Roger H. Miksad

From its start as a mechanism for academic exchange, through the growth of e-commerce and bottom-up cultural productions, the Internet has become an essential component of a well-functioning modern society. However, as its utility and ubiquity have grown exponentially, so too have the vulnerabilities that it has created. Companies, individuals, governments and nongovernmental organizations at the local, national and international levels have fallen victim to cyber attacks. The issue of where actors should turn for protection and redress from these attacks is extremely complex and raises the question: Who and what governs cyber security?[1]

Much of the relevant literature is hampered by the misconception that the problems of cyber security governance are so unique and unprecedented as to require entirely new solutions and structures. This view stems from addressing it as strictly a "cyber" problem rather than a problem of "governance." Further, there is a general perception that the Internet presents a materially different set of problems because its use has come about so quickly and broadly and outpaced existing governance structures that have not adapted adequately to its challenges. However, one thing is clear – cyber systems are technologies. Like all widely-used technologies, such as the telephone and the automobile, cyber systems are less a radically new problem in search of a radical new solution and more a set of complex and interrelated issues best addressed through an existing matrix of governing structures.

As such, the most expedient and effective way to address cyber security governance is to first take stock of existing and available governance tools and structures. Significant national, regional and international governance structures – both formal and informal – can be used to provide cyber security governance are already in place. By identifying the most capable among these, governments and other actors can determine how

best to direct their attention and resources, where to broaden the role of existing structures and whether to create new structures.

As nations build their cyber security capabilities, it will become apparent that international efforts will need to supplement national solutions. After all, the Internet is international in nature. Multiple international fora and organizations exist as venues for discussions of the challenges that nations face, and foster the development and coordination of strategies to address them. To determine which fora and organizations are best suited to address cross-border cyber security concerns, a thorough evaluation of core competencies is necessary, including an assessment of how well these groups build and enforce norms and rules.

Importantly, the private sector must take a leadership role to help establish effective strategies for addressing cyber security governance and capacity building at every level, nationally and globally. This is not only because the private sector owns the vast majority of Internet infrastructure, but also because the private sector has unique expertise, experience and capabilities (in many instances more advanced than governments) to develop effective policies and to create efficient market-based solutions wherever possible.

This chapter proceeds as follows. First, we discuss broadly what nations are doing presently to enhance cyber security and why their efforts necessitate international engagement. Section two examines a number of significant international groups that address cyber security, describes their current roles in cyber security governance and provides some analysis of their strengths. Section three outlines a framework for building cyber security governance through a systemic analysis of core competencies and an evaluation of norm building and enforcement capabilities. Section four addresses the role of the private sector, especially how and where it should become more engaged in cyber security policymaking. Finally, we offer some closing thoughts.

What Nations Do and Where They Fall Short

National governments undoubtedly have the most direct power over cyber security governance, and they express and implement this power in many ways. While this power can be vast, it is also limited, not only by the international architecture of the Internet but also by the breadth and depth of each nation's cyber security capabilities.[2]

National cyber security policy is typically expressed through three main vehicles: domestic Internet policy, the development of offensive and defensive cyber military capabilities and international diplomacy. Given the global nature of the Internet, the approaches taken by different governments in each of these areas – reflecting to some extent their national political ideologies and policy agendas – can affect international debates over cyber security governance directly.

DOMESTIC POLICY

To the extent that national governments have efficient and effective national cyber security strategies, they can improve domestic and global cyber security by building the capacity of their existing governing structures to limit the spread of cyber attacks and the damage they cause. Toward that end, many countries are designing and implementing national cyber security strategies to coordinate their internal security efforts and develop effective tools. For example, one of the primary challenges identified by President Obama's May 2009 cyberspace policy review is the lack of a uniform understanding of the authority and mandates of the various executive agencies that have a role in strengthening and managing U.S. cyber security policy.[3] In response, the executive branch took steps to prioritize the building of cyber security capacity and organized various agencies to implement cyber security policy. A cyber security coordinator position was created at the White House and executive departments were empowered to strengthen their capabilities. However, without clear mandates, agency turf battles arose

and separations between domestic and defense approaches to cyber security became more attenuated. In an effort to clarify jurisdictional mandates and roles, Congress has introduced multiple legislative initiatives, including some that seek comprehensive solutions. However, there too, jurisdictional issues have stalled efforts, and the complex, crosscutting and international nature of the Internet has complicated the establishment of clear governance prescriptions and the passage of comprehensive legislation. While it is widely agreed that some measure of increased central coordination of federal cyber security efforts is needed, the U.S. government should ensure that it makes full use of existing governance structures, agencies and powers to bolster cyber security capacity until a unified strategy is enacted.

Beyond improving central coordination of national cyber security efforts, one of the most significant areas of domestic policy to affect international cyber security governance is the enforcement, or lack thereof, of criminal laws regarding cyber malfeasance. For example, in 2000, the Philippines Department of Justice dropped charges against the creator of the "ILOVEYOU" virus, even though it caused billions of dollars of damage, because existing criminal laws in the Philippines did not apply to computer hacking. Today, the United States and many other countries are signatories to the Council of Europe Convention on Cybercrime, an international treaty that seeks to harmonize international laws on cyber crime and to promote international cooperation. Without effective cyber crime laws, cyber attackers might escape prosecution by basing themselves in countries that do not punish or extradite for their offenses.

DEVELOPMENT OF OFFENSIVE AND DEFENSIVE CYBER MILITARY CAPABILITIES

Another vehicle through which nations build cyber security capacity and develop its governance is under the rubric of cyber defense and warfare. The United States has bolstered its capabilities through the creation of the U.S. Cyber Command, which unifies many of its offensive and defensive cyber activities. In doing so, it has created a clearer structure to not only protect U.S. defense structures and information systems, but also to streamline policy and engage foreign partners. Other nations have also built and consolidated their defensive and offensive cyber military capabilities. The United Kingdom's armed forces are seeking to establish a cyber command that would both protect domestic interests and have the capability to launch counter attacks. China, for its part, has aggressively developed its military cyber capabilities and has instituted programs to integrate the networks and capabilities of its service arms.

However, the enlargement and consolidation of offensive and defensive military cyber security capabilities raise two significant problems. The first is the dichotomy between domestic and military cyber systems. For instance, while Department of Defense's (DOD) Cyber Command chief, GEN Keith Alexander, has stated that the military intends to rely heavily upon civilian agencies and industry to protect non-military national cyber resources, the United States may be too starkly dividing coordination of securing civilian and military assets. Such a division could lead to confusion and, in turn, burden the private sector by forcing it to expand significant efforts to meet parallel requirements. Some policies that the Cyber Command may institute to secure the broad military industrial complex may create overlapping cyber security requirements for the private sector, especially critical infrastructure and industries that service such infrastructure. Understanding this potentially significant problem, the DOD and the Department of Homeland Security (DHS) recently signed a memorandum of agreement to begin to bridge current overlaps and to deal with potential future redundancies.[4] However, tensions will inevitably arise as the military's cyber systems rely on classified networks that must also be safeguarded by private industry.

A second problem arising with the growth of military cyber capacity is the creation of new and greater insecurities. Governments are developing the offensive and defensive capabilities to launch or repel large-scale cyber attacks directed at national critical infrastructure through their cyber warfare programs. Some in the media have speculated about potential military or intelligence origins of prominent cyber attacks, such as the Stuxnet virus, and the 2008 cyber attacks on websites in the nation of Georgia.[5] As nations and rogue actors build their offensive capabilities, traditional military dangers loom that much larger given the broad dependence that countries have on the Internet. A cyber war could have catastrophic consequences. Given the relative ease with which attacks can be taken through the Internet without attribution, actions by non-state actors could easily trigger state-to-state escalation under false pretense. Thus, nations should seek international agreements that would constrain offensive action. The rhetoric of cyber defense is prominent in international debates about cyber security, and military research and priorities are likely to continue to drive cyber security development as well as insecurities.

INTERNATIONAL DIPLOMACY

Domestic and military efforts contribute to building cyber governance (though not always), but they are insufficient for solving what is essentially a global problem requiring global engagement and global solutions. Because enjoyment of the full economic and cultural benefits of the Internet necessitates a certain level of openness, the risk of cross-border cyber attacks is impossible to eliminate. Even mitigating this risk requires some level of international coordination.

National governments can play a key role in cyber security governance through their diplomatic efforts. They make up the membership of various intergovernmental organizations in which policy issues are discussed, norms are created and international agreements are struck.[6] Participation and advocacy in these organizations is a primary mechanism for national governments to shape the development of international cyber security governance.

Because enjoyment of the full economic and cultural benefits of the Internet necessitates a certain level of openness, the risk of cross-border cyber attacks is impossible to eliminate. Even mitigating this risk requires some level of international coordination.

Different countries focus on international cyber security diplomacy to varying extents and with divergent goals. For example, Russia has sought agreement on an international treaty on cyber warfare for years. In the United States, the Obama administration stated its goals in the Cyberspace Policy Review, and called for an increased focus on working with other countries to address the challenges of network security.[7] The State Department is addressing important international cyber issues, and it has established a coordinator for cyber issues who is leading the department's cyber security initiatives and acting as a primary liaison to the White House.[8]

While nations are beginning to take useful steps to engage on cyber security matters internationally, for the most part these efforts remain embryonic and insufficient in light of the global dependencies and vulnerabilities that the Internet has engendered. Given such vulnerabilities, it is important that nations take stronger action

internationally. However, determining where to turn for international answers and solutions requires serious reflection.

The Roles of International Entities

Despite the best efforts of national governments to address cyber security domestically, the global and diffuse nature of cyber threats necessitates international coordination.[9] International coordination can take many forms, including bilateral agreements between nations; informal working groups composed of public, private and academic thinkers; and formal multilateral agreements on international policy. To adequately address cyber security, it is likely that each of these forms of international collaboration will be necessary.

Much of this work is already underway. The problem today is not that there are too few international groups involved in Internet policy deliberation and/or governance. Rather, efforts toward constructing, promulgating and reinforcing international cyber security norms are hindered by resource inefficiency and lack of clarity regarding who is responsible. To efficiently devote resources toward norm creation and policy implementation, it is important to understand the current international governance environment. Below we introduce two of the more significant types of international governance organizations – intergovernmental organizations and international Internet technical organizations – and assess their relative strengths.

INTERGOVERNMENTAL ORGANIZATIONS

Many intergovernmental organizations (IGOs) focus on international cyber security issues. These IGOs vary dramatically in their size, subject matter expertise, authority and perceived legitimacy. They range from global treaty-based organizations with broad mandates, such as the United Nations, to fora for discussing regional economic and political issues with no formal policymaking authority, such as Asia-Pacific Economic Cooperation (APEC).

Intergovernmental organizations bring officials from different nations together to discuss conflicting policies and practices, and to craft strategies for possible domestic and transnational implementation. These organizations also provide a forum for the production and dissemination of research.

Similar to struggles on the national level, cyber security policymaking by IGOs has suffered from a lack of clarity with respect to the appropriate authority and expertise among the various organizations. Because the development of Internet technology and the Internet economy has broad application and relevance, many different organizations have launched cyber security initiatives. In some cases the efforts are complementary in that they address different aspects of the issue or focus upon different regions. However, in other cases, the efforts of these groups are redundant or even conflicting, with jurisdictional struggles or political differences among the groups. To give a sense of the spectrum of the work already underway, in Table 1 we briefly identify a number of IGOs that are addressing cyber security policy, discuss examples of how they approach the issues and offer some observations about the respective strengths of each organization.

INTERNATIONAL INTERNET TECHNICAL ORGANIZATIONS (IITOS)

Management and development of the Internet's technical protocols, standards and processes are conducted largely through a number of intertwined international nonprofit corporations and organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C). The memberships of these groups are primarily made up of researchers and scientists from the academic, private and public sectors. Although some of these groups evolved out of U.S. government-led projects, they are independent and strive to represent multinational stakeholders.

TABLE 1: SURVEY OF INTERGOVERNMENTAL ORGANIZATIONS

IGOs	MEMBERSHIP	GOVERNANCE/ LEGAL AUTHORITY	CYBER SECURITY ACTIVITIES	STRENGTHS
United Nations	The U.N. has 192 member states, including nearly every recognized sovereign nation in the world.	An international treaty-based organization with legal authority in matters of international security and an important consensus-building function on a wide range of international policy issues.	U.N. reports have addressed cyber crime, such as the July 2010 report and recommendations on "Developments in the Field of Information and Telecommunications in the Context of International Security." The U.N. organized the World Summit on the Information Society that resulted in nonbinding agreements on cyber security and created the Internet Governance Forum.	The U.N. is unique among IGOs in the scope of its international participation and mandate. The U.N. has an extremely broad membership and a high level of international legitimacy that makes it a useful forum for generating multinational consensus on high-level policy matters.
International Telecommunication Union (ITU)	The International Telecommunication Union is an affiliate of the U.N. It also allows for participation of industry and private individuals.	A treaty-based organization involved in coordination and policymaking related to issues of international telecommunications.	The ITU has identified "five pillars" in its Global Cybersecurity Agenda: legal measures, technical and procedural measures, organizational structures, capacity building and international cooperation. The ITU is also addressing cyber security through its standards development work.	Because of its well-established structure, technical expertise and broad experience with communications issues, the ITU is likely to have a significant role in future international cyber security policymaking.

TABLE 1: SURVEY OF INTERGOVERNMENTAL ORGANIZATIONS

IGOs	MEMBERSHIP	GOVERNANCE/ LEGAL AUTHORITY	CYBER SECURITY ACTIVITIES	STRENGTHS
European Union (EU)	The EU is a group of 27 member states.	A governing body with authority to enact binding policy on issues of trans-European economics, environmental protection, consumer protection, social justice and other matters.	The EU has passed relatively rigorous directives on electronic commerce, data protection and privacy and electronic communications. The EU's "Digital Agenda for Europe" includes trust and security as a main policy pillar for development over the next ten years.	The EU's institutional strength lies in its ability to create uniform policy across its membership through the adoption of binding legislation on issues within its subject matter jurisdiction. Although the EU's legislative power extends only to its membership, as a result of the global importance of the European market, EU policies have significant influence far outside the borders of the EU.
Council of Europe	The Council of Europe includes 47 mostly European member states and five observer states.	A forum that works through multilateral agreements and conventions that must be ratified as treaties and implemented by national signatories.	The Council of Europe Convention on Cybercrime is one of the most comprehensive multilateral agreements attempting to establish uniform laws prohibiting criminal activity on the Internet. However, of the 46 signatories, 17 countries have failed to implement the agreement domestically.	The Council of Europe Convention on Cybercrime offers a useful model of one type of multilateral agreement that could be of use in implementing a consistent international approach to cyber security governance.

TABLE 1: SURVEY OF INTERGOVERNMENTAL ORGANIZATIONS

IGOs	MEMBERSHIP	GOVERNANCE/ LEGAL AUTHORITY	CYBER SECURITY ACTIVITIES	STRENGTHS
Organisation for Economic Co-operation and Development (OECD)	The Organisation for Economic Co-operation and Development includes 34 member states from across the globe.	A forum focused on producing research and developing policy recommendations primarily concerned with economic and social issues. OECD initiatives can lead to agreements among member countries.	Cyber security has been an important part of the OECD's work regarding the Internet for many years. These issues were a primary focus at the OECD ministerial meeting on The Future of the Internet Economy held in June 2008 in Seoul and the resulting "Seoul Declaration for the Future of the Internet Economy."	The OECD is widely respected as a thought-leader, producer of quality analysis on a variety of issues, and forum for the generation of consensus on high priority issues of international policy. Although the OECD does not create binding rules, its work is likely to play an important role in helping governments, IGOs and the private sector identify more clearly issues and policy options to create and enforce norms.
Asia-Pacific Economic Cooperation (APEC)	APEC is a forum comprised of 21 member economies with Pacific Ocean coastlines.	A forum for discussion of economic and social issues and the development of policy recommendations for its member economies.	APEC's Telecommunications and Information Working Group in its 2010-2015 "Strategic Action Plan" identified as a key priority the need to "Promote a Safe and Trusted ICT Environment." It intends to accomplish this through the promotion of effective policies, information sharing, technical cooperation, increasing cyber security awareness and collaboration with the Internet technical community and private sector.	APEC has historically had some success in developing consensus amongst its members on high-level policy principles that can form the basis for further discussions among and within member economies.

TABLE 1: SURVEY OF INTERGOVERNMENTAL ORGANIZATIONS

IGOs	MEMBERSHIP	GOVERNANCE/ LEGAL AUTHORITY	CYBER SECURITY ACTIVITIES	STRENGTHS
The North Atlantic Treaty Organization (NATO)	NATO is comprised of 28 member countries.	A treaty based organization primarily designed for the collective defense and military cooperation of member nations.	In November 2010, NATO adopted a new "Strategic Concept" to serve as the organization's roadmap for the next decade and includes cyber defense as a key component.	NATO has resources and expertise that will make it important for efforts to develop international cyber defense capabilities. NATO will continue to play a "front line" role in defending alliance members against potential cyber attacks and in researching and developing new innovations in cyber defense.
Organization for Security and Co-operation in Europe (OSCE)	The Organization for Security and Co-operation in Europe is comprised of 56 member nations; OSCE has global membership despite being Europe-focused.	The world's largest regional security organization, offering a forum for political negotiations and decision-making in the fields of early warning, conflict prevention, crisis management and post-conflict rehabilitation.	The OSCE has held a number of forums and workshops designed to find a common approach to enhance cyber security among its members.	OSCE is Europe-focused, but has a global membership with a specific focus on security issues.

Some nations have questioned the legitimacy of the IITOs over the years. Much of this criticism stems from a perception of close ties between these Internet technical groups and the U.S. government. Although each of these groups now purports to operate independently of any one government, until recently many of these organizations were indeed closely tied with, or even a part of, the U.S. government. For example, the Internet Architecture Board (IAB) and the Internet Assigned Numbers Authority (IANA) both initially grew out of formal initiatives of the U.S. military's Defense Advanced Research Projects Agency (DARPA).[10] Similarly, ICANN originally operated under a direct contract with the U.S. Department of Commerce.

Assessing Institutions for Cyber Security Governance

International cyber security policymaking and governance is taking place in a multitude of venues (many of which are listed above) by a variety of parties, often with little cooperation among them or even awareness of each other. The lack of jurisdictional clarity and sufficient coordination means resources are being used inefficiently and parties with conflicting agendas are more often focusing their efforts on organizations that are sympathetic to their views, rather than engaging in the harder work of finding international consensus. Much of the literature on building international consensus focuses upon the unique challenges and complexities posed by cyber security, and some observers assert that new international structures are needed to properly manage cyber security efforts.[11] Although there is value in considering new organizational structures and policy regimes before committing to such a task, it would be more fruitful to fully examine existing institutional structures first.

IDENTIFYING INTERNATIONAL FORA FOR ADDRESSING CYBER SECURITY ISSUES

The international cyber security community should streamline its efforts and maximize the efficient use of its resources by identifying the most effective entities or groups in each of the sectors discussed above and supporting and/or expanding their actions. The goal is to identify those fora and participants that are best suited to host and lead the deliberations necessary to reach consensus, and to develop and enforce norms regarding the various aspects of cyber security. To achieve this goal, the fora and organizations selected must not only have sufficient expertise and capability for norm creation, but must also be perceived as having sufficient legitimacy by the international community. Cyber security should not be seen as a new, unique problem that calls out for a single grand solution; rather, international policymakers and others should look at various international organizations to determine those with the requisite expertise and jurisdiction to address specific cyber security issues.

Although a complete analysis of the various actors and organizations is outside the scope of this chapter, it is instructive to consider the sort of characteristics upon which this analysis would focus. Thus, for example, the International Telecommunication Union (ITU) has significant experience and expertise in managing network interconnection and technical issues, facilitating negotiations among sovereigns with occasionally competing interests, and formulating international policy. It also has experience with setting technical standards. These competencies would benefit the ITU in developing certain technical procedures and facilitating information sharing among actors in different nations. Moreover, as an affiliate of the U.N., the ITU's recommendations and resolutions are often highly persuasive to member countries. However, the ITU is a consensus-driven organization that often operates through smaller working groups, and the views expressed in certain situations may not always reflect those of each of its members.

The ITU also has no mandate in the area of criminal law or policy. As discussed above, currently the Council of Europe's Convention on Cybercrime

TABLE 2: SURVEY OF INTERNATIONAL INTERNET TECHNICAL ORGANIZATIONS

IITOs	STRUCTURE	AREAS OF RESPONSIBILITY	STRENGTHS	CRITICISMS
ICANN	Nonprofit Corporation	Manages core Internet functions including Internet protocol (IP) addresses and the Domain Name System.	Centrality to Internet functionality and long track record.	Historic ties to U.S. government.
ISOC	Nonprofit Corporation	"Organizational Home" for various Internet management groups (IAB, IETF, IRTF and others).	Recognized authority and influence due to long-running, clear leadership.	Little direct norm setting ability, acts through its sub-organizations.
IETF	Collaborative Forum of Volunteers	Develops and improves core technologies, standards and protocols.	Recognized technical leadership.	Builds technical independence, but avoids policy influence.
IRTF	Collaborative Forum of Volunteers	Identifies areas for future research and development.	High-level focus and industry independence allows freedom to assess broad initiatives.	Competes with IGOs and other bodies for influence over policy direction.
W3C	Collaborative Committees	Focuses on technical development of web standards (e.g., HTML, CSS).	Specialization in specific standards enables recognized expertise and control of key standards.	Narrowly focused on World Wide Web issues, may feel competitive pressures from other standards.

ICANN: The Internet Corporation for Assigned Names and Numbers
ISOC: The Internet Society
IETF: Internet Engineering Task Force
IRTF: The Internet Research Task Force
W3C: The World Wide Web Consortium

is one of the best multilateral agreements on the issue, however it has not been fully endorsed by the international community. Other groups within the U.N. and, importantly, other non-U.N. organizations have more experience and expertise in addressing issues of international law and may be more appropriate fora for discussions of normalizing national cyber crime laws. However, even some of the most successful efforts at establishing uniform international criminal systems, such as the International Criminal Court, have not been uniformly accepted. Thus, even as norms are developed on a broader international level, it is likely that real progress in this area will, to some extent, require regional consensus building as well as active bilateral work and agreements.

For their parts, ICANN, ISOC, IETF and many other international Internet technical organizations have in-depth understanding of the architecture and protocols of the Internet. Participation by these types of organizations will be essential to any international policymaking that emphasizes technical solutions to cyber security through enhanced security protocols or network-based authentication. These organizations have experience in international collaboration and hold tremendous technical expertise. However, they lack any formal lawmaking ability on either a national or international level (in fact they often have difficult and unclear relationships with governments), and, as previously indicated, distrust of the organizations by some nations could prevent them from making and enforcing any unilateral policy determinations going forward. As such, it may be useful for such organizations to serve as informational resources for other organizations that have the ability to implement more binding norms and policies, or as expert participants in policymaking activities located elsewhere.

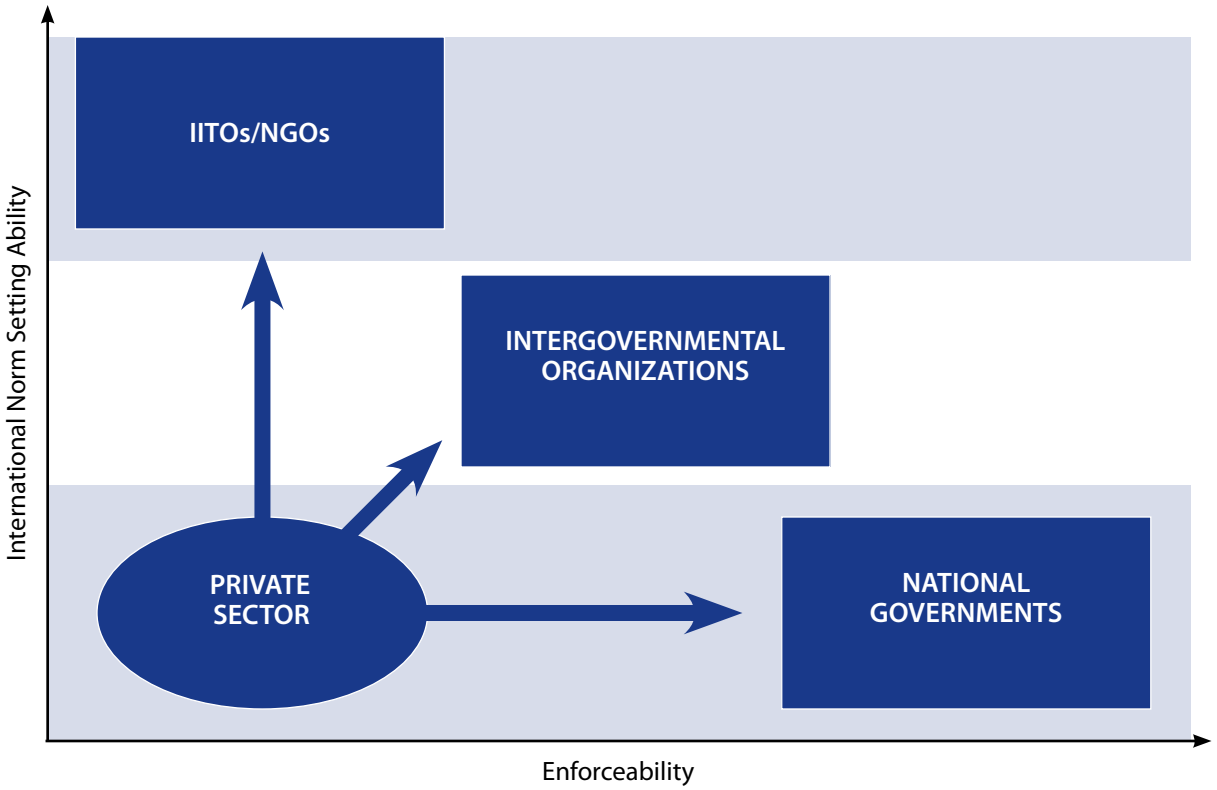
ASSESSING NORM CREATION AND ENFORCEMENT

Following an assessment of core competencies, an analysis should be made of an institution's ability to create, disseminate and then enforce cyber security norms. We have created a basic graphical presentation of how to do this (see Figure 1). This graphical technique plots an institution's "international norm setting ability" against its ability to create enforcement mechanisms for those norms, which can help illustrate the comparative advantages of utilizing one institution over another, or choosing one institution as a vehicle for norm formulation and consensus and another for norm enforcement.

We have not attempted to perform an actual institution-by-institution analysis, rather we explore a broad-based generic analysis for demonstrational purposes. As Professor Martha Finnemore explores in chapter six of this volume, creating and cultivating norms in the cyber security realm presents unique challenges that will drive the analysis of these groups and will involve the consideration of many factors beyond the scope of our presentation here.

In assessing this analysis, it quickly becomes apparent that there is a spectrum across which the groups will fall ranging from those that have strong norm setting ability, but little enforcement power, to those with powerful norm enforcement capabilities, but less ability as an institution to inject those norms into international policy deliberation. Effective international cyber security governance will require the generation of both high level and specific behavioral norms that are widely accepted as legitimate. This process will demand contributions from parties with significant experience, knowledge and expertise in managing both the technical and political sides of Internet governance. Finally, in many cases, norms and discursive fora will be insufficient, and binding national level law will be necessary. We believe this shows that multiple institutions will each have a role in future norm setting and adoption activities.

FIGURE 1: INSTITUTIONAL INTERNATIONAL NORM SETTING AND ENFORCEMENT CAPABILITIES



The Role of the Private Sector and Market Behavior

THE PRIVATE SECTOR

Private sector actors affect cyber security policy and practice domestically and globally in a variety of ways, including through their primary business activities, actions as market participants, and partnerships with and outreach to national and international organizations.

For many reasons, private enterprises have always been on the front lines of network security battles, although their important role has sometimes been minimized by government and the technical community. The role of the private sector regarding cyber security issues is critical and obvious as commercial network operators, software developers and equipment manufacturers have detailed firsthand knowledge of and influence over the nature and extent of cyber threats in real time. Combating cyber threats is a 24/7 activity for network operators who are constantly monitoring individual instances of suspicious activity as well as wider trends on the network.[12] The majority of cyber attacks exploit vulnerabilities in software applications or operating systems. As such, private sector entities work constantly to respond to the latest threats and disseminate patches and fixes. It is not an exaggeration to say that the fact that we have a usable Internet at all is a testament to the continuous effort of a global private sector community.

It is important to recognize that the private sector plays a vital role regarding building cyber security capacity by helping to find technical solutions and providing governments and IGOs with needed

public policy inputs, as well as by exploring creative and innovative market-based solutions. Network operators have begun the process (particularly through next generation networks) to improve security through various contractual activities. Using their vendor contracts and through the terms and conditions of their partnership and customer agreements, on the one hand, network operators can demand assurances and reserve rights that help them to prevent, identify and address cyber security vulnerabilities on their networks, while on the other hand offering (as they increasingly do already) various security options to their customers.

Even outside the technology and communications sectors, enterprise consumers have the potential to have a significant impact on cyber security development through these types of market-based activities. For example, financial services, health care and utility operations often demand networks that have greater security than is otherwise generally available. As these more secure networks become widely available, they can also become easier and less expensive for consumers to access. As a result, by virtue of their size and buying power, major enterprise consumers have the ability to demand certain warranties and protections that can have the effect of improving overall security for the entire network, including those services that are made available to the public. As an increasing amount of sensitive information is transmitted online, consumers are beginning to perceive the added value of enhanced security protections as well. Many consumers will be willing to pay a premium for the knowledge that the network operator is conducting additional active monitoring and has demanded a certain level of security from its underlying vendors. As this trend grows, content, application and service providers that are eager to gain access to the higher-end consumers, will conform their operations with the culture of increased security. In the near future, it will likely be commercially beneficial for Internet service providers to compete for market share not only based on price and speed, but also on security.

Market-based responses to cyber security challenges are also promoted by the participation of the private sector in various public-private partnerships and technical development efforts. The U.S. Department of Homeland Security has drawn upon significant private sector input in developing its National Infrastructure Protection Plan, which has focused on strengthening preparedness and improving responses to attacks against critical infrastructure and key resources, including in the communications and information technology sectors.[13] Moreover, in conjunction with public sector and academic representatives, private sector subject matter experts and researchers participate actively in the management and operations of the various Internet technical groups discussed above. Experts from major network infrastructure and application development companies have chaired working groups at organizations like IETF and W3C focused on developing more secure protocols for the Web and the Internet as a whole.

Finally, one of the most important ways that the private sector contributes positively to cyber security governance is through direct interaction with policymakers. Through participation in workshops, committees, hearings, consultations, rulemaking proceedings and the like, private sector entities are able to share their expertise and unique perspective with a broad range of public policymakers. This function is particularly well developed in places like the United States, where there is a strong administrative law tradition of public participation in policymaking through industry advisory groups, notice and comment rulemaking, and open, transparent proceedings.[14]

Influencing Cyber Security Development Through Market Behavior

Both the private and public sectors have the potential to wield influence over cyber security

policy indirectly through their procurement and other commercial activities. In addition to its more traditionally governmental actions, the United States and other governments can use their status as market participants to influence cyber security policy development. For example, as a large purchaser of technology, security requirements set by U.S. government procurement policies have the potential to become standardized for inclusion by other consumers, giving the government the ability to guide and direct industry developments in ways that would not be possible through legislation or regulation. To illustrate, DOD's Trusted Foundry program certifies potential providers of computer chips based upon the security of their manufacturing operations. The department has also supported the development of a Trusted Technology Forum to promote best practices in technology supply chain security, and DOD procurement standards for data encryption have become the benchmark against which all advanced encryption tools are measured. This is similarly true for major enterprise and institutional consumers. As mobile handset manufacturers seek to access the lucrative business user market with consumer devices, enterprise security requirements like remote wipe and on board data encryption are increasingly becoming standard.

Because contracts are "private law" (i.e., the governing relationship between parties) regarding the matters covered by the contractual relationship, they are an important and powerful adjunct to traditional governmentally-determined governance structures such as public laws and regulations. In the case of cyber security, private contracts that address the requirements and expectations of parties – both private parties (including individuals) as well as governments as purchasers – can be powerful and flexible tools.

Government policymakers should strive to understand and take advantage of the ways in which contractually driven policymaking can usefully supplant more formal regulatory and legislative processes. Carefully tailored contracts that influence or govern behavior can often be more flexible and nuanced than broad public law edicts. For example, a federal agency, through carefully crafted agreements, may be better able to promote cyber security best practices in very technical and specific circumstances. Furthermore, to be effective, cyber security must be nimble, and contracts, which can be amended, are much better able to keep pace with technology than are regulations. Policymakers may also find that private sector entities are more willing to commit to take important actions or to share sensitive information in the context of a private agreement rather than through precedent-setting rulemaking or legislation. Ultimately, the final security product is likely to be superior when developed through a private law agreement specific to the parties and issues at hand, rather than through more general rulemaking or statutory obligations.

Private sector and government purchasers should focus on identifying additional or new opportunities to leverage their market positions to demand security improvements in the technology products and services they procure. A growing body of research is emerging that suggests possibilities for government and enterprise purchasers to demand security assurances be taken by their providers of hardware and software components, and their own preceding suppliers.[15] Although by all accounts these so-called "supply chain security" techniques have substantial challenges yet to overcome, the potential impact is too great to dismiss.

Because of the variety of cyber threats, oftentimes the promulgators of system vulnerabilities are insulated from the economic consequences of their security lapses as the financial and reputational costs of the breaches are pushed downstream to other entities. Through creating a culture of marketing and acquiring products based upon security features, experimenting with new types of commercial and payment arrangements, and

demanding more robust warranties and assurances from their business partners and vendors, private sector marketplace actors can begin to create economic incentives for actors to internalize their security costs before vulnerabilities reach market. Through this sort of marketplace conduct, major corporations can be a force promoting global harmonization of cyber security policies.

PROMOTING DIRECT PRIVATE SECTOR INVOLVEMENT IN PUBLIC POLICYMAKING

There is a growing need for the direct involvement of the private sector in cyber security policy formulation and implementation. The private sector has expertise and experience necessary to properly educate policymakers, inform public debate and partner with national and international governments in implementing security solutions. There is a long history of private sector involvement in the development of the protocols, content and services of the Internet. Indeed, from the earliest days of the Internet, private sector researchers have worked alongside government and academic colleagues to design and improve upon the architecture of the Internet. These efforts must continue. But additionally, private sector subject matter experts need to interface with policymakers to ensure that any new international cyber security governance regimes are consistent with and relevant to the situation faced by global companies. Accomplishing this will take private sector recognition of the need to interact more with governance institutions, and a commitment by international organizations to facilitate this interaction.

Perhaps more than other nations, the United States has experience and comfort with public-private partnerships as a means to identify solutions to complicated problems. Statutes like the Federal Advisory Committee Act and the Administrative Procedure Act provide clear structures for participation by the public in policymaking activities, and key government agencies like the Federal Communications Commission (FCC), the Department of State and the Department of Commerce's National Telecommunications and Information Administration rely heavily on private sector cooperation and contributions to develop and implement policy initiatives. Although the system is not perfect, the result is that U.S. technology and communications regulation often benefits from a clear focus on market realities and a sense by the private sector of being invested in the outcomes.

As international cyber security structures develop, it will be important that the private sector participates fully. National governments, IGOs and IITOs will need to draw upon private sector knowledge and resources to understand the cyber security challenges faced and to develop sensible technological and market-based solutions. For their part, private sector organizations cannot afford to wait and see how things play out without their involvement. The risks are the development of an unworkable and ineffective international regulatory regime, or perhaps worse, an uncoordinated variety of national approaches to cyber security that place inconsistent demands on network operators and technology developers.

Nearly every strategic plan being released and developed by IGOs now recognizes the need for increased engagement of the private sector in the making and implementation of policy. However, some nations and IGOs still must embrace further the value of collaboration beyond merely with state actors.

IGOs and national governments need to examine their processes and identify mechanisms for enhanced private sector participation. Similarly, the private sector must also recognize the importance of participation and seek out opportunities to contribute substantively to policy making. The private sector should build upon its close cooperation with U.S. governmental bodies like the FCC, DHS, Department of State and Department of Commerce and engage equally actively in international venues.

Conclusion

Governments are just beginning to build internal structures to deal with the broad range of vulnerabilities created by the Internet and cyberspace. As they adjust, a focus on existing structures, both nationally and internationally, should come first. This is important from a national perspective because starting institutions from scratch has many costs and difficulties, and from an international perspective because the problem of cyber security is truly global.

As governments turn to international solutions they will also need to focus on where and how to establish norms that can be effectively enforced. To do that, governments should look to the broad range of existing international fora and organizations and determine which are best suited toward this end. This will require an evaluation of both core competencies and an assessment of how well these organizations can build and enforce norms. Furthermore, the private sector must have a key and central role in building cyber security in existing organizations and fora and in the creation of any new organizations.

Although the analysis recommended by this chapter may be helpful in identifying the appropriate fora for cyber security policy formulation, discussion and implementation, and the roles of the relevant parties, it only begins to provide solutions to some of the difficult substantive questions that will have to be answered before real progress can be made. Many of the challenges to implementing effective cyber security involve debates about political values and social norms and how the Internet should reflect them. For example, many parties believe that effective cyber security will require capacity at some point in the network to identify actors and attribute responsibility for attacks, while others worry that such technical changes could adversely affect privacy. In any event, the underlying technological structure of the network does not currently provide this functionality. However, by using the framework discussed in this chapter, we can begin to determine the appropriate bodies to develop the relevant technologies, and which of them will ensure the involvement of a broad range of stakeholders including national governments, the private sector and the technical community.

ENDNOTES

1. According to the International Telecommunication Union, cyber security is an evolving concept that generally can be defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; [and] Confidentiality."

2. These capabilities are dependent on multiple factors, including overall technological expertise, financial and knowledge-based resources, the level of development of the communications infrastructure and, to some degree, by the capacity of existing governing institutions to absorb and engage in cyber security policy. Political and social values also dictate the extent and type of efforts that countries undertake. As such, the level of involvement in cyber security governance is far from uniform across various nations, as is the nature of each nation's impact on cyber security governance internationally.

3. The White House, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

4. Department of Homeland Security, *Memorandum of Agreement Between The Department of Homeland Security and the Department of Defense Regarding Cybersecurity* (27 September 2010), http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

5. Josh Halliday, "Stuxnet Worm is the 'Work of a National Government Agency,'" *The Guardian* (24 September 2010), http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency; and John Leyden, "Russian Spy Agencies Linked to Georgian Cyber-Attacks," *The Register* (23 March 2009), http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/.

6. The White House, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 2009): 20, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

7. Ibid.

8. Department of State, *Quadrennial Diplomacy and Development Review: Leading Through Civilian Power* (2010): 45-46, http://www.state.gov/s/dmr/qddr/; and Secretary of State Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," Address at the George Washington University (15 February 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm.

9. While governments do have broad powers over Internet use and content inside (and sometimes outside) their borders, as demonstrated by Egypt's ability to shut down its communication and Internet services during its recent turmoil, the paths that lead to balkanization of the Internet are not in the best long-term interest of any modern state.

10. The Internet Society, "Histories of the Internet," http://www.isoc.org/internet/history/.

11. Robert Knake, "Internet Governance in an Age of Cyber Insecurity," Council on Foreign Relations, Council Special Report No. 56 (September 2010).

12. For example, at a workshop on cyber security issues at the Federal Communications Commission, network operators described how they constantly monitor activity across their networks and employ sophisticated network management techniques to be able to distinguish between normal spikes in usage – such as increases in SMS traffic due to *American Idol* voting – and malicious surges that could be produced by a distributed denial-of-service cyber attack. See John Nagengast, Executive Director, Strategic Initiatives, AT&T Government Solutions, "Remarks at the Federal Communications Commission's Cyber Security Workshop" (30 September 2009), http://www.broadband.gov/docs/ws_26_cyber_security.pdf.

13. Department of Homeland Security, *National Infrastructure Protection Plan,* http://www.dhs.gov/files/programs/editorial_0827.shtm.

14. For example, the Federal Communications Commission has chartered a Communications Security, Reliability and Interoperability Council (CSRIC) whose mandate is to provide recommendations to the FCC on matters of security and reliability of the communications infrastructure. Currently, CSRIC's working group on cyber security best practices is co-chaired by private sector representatives and includes participants from a range of communications service, device and infrastructure providers as well as federal and state government, the public safety community and academia. The same is true for various advisory committees that address these issues in other parts of the federal government, such as at the Departments of State and Commerce; Federal Communications Commission, "Communications Security, Reliability, and Interoperability Council," http://www.fcc.gov/pshs/advisory/csric/.

15. Jon Oltsik et al., "Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure," Enterprise Strategy Group (November 2010), http://www.enterprisestrategygroup.com/media/wordpress/2010/11/ESG-Research-Report-Cyber-Supply-Chain-Security-Nov-10.pdf; and Robert J. Ellison, et al., "Software Supply Chain Risk Management: From Products to Systems of Systems" Carnegie Mellon University Software Engineering Institute (December 2010), http://www.sei.cmu.edu/reports/10tn026.pdf.

CHAPTER VIII:
WHY PRIVACY AND CYBER SECURITY CLASH

By James A. Lewis

America's Cyber Future

Security and Prosperity in the Information Age

WHY PRIVACY AND CYBER SECURITY CLASH

By James A. Lewis

The Internet diminishes privacy. Perhaps it will ultimately destroy it. The effect of digital technology on an individual's ability to control personal data raises a serious concern: Does disappearing privacy also mean the end of civil liberties? Not necessarily. Understanding how to preserve political liberties while privacy shrinks is an essential task for the digital future.

But privacy has come to mean more than the protection of personal data. Jerry Berman, one of the pioneering thinkers on the issue of privacy, describes the Internet as a "revolutionary force."[1] Embracing this view, privacy has come to mean preserving an unconstrained space for individual action and protecting the original sense of unlimited opportunity the Internet seems to offer.

The expansive definition focuses privacy policy on three issues. The first is grounded in the traditional understanding of privacy and seeks to limit the effect of network technologies on individual control over personal data, which retains as much as possible of our pre-Internet seclusion. The second is to reduce or constrain the role of government in cyberspace in order to protect civil liberties. The third is to safeguard the Internet's potential for innovation. Privacy policy advocates assert that these three issues are linked and depend on defending an open and free Internet.

Many assumptions underpin these ideas. The most problematic are that we can restrict or eliminate government involvement in the Internet without risk; that anonymity is always beneficial; that an open, unsecure Internet is crucial for innovation; and that digital technologies have not eroded earlier conceptions of privacy as they have done with so many other concepts in business and politics. In looking at these assumptions, we must ask if trends in technology and governance have made some aspects of privacy policy obsolete.

The privacy debate takes place in the context of the powerful political effect of digital technologies, which are reshaping concepts of allegiance and legitimacy – the acceptance by citizens of a government's right to exercise authority over them. These changes in turn reshape views of the relationship of the state to privacy and civil liberties. Privacy provides the terms for a larger political debate over the role of government, government's loss of legitimacy and the increase in public disillusionment and distrust that has marked politics since the 1960s. These trends shaped pioneering notions of Internet governance and the Internet community's relation to the state. Differing views of authority, economics and the role of government explain why cyber security initiatives so often meet with opposition from the privacy community and why cyber security can be seen as detrimental to civil liberties, innovation and economic growth. The central issue in the relationship between privacy and cyber security is trust in government.

Throughout the history of cyber security policy there has been a close relationship between the idea of the untrammeled Internet – a self-organizing community where states have only a limited role – and the largely feckless cyber security measures the United States has adopted over the last fifteen years. Preserving an unconstrained Internet has been the primary objective for U.S. policy for the three successive U.S. presidential administrations, which have all grappled ineffectively with cyber security.[2] This idea leaves the United States more vulnerable than potential opponents who do not carry this ideological burden. More importantly, it limits the U.S. ability to define problems and to identify new solutions.

Other nations once accepted, without question, the pioneering American vision for the Internet: that it is borderless; works better without government intrusions; and is innately open and free. These concepts are now being rejected and replaced. New approaches to cyber security require that governments extend law, regulation and sovereign control into cyberspace. They must develop international agreements on responsible behavior and individual countries or groups of countries must adopt active defense measures.

But privacy and civil liberties are not the same, nor are they linked. We can imagine a situation where individuals have full civil liberties but no privacy.

Even without the incentive of security, many nations are eager to assert sovereign control. Cyberspace will become like any other global infrastructure, with rules and institutions for governance where governments play a major and leading role. The risk in this extension of sovereignty is that there will be increasing challenges to the values of openness, free access to information and free speech. The larger problem, however, is that the American perspective on privacy and Internet governance is unique. The United States once dominated the governance of the Internet. But that governance is shifting to a global community of nations, and so the United States must do away with old ideas in order to retain its influence to defend core values for the rules, institutions and technologies of the Internet.

The new approaches to cyber security clash with the vision of cyberspace reflected in the work of many privacy organizations. Changing attitudes toward legitimacy make the connection between the privacy community and cyber security complex and largely antagonistic. Consider the battle over control of encryption software. The fierce battle over encryption policy shaped the relationship between the privacy community and the government and helped cast it in decidedly antagonistic terms.

How the Crypto Wars Shaped Privacy and Cyber Security

At the beginning of the Internet age, the United States, alone among industrialized nations, controlled encryption products as a munition for export purposes (and export controls provided some influence over the domestic market). Encryption was a hardware product sold mainly to the banking industry and to friendly governments, so these tight controls were not a problem. But the advent of personal computing and the Internet allowed messages to be encrypted by software, rather than specialized hardware. The Internet and e-commerce offered a giant new market for encryption software. Munitions controls restricted the ability of U.S. industry to sell encryption to this global market.

The intent behind export controls was to deny access to encryption both abroad and domestically. Neither the National Security Agency nor the FBI wished to see widespread use of encryption, as this would damage their communications intercept capabilities.[3] This put them squarely at odds with the American business community. Efforts at a compromise, by offering "government friendly" encryption that preserved law enforcement access to communications did not solve the problem, as these products did not appeal to foreign markets. The U.S. controls resulted in creating foreign competitors who produced similar products that gobbled market share, rather than denying other nations access to the controlled technology. Encryption controls were self-defeating, as they created foreign producers who could sell advanced encryption in both the United States and other countries.[4]

For the privacy community, the intent of government agencies to deny private citizens the ability to encrypt their messages and to preserve (some would say expand) governmental abilities to intercept communications posed a direct challenge to privacy, civil liberties and the innovative potential promised by the new technology. The encryption debate expanded mistrust of government, especially since many privacy advocates were convinced that U.S. agencies had built "back doors" into any encryption it could control to allow easy access. The encryption debate shaped and confirmed an oppositional relationship between the privacy community and the government.[5]

This adversarial relationship is in many ways peculiarly American, reflecting a historic concern for restraining the authority of the sovereign that dates back to the separation of powers built into the U.S. Constitution. The relationship between government and citizens or government and industry in other developed nations is less conflictual, reflected in their more accepting attitudes toward government surveillance. The antagonism to government is built into American politics to a degree not found elsewhere. In the United States, encryption set a course for conflict, but the inclination was already there.

Encryption controls, had they continued, would have protected government capabilities to monitor communications. They would have also damaged American leadership in information technology, by putting U.S. companies at a disadvantage relative to their foreign competitors. This economic concern was accompanied, however, by an assertion that encryption controls would damage civil liberties. The idea that lawful communications intercepts damage civil liberties makes sense in the context of declining legitimacy and trust of government. However, it only makes sense if we accept that privacy and civil liberties are inextricably linked, and one cannot exist without the other.

Privacy and Civil Liberties

But privacy and civil liberties are not the same, nor are they linked. We can imagine a situation where individuals have full civil liberties but no privacy. This thought experiment is important. As the Internet and associated digital technologies gradually increase the amount of information

publicly available about individuals, we are moving ineluctably into an era of decreased privacy, which makes it important to determine if civil liberties are affected as privacy diminishes. Our future will be one of less privacy, but this need not reduce civil liberties.

The issue of political legitimacy frames assumptions about the linkage between privacy and civil liberties. If the state's authority is not legitimate, it is an opponent rather than a protector of civil liberties. Declining legitimacy combined with a lack of consensus among citizens on social and political norms and values reinforces the perception that the state is more likely to encroach upon freedom than protect it, and that external, nongovernmental bodies are required to counteract this.

The rise of nongovernmental organizations (NGOs) is a symptom of changing political attitudes. The declining legitimacy of formal governments propels private groups to assume functions or provide services where they believe government action is inadequate. Nongovernmental organizations are self-appointed governance bodies whose legitimacy derives from adherence to an ideal or by representing some community that is underrepresented in formal political processes. They are alternate governance structures whose complex relationship with national governments – sometimes competitive, sometimes supportive – reflects the belief that formal government institutions are inadequate.

There is a parallel in a decline of legitimacy to Durkheim's idea of "anomie," which describes the breakdown of social norms and values.[6] Declining legitimacy combined with a lack of consensus on norms and values reinforces the perception of the state as hostile to freedom. Like the separation of powers in the constitution, this perception is also consistent with a strain in American political tradition that dates back to the revolution: Civil liberties must be protected from government, instead of government being civil liberties' protector.

Key civil liberties – freedom of expression and freedom of assembly – are public functions. Civil liberties provide the ability to speak, publish, assemble and to challenge rulers. Their roots are in pre-industrial societies with much more limited notions of privacy. The intent of civil liberties is to promote free public discourse, engagement among the polity and allow for challenges to leaders and policies. Civil liberties make it unlawful for the state to use coercive measures designed to block or distort this public discourse. If a state can lawfully engage in coercion against political acts, there are no civil liberties. They exist only if a person can freely express opposition to government policies without fear of retribution and even work to displace the existing rulers.[7]

The chief risk to civil liberties is the use of coercive acts to suppress them. Privacy offers only limited protection against coercion. Protection against political coercion comes from some deeper causality based on political norms and culture that explain tolerance and protection of political liberty by the state. The basis for this tolerance of opposition lies in the historical experience of democratic nations. Norms and institutions developed to deal with dissent, which provides an alternative to coercion. A person who objected to a ruler or policy in the 16th century was likely to face violence or be imprisoned; there were few other mechanisms for dealing with dissent. By the 18th century, new norms and institutions allowed dissent and the peaceful transfer of power.

There is a simple parallel with the introduction of the printing press, which created new sources of information and challenged existing political models. Books and Bibles were rare, handmade commodities, available only to the elite. With the press, citizens could read the Bible and in it, they found no reference to the divine right of kings or to aristocratic hierarchies. Mass produced Bibles were profoundly subversive. The authority and legitimacy of the sovereign came under

question and it took decades for the birth of new political models that better accommodated newly empowered citizens. This is rough history, but the Internet produces a similar questioning of authority and legitimacy to which governments will need to adjust and accommodate. This process of adjustment to the political effects of the Internet is still ongoing.

Democratic societies learned to deal with dissent and disagreement through debate and inclusion in the political process. Democracies do not prohibit alternative points of view or information that contradicts the government's positions and policies. The reliance on debate and inclusion has grown out of the principle that no single party or group has an unchallengeable right to rule, and that governments can be voted from office, or otherwise dislodged, without violence if interested and sufficiently powerful publics decide it is best.

However, authoritarian governments do not have these mechanisms for dealing with dissent. They attempt to repress opposing views. The techniques of physical repression have been refined over decades and have been extended into cyberspace. The state's control of the media and communications reinforce this repression, and it remains an open question as to whether authoritarian governments will succeed in their efforts to control new technologies. Sophisticated authoritarian regimes are adopting tactics that can be termed as "selective repression." Politically active individuals are targeted for coercion, while the general population is left unconstrained. The idea is as old as Herodotus, and avoids the resentments created by mass restrictions. Selective repression allows a government to tolerate speech, assembly, religion, travel, gun ownership and even incomplete surveillance, as long as the population is politically inactive or passive.

Conversely, societies with strong central governments and extensive surveillance can respect the civil liberties of their citizens, if they respect freedoms of speech and assembly.[8] No one would say that France and the United Kingdom, for example, are police states where the fundamental right of citizens to engage in politics and to change governments, policies and leaders through persuasion and elections are constrained. Cultural attitudes toward privacy and the role of government differ in these and other countries. Europeans are, if anything, stricter in their protection of individual privacy in commercial activities, but also are much more tolerant of government action, including surveillance.[9]

The democratic state is the bulwark of civil liberties. Yet the privacy debate often focuses on the state as the greatest threat. Some of this can be explained by the history of the privacy movement. One of the first privacy organizations, the American Civil Liberties Union (ACLU), was founded in 1917 in opposition to the American entry into World War I and to the draconian measures used by the federal government against opponents of the war. These opponents included pacifists and isolationists, but they also included a very small number of militant socialists who were not adverse to the use of violence. The ACLU and its founders, Chrystal Eastman and Roger Baldwin, set a precedent linking privacy to "progressive" political causes.[10]

Looking back, we can see that the Justice Department and local officials used the war and the threat of a "red" insurgency as an excuse to suppress political opponents. Free speech was restricted. The most telling example was the jailing of Eugene Debs, the Socialist candidate for president. Other acts of official violence against political opponents happened during the war and for some years afterwards. While a few radicals waged a campaign we would now describe as domestic terrorism, such as exploding a bomb on Wall Street, the overreaction of the political leadership and the blending of business interests and anti-immigrant sentiment was one of the major lapses in civil

liberties. By my count, there have been five since 1917.[11] These occur whenever America faces new, dangerous and unexpected security challenges.

Such outbreaks in American history are likely unavoidable, and the result of some central imperfection. There are times when the political leadership will be incapable of policing itself, and nongovernmental bodies like the ACLU are essential in mitigating the scope of these outbreaks. Privacy, however, was not the main consideration for this mitigation. Americans enjoyed a much greater degree of privacy in 1919 than they do today, yet their civil liberties were clearly at much greater risk in that era.

Research shows that privacy, in the sense of limiting access to information about an individual, enables independent personal choices that may otherwise be chilled. A person who is being observed, or who believes that he or she is being observed, will often act differently than a person who believes that he or she is unobserved. But one must make a number of assumptions to link this loss of privacy and a decline in autonomy to a chilling effect on civil liberties. One must assume that individual attitudes toward privacy remain the same. Indeed, individuals who are more comfortable with less privacy may not experience the same chilling effect. One must also assume that the increased ability for communication and publication provided by the Internet does not offset the potential loss of autonomy. A more extroverted society will not experience a chilling political effect.

Less privacy does not automatically lead to less political freedom and fewer civil liberties if free speech and freedom of assembly are protected.[12] This suggests the best protections for civil liberties are to avoid regulating content,[13] and, as it becomes increasingly easy to obtain personal information, to expand transparency in governmental activities and place clear limitations on the use of information that governments and companies collect. With these limitations on governments and companies in place, if free speech and freedom of assembly are protected, less privacy will not lead to decreased political freedom and civil liberties in democratic states.[14]

Anonymity and Civil Liberties

If the state is a threat, hiding from it is essential. The Internet makes it easy to hide. It was not designed to provide strong authentication of identity. This lapse is the result of a close focus on the imperatives of building strong connectivity because no one expected this technology to become a world-circling infrastructure used by hundreds of millions. The Internet lets one assert any identity online, including a null assertion or anonymity. Anonymity is the inescapable "default position" on the Internet, and this is damaging.

The opposite, an ability to completely identify each individual also holds some risk, but the risks to civil liberties in a democratic nation are overstated. In the absence of adequate privacy safeguards, anonymity is an important protection for consumers. It is reasonable, for example, to want to deny your insurance company the chance to find out what health websites you visit, as they may use this against you. Many in the privacy community believe that anonymity is also essential for civil liberties. The examples given are always a human rights activist in Central America or a dissident in China. They are not drawn from western democracies. Of course, some of the more extreme privacy advocates would argue that democracies like the United States or those in Western Europe are charades. Others believe that governments constantly seek to increase the power of the police, and major privacy organizations in the United States fear that "we are constructing a national surveillance state."[15]

We know what surveillance states look like. Their most prominent feature is a massive domestic security apparatus, which employs tens of thousands of

people. Stasi, the East German Ministry for State Security, had more than twice as many employees as the FBI does now, for a population that was one-twentieth the size of the United States. The FBI would have to be expanded forty-fold to match Stasi. Domestic security agencies in surveillance states are excused from observing most laws and have broad authority to arrest or detain people for political reasons rather then criminal acts. Extensive monitoring of domestic communications for political purposes is routine, and most surveillance states employ thousands of local informants. The most advanced agencies also use sophisticated computer programs to collate deep personal information.[16] All of these powers are gathered in a single agency that reports directly to the political leadership, without any external oversight. There are no surveillance states among the western democracies. A close examination of policy and spending would show that the fear of a surveillance state in the United States is a wild exaggeration, perhaps reflecting the eroding legitimacy of federal institutions, but this belief helps explain some of the desire to protect anonymity.

Anonymity as a virtue reflects the ideology of the Internet pioneers that government threatens rights rather than protects them and that anonymity is essential for the exercise of freedom of speech. In non-democratic states, where speech is suppressed, anonymous statements may provide some degree of political liberty if the security services are lethargic or unsophisticated. Aggressive security services can manage the challenge of anonymous communications. In a country that provides for freedom of speech, anonymity can have an anti-democratic effect. The effect of anonymity in democratic states can be to cut the link between citizen and personal responsibility, which damages the essential communal nature of politics. Anonymity can allow the expression of opinions without fear of retaliation, such as an employee revealing misdeeds by an employer. In a country that provides freedom of speech, it can also undermine the legitimacy of democratic institutions and, as a result, weaken the protections they provide for civil liberties.

The Internet and associated new technologies create a complex political environment. They provide new ways for individuals to identify with groups and to attach loyalty. They disconnect public discussion from physical location, and may increase the risk that community will increasingly be defined as those who think like us rather than those with whom we share a space. Before the Internet, people with extreme views may have been isolated in their communities. Now, they can go online and find that there are thousands who share their beliefs. They can organize and recruit. This may be only a temporary phenomenon, however, as democratic political systems adjust to the widening of participation in political life.

The pioneers of the Internet believed it would be a democratizing force. John Perry Barlow said: "The Net is about taking power away from institutions and giving it to individuals."[17] The pioneers were right, if by democracy we mean greater participation in the political process. The effect of the new technologies is not democratic in the sense of endorsing western values, including freedom of expression and assembly. Over the long term – perhaps decades – greater access to information and greater participation will expand democracy, but the immediate political effect of the Internet has been to resurrect, expand and energize extremist views.[18] Access to the Internet reinforces existing political trends, both favorable and unfavorable. When certain conditions are present – simmering discontent, a triggering incident and perhaps charismatic opposition leaders – the new technologies and the Internet provide a tool for strengthening this opposition and for more easily coalescing discontent into action. Absent these conditions, however, the political and democratizing effect is limited, and we should avoid overstating the causal role of the new technologies in places like Egypt, Tunisia or Libya.

One way to approach the issue is to ask: If there were no anonymity, would American politics be noticeably different? Anonymous contributions to the political debate are scarce. While press accounts may quote anonymous sources, the reporter or editor usually knows the identities of these sources. Standing for office requires strong authentication of identity. Democracies enfranchise participation in the political process to all eligible residents of a region (although the conditions of eligibility have been a longstanding source of contention) through a process of enrolment and identification. It is important for ballots to be anonymous in order to prevent coercion, but it is equally important for voter eligibility to be fully authenticated in order to prevent fraud. A public discussion or debate may allow an individual to question or shout comments without identifying themselves, but their physical attributes are not concealed and they are often known to members of the audience. Anonymity may give voice to the powerless, but in democratic societies, it can also corrode an essential trust.

A conversation with members of the group "Anonymous," who launched annoying revenge exploits against the public websites of companies that had taken action against WikiLeaks, highlight the weaknesses of anonymity. These individuals compared their actions to the civil right protestors in Selma and the Greensboro sit-ins. But the protestors in Selma and Greensboro were not anonymous. They did not hide. Their actions were heroic, and it was this heroic confrontation that had political effect. In contrast, the effect of the anonymous WikiLeaks "paybacks" was ephemeral.[19]

The companion of anonymity, weak authentication of identity, is of course also a key enabler of cyber crime. Better authentication of online identity could improve cyber security (although we do not want to exaggerate the scope of any improvement). The more important issue is that anonymity creates a lack of trust, which is among the Internet's biggest problems. The lack of trust hampers the growth of new Internet applications that offer new services and new savings. A complete lack of anonymity conjures up images of an Orwellian police state. Complete anonymity in turn produces a Hobbesian state of nature. Neither extreme is preferable. Our current situation, reflecting the proclivities and assumptions of the Internet pioneers, is closer to a Hobbesian state of nature than may best serve the public interest. This is a complex and emotional subject. Law and social practice will need to adjust to the potential for anonymity provided by the Internet, and this will require norms, rules and technologies that preserve anonymity in some areas and constrain it in others, rather than making it the default option for the Internet.

Preserving the Open Internet to Promote Innovation

Privacy advocates oppose some cyber security measures alleging that they threaten the open Internet and innovation. We should again undertake our thought experiment, which asks what effect a complete absence of privacy would have on an economy that observed the rule of law and had strong protections for intellectual property. The deciding factors, this experiment suggests, is an ability to restrict the temptation for existing businesses to block innovations that could threaten their profitability and to protect innovators and entrepreneurs from the theft of their new ideas. If incumbent power were restrained and intellectual property protected, innovation would continue irrespective of the status of privacy or Internet freedom.

Yet one leading privacy organization states that it "strongly believes that [privacy] is essential to keep the Internet open, innovative and free."[20] The belief that a "free and open" Internet is linked to innovation deserves greater attention, but some discussion is necessary as the belief forms an important element of the rationale for blocking cyber security initiatives if these involve a larger role for government (rather than individual, voluntary actions).

The role of the privacy community in the dispute over net neutrality helps to illustrate this point. Net neutrality, the idea that service providers should not be able to limit access to content or create tiered levels of service and that all traffic should be treated equally, has little to do with the protection of personal information. Yet every major privacy organization supported it as essential for preserving the open environment needed for innovation. Privacy's economic agenda seeks to preserve the Internet in its unconstrained, pioneering state as a driver for economic growth.

Law and social practice will need to adjust to the potential for anonymity provided by the Internet, and this will require norms, rules and technologies that preserve anonymity in some areas and constrain it in others, rather than making it the default option for the Internet.

Privacy and economics overlap in three ways. First, the new technologies lead entrepreneurs to find new ways to take advantage of networked technologies, by collecting information on consumer preferences and habits, often without the consumers' knowledge or consent. The amount of information generated by the Internet on consumers is unprecedented, and the technologies developed to collect this information usually fall outside the ambit of existing law. This is a particularly important problem for the United States, where the laws regarding such collection and exploitation activities by businesses are weak. Here, innovation unconstrained by law is antithetical to privacy.

Second, the disruptions created by the new technologies prompt companies to defend existing business models by using law and regulation to limit competition. This is particularly true in telecommunications and broadcast industries, where incumbents and existing companies often exercise extensive power to safeguard their interests. The relationship between the privacy community and business involves a degree of discomfort. There is an affinity between privacy advocates and the "new" tech companies who threaten the old giants. The efforts of incumbents to protect intellectual property or create new revenue streams by exploiting consumer information usually run afoul of privacy. At the same time, the privacy community's advocacy of a free Internet and limited role for government attracts support from business interests that seek to limit regulation and liability. The argument that the Internet must remain free to empower innovation has become a useful blocking tool in policy debates and in Congress.

Third, the Internet is seen as a wellspring of innovation. This probably reflects a misunderstanding of the innovation process. Innovation, the creation of new ideas, services and technologies, allows economies to grow and use resources more efficiently. Recognition of the importance of innovation grows out of a long sequence of work in economic theory. Joseph Schumpeter and other late 19th century economists identified innovation and entrepreneurship as essential economic factors. Twentieth century economists like Robert Solow, Kenneth Arrow and others, demonstrated that technological innovation is the key determinant of growth.

Digital technologies now drive growth. The issues for consideration are the rate of that growth and the policies that best accelerate it. The expanded production of digital technologies (such as computers) has been a source of economic growth as the information technology (IT) manufacturing sector expanded to meet demand, and as companies outside of the IT sector used digital technologies to become more efficient. Digital technologies allowed the creation of new network services. While the first two elements – IT production and increased efficiency in non-IT industries – are more important in explaining economic growth, the third element – e-commerce and the creation of new, mass-market network services – has come to represent digital innovation.

Some economists at first believed that the contribution of digital technologies was entirely overstated. As more data became available, the contribution to growth became clearer. In combination, the expanded production and increased efficiency probably accounted for a third of U.S. productivity growth in the late 1990s.[21] But growth did not increase at a constant rate. Companies outside of the IT sector reaped the largest efficiency gains early on; the rate of increase in improvement gains for these companies is now smaller. Economists would be familiar with this, recognizing it as the concept of diminishing marginal returns.

In contrast to the initial skepticism of economists, advocates of the new technologies concluded in the 1990s that we were entering a "new economy," where a technology-fueled productivity boom would eliminate business cycles and recession. The notion of permanent growth had appeared in the stock market bubble in the late 1920s, which, like the new economy of the 1990s, was fueled by lax monetary policy, rather than some underlying and permanent change. The commitment to a free Internet as a source of growth retains a tinge of this dot-com era belief in a "new economy" where constraints on growth had been eliminated by information technology.[22]

Any discussion of the economic effects of the Internet and digital technology is necessarily complicated by the larger problems in measuring and explaining growth and innovation. Innovation involves many factors. Access to information technology is one factor, but it is not the most important. An educated workforce, appropriate fiscal and tax policies that create the financial resources needed for investment, balanced protection of intellectual property rights and minimal regulatory impediments (at all levels of government) are key, along with adequate infrastructures and openness to trade. Progress in these areas is necessary to increase innovation, but each may require difficult political decisions that go well beyond a commitment to preserving an open Internet.

Open platforms encourage innovation in some areas, but that does not mean that innovation and growth would cease or slow if the open platform was unavailable. Robert Fogel's point, first raised in his landmark study of how a new "networking" technology affected American growth in the 19th century,[23] is that the actual contribution to economic growth of a new technology is determined by asking what growth would have been if the new technology had never been invented. For other major innovations, the rate of change is incremental, not revolutionary. We need to be cautious in ascribing a broad range of economic virtues to a single technology if we are to avoid damaging missteps that impede both growth and security.

That an open and free Internet is essential for innovation has become a defining myth and reinforces arguments that the Internet must remain unregulated and the role of governments constrained. But there is more to innovation than creating a new app or social network site. The most telling evidence against the link among an open Internet, innovation and growth lies in Asia,[24] where nations with much less privacy and very different conceptions of it are moving to displace the United States as the leading

global innovators. They have already displaced Europe. The best explanation for this tectonic shift is that privacy is largely irrelevant to innovation.

Futures for Privacy

The technological and social context for privacy and Internet governance is not static, and further changes will reshape privacy. The new ways in which people connect to the global network will affect privacy. The old hobbyist model of computing, where personal data was stored on a box next to your desk, is being replaced by technologies where data and applications are stored and managed remotely. The ability to exploit information gleaned from an individual's Web activities is growing. Access to and control of personal data will be shared, controlled by third parties and governed by laws and contracts that are often inadequate.

We can find a precedent for this transition in the history of other utilities. For a brief period at the start of the electrical age, people who wanted electricity had to provide it themselves, using generators in basements or carriage houses. They had to maintain the machinery, upgrade it and worry about safety. Sometimes they sold power to their neighbors, which created local networks. This was neither efficient nor safe. People now buy electricity as a service without any knowledge or concern as to where the power is being generated or by whom, but the provision of this service is highly regulated to protect the public. A similar transition is occurring with the Internet. The move from disaggregation to the cloud changes the relationship between privacy and cyber security. In this cloud-computing environment, we will rely on third parties for essential computing and network services, and as a result, third parties will play the central role in cyber security.

This is a significant departure from the past, where each enterprise, agency or user was responsible for its own data and its defense. The Internet was designed to put responsibility for all but the simplest addressing functions, including security, at the devices' end points. The advantage of this disaggregated approach to security is that it minimized political problems that revolve around the role of government in supplying a public good – there is less need for regulation and there is an implicit protection for privacy as third parties are not involved. The disadvantage, of course, is that even an unskilled opponent can easily defeat a disaggregated defense.

The Department of Homeland Security's Einstein Program point to the future, where cyber security functions will be automated across networks. These new approaches, called active defense or dynamic defense, monitor traffic for known malware and, in some cases, for anomalous activity. These systems block such traffic before it can penetrate the network being protected. Once problematic traffic is identified, dynamic defense systems use pre-programmed decisions that tell the system what action to take when it identifies a particular signature or class of signatures as malicious. Dynamic defense parallels "network-centric warfare," with its emphasis on networks rather than platforms and information sharing to increase situational awareness and speed.

However, these dynamic techniques are intrusive and can require a high level of monitoring. To be maximally effective, they need to be informed by intelligence data and by combining traffic data from multiple service providers. The combination of monitoring, speed and intelligence involved in a dynamic approach to cyber security, whether for government networks or some broader set of infrastructures, creates immense problems for the privacy community. We can legitimately ask, however, whether monitoring that is limited to identifying malware and does not produce new information or knowledge on the content of traffic for government use, and that is carried out by machines without human intervention, poses any risk to civil liberties.

One response to this change has been to assert that dynamic defense does not actually work. This is a rhetorical device – to object to technologies on the grounds that they are ineffective. The problem is that these charges are often divorced from data. We now have the capability to count and measure the effectiveness of techniques and technologies in blocking attacks and mitigating risk. The data suggests that active, networked defense is more effective than disaggregated, point defense. Interviews with leading network service providers who use these technologies on their own networks to protect their customers and service suggest that active defense is a significant improvement.

In the future, as personal data becomes increasingly ubiquitous, privacy may need to enable greater individual control over the use of data rather than seeking to prevent its discovery.

Given the potential intrusiveness of active defense, strengthened oversight procedures and limitations on the use of personal data are essential. The challenge for the privacy community is to find a way to help provide new rules for oversight without blocking the use of the new defensive technologies. Doing this will require moving away from the ideological precepts of the Internet pioneers and becoming partners in deployment rather than opponents of technological change.

Attitudinal changes among the electorate toward privacy also need closer examination. One challenge for privacy organizations is that the political impulse that led to their creation may be fading because of generational change. There is less privacy now than in pre-Internet days, but the fact that people are more willing to share personal information does not mean they are then willing to have that information collected or used without their consent. The decline in privacy is, in part, a result of technologies that make it easier to publish, find and access information, and, in part, a matter of personal choice, as people choose to publish more personal information (perhaps in some cases without realizing that they have made it public).

While we do not want to overstate "the end of privacy" or a generational shift in attitudes on sharing personal information with strangers, network technologies enable greater access and sharing. We might be seeing the effect of a change in the economics of sharing. People did not share personal data widely before the Internet; we assumed this reflected a preference. An alternative explanation is that they did not care if information was shared, but were unwilling to pay the price in time and money to do so. Their attitude has remained the same – they do not care – but the Internet has lowered the price of sharing and access. Attitudes toward privacy will change because of lower costs, and the urban individualism of the industrial age. The ideal of pre-digital privacy is gone forever.

Privacy is shrinking as the world becomes interconnected. The increased incomes of the 19th and 20th centuries allowed people to occupy greater personal space instead of the crowded and close villages and towns of an earlier era, where there were far fewer secrets. The growth of transportation technologies increased the opportunity for anonymity (or pseudonymity) by allowing an individual to rapidly relocate to a place where he or she was a stranger. The Internet, by eliminating physical constraints, undermines this old-style privacy. As privacy changes, the expectations of the Internet pioneers and the policies that result

from them will also be undermined. In the future, as personal data becomes increasingly ubiquitous, privacy may need to enable greater individual control over the use of data rather than seeking to prevent its discovery.

Internet Governance and the Closing of the Electronic Frontier

It is reasonable to ask if concern about government cyber security programs would decrease if the United States had a comprehensive set of protections for privacy in commercial activities. The likely answer would be that this would not greatly change the privacy community's views of cyber security. Concerns over the role of government would remain, as would the imperative of preserving the Internet's open frontier so cherished by its creators.

The question we have been reluctant to ask is whether the beliefs of the early 1990s, when the Internet was smaller, largely American and not a global infrastructure, are still adequate and retain persuasive force in the changed international environment. U.S. policy was seminal in shaping Internet governance and the visions of the Internet pioneers shaped this policy. In turn, this vision and policies shaped how the world perceived the Internet. U.S. policy was seminal in shaping Internet governance and the visions of the Internet pioneers shaped this policy. In turn, this vision and policies shaped how the world perceived the Internet. The decision of the United States to take a minimalist approach to regulating the Internet initially had considerable influence on other nations. In part, this reflects U.S. efforts in multilateral fora like the Organisation for Economic Co-operation and Development and the United Nations Commission on International Trade Law, where the U.S. led efforts to adopt policies that emphasized private sector control. The American origins of the new technology and the rapid growth of the American economy in the 1990s made other countries more accepting of this leadership.

For reasons both good and bad, this intellectual construct is now collapsing. It is inadequate to the tasks of managing the new technologies and this inadequacy reinforces the growing tendency of other nations to question the old dogma and undertake efforts to restructure Internet governance. The unpopular war in Iraq and the general attribution of the global financial panic to American irresponsibility has tarnished the luster and reduced the influence of the United States. Challenge by new economic powers was inevitable, but the United States is in a weaker position to respond to it, and this poses a risk to democratic values.

We are in a transition to a new kind of Internet governance. Two related trends drive this transition – the extension of sovereign control into cyberspace and the collapse of the pioneering, communal, American vision for governance. Managing this transition in a way that preserves the values of free speech and open access to information will be difficult. Continued espousal of the pioneering concepts will keep the United States on the defensive, as it tries to preserve an increasingly inadequate Internet governance model, and may even condemn the United States to irrelevance, as other nations move to new approaches where governments play the same role in cyberspace that they play in other multilateral activities. A strategic approach to cyber security, and a framework for privacy suited to the new social and technological environment, requires new ways of thinking.

The view that the Internet must remain a "free" and open frontier is a serious impediment for taking full advantage of network technologies. There will be unhappiness as governments move to play a stronger role in protecting the Internet frontier, and these efforts will be cast as a threat to civil liberties and the economy. But it is time to extend the rule of law into cyberspace and abandon the pioneering concepts that shape Internet governance and privacy policy. They no longer make sense for a global network where there are increasing challenges to

security and to the values of openness, free access to information and free speech. To do this, conceptions of privacy and its connection to civil liberties and innovation must be refocused and renewed.

The global governance debate revolves around the issues of sovereign control over access to information and the role of the state. One possible outcome of this debate is a slow fragmentation of the Internet into linguistic and regional blocs, which authoritarian governments will shape to serve their needs. This outcome is not in the U.S. interest, nor in the interest of the world, but if the United States cannot offer some new conceptual framework that escapes our pioneering vision of Internet governance, it is the most likely.

While there is no global consensus on privacy, just as there is no global consensus on free speech, the one area where citizens in most countries agree is that they should have untrammeled access to information,[25] and that access to information should be a new fundamental human right. Not all governments share this belief, but it offers an opportunity to build a new consensus on Internet governance, security and civil liberties based on expanding access to information. Otherwise, a more fractured Internet may emerge, with privacy protected for some and fewer civil liberties for many others.

The United States is unaccustomed to seeing major international initiatives undertaken without its leadership, but this is what is happening because of an American inability to move past the Internet's pioneering ideology. The pioneering framework is broken; it failed to provide security and did not meet the needs of many nations. It is incapable of guiding policies to make the Internet more secure. There has been a long and sustained political effort in the United States to attack and diminish the role of government and the private sector as an alternate governance structure. (The American Enterprise Institute, for example, describes some of its early publications as portraying "private enterprise as a form of voluntary social cooperation undergirding strong communities and democratic self-government."[26]) Yet this concept is alien to other nations and makes U.S. public policy debates markedly different from that in other nations. The pioneering Internet notion of private sector lead and small government role is also alien to these nations.

The current structure of Internet governance grows from uniquely American cultural and political roots. The Internet is the product of the times, and much of its governance structure is a legacy of the politics of earlier eras. Predictions about the demise of the nation-state and the emergence of a "borderless world" were a regular feature of discussions of international relations in the 1990s and helped shape views on Internet governance. They have now become somewhat muted, as these predictions overstated the effects of globalization and did not take into account the ability of nation-states to adjust to the new circumstances.[27] The Internet did not eliminate borders; it shrank the time to traverse geographic space. It did not replace governments with a self-governing global commons shaped by private action, where formal state mechanisms were unneeded. Governments will adapt to the new technology and nation-states will remain the most powerful actor on the global stage and assert themselves in cyberspace. As governments reassert themselves in cyberspace and develop ways to "strengthen" borders, those who continue to espouse the pioneering ideology risk being condemned to irrelevance.

The next few years will see governments extend sovereign control into cyberspace. They have realized that the notion that the cyber domain is somehow outside the realm of sovereign control is inaccurate and does not reflect how networks are constructed and operated. In light of this, a reassessment of Internet governance is essential. For privacy policy, this reassessment would ask how it would be different if the pioneering Internet

ideology were no longer its foundation. The most likely changes would be an end to the belief that a completely open and free Internet is necessary for innovation, and that the role of the state in cyberspace should be smaller than it is for other social or economic activities. A more difficult reassessment would look at the changes in attitudes toward privacy, particularly generational changes.

Any process of reconceptualization will be difficult. Thomas Kuhn, in a seminal study of how scientific concepts change, noted that new ideas rarely persuade adherents of the old ideas to change their minds, and that the believers in the older concept eventually die and are replaced by those with new thoughts.[28] This gloomy prognosis is not entirely appropriate for the Internet. There is no guarantee that the United States will adopt this new mindset, but there are some reasons for hope. Until recently, debate over Internet policy was largely confined to specialists, often from a technical background or from the IT industry. They were largely American, with views shaped by the American political experience. Now that the Internet has become a central element of daily life, new interest groups and countries with different political views will become involved in these debates, which will dilute the influence and question the beliefs of this older community. The challenge for the United States will be to manage this transition so as to not lose the virtues of American ideology – the commitment to openness and individual freedom – while moving to mature governance for the new global infrastructure.

ENDNOTES

1. Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008): 50.

2. The most recent expression of this can be found in the "2009 Administration Review of Cybersecurity Policy."

3. National Security Agency was also deeply concerned that the new Internet was fundamentally insecure. One of the motives for the ill-fated "Clipper chip" was to build encryption into the new networks to make them more secure.

4. The United States briefly considered adding import controls on encryption to counter this.

5. There is no adequate history of the crypto wars, in part because much of the material remains classified. The default account is Steven Levy's *Crypto: How the Code Rebels Beat the Government* (New York: Penguin Putnam, 2001), but it suffers from sourcing limitations.

6. Emile Durkheim, *Suicide* (New York: The Free Press, 1951).

7. Asserting that privacy is itself a civil liberty is a somewhat circular contention. That courts have endorsed this idea is not in itself conclusive, as many assertions by courts, even the U.S. Supreme Court (such as the Dred Scott case) have rightly been reconsidered and as new information became available or as attitudes changed.

8. See, for example, "The clash of data civilizations," *The Economist* (17 June 2010), http://www.economist.com/node/16377097.

9. According to Benjamin Goold, "European attitudes towards surveillance may be indicative of a more balanced and less politicized approach." See "Making Sense of Surveillance in Europe," *European Journal of Criminology* (March 2009).

10. "Throughout the 1920s, labor and political speech issues predominated [in the ACLU]. The organization remained silent on such issues as the Volstead Act, the *Olmstead* wiretapping case and other due process or privacy law questions." "American Civil Liberties Union Records, The Roger Baldwin Years; 1917-1950: Finding Aid," Princeton University Library, Department of Rare Books and Special Collections: 5, http://diglib.princeton.edu/ead/pdf?id=ark:/88435/rj430454b.

11. These include the Red Scare of the 1920s; the 1941 internment of Japanese-Americans; the 1950s McCarthy/House Un-American Activities Committee; the surveillance of the 1960s and 1970s, including Watergate; and the post-9/11 actions to monitor for terrorist activities.

12. To take a recent example, the actions of the Bush administration's warrantless surveillance program raised serious concerns, but had no effect in reducing political debate over the administration's policies, as it was not used for domestic political purposes.

13. American and European democracies differ on control of content. Europeans restrict "hate speech." They assert that their restrictions are bounded by the need to show an imminent risk of harm, which minimizes the effect on civil liberties. Restrictions on hate speech were an important complication in negotiating the Council of Europe Convention on Cybercrime.

14. Assuring transparency will require creating oversight bodies within government and a more active role by the Congress.

15. The Electronic Privacy Information Center, *EPIC Annual Report* 2007/2008:2, http://epic.org/epic/annual_reports/2007.pdf.

16. This is similar to what data aggregators in the United States.

17. See, for example, Roy Rosenzweig, "Wizards, Bureaucrats, Warriors & Hackers: Writing the History of the Internet," *American Historical Review* (December 1998); John Markoff, *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry* (New York: Penguin, 2006); Fred Turner, From Counterculture to Cyberculture (Chicago: University of Chicago Press, 2006); Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Reading, MA: Addison-Wesley, 1993): 38-64; and Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World* (New York: Basic Books, 1995).

18. Michael Barkun, "Conspiracy Theories in Politics," *The New York Times* (22 April 2011), http://www.nytimes.com/roomfordebate/2011/04/21/barack-obama-and-the-psychology-of-the-birther-myth/conspiracy-theories-in-politics.

19. "'Operation Payback' Targets WikiLeaks' Foes," NPR (9 December 2010), http://www.npr.org/2010/12/09/131937254/-operation-payback-targets-wikileaks-foes.

20. Center for Democracy and Technology, http://www.cdt.org/about.

21. Robert Solow famously said in 1987, "You can see the computer age everywhere but in the productivity statistics." Stephen Oliner and Daniel Sichel, "Information technology and productivity: where are we now and where are we going?" Federal Reserve Bank (10 May 2002); Kevin Stiroh, "What Drives Productivity Growth," *Economic Policy Review* 7:1 (March 2001); and Robert Litan and Alice Rivlin, "Projecting the Economic Impact of the Internet," *The Capco Institute Journal of Financial Transformation, 2* (July 2001): 35-41.

22. Jennifer Rheingold, "What We Learned in the New Economy," *Fast Company* (1 March 2004), http://www.fastcompany.com/magazine/80/neweconomy.html?page=0%2C1; and Alan S. Blinder, "The Internet and the New Economy," The Brookings Institution (June 2000), http://www.brookings.edu/comm/policybriefs/pb60.pdf.

23. Robert Fogel, *Railroads and American Economic Growth: Essays in Econometric History* (Baltimore: The Johns Hopkins University Press, 1970).

24. China, a country that has infinitely less Internet freedom than the United States, is growing four times as fast. China threatens, if the American scientific community can be believed, to overtake us in technology and engineering. China's example suggests that close attention to fiscal and economic fundamentals are more important for growth than a free and open Internet.

25. "Internet access is 'a fundamental right," BBC (8 March 2010), http://news.bbc.co.uk/2/hi/technology/8548190.stm.

26. American Enterprise Institute, "History of AEI," http://www.aei.org/history.

27. Kenneth Waltz, "Globalization and Governance," *PS Online* (December 1999), http://www.mtholyoke.edu/acad/intrel/walglob.htm.

28. Thomas Kuhn, *The Structure of Scientific Revolutions* (Chicago: The University of Chicago Press, 1962).

CHAPTER IX:
INTERNET FREEDOM AND ITS DISCONTENTS: NAVIGATING THE TENSIONS WITH CYBER SECURITY

By Richard Fontaine and Will Rogers

America's Cyber Future

Security and Prosperity in the Information Age

INTERNET FREEDOM AND ITS DISCONTENTS: NAVIGATING THE TENSIONS WITH CYBER SECURITY

By Richard Fontaine and Will Rogers

American national security policymakers today are engaged in two simultaneous and potentially contradictory efforts. On the one hand, they seek to secure the United States against cyber attacks, pushing for greater online transparency and attribution. On the other, they promote Internet freedom, advocating privacy and providing tools through which individuals can act anonymously online. These dual efforts create tensions that are not often explored carefully. Though these tensions are real, and in some cases will force difficult choices, they should not be an obstacle to a robust U.S. effort both to secure cyberspace and promote Internet freedom abroad. In adopting a new set of principles and policies, the United States can strike the appropriate balance between security and the promotion of Internet freedom abroad.[1]

But actually promoting Internet freedom is complicated. At a time of increased attention to the threats emanating from cyberspace — including cyber attacks by nation-states, criminal syndicates and sophisticated hackers — American policymakers must tread carefully in balancing the nation's cyber security interests with the need to promote and preserve freedom of expression on the digital frontier. There are, at first glance, numerous dilemmas presented by the efforts to promote these two goals. Some cyber security experts urge greater accountability and attribution online, for instance, as a way of identifying those who cause harm to American cyber systems – a principle that contradicts the anonymity urged by Internet freedom proponents. Pending congressional legislation would empower the president to restrict Internet traffic in a cyber emergency, which seems to conflict with the push for the unrestricted flow of information over the Internet abroad, particularly when embattled regimes in Egypt and Libya turned off Internet access entirely. The military's push for an "active cyber defense" that uses scanning technology to detect and stop malicious code in domestic and foreign networks alike could be cited

by autocracies as justification to remove software code and websites they deem threatening, including from political dissidents and human rights activists. Export controls on software that could be used by terrorists and criminals may also prevent the use of cyber tools by dissidents and protestors living under dictatorships. Meanwhile, autocracies routinely push for international cyber security norms and agreements that define "security" in a way that would restrict political expression.

To their credit, Bush and Obama administration officials have made public and private efforts to address some of these tensions, including Secretary of State Hillary Rodham Clinton's recent speeches on Internet freedom. Yet conversations about America's cyber security and Internet freedom policies have, by and large, taken place in isolation from each other. The former has been led largely by the national security community; the latter by the technology community and a handful of human rights activists.

Even as Internet freedom has slowly garnered greater attention in Washington and in mainstream foreign policy discourse, cyber security and Internet freedom have received disparate treatment from the top echelons of the U.S. government. The United States has devoted increasing resources and attention to addressing the challenges inherent in cyber security, but very little to cyber freedom. To cite one example, the government has produced a Cyberspace Policy Review, intended to review the nation's cyber security policies.[2] While the review acknowledges the government's dual challenges of preserving the Internet as a forum for social engagement, economic activity and freedom, and safety and security online, the review failed to mention Internet freedom.

Despite these discrepancies, opportunities exist for American policymakers to navigate the tensions between cyber security and Internet freedom, and work together toward a cyberspace strategy that balances both interests. This paper seeks to contribute to this necessary discussion. As part of a broader study by the Center for a New American Security (CNAS) to develop a new path forward for Internet freedom as an element of American foreign policy, this chapter first defines "Internet freedom" for security practitioners unfamiliar with this sometimes fuzzy issue. Second, we examine the tensions between cyber security and Internet freedom in order to illustrate the inherent challenges in developing a policy that balances both interests. We focus narrowly on these tensions as they relate to U.S. efforts to develop cyber security norms and promote Internet freedom on the international stage, and discuss domestic concerns only to the extent that they impact Internet freedom and cyber security efforts abroad.[3] Finally, we offer a way ahead for policymakers. While there are no perfect formulas or solutions to these complex policy issues, this paper attempts to offer a way toward a balanced cyberspace strategy that best ensures America's security while promoting the online values we hold dear.

Internet Freedom: Freedom of Expression on the Digital Frontier

In January 2010, Secretary Clinton gave what was theretofore the most complete articulation of the U.S. government's approach to Internet freedom. Citing President Franklin Delano Roosevelt's 1941 Four Freedoms speech, she added a fifth freedom, the "freedom to connect – the idea that governments should not prevent people from connecting to the Internet, to websites or to each other."[4] In this speech and in a second she delivered in February 2011, Secretary Clinton stated America's "global commitment to internet freedom, to protect human rights online as we do offline," including the freedoms of expression, assembly and association.[5] These speeches represent the Obama administration's clearest expression of its Internet freedom strategy. Yet questions remain about the overall objective of America's Internet

freedom efforts. Is the U.S. Internet freedom strategy committed to promoting the online freedoms of expression, assembly and association as intrinsic goods, regardless of whether their exercise engenders democratic change offline? Or does the United States support online freedom abroad both because of the country's long-standing commitment to freedom of expression and because of a belief that, on balance, a freer Internet will promote democratic political change? The way in which "Internet freedom" is defined has implications for the nature of the tensions with cyber security.

What is "Internet Freedom"? Freedom of the Internet versus Freedom via the Internet

Indeed, much confusion surrounds Internet freedom because multiple observers employ the term to designate different concepts. It is useful to differentiate, as a number of experts increasingly have, between two linked but distinct concepts: freedom *of* the Internet and freedom *via* the Internet.[6]

Freedom *of* the Internet refers to the ability to engage in unfettered expression in cyberspace. This vision of Internet freedom, as scholar Evgeny Morozov points out in his book *The Net Delusion*, draws distinctly from Isaiah Berlin's promotion of negative liberty, that is, "Freedom *from* something: government online surveillance, censorship [distributed denial-of-service (DDoS)] attacks."[6] The principles undergirding freedom of the Internet are rooted in such documents as the U.N. Universal Declaration of Human Rights, which describes as inalienable the right to receive and impart information without interference.[7] In this sense, Internet freedom is little different from the advocacy of free expression that has for decades been an element of U.S. foreign policy. America has long stood for free expression as a universal human right; the country advocates for freedom of the Internet because it accords not only with American values, but with rights American leaders believe are intrinsic to all humanity. As a result, promoting a digital arena for free speech and online assembly is a logical objective of U.S. policy.

Freedom *via* the Internet is both a more alluring and complicated idea. At root, its advocates suggest that more online freedom can lead to more freedom outside cyberspace; that is, that there is a democratizing quality to the free flow of ideas over the Internet. It is freedom via the Internet that has captured the imagination of many in Congress, the media and elsewhere (including dissidents and autocrats) who have witnessed the potentially transformative effects of Facebook, Twitter and other applications – most recently in Tunisia and Egypt, but in other countries around the world as well.

Yet the Internet's role in producing political change remains hotly contested and opinions differ widely about its efficacy in promoting democracy. Some have oversimplified matters, seeming to suggest that access to the Internet alone represents the silver bullet for quashing authoritarian regimes abroad: Give the people Facebook and Twitter and repressive regimes will crumble. Egyptian Google executive Wael Ghonim, who played a key role in the protests in Cairo, said after the toppling of President Hosni Mubarak, "If you want to liberate a society, just give them the Internet."[8] Similarly, a former Bush administration deputy national security advisor said after the 2009 protests in Tehran, "Without Twitter, the people of Iran would not have felt empowered and confident to stand up for freedom and democracy."[9] Others meanwhile are less sanguine, charging the Internet with failing to provide any organized social or political change. "The platforms of social media are built around weak ties," *New Yorker* writer Malcolm Gladwell wrote, describing the difference between social media activism and the kind of activism the United States witnessed in the 1960s during the civil rights movement. "Weak ties seldom lead to high-risk activism."[10]

It is beyond the ambit of this paper to try to resolve these contradictory claims, though it appears that both schools stake out too extreme of a position. The authors examine them in some depth in the full CNAS report on the role of Internet freedom in U.S. foreign policy.[11] An initial review of events in places like Iran, Tunisia, Egypt and elsewhere suggests that the Internet and related technologies (such as short message service [SMS] and text) have served as critical tools for organizing protests, spreading information among dissident parties and transmitting images and information to the outside world, some of which moved onto satellite television channels, which further boosted their influence. For the purposes here, it is perhaps enough to observe that both dissidents and dictatorships seem to believe that the Internet can play a transformative role, and the U.S. government is firmly on the record as actively supporting Internet freedom abroad – at least implicitly because of its potential to assist in democratic change.

How the U.S. Promotes Internet Freedom

There are two distinct ways in which the U.S. government promotes Internet freedom. The first is at the normative level, where the United States aims to inculcate the principles of online freedom as international norms and values, not unlike human rights and the protection of intellectual property. The second is through the provision of circumvention and other Internet and telecommunications technologies to users in closed regimes that allow them to break beyond restrictive firewalls and censorship practices and to communicate securely. The provision of these technologies is often coupled with government-sponsored training for dissidents and nongovernmental organizations and diplomatic efforts (working, for example, to secure the release of imprisoned bloggers).

At the normative level, the United States has attempted to promote Internet freedom by extending to the digital frontier the freedoms articulated in long-standing and accepted international norms, such as those espoused in the U.N. Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. As Article 19 in the Universal Declaration of Human Rights states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers*." (Emphasis added.) Similarly, Article 20 of the declaration protects the right of everyone to peacefully assemble and associate, a right that, Secretary Clinton has argued, is guaranteed in cyberspace as well. "In our time," she said, "people are as likely to come together to pursue common interests online as in a church or a labor hall."[12] The 2005 World Summit on the Information Society, a U.N.-sponsored gathering of 174 countries, produced a consensus statement recognizing that "freedom of expression and the free flow of information, ideas and knowledge, are essential for the Information Society and beneficial to development."[13]

The most visible – and most contentious – way that the United States promotes Internet freedom is by providing censorship circumvention and other technologies that allow for anonymity and encrypted communications online.

The United States has also recognized that, as a developer of both social media platforms and Internet infrastructure, the private sector has a critical role to play in promoting Internet freedom. For example, the U.S. government has encouraged

the work of the Global Network Initiative (GNI), a coalition of technology companies, non-profit organizations, universities and others that have agreed upon a set of shared principles for how companies should respond to government requests for information, including making those requests transparent and protecting users' rights to privacy. Members of Congress in particular have been outspoken in their calls for companies to join the GNI, which, to date, has just three tech companies.

The most visible – and most contentious – way that the United States promotes Internet freedom is by providing censorship circumvention and other technologies that allow for anonymity and encrypted communications online. The State Department has awarded approximately 20 million dollars since 2008 for competitive grants to develop circumvention technologies and promote digital activism, with a plan to award more than 25 million dollars in additional funding in 2011.[14] The Broadcasting Board of Governors (BBG), which includes the Voice of America, Radio Free Europe/Radio Liberty, the Office of Cuba Broadcasting, Radio Free Asia and Middle East Broadcasting Network, also engages in significant technology-related Internet freedom efforts. The BBG, which had its roots in broadcasting to the Soviet bloc during the Cold War, has focused to an ever-greater extent on disseminating materials online. Numerous governments around the world have responded by blocking BBG websites, and as a result the Board has put into place a robust effort to allow foreigners to access its content, including through proxy servers and other firewall-circumvention technology. Though these circumvention tools land a user on a BBG website, the user can then use the same tools to access other, non-BBG sites free from censorship and monitoring.

Such tools pose at least a theoretical challenge to efforts by cyber security officials attempting to prevent anonymous activity online by tracing cyber attacks and intrusions and holding the perpetrators accountable. For example, while secure encrypted communication tools can help cyber dissidents freely communicate without digital harassment by authoritarian regimes, and circumvention technologies can allow users in closed societies to access a broad range of banned media outlets, those same tools could enable criminal networks and terrorist organizations to circumvent protective measures taken by states to thwart illegal activity.[15] Indeed, this point is frequently raised and revisited as a key tension between proponents of cyber security and Internet freedom.

The Tensions Between Cyber Security and Internet Freedom

There exists a real challenge in balancing the principles of freedom of expression on the Internet, in which users can act anonymously, and a secure environment in which users seeking to do harm can be identified and stopped by responsible governments. What worries Internet freedom advocates is that security concerns will trump the unfettered right of individuals to freely communicate online. In order for policymakers to navigate the tensions between cyber security and Internet freedom, they first must understand precisely where those tensions exist.

ANONYMITY VERSUS ATTRIBUTION

Cyber security proponents generally wish to have greater transparency in online behavior and have focused on improving the ability of security monitors to reliably identify malicious users and track their activities. "Anonymity is the fundamental problem we face in cyberspace," said Stewart Baker, former Chief Counsel for the National Security Agency, at an April 2010 Internet conference in Germany.[16] Online transparency and attribution, according to security practitioners, allow law enforcement to pinpoint the origins of cyber attacks and intrusions, which could serve as an effective deterrent mechanism. Former Director of National Intelligence ADM Mike McConnell has argued for modifying the Internet to make

anonymity more difficult, saying "We need to re-engineer the Internet to make attribution, geo-location, intelligence analysis and impact assessment – who did it, from where, why and what was the result – more manageable."[17]

Similarly, the administration is reportedly debating whether to require Internet communications services to include surveillance capabilities in their products that could enable law enforcement agencies to access digital information (presumably pursuant to a warrant). Speaking to a congressional committee, the FBI's top lawyer referenced a child predator using a social networking site that, she said, lacked "the necessary technological capability to intercept the electronic communications."[18] It is easy to see how requiring online communications to have a back door available for government intercepts could undermine U.S. efforts to promote Internet freedom. Not only would such a requirement set a precedent for autocratic states to cite in establishing their own practices, but repressive regimes might demand access to the same back door that private companies opened for the U.S. government.

These impulses bump up against the Internet freedom agenda, which emphasizes online anonymity. The BBG, for instance, has provided funding to technology companies to develop so-called "anonymizing" systems. Such recipients include Freegate and Psiphon, which operate through proxy servers, and the Tor Project, which received nearly 750,000 dollars from the BBG between 2006 and 2010.[19] Tor uses an "onion routing" network (in which messages are encrypted and pass through several network nodes known as "onion routers") developed by the U.S. Navy to encrypt communications between proxy servers, removing layers of encryption as information is transmitted among proxy servers around the world. The network allows users to hide their location from websites they are visiting, enabling them to evade governments and others attempting to trace their location. (For example, a Tor user in Iran might appear on a website registry as a user in Germany if the last proxy server used was located in Germany.) It is important to note that these types of networks are designed with no back door for the U.S. government or other law enforcement agencies to access and monitor the secured communication or Web traffic. Experts at Tor, for example, argue that because their software is open source, users could identify any back door in the source code, compromising the software's integrity and prompting users to find other programs without a back door. They also maintain that systems containing a back door or "lawful intercept" feature are insecure by design. Criminal networks and others seeking to monitor law enforcement users can exploit any back door that can bypass the controls and auditing functions.

Concerns about the implications of anonymous Internet use go beyond cyber security threats to the threat online users can pose to other elements of American national security. Technologies such as Tor, for instance, have come under question from those who worry they will be used not only by dissidents and democracy activists, but also by criminals and terrorists.[20] The very anonymizing tools and point-to-point encrypted communication technology that the State Department and BBG are funding could, some experts caution, be used by international terrorist organizations to coordinate and carry out attacks undetected by the U.S. government agencies charged with defending the country.[21] While not reacting specifically to government-funded anonymity tools, the FBI has been outspoken for years about the potential risks associated with the spread of sophisticated encryption technologies.[22] As early as 1993, the National Security Agency developed a "Clipper chip" designed for use in secure voice transmissions by telecommunications companies – but with a back door for the U.S. government.[23] (After a public outcry by privacy activists, the program was abandoned.)

The primary purpose of BBG programs is to provide foreigners access to its own online materials – so, for instance, a Chinese citizen can access news stories on Voice of America's website, which is blocked in China. However, while BBG-provided proxy servers and other technologies land users on a BBG website, they do not require users to stay there – so even if users do not use them for direct peer-to-peer communication, criminals or terrorists could nevertheless use BBG proxy servers to access terrorist propaganda or websites that teach bomb-making and other illicit skills. Similarly, activists seeking to evade government surveillance can purchase prepaid mobile phones that lack unique identifiers, and the U.S. government is reportedly hoping to fund projects that would leverage mobile technology. But because criminals and terrorists also seek to use such phones, a number of governments have begun outlawing them.[24] As Evgeny Morozov points out, "The frequent use of new technologies by terrorists, criminals, and other extreme elements presents a constant challenge to Western governments who would like to both empower democratic activists and disempower many of the sinister non-state groups that are undermining the process of democratization."[25]

The issue is further complicated, however, by the fact that U.S. government-supplied circumvention tools are not the only option for individuals wishing to communicate anonymously or access banned websites. Providers of these technologies acknowledge they could be used by bad actors, but argue that criminals and terrorists are far more likely to use botnets (collections of compromised computers running automated software, generally without the knowledge of their users) and other illicit tools instead of settling for the less effective tools offered by the U.S. government (the government-sponsored tools can be slower than others, have restricted bandwidth and contain other features that make illicit tools more attractive by comparison). "Mujahideen Secrets 2," for example, is a jihadi-developed encryption tool designed to allow al Qaeda supporters to communicate online.[26] Hijacking computers, employing botnets and stealing identities are intrinsically illicit activities, and as a result criminals are much more likely than activists to employ such tools and techniques to access banned information and ensure anonymous communications.

The tension between Internet freedom and cyber security becomes yet more complicated as providers of anonymity technologies tout their use to security personnel themselves. It has been the case, for example, that law enforcement officials have attempted to access child pornography sites in order to track down and then arrest violators. By using tools to do so anonymously, they can ensure that the managers of these illicit websites do not realize they are being watched by police. To do this, law enforcement personnel have used the very same technologies that sometimes worry them in other contexts.

On balance, while it is impossible to eliminate the possibility that government-sponsored technologies will be used by bad actors, it is important to note that average citizens often have no such alternative. As a result, it seems reasonable to wager that even if some bad actors use these technologies, they will pale in comparison to the number of users simply wishing to access neutral media. (Beyond the availability of more effective alternatives, one must also wonder whether programs sponsored by the BBG would be al Qaeda's first technology of choice.)

Perhaps more important is ensuring that the technologies sponsored by the U.S. government actually work. In 2010, for instance, Haystack, software developed by the now-defunct Censorship Research Center that aimed to circumvent Iranian censors, captured the imagination of officials at the State Department and on Capitol Hill. Yet its developers did not submit the technology for

independent analysis before release, and a group of experts was subsequently able to crack its encryption in less than a day – suggesting that the Iranian regime might have been able to identify Haystack's users.[27] This episode illustrates the need to subject any circumvention technologies to rigorous technical review and independent evaluaion – including by outside experts when necessary – before they are deployed. To do otherwise risks not only wasting taxpayer dollars but also putting dissidents and activists at great risk.

INTERNATIONAL CYBER SECURITY NORMS VERSUS INTERNET FREEDOM PRINCIPLES

International norms that define appropriate cyber security behavior could pose a threat to Internet freedom if not carefully crafted. Indeed, the international community has expressed renewed interest in discussing international cyber security norms. Recently, British Foreign Secretary William Hague announced at the February 2011 Munich Security Conference that the United Kingdom was prepared to host an international conference to discuss international norms for cyberspace by year's end, and France sought to elevate such issues in the May 2011 G8 discussions.

The effort to develop international norms governing conduct in cyberspace touches both cyber security and Internet freedom. American policymakers have struggled to find common ground with U.S. allies and partners on defining permissible speech in the context of cyberspace. Internet freedom advocates are equally plagued by how to deal with friendly governments that restrict content that would otherwise be appropriate in the United States.

One difficulty is the lack of agreement by states on how precisely to define cyber security. Western governments talk about cyber security as protecting against assaults on and intrusion of cyber systems and critical infrastructure, such as electric utilities, government servers, financial systems and telecommunications networks. In contrast, some governments have taken a very different view of cyber security, one that encompasses "information security," including limits on speech and free expression. Russia, for example, has employed the term "information war" or "information terrorism" to describe the menace against which governments must secure themselves in the cyber realm. At an April 2008 U.N. conference, a senior Russian official argued, "Any time a government promotes ideas on the Internet with the goal of subverting another country's government – even in the name of democratic reform – it should qualify as 'aggression.'"[28] Russia successfully moved this concept of "information war" forward when the term was adopted by the six-member Shanghai Cooperation Organisation in a 2009 accord. Reports indicate that the accord defined "information war," in part, as an effort by a state to undermine another's "political, economic and social systems."[29] These examples demonstrate that at least some autocracies conceptualize cyber security differently than does the United States – and that their definitions cannot be embraced by the United States without unacceptable infringements into basic freedom of expression. It also shows how wary the United States must be of attempts by other governments to create international agreements and norms that would define "information security" and similar concepts in a way that would limit the online freedom the U.S. government seeks to promote.

But the normative challenges extend well beyond definitions of what constitutes cyber security. Indeed, some experts have debated norms that would hold nations responsible for attacks emanating from their networks or servers. Critics from the cyber security community argue that such a norm would be unacceptable to the United States because America has the largest volume of cyber attacks stemming from its networks. Yet equally important is the chilling effect that such a norm could have on online expression in authoritarian countries.

The emergence of such a norm could provide an incentive – or at least an excuse – for governments to crack down on cyber dissidents, censor content and limit Internet traffic, citing their responsibility to monitor any potential attacks emanating from anywhere on their networks.

In his book *Cyber War*, former U.S. cyber czar Richard Clarke advocates a private secure network for the federal government – a "Govnet" – as well as potentially secure networks for other critical industries, such as financial institutions, the medical community, electrical utilities and the transportation industry (e.g., air traffic control).[30] While Clarke does not advocate abandoning a public Internet, the development of separate, secure Intranets could prompt governments that wish to insulate their societies from the global Internet to develop national Intranets. Iran is reportedly at work on developing a nation-wide Intranet, and in the extreme case of North Korea there exists a completely isolated domestic Intranet. This balkanization of the Internet would quite obviously erode online freedom and diminish the benefits of interconnectedness that has made the Internet a transformative tool in societies around the world.

Constructing acceptable international norms that balance America's cyber security interests with the desire to maintain an open and free Internet can be difficult, given the opposition of authoritarian regimes. But it is made harder still because of the disjunction between the U.S. position on free expression and those of even America's closest democratic partners. While the U.S. government recognizes some limits on free expression – child pornography, slander, perjury, "fighting words" and other expressions are illegal, online or off – its commitment to free speech is nevertheless the most absolute of any major country. Germany, for instance, prohibits Holocaust denial online; France does not allow the sale of Nazi paraphernalia over the Internet; and Turkey banned YouTube for two years because it refused to remove videos the courts deemed insulting to Mustafa Kemal Ataturk. Governments in Britain, Italy and Germany have also established lists of blocked websites – particularly those containing child pornography, online gambling or hate speech – but again, these lists are often neither transparent nor accountable to the public.[31]

While the U.S. government recognizes some limits on free expression – child pornography, slander, perjury, "fighting words" and other expression are illegal, online or off – its commitment to free speech is nevertheless the most absolute of any major country.

At first glance, such moves provide an opening to autocratic governments that seek to ban online content. Why, after all, should it be legitimate for France to ban online speech that incites racial or religious hatred (as it does), but not legitimate for China to outlaw online speech that criticizes the Communist Party? As autocratic governments may increasingly point to these examples in an effort to justify their own Internet repression, it is incumbent upon the United States to articulate vocally the distinction between restrictions on free speech put into place by democratic political systems and those enacted by dictatorships. While Americans may disagree with the limits on online expression enforced by democratic partners, it is nevertheless the case that their decisions are made by governments ruling with the consent

of the governed. Decisions to censor or otherwise restrict the Internet in countries like China and Iran, on the other hand, are handed down by diktat by autocratic governments that view free expression as a threat to their political power.

Nevertheless, there are additional tensions provoked by America's democratic partners beyond their specific restrictions on particular forms of expression. The Additional Protocol to the European Convention on Cybercrime is emblematic of these. The convention is designed as a mechanism by which states can harmonize their domestic laws relating to various types of cybercrime. At first glance, this would seem precisely the kind of effort that the United States would wish to support on security grounds. Yet the protocol requires signatory states to criminalize such activities as distributing xenophobic or racist material through a computer system; expressing denial, "gross minimization" or approval of a genocide or crimes against humanity through a computer; distributing insults to people because of their race, color, religion, national or ethnic origin through a computer system or aiding and abetting any of these acts. The Additional Protocol has been signed by Albania, Cyprus, Denmark, France, Slovenia and Switzerland. While the United States ratified the underlying convention in 2006, it declined to join the Additional Protocol, believing it to be inconsistent with constitutional guarantees.[32]

In the midst of these competing normative definitions of cyber security, cyber crime and information security, the United States has a key role to play. Much of the time it will be defensive; the U.S. government should push back hard against the kinds of definitions adopted by the Shanghai Cooperation Organisation and that are routinely offered by Russia at the United Nations. It will need to continually articulate the distinction between political speech permissible under such regimes as the Universal Declaration of Human Rights and truly illicit online activity. There will be instances in which the U.S. government will need to oppose the drives for more restrictive international norms spearheaded by some of America's closest friends. And the United States will need to develop a more coherent position on how to deal with American companies that provide technologies to autocratic governments that aid in censoring, monitoring and other activities the United States deems illegitimate.[33]

DEFENDING AGAINST ATTACKS VERSUS EMBOLDENING AUTOCRACIES

Beyond the provision of technology and the establishment of international norms, the very effort to preserve security can have implications for America's Internet freedom agenda. In 2010, some 250,000 classified and unclassified diplomatic cables were stolen from the government and subsequently posted on the website WikiLeaks. Some Internet freedom advocates have criticized the administration for not publicly dissuading patriotic hackers from attacking the website.[34] A central concern of these experts is that authoritarian regimes could tacitly support or overtly encourage similar DDoS attacks against domestic sites that host threatening political content or that publish what the regime defines as "state secrets." To be sure, such regimes do not need American precedent to engage in Internet repression, but the United States should avoid handing them any additional rhetorical or normative ammunition. The American drive to expand the international observance of Internet freedom norms is based, in part, upon its own credibility in this domain. It is thus incumbent to make clear the distinction between impermissible speech as defined by democracies with the rule of law and due process, and by autocracies seeking to prevent expression that could threaten their regimes – or that merely criticizes their policies and officials. Yet this will continue to be a difficult case to make; each instance in which the United States attempts to defend its security online will have to be examined and the reasons behind it articulated anew.

The U.S. military has outlined a cyber security strategy based on active defense, which includes defending defense networks from malign programs and actively blocking malicious software before it attempts to enter military networks.[35] Although such instances of hunting down destructive content outside defense networks would be rare, the head of the military's newly established Cyber Command has argued that the United States must have offensive cyber capabilities to shut down attacking systems.[36] Even before it announced the new approach, the U.S. military reportedly attempted to take down a website based in Saudi Arabia that was suspected of facilitating suicide bombings in Iraq. In its attempt to disable the site, the military inadvertently disrupted some 300 servers in the Middle East, Europe and the United States.[37]

The U.S. Congress last year debated a bill that would authorize greater government control over the digital infrastructure in the event of a nationwide cyber attack.[38] Though media reports about a so-called Internet "kill switch" are erroneous (and a newly introduced version explicitly prohibits any government employee from shutting down the Internet), the bill nevertheless raised concerns that providing such authority would have deleterious effects on Internet freedom. While interpreting the bill remains contested territory, an expert with the Electronic Frontier Foundation, for instance, warned, "The president would have essentially unchecked power to determine what services can be connected to the Internet or even what content can pass over the Internet in a cyber security emergency."[39] The bill's sponsors would likely contest this characterization and note that the president's powers could be exercised only in extreme emergencies and pursuant to limitations. Nevertheless, the notion that the United States is facilitating the government's ability to restrict traffic over large portions of the Internet could complicate its efforts to promote online freedom norms.

It is critical to establish precise, widely understood scenarios under which the government can declare an emergency and the powers it could exercise in such an instance. Loosely defined legal notions of what constitutes a "national cyber emergency" that would give national leaders emergency powers to restrict Internet activity could set a precedent by which authoritarian regimes shut off the Internet during their own "cyber emergency" – such as widespread anti-government protests. Yet again, there is a distinct difference between a presidential order to restrict some forms of Internet traffic in the face of a cyber attack on America's critical infrastructure and President Mubarak's decision to shut down his nation's Internet during the democratic revolt in Egypt. In drafting legislation intended to protect the nation's cyber systems and infrastructure, the U.S. government must tread carefully and quash any perceptions that it is acceptable to use a "national cyber emergency" to trample on freedom of expression.

CONTROLLING CYBER TOOLS VERSUS EXEMPTING INTERNET FREEDOM TECHNOLOGIES

U.S. export controls present a particular challenge in balancing America's cyber security and Internet freedom interests. For years the United States has relied on controls enforced by the Departments of Commerce and Treasury to regulate overseas sales of merchandise and materials to states that pose a threat to U.S. national and economic security. In addition to depriving sanctioned states of the economic benefits of U.S. manufacturing goods and merchandise, these export controls are intended to prevent the transfer of goods that could be used to bolster military or intelligence gathering capabilities or for other malign purposes. The export of sensitive computer hardware and software, such as cryptographic programs and other encryption technologies that scramble messages and data, have been controlled, in part to prevent unfriendly states from acquiring cyber capabilities that could be used against the United States or its allies. Until

recently, basic Internet communications services had also been treated as a controlled export to states such as Cuba, Iran and Sudan.

The Obama administration in 2010 launched an initiative to reform U.S. export controls across the board, in an effort to relax restrictions on technologies that are already widely available in other markets while bolstering the security of the most sensitive American exports.[40] Some of these controls have prevented the kind of free online expression that the U.S. government now has a policy of promoting. Last March, the Treasury Department issued a general license for Internet service technologies that would allow technology companies to export photo sharing and other social networking and communications services to users in Cuba, Iran and Sudan. Administration officials have cited this move explicitly as an element of the government's Internet freedom agenda.[41] In June, the Commerce Department revised its restrictions on the export of most mass-market electronic products with encryption functions and eliminated a technical review of these items, including cell phones, laptops and computer drives, allowing them to be exported without a license.[42] This step, too, by making available encrypted communications products to activists and others abroad, may constitute a step forward in promoting Internet freedom.

An array of cyber security programs can, when aimed at dissidents, human rights activists and others, constitute a significant step in the direction of greater Internet freedom.

Yet export controls remain burdensome in a number of areas. Administration officials themselves have privately stated that complex and overlapping export control regulations have a chilling effect on commercial industry. U.S. export controls currently restrict, for instance, the transfer, transmission and download of open source code that is already widely available for free online. This open source code includes encryption code for secure communications and a suite of other tools that could potentially give cyber dissidents and other online activists a wider range of options for communicating securely and accessing banned content. But current export controls require websites that host open source code to block access to users in sanctioned or blocked countries. Companies that host open source code, such as Google and Mozilla, face potential criminal liability for noncompliance, and as a result these companies block the Internet protocol (IP) addresses for their open source code sites when they are accessed in countries subject to the restrictions.

Reforming U.S. export control restrictions on information technologies and open source code could further the country's Internet freedom objectives. Currently, the State Department receives a blanket license that exempts it from export control restrictions when granting funds for circumvention technologies and other software for use in export controlled states, such as Iran. Yet the license does not apply to the same technology if created and exported by an organization that is not a State Department grantee. According to some administration officials, the investment value of blocked open source technology and other software and hardware barred by export controls would dwarf the State Department's current investment in circumvention and other technologies.

Toward a Balanced Cyberspace Strategy: Principles for the Way Ahead

Forging a balanced cyberspace strategy – one that preserves U.S. security while maintaining America's ability to promote Internet freedom – is possible. It will require making choices and thinking about old concepts anew. Here we present our proposal for a path forward.

USE CYBER SECURITY TO ADVANCE INTERNET FREEDOM

To the extent possible, the U.S. government should move toward cyber security *as* Internet freedom. While funding for circumvention technologies remains critically important, an array of cyber security programs can, when aimed at dissidents, human rights activists and others, constitute a significant step in the direction of greater Internet freedom. These individuals operating in autocratic environments are often highly vulnerable to cyber security breaches, whether via government monitoring, malware infections, DDoS attacks, botnets or other hijacking of their systems, or destruction of their online archives. In helping targeted individuals abroad make their own online operations more resilient, the U.S. government can harness cyber security knowledge and programs in the service of Internet freedom.

Some of these efforts do not require a great deal of technical sophistication. Cyber security experts argue that merely teaching good "cyber hygiene" (e.g., instructing users not to open email attachments from unknown senders or click on suspicious links), coupled with providing commercially available antivirus and malware suites, can prevent up to 90 percent of cyber attacks and intrusions.[43] Similarly, the U.S. government can incorporate into its Internet freedom training programs elements aimed at helping individuals evade government monitoring. Online activists frequently err, for instance, by inadvertently exempting Web browser certificates that allow governments to monitor user activity. Simply educating individuals to carefully review the dialog boxes requesting permission for government-registered certificates can reduce the chances that they will be subject to online surveillance. Similarly, demonstrating for activists abroad how to employ password protection techniques, avoid keystroke captures and so on can be elemental but critical to maintaining security. These and other training and technologies are generally thought of as "cyber security" efforts rather than Internet freedom promotion – and yet they can be both at the same time. Similarly, government efforts can focus on moving nongovernmental organizations toward secure databases, including those containing information related to human rights abuses, and protecting them from compromise.

In some cases, however, the government will simply have to choose. For example, it is inevitable that, barring a back door, some will use U.S. government-provided circumvention and communications technologies for malign purposes. Not only does this risk enabling malign actors directly, but should it ever emerge that, for example, terrorists were organizing plots with U.S.-funded secure communications technologies, the political reaction would be understandably severe. But given the availability of alternatives to bad actors, and the relative dearth of tools that would otherwise be open to dissidents and activists, it is reasonable to continue to fund such programs, betting that the net benefit will accrue to good actors and not bad. In addition, we must imagine for a moment how the balance of power would shift from activists to autocrats should such tools no longer be available. Governments and dissidents are engaged in a continual cat-and-mouse game, fighting each other over censorship and circumvention, monitoring and evasion. Governments have no reason to cease their efforts, but to the extent that their populations have fewer technological options because of a cessation of U.S. government support, they will be weaker in this contest. None of this is to say

that providing technology is a silver bullet, or that only democratically minded dissidents will employ U.S.-funded technologies, or that those who do will access mostly political content and communicate about political change. It is to say, however, that should the United States cease its efforts to support these technologies, it would shift the balance of power away from any dissidents seeking to use the Internet and toward bad private actors (who can employ botnets and other illicit tools) and bad public actors (who would now find monitoring and censoring their citizens easier).

REALIZE THAT TECHNOLOGY IS JUST PART OF THE ANSWER

The U.S. government should build into both its cyber security and Internet freedom agendas an array of non-technology elements. Despite its appearance, the most prominent recent online security lapse – WikiLeaks – was not a cyber attack but a human intrusion of a secured network – an inside job. The alleged violator used his access to the network to download classified information with basic CD-ROM writing software. While technology enabled the intruder (it is easier and more discreet to download information to a CD than to carry out 250,000 paper files or entire filing cabinets), it is nevertheless the case that despite the advanced cyber security systems used to protect classified U.S. information from external intruders, these systems are still susceptible to human intrusions from the inside.

In protecting U.S. systems from the "human element," the government should glean lessons that can be applied to its Internet freedom promotion efforts – and vice versa. In addition to the sophisticated technology arrayed against them in places like China and Iran, cyber dissidents and activists remain vulnerable to non-cyber efforts to monitor and stop their efforts. A user might have the most secure point-to-point communications service, for example, but that platform becomes moot if the state employs traditional surveillance techniques like bugging the user's apartment or placing surveillance cameras in Internet cafes. Even the most secure networks and advanced circumvention technologies cannot fully protect individuals against human intrusion into networks or human surveillance of cyber dissidents living under authoritarian regimes.

One answer to these vulnerabilities is education. Training programs for dissidents and nongovernmental organizations should focus not only on ways to employ technology but also about how to remain secure from non-Internet surveillance practices. In this effort, the government should regularly convene practitioners in the fields of cyber security and Internet freedom with the aim of harvesting from their deliberations lessons that could advance both arenas beyond the field of technology. Another role for government is in the realm of old-fashioned diplomacy. Any Internet freedom agenda will require an array of "offline" diplomatic efforts, including lobbying foreign governments to liberalize restrictions on freedom of speech, advocating for American companies (when they seek such diplomatic assistance) under pressure from foreign regimes to turn over private data, pressing governments to release political prisoners and so on.

REVIEW CURRENT EXPORT CONTROL RESTRICTIONS

The U.S. government should devote particular attention in its ongoing export controls review to restrictions on Internet and telecommunications services and technologies, with the aim of exempting most, if not all, services and technologies that are already widely available worldwide and that could be used by dissidents and activists. While the administration has made modest efforts to exempt targeted states (e.g., Cuba, Iran and Sudan) from existing restrictions on some technologies (generally those restricted to personal use), this effort should be expanded. To the extent possible, the U.S. government should move away from state-specific export control exemptions for Internet and telecommunications services and

technologies and instead apply them universally. Doing so will involve difficult tradeoffs; certainly no one wishes to make available technologies that could, for example, aid the Iranian regime's repression or its illicit nuclear weapons program. But modest changes in restrictions on open source software, for instance, could enable individuals to build platforms through which they can communicate beyond the government's watchful eye. While each existing control will by necessity be considered on an individual basis, government agencies should do so with close consideration of the potential role each technology might play in furthering America's Internet freedom agenda. The effort should also include a public campaign that communicates in simple terms which types of commercial services and technologies are exempt from sanctions and restrictions.

For example, applications like MSN (Mircosoft Network) Messenger and Skype were unavailable to Iranians until March 2010 because of U.S. export controls.[44] That month, the Treasury Department changed its regulations to allow the export to Iran, Sudan and Cuba of services and software "incident to the exchange of personal communications over the Internet," including instant messaging, email and chat, social networking and photo and video sharing, and Web browsers and blogging.[45] In order to qualify for the exception, the applications must be publicly available at no cost to the user. The department explained that "personal Internet-based communications are a vital tool for change," noting that the sanctions as they then existed could "have an unintended chilling effect on the ability of companies to provide personal communications tools to individuals in those countries."[46]

This change in U.S. export control regulations is a good start. The government should review its export controls to ensure that circumvention and anonymity technologies – particularly those that are similar to tools funded by the U.S. government – are not sanctioned. It should also include examining restrictions on the export of technologies to countries like Syria, which was not included in the Treasury Department's 2010 revision.[47] In addition, and as discussed above, it is necessary to review current controls on the export of technology that is not for personal use only, such as websites that host open source code freely available to individual users. It should draw a distinction between those technologies that contribute to free online expression (e.g. open source code, basic encryption, social networking and communications applications), which should be more accessible, and others that are used by foreign governments to clamp down on such expression (e.g. filtering and monitoring technologies).

LEAD INTERNATIONALLY ON BOTH CYBER SECURITY AND INTERNET FREEDOM

The United States should take the international lead in attempting to resolve the normative issues surrounding cyber security and Internet freedom. Leading an international conversation on cyber security that pushes for a greater acceptance of the principles of Internet freedom should by necessity make clear what the United States believes constitutes legitimate security activities in cyberspace. Part of this effort will require working against efforts by governments such as Russia and China to inculcate cyber security norms that condone restricting online freedom. A global conversation on digital freedom of expression began in Geneva in 2003 during the first World Summit on the Information Society (WSIS) and continued in 2005 when international negotiators met in Tunis, Tunisia.[48] As noted above, the participating states agreed at Tunis that the principle of free flow of international communication and information should be respected, but a number of issues remain unresolved, including the question of what kinds of protection individuals should have from government censorship on the Web.[49] U.S. leadership at the international level should help fill this vacuum or, at a minimum,

Now is the time to move beyond two sets of segmented activities, the first carried out by security-minded officials at the Pentagon, the National Security Agency, the Department of Homeland Security and the FBI, the other implemented by freedom-minded advocates at the State Department, USAID and the Broadcasting Board of Governors.

neuter attempts to define cyber security in a way that will infringe on the American vision of universal Internet freedom.

Part of this effort requires clearly articulating American efforts to secure cyberspace at home. For example, the U.S. government must have a clearly defined and publicly understandable notion of what constitutes a national security threat in cyberspace. Making clear that any actions associated with protecting against a "national cyber emergency" or similar effect by restricting Internet traffic will be done according to firm principles (e.g. not to target political speech, in accordance with due process, etc.) is important. Repressive states will use American actions as an excuse for their own crackdowns irrespective of what the United States does or says, but government policy – and government statements in particular – should aim to diminish their ability to do so.

The United States cannot do this alone. It should push for wider acceptance of norms in global forums (as it did in the WSIS), recognizing that such efforts will meet with modest success given the wide disagreements among states. It should push back against the efforts by any states seeking to agree on their own, more repressive principles, to ensure that such principles have no chance of calcifying into broader norms. Most importantly, it should work together with democratic partners around the world to push for a vision of Internet freedom and cyber security that is fundamentally conducive to our own interests and values. Disagreements over legitimate and illegitimate speech will endure among the democracies, just as discord about security notions will continue. It has always been thus, but there is much more that unites democratic states on these issues than divides them. Articulating the distinction between countries like the United States and Britain, which give law enforcement access to otherwise private data pursuant to procedures based on due process, and countries like China, which access private data without such process, is critical. Doing so together with a broad coalition of like-minded countries helps to demonstrate that such notions are not merely an American (or even a Western) invention or an outside imposition, but instead are rooted in truly universal human rights. The United States should not merely push back against attempts like Russia's to introduce restrictive norms on cyber security, but actively work with other innovative, economically powerful market democracies to seize the norm-building initiative.

Conclusion

In 2011, it is likely that the U.S. government will spend more money than ever before on securing cyberspace. It will also spend an unprecedented amount on promoting Internet freedom. Now is the time to move beyond two sets of segmented

activities, the first carried out by security-minded officials at the Pentagon, the National Security Agency, the Department of Homeland Security and the FBI, the other implemented by freedom-minded advocates at the State Department, United States Agency for International Development and the BBG. The government as a whole, together with the private sector, activists outside government and others, should together move toward a more balanced approach to cyberspace – one that makes difficult choices between security and freedom where they must be made, and that combines the two aims where possible.

There are certainly tensions between securing cyberspace and promoting Internet freedom, but they should not be treated as if they are in fundamental opposition. This chapter attempts to provide several principles by which policymakers can guide policies that would attempt to pursue both. To make progress, the discussion about these matters must move beyond the world of technology, cyber security or human rights policy alone. As a look at the headlines of any recent newspapers demonstrates – the Stuxnet worm targeting Iran's nuclear program; the leak of a quarter-million State Department cables to WikiLeaks; the toppling of governments in Tunisia and Egypt after widespread cyber activism; a major attack on the Pentagon's classified computer systems – these issues are no longer the province of specialists. Indeed, they are some of the most consequential questions that drive international affairs today. It is time to treat them as such.

ENDNOTES

1. In defining "Internet freedom," we distinguish between two aspects – i.e., freedom *of* the Internet (the freedom to access information and express oneself online) and freedom *via* the Internet (the enhancement of basic human rights and freedoms produced by individuals using Internet-based tools to communicate, protest, organize, etc.). We use "cyber security" to mean the protection of data and systems in networks that are connected to the Internet. For more on these definitions and the othe rmain themes of this chapter, see Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age," Center for a New American Security (June 2011).

2. The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (29 May 2009), www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

3. As a result, this paper does not discuss at any length issues related to net neutrality, antitrust law, the FBI's cyber law enforcement activities or the role of the Federal Communications Commission.

4. Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," The Newseum, Washington (21 January 2010).

5. Secretary of State Hillary Rodham Clinton, "Internet Rights and Wrongs," The George Washington University, Washington (15 February 2011).

6. Evgeny Morozov, *The Net Delusion*: *The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), 230. Emphasis in the original.

7. Universal Declaration of Human Rights, Article 19. The International Covenant on Civil and Political Rights is another key document that articulates basic freedoms of expression applicable to Internet-based activity.

8. Alexei Oreskovic, "Egyptian Activist Creates Image Issue for Google," Reuters (12 February 2011), http://www.reuters.com/article/2011/02/12/us-egypt-google-idUSTRE71B0KQ20110212.

9. Mark Pfeifle, "A Nobel Peace Prize for Twitter?" *The Christian Science Monitor* (6 July 2009), http://www.csmonitor.com/Commentary/Opinion/2009/0706/p09s02-coop.html.

10. Malcom Gladwell, "Why the Revolution Won't be Tweeted," *The New Yorker* (4 October 2010), http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=1.

11. Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age," Center for a New American Security (June 2011).

12. Secretary of State Hillary Rodham Clinton, "Internet Rights and Wrongs," The George Washington University, Washington (15 February 2011).

13. World Summit on the Information Society, Tunis Commitment, paragraph 4 (18 November 2005), http://www.itu.int/wsis/docs2/tunis/off/7.html. The Tunis Commitment reaffirmed the 2003 Geneva Declaration of Principles, which held, "Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers."

14. Secretary of State Hillary Rodham Clinton, "Internet Rights and Wrongs," The George Washington University, Washington (15 February 2011).

15. According to Ethan Zuckerman, "we're not just talking about running an ISP – we're talking about running an ISP that's very likely to be abused by bad actors. Spammers, fraudsters and other internet criminals use proxy servers to conduct their activities … I'm skeptical that the US State Department can or wants to build or fund a free ISP that can be used by millions of simultaneous users, many of whom may be using it commit clickfraud or send spam." See, for example, Ethan Zuckerman, "Internet Freedom: Beyond Circumvention," My Heart's in Accra (22 February 2010), http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/.

16. John Markoff, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia," *The New York Times* (15 April 2010), http://www.nytimes.com/2010/04/16/science/16cyber.html.

17. Ryan Singel, "Cyberwar Hype Intended to Destroy the Open Internet," *Wired Magazine* (1 March 2010), http://www.wired.com/threatlevel/2010/03/cyber-war-hype/.

18. Jennifer Martinez, "Feds want new ways to tap the Web," *Politico* (7 March 2011), http://www.politico.com/news/stories/0311/50755.html.

19. "Tor: Sponsors" TorProject, http://www.torproject.org/about/sponsors.html.en.

20. David Talbot, "Dissent Made Safer," *Technology Review* (May/June 2009), http://www.technologyreview.com/printer_friendly_article.aspx?id=22427. Also see the questions by Harvard Law School's John Palfrey to Ron Deibert, Director of the University of Toronto's Citizen Lab: "What's going to happen when someone does something terrible using Psiphon, plans a terrorist attack, for instance? What's Psiphon's liability?", http://www.ethanzuckerman.com/blog/2007/01/31/ron-deibert-on-the-history-and-future-of-psiphon/.

21. According to Robert Vamosi, "TOR is endorsed by the Electronic Frontier Foundation (EFF) and is designed for individuals to circumvent Web censorship in countries such as China, however, the network could be used by criminals or even terrorists." See CNET Reviews (20 October 2006), http://reviews.cnet.com/4520-3513_7-6654986-1.html?tag=untagged.

22. The FBI and others have been relatively vocal about their concerns regarding anonymity provided by encryption technologies for over a decade. See, for example, Dan Froomkin, "Deciphering Encryption," *The Washington Post* (8 May 1998). "FBI Director Louis Freeh is the most outspoken advocate of encryption restrictions … now, Freeh complains, new technology is helping criminals more than the police. One Freeh proposal is that all users of powerful encryption software be asked to turn over their keys to a third party, so that law-enforcement officials can gain access to them with a court order." Dr. Marco Gercke, Director of the Cybercrime Research Institute, has also written that, "Encryption is a classic example of a neutral technology, since as it is not only used to hinder investigations but also to prevent unauthorised

access to information … The latest operating systems offer the possibility to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data." See "From Encryption to Failure of Traditional Investigation Instruments," *Freedom from Fear Magazine* (2010), http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=311:from-encryption-to-failure-of-traditional-investigation-instruments&catid=50:issue-7&Itemid=187.

23. "Clipper Trip," Cryptomuseum (2011), http://www.cryptomuseum.com/crypto/usa/clipper.htm.

24. Evgeny Morozov, *The Net Delusion*: *The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), 176. Emphasis in the original.

25. Ibid.: 177.

26. Jaikumar Vijayan, "U.S. Web site said to offer strengthened encryption tool for al-Qaeda backers," *Computerworld* (23 January 2008), http://www.computerworld.com/s/article/9058619/U.S._Web_site_said_to_offer_strengthened_encryption_tool_for_al_Qaeda_backers?taxonomyId=16&intsrc=hm_topic.

27. "Another U.S. Deficit – China and America – Public Diplomacy in the Age of the Internet," A Minority Staff Report, prepared for the use of the Senate Committee on Foreign Relations (15 February 2011): 42.

28. Tom Gjelten, "Seeing the Internet as an 'Information Weapon,'" National Public Radio (23 September 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

29. Ibid.

30. Richard Clarke and Robert Knake, *Cyber War: The Next Threat to Cyber Security and What to Do About It* (New York: Ecco, 2010): 275-276.

31. "Europe," Regional Profile, Open Net Initiative, http://opennet.net/research/regions/europe.

32. Details related to the Additional Protocol to the "Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems" come from extraordinary research assistance by the Harvard Law National Security Research Group, under the direction of Ivana Deyrup. For American concerns about the Additional Protocol, see Department of Justice, "Council of Europe Convention on Cybercrime: Frequently Asked Questions and Answers," http://www.justice.gov/criminal/cybercrime/COEFAQs.htm.

33. While articulating a strategy for how to deal with the role of American companies aiding Internet repression abroad is beyond the ambit of this paper, the authors treat the question in some depth in CNAS's longer study of Internet freedom. In that study, the authors offer as one potential framework a sliding scale under which the U.S. government would prohibit American companies from the most egregious activities (e.g. handing over the private data of dissidents fearing arrest to the security forces of autocratic governments) while leaving to nongovernmental efforts (such as the Global Network Initiative and organizations demanding greater corporate transparency) harder cases of less egregious activity. See Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age," Center for a New American Security (June 2011).

34. Several comments were made during an off-the-record CNAS working group. For more, see Evgeny Morozov, "Freedom.gov," *Foreign Policy* (January/February 2011), http://www.foreignpolicy.com/articles/2011/01/02/freedomgov?page=0,1.

35. Ellen Nakashima, "Pentagon considers preemptive strikes as part of cyber-defense strategy," *The Washington Post* (28 August 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849.html.

36. "We have to have offensive capabilities, to, in real time, shut down somebody trying to attack us," said GEN Keith Alexander. "You need autonomous decision logic that's based on the rule of law, the legal framework, to let network defenders know what they are allowed to do in the network's defense." C. Todd Lopez, "LandWarNet opens with 4 keys to Internet security," *Army News Service* (3 August 2010), http://www.army.mil/-news/2010/08/04/43256-landwarnet-opens-with-4-keys-to-internet-security/.

37. Ellen Nakashima, "Pentagon considers preemptive strikes as part of cyber-defense strategy," *The Washington Post* (28 August 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849.html.

38. The Protecting Cyberspace as a National Asset Act of 2010, introduced by Senators Joe Lieberman, I-Conn., Susan Collins, R-Maine and Ted Carper, D-Del.; the senators in February 2011 introduced a reworked bill, the Cybersecurity and Internet Freedom Act.

39. Declan McCullagh, "Internet 'kill switch' bill gets a makeover," *CNET News* (18 February 2011), http://news.cnet.com/8301-31921_3-20033717-281.html.

40. Howard Schneider, "Obama Poised to Loosen Rules on Export of Technology," *The Washington Post* (31 August 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/30/AR2010083005331.html.

41. Mark Lander, "U.S. Hopes Exports Will Help Open Societies," *The New York Times* (7 March 2010), http://www.nytimes.com/2010/03/08/world/08export.html.

42. Press release from the Department of Commerce Bureau of Industry and Security, "BIS Updates Encryption Export Rule; Revised Rule Streamlines Review Process, Enhances National Security" (25 June 2010), http://www.bis.doc.gov/news/2010/bis_press06252010.htm.

43. William Lynn, "Remarks at Stratcom Cyber Symposium" (26 May 2010), http://www.defense.gov/speeches/speech.aspx?speechid=1477.

44. Evgeny Morozov, *The Net Delusion*: *The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), 205-6. Emphasis in the original.

45. Department of the Treasury, Office of Foreign Assets Control, 31 CFR Parts 515, 538, and 560, Cuban Assets Control Regulations; Sudanese Sanctions

Regulations; Iranian Transactions Regulations; *Federal Register* (10 March 2010): 10997-11000.

46. Ibid.

47. Restrictions on exports to Syria are based in legislation; for a discussion of the restrictions and the effects on Internet users in Syria see Jillian York, "US gives Iran more net freedom – but what about Syria?" *Guardian.co.uk* (16 June 2010), http://www.guardian.co.uk/commentisfree/libertycentral/2010/jun/16/internet-iran-syria-export-controls.

48. "UNESCO advocates freedom of expression at World Summit on the Information Society" (12 May 2003), http://portal.unesco.org/en/ev.php-URL_ID=17533&URL_DO=DO_TOPIC&URL_SECTION=201.html.

49. Ayman El-Amir, "Last frontier of free speech," *Al-Ahram Weekly Online*, Issue No. 770 (24-30 November 2005), http://weekly.ahram.org.eg/2005/770/op8.htm.

CHAPTER X:
THE UNPRECEDENTED ECONOMIC RISKS OF NETWORK INSECURITY

By Christopher M. Schroeder

FROM THE AUTHOR

I am neither an academic nor policy expert and have no technology or programming background. I am a Chief Executive Officer and investor, who has spent much of my career building companies in environments of rapid change and behavioral paradigm shifts enabled (if not unleashed) by interactive and mobile technology. I have also traveled across the globe and seen first-hand the borderless connections and interdependencies that are at the foundation of these shifts.

My journey into the vast literature on what is referred to as "cyber security" here on the East Coast and "network security" on the West Coast has been eye-opening for two reasons. First, the quality and quantity of people involved is stunning. These women and men are working daily to understand and strengthen our society from terrible, disparate, asymmetric, highly sophisticated actors who wish to steal from us all or worse. Notwithstanding what I have written here, they have done and do God's work.

Second, despite my Internet background, I and my companies fall into virtually every trap of denial, every desire to wish-away these threats. This causes the inaction – or perhaps better said, dulls our willingness to question whether we are doing enough – that is the central obstacle to improving security. I simply cannot get my mind around our electrical or energy grids going down for months or more, and presume our great security apparatus is making sure that it does not – a presumption this paper calls into question. In my own companies, I assume my tech team is on top of any security issue, thus I never stop to consider that by merely losing my iPhone, I may be inviting a significant economic threat to my company, my customers and my family.

In network security, and its economic ramifications, we are clearly all in it together.

THE UNPRECEDENTED ECONOMIC RISKS OF NETWORK INSECURITY

By Christopher M. Schroeder

In February 2011, James Lewis of the Center for Strategic and International Studies (CSIS) testified before Congress, and painted a grim picture of the past year in cyber security. He outlined an extensive – but hardly exclusive – list of network attacks (see "Major Network Attacks from January 2010" text box). Disturbing as they are, significant attacks like these were found and thwarted. This news may seem encouraging, but we should not allow it to lull us into a false sense of security.

Attacks on America's technological infrastructure, targeted industries and businesses are costing the United States economy hundreds of millions of dollars per year, despite significant analysis and actions across the public and private sectors. In fact, the real number is likely in the billions, as the vast majority of economic attacks go unreported and undetected (see "Network Insecurity's Cost to U.S. Businesses" text box).[1] Network attacks are an unprecedented challenge to American economic health and prospects for growth, compounding the broader global and domestic economic pressures of excessive debt and instability. The attacks are borderless, insidious, constantly changing and difficult to source and stop. As Lewis testified: "Despite all the talk, we are still not serious about cyber security."[2]

The connection between the private sector and national security has never been more intertwined than in the area of network security. Network attacks that cost the U.S. military sensitive losses of intellectual property are of the same nature as those that jeopardize the deposits in major banks. In fact, it is increasingly likely that two such seemingly separate attacks could be part of the same orchestrated attack.

Through the prism of the private sector, but with clear link to broader national security concerns, this chapter will explore three areas: the scope of the economic ramifications of weak network security; the barriers blocking greater progress in addressing

Major Network Attacks from January 2010

January 2010: Chinese agents allegedly penetrate Google and 80 other U.S. high-tech companies' networks to gain access to activist Gmail accounts and password management systems.

January 2010: Intel experiences a harmful cyber attack.

March 2010: NATO and European Union networks report "significant" activity and cyber attacks on their networks.

March 2010: The legal defense team of Australian company Rio Tinto is hacked to gain inside information on the trial defense strategy.

April 2010: Hackers break into classified systems belonging to the Indian Ministry of Defence and Indian embassies around the world – accessing information on defense and armament planning.

May 2010: Someone leaks a Canadian Security and Intelligence Service report, underscoring the nature of specific threats to the government of Canada, Canadian universities, private companies and individual customer networks.

Source: Carole Theriault, "CSIS Expert Lists Worst Cyber Security Breaches since January 2010," Naked Security (21 March 2011).

October 2010: Stuxnet, a malicious software that interferes with a computer's normal functioning, attacks Siemens-produced industrial control systems in Iran, Indonesia and elsewhere, resulting in significant physical damage.

October 2010: Hackers steal over 12 million dollars from five banks in the United States and Britain using Zeus malware, available on the black market for 1,200 dollars.

December 2010: Hackers pretending to come from the White House attack the British Foreign Ministry, a defense contractor and other British interests.

January 2011: The Canadian government reports a "major cyber intrusion" involving defense research requiring them to disconnect the Finance Department and Treasury Board from the Internet.

March 2011: Hackers attack French government computer networks for sensitive information on upcoming G-20 meetings.

March 2011: Foreign hackers penetrate the South Korean defense networks in an attempt to steal information on the American-made Global Hawk unmanned aircraft.

these weaknesses despite the clear evidence of their impact; and the limits of some of the current recommendations to strengthen cyber security.

This chapter outlines three conclusions. First, while communication between the private and public sectors is improving, vast insight and experience remain highly compartmentalized within industry sectors and among individual branches of national, state and local governments. Second, most organizations themselves are compartmentalized. These organizations often presume network security is a "tech" issue rather than one that affects all individuals and areas of operations. Third, by breaking down external and internal compartmentalization, there can be shared learning, not only about technology and foiling attacks, but about the significant shifts in human behavior triggered by social networks. These behavioral shifts, as much as technological sophistication, are understood and exploited by those who wish to do us harm.

Scope of Problem

Two studies have become the preeminent analysis on the direct economic impact of penetration

Network Insecurity's Cost to U.S. Businesses

2010 PONEMON INSTITUTE SURVEY OF 45 BUSINESSES

"…the median annualized cost of cyber crime of the 45 organizations in our study is $3.8 million per year, but can range from $1 million to $52 million per year per company."

"The most costly cyber crimes are those caused by web attacks, malicious code and malicious insiders, which account for more than 90 percent of all cyber crime costs per organization on an annual basis."

"The average cost to mitigate a cyber attack for organizations with a high SES ("high security effectiveness" score, a method created by PGP Corporation and Ponemon based on a ranking on 24 security features or practices) is substantially lower than organizations with a low SES score."

"On an annualized basis, information theft accounts for 42 percent of total external costs. Costs associated with disruption to business or lost productivity accounts for 22 percent of external costs."

Sources: Ponemon Institute, "First Annual Cost of Cyber Crime Study" (July 2010): 1-2; New School Security, "A critique of Ponemon Institute Methodology for 'Churn'" (25 January 2011); and "Another Critique of Ponemon's Method of Estimating 'Cost of Data Breach'" (26 January 2011).

MCAFEE'S 2009 "UNSECURED ECONOMIES" REPORT OF INTERNATIONAL COMPANIES

"…more and more vital digital information, such as intellectual property and sensitive customer data, is being transferred between companies and continents—and lost. The average company has $12 million (USD) worth of sensitive information residing abroad. Companies lost on average $4.6 million worth of intellectual property in 2008."

"The global economic crisis is poised to create a perfect information security risk storm, as increased pressures on firms to reduce spending and cut staffing lead to more porous defenses and increased opportunities for cybercriminals. Forty-two percent of respondents interviewed said laid-off employees are the biggest threat caused by the economic downturn."

"Geopolitical perceptions are influencing data policy reality, as China, Pakistan, and Russia were identified as trouble zones for various legal, cultural and economic reasons."

"Cyberthieves have moved beyond basic hacking and stealing of credit card data and personal credentials. An emerging target is intellectual property."

Source: McAfee Corporation, "Unsecured Economies: Protecting Vital Information" (29 January 2009): 3.

of U.S. networks. The Ponemon Institute's July 2010 study benchmarked the magnitude of specific costs to businesses from average breaks in network security. Also, a 2009 McAfee study focused specifically on the intellectual property, data and business risks inherent in the basic ways we all do business today (see "Network Insecurity's Cost to U.S. Businesses" text box). Both studies are eye opening – even with major crises so far averted – and underscore that we remain generally unprepared for the magnitude of network insecurity. While the United States may not be totally asleep at the switch, our good fortune has made us complacent. In fact, coming through the economic downturn, there is evidence that the United States is nationally spending less time and money to protect network infrastructure. In 2010, a CSIS study found that two-thirds of American firms had reduced information security spending in the past year and 27 percent of those reductions exceeded 15 percent.[3]

Thinking in broad, aggregate numbers can be paralyzing – millions per business, billions for entire sectors or a trillion or more globally; it suggests only radical, massive intervention can

address the problems. But breaking down the issues by industry segment and cost vulnerabilities makes the issues more clear and opportunities more digestible.

The following are specific examples of the direct costs to four specific business sectors (electricity, oil, small business and cloud computing); the indirect threat posed to a sector or companies' supply chains; and the reputational costs in the loss of intellectual property and brand value. In addition, the recent earthquake tragedy in Japan – a real-life, real-time example of the ramifications on a highly integrated economy by a different force of disruption – highlights how these costs can interconnect and compound due to unexpected attacks.

DIRECT COSTS IN ELECTRICAL POWER, OIL, SMALL BUSINESSES AND CLOUD COMPUTING

The United States has experienced significant recent network attacks on its electrical grid – both direct and immediate attacks, and "softer" penetrations that steal data and enable attacks to disrupt the infrastructure itself on a later date. Notably, many of the intrusions were detected not by the companies themselves, but by U.S. intelligence agencies worried about network attackers taking control of electrical facilities, nuclear power plants, sewage and financial networks. To get a sense of the economic ramifications far short of an Armageddon-like shutdown of the grid for months, one can look as far back as 2000. Then, a single, disgruntled employee rigged a computerized treatment plant in Australia, releasing over 200,000 gallons of sewage into parks, rivers and grounds around a Hyatt Hotel, and costing millions in damage and cleanup. In the subsequent decade, countless network attacks to power equipment have been reported in multiple regions outside the United States followed by costly extortion demands by the attackers.[4] One would think small, but significant, events like these would put urgency into action to improve the systems. But last month, the U.S. Department of Energy inspector general found that federal testing revealed that standards did not always include controls commonly recommended for protecting critical information systems, including tough password and login protections, noting: "The plodding implementation isn't happening fast enough; risks to the nation's power grid aren't being mitigated or addressed in a timely manner."[5] In fact, there are few universally agreed upon definitions of "critical infrastructure," leading to lack of clarity of when to report an event. The inspector general found that "lack of stringent requirements for defining critical assets contributed to significant underreporting of these assets." Federal officials said power companies had probably undercounted their critical assets and associated critical cyber assets. Undercounting often occurs as definitions of "assets" are not only imprecise but companies do not like to report incidents with specificity in order to protect their reputations. The cost in such compromised assets and subsequent business, therefore, is undoubtedly significant and greater than we think.[6]

U.S. oil and gas industries share similar vulnerabilities. When companies such as ExxonMobil, Marathon Oil and ConocoPhillips were targeted in 2008, their management teams did not fully appreciate the magnitude until the Federal Bureau of Investigation (FBI) alerted them. The intruders accessed things like email passwords and messages, and stole information from the types of executives who would have access to proprietary exploration and fossil fuel discovery information. These events have included the use of custom-made spyware that usual antivirus and electronic defenses could not detect, which at times specifically targets high-level executives (vice president and above). Indeed, some experts say the best traditional defenses still miss more than 20 percent of even basic Trojan attacks, as noted in 2010 by an investigative reporter at The Christian Science Monitor. As these companies spend hundreds of millions on energy

exploration, an attacker would gain enormous financial and timing advantage by knowing what they know. "Identity theft is small potatoes compared to this new type of attack we've been seeing the past 18 months," noted Scott Borg, who heads the U.S. Cyber Consequences Unit, a nonprofit that advises government and the private sector. "This is a gigantic loss with significant economic damage."[7]

Smaller and medium sized businesses – representing the lion's share of U.S. business interaction and job creation – are often more vulnerable, less sophisticated and the least able to spend on network security. With these structural vulnerabilities, and bank accounts larger than average citizens, small and medium sized businesses are increasingly targets of criminal intent.[8] By using 100 to 200 dollar off-the-shelf "do it yourself" toolkits, cyber criminals can easily gain access to the balance sheets of companies; manipulate stock behavior; locate payroll information; get a hold of corporate bank statements and transfer money from that business or make transfers between accounts; gain access to companies' budgets and private financial statements; steal companys' product roadmap and research and development work-plan for industrial espionage; capture companies' credit card numbers for purposes of fraud; or steal intellectual property.[9] Larger retailers Marshalls and TJ Maxx recorded an after-tax cash charge of near 118 million dollars stemming from a January 2007 attack.[10] Smaller retailers could be knocked out of business entirely.

Most recently, Virginia Tech and many other small colleges in the United States, which are all about the same size as medium businesses, have been affected. In February 2011 Virginia Tech discovered that the Zeus virus had entered its computer systems through its controller's office. The Zeus virus "operates by gaining access to information stored on a hard drive and entered online, and it can record keystrokes and take screen shots on a computer it has infected," and in this case hackers "accessed a spreadsheet of social security numbers and other personal information for 369 employees."[11]

Technological innovation for both large and small business has garnered enormous efficiency and cost benefits but has introduced new vulnerabilities in business opportunities. Cloud services companies enable businesses and institutions to secure business and personal data and services to be hosted independently on external servers. These are enormous growth businesses for established players such as Amazon and Google and many innovative, early stage companies. One of the core propositions of these enterprises, however, is offering these services in utterly safe and secure environments. The impact to these businesses of a successful network attack could be existential. They raise costly, unresolved considerations. There is no clear answer on which – the cloud company, the company reliant on the cloud or the user – is financially liable for the damage caused by a cloud attack.[12] Real examples of data penetration, vulnerability and economic risk in the cloud happen regularly, though often underreported, such as thought-to-be private MySpace photos stolen several years ago, regular "disappearances" of credit card numbers across sectors and the April 2011 cloud outage at Amazon Web Services.

SUPPLY CHAIN COSTS

Inadequate network security carries a high direct price tag, yet costs extend well beyond the loss of internal data, process operations and personal information. The increased reliance on real-time supply chain and distribution networks creates compounding risk. Consider, for example, that Japan supplies 40 percent of flash memory chips and one-fifth of semiconductors to global consumer electronics industries.[13] These numbers are, in all likelihood, understated since disclosures of origin are vague and many non-Japanese manufacturers market products sourced in Japan. The ramifications of supply chain disruption here would be significant. Early reporting

on automakers, while somewhat speculative, estimated that around 320,000 units in projected vehicle production lost were lost because parts and components were delayed by Japan's crisis. Inventories helped to guard against disruptions, but eventually they run out. Businesses were forced to alter production plans in other ways. General Motors Co., for example, asked employees to limit travel and expenses, Nissan halted production at four factories, Toyota closed two assembly plants and Sony closed at least six factories.[14] Such shutdowns have compounding behavior on unemployment and purchasing potential.

There is, at the same time, a "new" sphere of supply chain vulnerability that covers not only the operational, product creation and distribution of an enterprise but touches every critical relationship of a company necessary to thrive. "Hacktivists" combining physical and network attacks, often hard to track or address, seek to bring companies to their knees by disrupting their supply chains and every related company relationship. The most infamous example came several years ago from Stop Huntingdon Animal Cruelty (SHAC). According to its websites, SHAC is "an international animal's rights campaign to close down Huntingdon Life Sciences," a company that "tested medical and non-medical substances on 75,000 animals every year from rats to primates."[15] Putting aside one's view on the issues, stop and consider the tactics that landed many of the SHAC founders and its agents in prison. Targets were not merely addressed by lawful protests of the company, but physical and network attacks on its employees, employees' families, shareholders, customers, company business partners, their business partners' business partners, insurers, caterers, cleaners, children's nursery schools and office suppliers. Many of the most egregious attacks occurred in the "physical" world – threats, intimidation, violent vandalizing – but stolen data on activities, names, addresses were all seized, shared and made available online.[16]

INTELLECTUAL PROPERTY AND BRAND COSTS

The essence of all businesses of any size is the trust and credibility they create among their clients, employees and other constituencies. Of all the costs, the value of that trust – manifested in a company's brand and the proprietary information and expertise created – may appear harder to pinpoint. The American National Standards Institute notes the federal government tried to put a number on the issue of damaged brands and stolen intellectual property. It believes that the global cost from cyber attacks around intellectual property alone exceeded 1 trillion dollars in 2009 due to theft of personally identifiable information, system inefficiency and down time, loss of customers and negative impacts on corporate share values.[17] If the numbers were half of this, it would be stunning.

Consider the infamous case from 2009, as cyber actors broke into the Pentagon's 300 billion dollar Joint Strike Fighter project and copied and stole several *terabytes* of data related to the costliest weapons program in U.S. history. The data compromised related to electronics systems and other designs that focused on defenses against the fighter. Two or three contractors involved in the fighter's development had significant vulnerabilities in their networks.[2180] The national security ramifications were staggering and little detail was made public. Economically, however, while the direct costs of the event and the costs to fix it (assuming it can be fixed) were not released, and the government claims that the most sensitive material was not stolen, the economic questions are enormous. Beyond the direct costs, what are the costs of unique intellectual property becoming no longer unique? What are the costs of credibility? How does one measure the cost to Lockheed Martin, and its suppliers, in future contract bids?

AN INSTRUCTIVE ANALOGY: JAPAN'S TRAGEDY

As serious as cyber attacks have been to the American economy, the United States has so far avoided a large scale systemic attack. To make

The American National Standards Institute believes that the global cost from cyber attacks around intellectual property alone exceeded 1 trillion dollars globally in 2009.

concrete the potential repercussions from a broader coordinated breach across the interconnections among the direct, supply chain and intellectual property costs, it is worth considering the very real example of an analogous, unexpected systemic attack. While there are certainly differences between a natural disaster and a coordinated network security crisis, the March 2011 tragedy in Japan – still very much in motion with outcomes uncertain – can be highly instructive.

The challenge is to learn the right lessons. Some suggest the resilience of American and Japanese societies and economies is high and they are able to bounce back strongly. On one hand, Goldman Sachs, the International Monetary Fund and others have come out analyzing Japan through the lens of past earthquakes and natural disasters, noting that while the cost in lives is tragic, in economic terms the impact will be in the short term. Goldman looked at Hurricane Katrina and the earthquakes in Kobe, Irpina, Sichuan and Los Angeles, and noted the short-term hit to gross domestic product (GDP). With enough inventories, construction, shifts of economic benefit and government spending, growth rebounded within months. After Kobe, Japanese GDP fell 2.6 percent month over month following the disaster, but gained again 2.2 percent the following month. Many analysts thought it would take 10 years to bring Kobe back, but in 18 months, manufacturing output was back to 98 percent of capacity. All debris was cleared and infrastructure was functioning within two years. Some conclude that not only was the hit to GDP minimal, but that Kobe and other Japanese cities were made stronger by lessons learned.[19]

But one may fall into the same trap of complacency in these conclusions as we may in network security more broadly. As Nassim Taleb, the provocative expert on risk management cautions: "We respect what has happened, ignoring what *could have* happened."[20] Focusing thus more critically on what could go wrong – in fact, what is still going wrong differently in today's catastrophe versus the past – it is clear that the driver of fast recovery is based on how long systems are down. The core predictor of the economic impact is a combination of enough plans and processes in place, speed to get power and electricity back on line and significant government resources. Thus, in learning from the current tragedy and possible ramifications of a significant cyber incident in the United States, it is more instructive to note as Goldman Sachs did:

The economic consequences are significantly greater than past events. Estimates suggest Northern Japan is already 1.6 times Kobe in cost estimates.

Factors can make the length of "down time" unpredictable, thus complicating the prognosis of recovery. In Japan, the nuclear aspect makes scenarios still unpredictable, increasing the likelihood of much longer time than past events for electricity to come back up to full capacity. In addition, there are significant unintended consequences as other nations, like Germany, shut down or review their own nuclear programs.

The scale of downed power capacity overall nationwide can be worse than expected. In Japan, the crisis shut down 10 to 12 percent of power station capacity.

Supply chain issues are generally unclear until they manifest. In the case of Japan, we are only beginning to see the ramifications in trade in items such

as semiconductors, digital cameras petrochemical products. Inventories across the board appear to be able to last six weeks or so, but disruption could be longer. Unintended and far reaching surprises can create compounding crises. *The New York Times* reported that not only Japanese ports have been closed or shifted due to radiation, but Xiamen ports detected radiation in Mitsui container ships and instituted time-lengthy processes of reviewing containers around the world. One German container shipping company, Hapag-Lloyd, stopped service to Tokyo and Yokohama outright.

Governments are now especially ill prepared fiscally to deal with this scale of catastrophe. Deficits in 1995 in Japan were 92 percent of GDP, but 221 percent at the time of the March 2011 disasters. Key countries that could step up to support are in similar circumstances.[21]

Who can predict the spiraling nature – structurally and psychologically – of a systemic disruption of U.S. energy supplies, or the massive loss of private or business data and intellectual property, or the differences between a "brief" issue of a few days versus a few months? Who will put their neck out on predicting the unknowns – the uncertainty of nuclear issues in the case of Japan or network worms or viruses planted today that may change or not manifest themselves until a later date?

Where and Why Resistance?

With the problem so clear, the ramifications so significant and so much activity in place, it may seem remarkable that there is still resistance to addressing the issues and talking about them more openly. A Verizon study in 2008 noted that part of the issue was basic awareness. More than two-thirds of victims are unaware that compromised data is on their systems to begin with. Seventy-five percent of attacks are not discovered by the victims themselves.[22] But this does not explain, as many analysts believe, that fewer than 10 percent of attacks are actually reported to authorities.

Greg Day, Director of Security Strategy at McAfee, argues that businesses do not want to share what happened out of embarrassment and out of fear of what kind of impact it will have on their reputation with customers.[23] Bruce Schneier is one of the great thought leaders on network security and the most circumspect voice, balancing the importance of the issue but not panicking about it. He notes that the overall complexity of the problem breeds fear and complacency, "Because we do not understand the risks, we make bad security tradeoffs."[24]

Nassim Taleb notes that heroes are rarely recognized for the problems they have prevented,[25] and there is even less recognition from one's investors or even customers.[26] How many of us, in our organizations, have rewarded someone for something that *did not* happen?

Too often, the whole issue of network security is relegated as a "tech" and "tech team's" problem. As one study notes, this leads to:

> The dangerous situation wherein most employees don't feel that they need to be responsible for the security of their own data. So although a corporation's finance, human resources, marketing, legal and other departments all own data, the tendency is to believe that the responsibility for securing that data rests down the hall with the IT department. This attitude substantially weakens overall corporate and organizational security.

Companies often think compliance is security – no need to raise questions, just make sure the boxes are checked.[27]

Much of the resistance boils down to a misalignment of incentives. Schneier notes that systems often fail because the people who could protect a system are not the ones who suffer when something goes wrong.[28] Examples in business can be instructive for incentive challenges in any organization. He cites how retail understood incentives for in-store security and employee theft by initiating "your purchase is

free if you don't get a receipt." On the surface, this seemed like a form of customer service when it was more about aligning incentives toward security. But the genius was that by aligning incentives of customers and store workers by compelling documentation – which created a track record – employee theft all but disappeared. He also notes that when ATM cardholders in the United States complained about phantom withdrawals from their accounts, courts generally held that banks had to prove fraud. Here the incentives for banks were clear and improving security was high on their agenda in order to keep costly fraud low since they paid the costs. In the United Kingdom, the reverse was true as the courts presumed most fraud was cardholder based, so the banks had little incentive to spend the money on security infrastructure and did next to nothing.[29] Tyler Moore of Harvard agrees, "The party making the security-efficiency trade-off is not the one who loses out when attacks occur. This naturally leads to suboptimal choices about where to make the trade-off."[30] Incentive alignment throughout an organization, and throughout functions, may be the best predictor of security improvement.

At the same time, one has to be realistic and flexible, especially as the private and public arenas connect. Even with the best efforts and intents, incentives can clash, and this has to be accepted as part of the realities. Schneier notes that the security system is based on policy defined by an array of players with subjective understandings of the problem. "The whole process is situational, subjective, and social. Understanding, and working with, these various agendas is often more important than any technical security considerations. It's pointless to hope that a wave of selfless, nonsubjective security sensibilities will suddenly sweep across society."[31] While solutions must be sought, cognizant of these structural and behavioral realities, we cannot be held captive by them. It leads directly to the insufficient creativity, transparency and open communications regarding what is required.

Are Policymaking and Regulation Enough?

Policymakers typically focus on the hammers at their disposal – pressing for changes in legislation and regulation – as the required means to greater security. These tools have their places but the solutions often raise their own limitations.

One path has been to align incentives and clarify where liabilities lie. Schneier recommends what he calls one step with two consequences. First, start by enforcing liabilities. If CEOs and government executives alike are to spend significant resources on security, they must be liable for mishandling their customers' data. Software developers should also be liable for a level of security vulnerabilities in their products without compromising their ingenuity. Two consequences follow. First, parties must be more easily able to transfer liabilities to insurance companies. In the offline world businesses purchase physical security such as locks and alarms because their insurance rates go down. This, in turn, makes insurance companies serious about risk analysis and the effectiveness of security products. Second, where companies focus internally on their mechanisms to manage risk and outsource services, similarly, the system will be more reliable.[32]

Private sector entrepreneurs like Drew Bartkiewicz believed there was a business opportunity here and jumped on the liability bandwagon. He launched CyberFactors, a company that evaluates cloud providers for risk. It creates warranties to help customers and cloud policies for insurers. He says cloud companies are currently not addressing their financial liabilities. Cloud companies cap their indemnification at the value of the contract. But, while a contract may be worth 10,000 dollars, the stolen data could be worth much more. Bartkiewicz says the average cyber incident could cost 4.5 million dollars.[33]

Despite this logic, network security insurance has never really taken off. As Moore explains:

> On the demand side, insurers complain of a lack of awareness to cyber-risks by firms … Consequently, policies that increase disclosure of cyber risks and incidents would help stimulate further growth in the cyber-insurance market … but, in addition, responsibility for dealing with cyber-incidents must be clearly assigned to the appropriate party, otherwise no claims will need to be made. On the supply side, information asymmetries – in particular the difficulty of assessing the security of an insured party – help explain why insurance companies still don't differentiate premiums based on technical criteria.

He concludes rightly that while insurance may eventually be part of the long-term solution to improve network security, it will require adequate policies to help make it happen.[34] In addition, there is little agreement on whether or where to hold software developers responsible at the cost of suffocating the very innovation central to U.S. competitiveness and growth. Incentives, rather than penalties, can be stronger.

Melissa Hathaway led President Obama's cyberspace policy review and President George W. Bush's "comprehensive national cybersecurity initiative." She argues that regulatory clarity and teeth are required because the issues at stake are so significant they require compelling mechanisms. As network security is a public good that government cannot provide due to the very nature of information technology architecture, some kind of intervention is needed to correct potential market failures. She recommends turning to three regulatory agencies to help. First, the Securities and Exchange Commission can require CEOs to validate their companies' information infrastructure, which should include the ability to protect data, erect appropriate safeguards and respond effectively to cyber security incidents. Second, the Federal Communications Commission can tap into the private sector's talent and have core telecommunications providers and Internet service providers (ISPs) do more to protect infrastructure. ISPs have great insight into global networks and early pattern behaviors, and they can alert consumers that they may be affected. Comcast is a good example, having launched a Denver pilot of emails to ask consumers to visit their security pages, offering them free antivirus and security software. Germany has enforced this, explicitly going after botnet infestations. The German Federal Office for Information Security mandated that its ISPs track down infected machines and advise users on how to clean their computers. Hathaway argues for a completely inclusive group – AT&T, Verizon, Sprint, Comcast, Cox, Time Warner, Google, Microsoft, Amazon and any company that provides cloud service regardless of wired or wireless. Finally, the Federal Trade Commission can extend its role to be more proactive. It could add warning banners or labels, like those used for tobacco and alcohol, that inform customers when they are undertaking e-commerce transactions that may not be secure.[35]

Industry, of course, objects strenuously to further regulation and prefers the self-regulated approach. But Hathaway's recommendations get to two fundamental issues at the core of greater network security that can and should be self-imposed: Organizational buy-in from the top that network security is not an isolated activity but core to every member of that organization; and increased transparency and information sharing among all internal and external players to raise alerts, best practices and insight to keep ahead of the attackers.

The Key – Broad Organizational Buy-In and Greater Openness, Transparency and Knowledge Sharing

For any organization of any size, a critical need is in changing the mindset that network security is only a tech division problem, and promoting an active awareness and sensitivity in all functions. In the same way civilians are encouraged to report or be aware of strange activity at airports today, every

member of our organizations see daily activities that may make the organization collectively smarter and more secure. It further means those who directly act on security activities should not be viewed as "chief naggers," but core parts of the strategic planning. This mindset has many ramifications beyond enhanced alert detection. It also helps to instill in the culture flexibility to react to a constantly changing world that will make the enterprise overall more secure. As Schneier notes, "Good security systems are resilient. They can withstand failures; a single failure doesn't cause a cascade of other failures. They can withstand new attackers, including attackers who cheat. They can withstand new advances in technology. They can fail and then recover from failure."[36] The key is that a network security culture is not about merely compliance but always thinking of the next challenge and opportunity to be "secure now" (which we never are). As an example of this awareness, Citigroup and others not only encourage security throughout their organizations, but proactively employ so-called ethical hackers to test their security systems from weak points. How many businesses and government organizations can say the same?

Employees are critical; so is the question is which strategic assets employees have access to. Securities and commodities exchanges are vetting traders using their private network so in theory exchanges and financial institutions should know who is on their networks at all times. In fact, studies show the weakest link is often employees – as much by accident as by intent. Increasingly hackers are using Facebook, LinkedIn and Twitter and quick access to mobile devices to build relationships and interconnections with key individuals at firms. "It only takes one person to click on a link for hackers to gain access," notes Mark Harris, vice president at financial IT vendor SophosLabs.[37]

Perhaps the greatest impact, however, comes by simply greater clarity and openness in communication, and sharing learning among companies, industries and the private and public sectors. Debates rage about the good and the bad of the progressively transparent societies we are becoming, but the debates are moot. This Pandora's Box is forever opened and, most important in the context of network security, those who wish us harm are excellent at exploiting it. The benefits to open source development in the software development fields are clear: the power of crowd-sourced information and reporting appear in the news now daily. While there are risks to both the public and private sectors of opening up to their attacks and best practices, the risks of not doing so are profound.

Last year, Google publicly discussed a set of cyber attacks known as Operation Aurora (likely originating in China), which helped generate faster defenses and solutions. Some hoped this experience will lead to greater openness on the part of companies. But resistance to more public information sharing is significant, including "Lack of trust between parties; law and regulations that discourage full disclosure of information; the vested interests of security vendors; fear of bad publicity and customer backlash; silos and turf wars within government agencies," as Erik Battaler noted in *InformationWeek*. Many executives fear the cost of exposing a vulnerability to competition or consumers and believe the risks associated with sharing information are greater than the risks associated with a network security attack. But they overestimate these concerns in a progressively transparent world. In fact, the path is clear: "First, the public and private sectors need to share more information – more parties must be included and new platforms used. Second, they must pay more attention to defending against attacks that threaten critical IT infrastructure and even damage physical facilities. Third, their collaboration must be ratcheted up to the next level: real-time identification and response to threats occur and, more to the point, "moving security practices from a

reactionary posture to one that's proactive and pre-emptive," says Rich Baich, leader of Deloitte's cyber threat intelligence group.[38]

Paul Rosenzweig, formerly the Deputy Assistant Secretary for Policy at the Department of Homeland Security, notes that security clearance issues can be particularly challenging. "As observers have noted, there is a disconnect between our counter-intelligence, which is often aware of risks to our cyber supply chain, and our procurement processes, which cannot have access to classified information regarding supply chain threats."[39] He adds:

> Private sector actors are notoriously distrustful of government interference and regulation. And the converse is also true – government institutions like the NSA (National Security Agency) with (perhaps) superior knowledge of threat signatures and new developments in the arsenal of cyber attackers are deeply reluctant to share their hard won knowledge with the private sector at the risk of compromising their own sources and methods.[40]

But the classic reasons not to be open fly in the face of the benefits of significantly greater and open communication. As Moore notes:

> If the remote login to a power stations' controls is compromised and the utility keeps mum about what happened, then other power companies won't fully appreciate the likelihood of an attack. When banks don't disclose that several business customers have quickly lost millions of dollars due to the compromise of the company's online-banking credentials, the business customers that have not yet fallen victim remain ignorant to the need to take precautions. Thus in cyber security, we face information asymmetries across firms, not only between consumers and firms.[41]

The basic models are there. For years each industry has formed membership-based Information Sharing and Analysis Centers (ISACs) to share, on an anonymized basis, information on attacks. The Department of Homeland Security subsequently defined 18 areas of analysis centers including the agriculture, banking, chemical and defense industries as well as government facilities. Information Sharing and Analysis Centers possess an outreach and connectivity network that is approximately 85 percent of the U.S. critical infrastructure.[42] The challenge, though, remains that each industry is siloed and the free flow of information among industries and with government is still challenged. Rosenzweig concedes, "despite efforts within the ISACs, we have yet to successfully develop the political will to create the culture where information sharing enables cyber security improvement."[43] The finance sector is viewed as a leader overall in this communication. It created a broader, senior level group – the Financial Services Sector Coordinating Council (FSSCC), including Bank of America, Citigroup, Morgan Stanley and Visa – under which their ISAC looks at technical issues. The FSSCC coordinates the protection of IT and other infrastructure operated by banks, insurance companies and other financial services at a strategic and CEO level. It does that work in collaboration with the Departments of Homeland Security and Treasury and is expanding its coordination.[44] Director of the Cyber Statecraft Initiative Jason Healey characterizes this as "close to perfect" with the industry and government groups regularly meeting separately, but often on the same day and in the same location. "Then they gather together immediately and compare notes and learning. Then they all go out and have dinner. It builds trust and relationships."[45] These are relationships among companies, among industries and between the public and private sectors.

There can be no more delay in breaking down the barriers to openness, the dated excuses of security that often mask territoriality and concern about protecting one's own vested interests. Everyone is

vulnerable; everyone has had issues; everyone has outstanding experience and learnings that shared can have significant ramifications across industries and among the public and private sectors.

A New Engagement

There is also a different kind of information sharing – and outreach to significant, untapped expertise in the security equation – that would open all the existing players to thinking differently and reframing their approaches. It is imperative here to understand that the new threats we face are enabled by technology but also facilitated by core understandings of human behaviors. Information technology has unleashed the ability for anyone, anywhere, to find what they want on their terms when and how they want it; to connect with people in extensive new forms of community and share information, ideas, emotions and locations at unprecedented size, scale and speed over multiple and mobile devices. How people form these connections, what they share, how they share it, how the organize and take action in both the online and offline world have been manipulated by those who wish to do us harm. This core behavioral expertise and understanding is found in the great consumer-facing technology enterprises – Amazon, Google, Facebook, Twitter and many enormous multiplayer gaming experiences – as well as in up-and-coming innovators and entrepreneurial communities. In fact, the United States is unique in entrepreneurial innovation and understanding and the behavioral ramifications that come with them. Yet these behaviors, and relationships with these enterprises, are often utterly foreign to most traditional businesses and government institutions at all levels.

The goal of greater engagement here is not to compare best practices in security technology – though some of this already happens with Amazon, Cisco and many others to great mutual benefit and insight. The more of this, the better. Nor should greater engagement concern privacy advocates as it is not about a creepy or inappropriate "snooping around" of individuals' personal behaviors. It is, rather, a better understanding overall of how individuals define themselves over time, communicate, build networks, share ideas, take actions, use mobile devices and rely on geo-location through technology. Social networks and search and mobile companies all are essentially gurus of human behavior – not of what people say they do, but by what they actually do. These enterprises, perhaps more than any, understand the minds and opportunities to improve peoples' lives and engagement – great goals manipulated and befouled by the intent of attackers. This understanding is often all but untapped by and unconnected to other industries and policymakers alike thinking through network security.

It is a common cliché to talk about the "new new normal" wrought by the changes surrounding us by technology and evolving behaviors. The uncertainty this offers, the shoulder shrugging "we can never protect everything" attitude it conjures and the smug arrogance that certain executives or policymakers "don't get it," at best misses the point. At worst, it drives decision makers to do the minimum or seek merely tried and true systems and analogies to address the very real and different issues we face. The fact is that network security issues are not new per se, but are ever changing and push our existing frameworks continuously. As concerning as this is, the amount of experience, judgment, technical skill, technical capability and behavioral understanding at our finger tips is unprecedented. Connecting the dots of these capabilities and seeking new kinds of expertise is the best way to stay ahead of the new and ever changing threats of network insecurity economically and in terms of broader national security.

ENDNOTES

1. Homeland Security News, "Call for Creating a U.S. Cybersecurity Emergency Response Capability" (13 April 2011).

2. Carole Theriault, "CSIS Expert Lists Worst Cyber Security Breaches since January 2010," Naked Security (21 March 2011).

3. Cited in Internet Security Alliance and American National Standards Institute, The Financial Management of Cyber Risk (2010).

4. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *The Wall Street Journal* (8 April 2009).

5. Mark Clayton, "America's Power Grid Too Vulnerable to Cyberattack, US Report Finds," *The Christian Science Monitor* (3 February 2011).

6. Ibid.

7. See, for example, Mark Clayton, "US Oil Industry Hit by Cyberattacks: Was China Involved?" *The Christian Science Monitor* (25 January 2010); and Mark Clayton, "Report: Chinese hHackers tTargeted bBig oOil cCompanies, sStole dData," The Christian Science Monitor (10 February 2011).

8. Ericka Chickowski, "Sound the Alarm," *Entrepreneur Magazine* (June 2010).

9. Yuval Ben-Itzhak, "Businesses Under Cybercrime Attack: How to Protect Your Corporate Network and Data Against Attack," CXO Europe (26 March 2011).

10. Ibid.

11. Ben Wieder, "Data-Stealing Virus Hits Virginia Tech, Potentially Compromising 370 Employees," The *Chronicle of Higher Education* (14 March 2011).

12. Arik Hesseldahl, "Are Cloud Companies in Denial About Risk?" All Things Digital (16 March 2011).

13. Noel Randewich and Miyoung Kim, "Japan Quake Strains Supply Chain from Chips to Ships," Reuters (14 March 2011).

14. William Alden, "Japan Disaster Threatens Economic Recovery, Affects Economies Globally," The Huffington Post (15 March 2011); David Welch, "Automakers May Lose 600,000 Vehicles as Quake Hits Parts," *BusinessWeekBloomberg* (26 March 2011); and Terje Langeland, "Sony, Toyota Shut Factories After Power Shortages Follow Earthquake Damage," Bloomberg News (14 March 2011).

15. Facebook, "Stop Huntingdon Animal Cruelty" (as of 17 May 2011).

16. BBC News, "A Controversial Laboratory" (18 January 2001); Sandra Laville, "Animal Rights Extremists Still Targeting Lab," *The Guardian* (24 December 2008); and interview with Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic Council.

17. Internet Security Alliance and American National Standards Institute, The Financial Management of Cyber Risk (2010).

18. Siobhan Gorman, "Computer Spies Breach Fighter-Jet Project" *The Wall Street Journal* (21 April 2009).

19. Peter Drysdale, "Japan's Earthquake and Its Economic Impact," East Asia Forum (14 March 2011).

20. Nassim Taleb, *The Black Swan* (New York: Random House, 2007): 132.

21. Keith Bradsher, "Global Supply Lines at Risk as Shipping Lines Shun Japan," *The New York Times* (25 March 2011); Goldman Sachs, *The Economic Impact of Japan's Earthquake* (24 March 2011).

22. The Verizon Business Risk Team, 2008 Data Breach Investigations Report (June 2008).

23. Rachel Wolcott, "Hacking Raises Security Questions at Exchanges," Financial News (21 March 2011).

24. Bruce Schneier, *Beyond Fear* (New York: Springer, 2003): 31.

25. Nassim Taleb, *The Black Swan* (New York: Random House, 2007): xxiii.

26. Nassim Taleb, *Fooled by Randomness*, Second Edition (New York: Random House, 2005): 26.

27. Internet Security Alliance and American National Standards Institute, The Financial Management of Cyber Risk (2010): 12-13.

28. Bruce Schneier, *On Security* (Hoboken, NJ: Wiley, 2008): 145.

29. Ibid.: 148.

30. Tyler Moore, "Introducing the Economics of Cybersecurity," in *Proceedings of a Workshop on Deterring CyberAttacks* (Washington: The National Academies Press, 2010): 7.

31. Bruce Schneier, *Beyond Fear* (New York: Springer, 2003): 42.

32. Bruce Schneier, *On Security* (Hoboken, NJ: Wiley, 2008): 153.

33. Arik Hesseldahl, "Are Cloud Companies in Denial About Risk?" All Things Digital (16 March 2011).

34. Tyler Moore, "Introducing the Economics of Cybersecurity," in *Proceedings of a Workshop on Deterring CyberAttacks* (Washington: The National Academies Press, 2010): 13.

35. Melissa E. Hathaway, Creating the Demand Curve for Cybersecurity (Washington: Atlantic Council, December 2010).

36. Bruce Schneier, *Beyond Fear* (New York: Springer, 2003): 120.

37. Rachel Wolcott, "Hacking Raises Security Questions at Exchanges," Financial News (21 March 2011).

38. Erik Bataller, "Why Cybersecurity Partnerships Matter," InformationWeek (26 March 2011).

39. Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," in *Proceedings of a Workshop on Deterring CyberAttacks* (Washington: The National Academies Press, 2010): 250.

40. Ibid.: 254.

41. Tyler Moore, "Introducing the Economics of Cybersecurity," in *Proceedings of a Workshop on Deterring CyberAttacks* (Washington: The National Academies Press, 2010): 13.

42. Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," in *Proceedings of a Workshop on Deterring CyberAttacks* (Washington: The National Academies Press, 2010): 255.

43. Ibid.

44. Erik Bataller, "Why Cybersecurity Partnerships Matter," InformationWeek (26 March 2011).

45. Author interview with Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic Council.

Acknowledgment: I wish to thank Matt Devost of Fusion X LLC., and Jason Healey of the Cyber Statecraft Initiative, whose extensive careers and wisdom on these issues have been invaluable. I also wish to thank Lucie Leblois of HealthCentral who helped research this paper.

CHAPTER XI:
HOW GOVERNMENT CAN ACCESS INNOVATIVE TECHNOLOGY

By Daniel E. Geer, Jr.

America's Cyber Future

Security and Prosperity in the Information Age

HOW GOVERNMENT CAN ACCESS INNOVATIVE TECHNOLOGY

By Daniel E. Geer, Jr.

The U.S. government does not take sufficient advantage of innovative technology except, possibly, within "black" budgets. The U.S. government is missing a river of innovative technology, and it is both broad and deep. No one technology missed is a crisis, but in the aggregate, the U.S. government is falling behind in what it could do and what it is expected to do to protect the nation from cyber security threats. Strategies for accessing that technology must account for both the breadth and the depth of what is being missed. The setting of priorities is necessary. A prudent priority ordering might begin with 1. preventing accidental cyberspace incidents; 2. preventing sentient opponents from seizing an opportunity to disrupt systems; and 3. avoid wasting resources that could be spent on the first two. The accidents will largely be ones causing loss of availability of information; the sentient opponents will largely target confidentiality and integrity of information upon which the U.S. government relies; while efficiencies are those that use information to make products, processes or grids "smart" without creating opportunities for either accidents or opponents. Just as information without security has negative value, consistently missing innovation in cyber security technology consistently decreases the value of information that the U.S. government does hold, perhaps to the point of turning an information asset into a liability.

The question with respect to cyber security technology: Is the U.S. government's consistent problem one of availability or of access? This chapter answers "both" and then explores the implications of that answer.

The first rule of statistical inference is that all data has bias; the question is whether one can correct for it. So that the reader can correct for my biases, they are:

1. Security is a means and not an end. Therefore, cyber security policy choices must be about

the means to a set of desirable ends, and about affecting the future – which is why security is about risk management and why the legitimate purpose of risk management is to improve the future, not to explain the past.

2. Security investment in the absence of security metrics will only result in overspending or underprotecting. No game play improves without a means of keeping score; decisions about developing, implementing and terminating cyber security programs are no exception. In fact, improving cyber security metrics programs is a meaningful goal in its own right. Meaningful metrics were the core of public health interventions that have saved more lives than has any single medicine.

3. The problems with cyber security are the same as many other problems, yet they are also critically different. However, humans often misclassify which characteristics are the "same" and which are "different," beginning with the sharp differences between the realities of time and space in the physical world and in the digital world. (For example, if digital data is stolen, the owner likely still physically possesses it. Another example includes the speed of cyber crime – no law enforcement works at the speed of light whereas electronic crime does.) Nevertheless, we have no choice but to analogize wherever we can. There is no time to invent everything from scratch.

4. The cyber security problem cannot be solved absent a succinct mission goal. Reactive actions, however good, cannot drive policy. At the highest level of abstraction, the mission goal of cyber security is to:

- Move from a culture of fear.
- Move to a culture of awareness.
- Move to a culture of measurement.

Summary of Key Points

- There is no ready way to "force" more good ideas to appear per unit time.
- Incentives can meaningfully reorder those who have the earliest access to evolving cyber security realities, but cannot limit who ultimately has access.
- Quality cyber security information is better bought than seized.
- Dependence on any cyber technology progresses to risk, unless purposefully checked.
- For mature cyber technology, reduce the mean time to repair.
- For new or quickly evolving cyber technology, increase the mean time between failures.
- The U.S. government cannot limit itself to U.S. cyber security technology.
- Where the U.S. government cannot accelerate deployment of cyber security technology, it must decelerate deployment of any other cyber technologies that increase complexity.

While this mission goal is not operationalizable, *per se*, it is consistent with the notion of security as a means, and the notion that no game play improves without a way of keeping score.

Incentives

The cyber security market is an atypical market. The rate of change is its dominating driver, and there are no willing customers except those who are recently embarrassed or who are facing an audit that they know they cannot pass. No jurisdiction needs laws against things which are impossible, for example, yet the instantiation rate of previously impossible things is nowhere so high as it is in cyber security. As such, incentives must be future-driven and audits must be anticipatory if policy is not to be embarrassment-driven.

Complexity is the chief enemy of security. Some of the complexity is unavoidable, but much of it is not. It is hard to encourage simplicity – every critic will find another security issue that has to have its own countermeasure, its own special case. Because all novel attacks are special cases, cyber security is becoming a catalog of special cases – and the more security products we install, the greater the complexity we create due to the interactions of security products with each other and with what they are installed to protect. This is the heart of the enmity between complexity and security; security's task list is all multi-way interactions, all the time. (Technically, value rises fast[1] but risk rises faster.[2])

How does the U.S. government encourage the timely availability of both passive and active defense at rates that scale with the threat? Logically, there are three alternatives:

1. If such solutions just appear on their own, then the U.S. government focus would be locating, acquiring and deploying them early.

2. If such solutions do not just appear on their own but good ideas do, then the U.S. government focus would be encouraging good ideas to become solutions.

3. If good ideas do not just appear on their own, then the U.S. government focus would be increasing the supply of people in a position to have good ideas.

It is my judgment that good ideas are rare and that there is no ready way to "force" more good ideas to appear per unit of time. Put differently, when research is fully funded, adding more money does not help and may hurt as it draws in increasingly unqualified actors. We can argue about what constitutes "fully funded" with respect to cyber security research, but the production of academic papers related to cyber security has been increasing at a compound annual growth rate of 20 percent for three decades.[3] For the moment, let us therefore accept that exponential growth in cyber security papers does actually reflect an exponential growth in cyber security knowledge. Assuming an exponential growth rate in cyber security knowledge is sufficient for the U.S. government needs, the question is then the rest of the lifecycle:

(nil)→ idea→ solution → detected → acquired → deployed

INCENTIVES: WELLSPRINGS

With a growing supply of good ideas to mine, my question is whether turning good ideas into solutions is constrained by the willingness of good idea creators to move forward with solutions. What powers this process? It is rarely academia; academia rewards those who publish most frequently, which creates incentives to publish multiple papers on different aspects of an idea rather than developing a working prototype. Among independent researchers, such as endowed institutes and corporate research departments, working prototypes are the checkpoint of a successful project rather than an entry in an academic bibliography. However, to the extent that such work tends to be entirely consumed by and within its sponsors, there is no assurance that an idea turned into a solution within such an institution will ever be available to the U.S. government in a directly consumable form. Put differently, a happy result in the laboratory that nevertheless turns out to be off-strategy or self-competitive will not appear in next year's catalog regardless of its utility to the government.

Where working prototypes do exist, there might well be some U.S. government-driven incentives that would work. Beginning with an analogy, the "orphan drug" programs of various governments exist to ensure that good ideas (therapies) that would not otherwise come to market have an alternate path for doing so. There are several mechanisms, but taken together they dramatically reduce the size of the minimum

economically addressable market, thus increasing the probability that the possible product becomes an actual product. (Mechanisms include tax incentives, enhanced patent protection and marketing rights, clinical research financial subsidization and creation of government sponsored enterprises, inter alia.)

Within cyber security, antivirus firms illustrate this experience exactly. An antivirus firm simply cannot afford the lifecycle cost of bringing a countermeasure to market unless there are 20,000 to 30,000 victims.[4] Attacks face no active defenses until those attacks are no longer rare and will face no active defenses at all if they stay rare. One could imagine that what has been learned in making therapy available for rare medical diseases may apply directly to treating rare cyber security maladies. (One must particularly note that "targeted cyber attacks" are purposefully unique and hence rare in the wild, so the analogy holds up especially well given sentient opponents.) The U.S. government might consider lowering the minimum economically addressable market (the number of people willing to buy a product in order to make production viable) for cyber security products so that solutions known to be possible become solutions known to be available.

This is easier said than done, and the analogy with orphan drugs is limited; the patients needing an orphaned drug are identifiable whereas the patients needing an undeveloped cyber security therapy are not. In the case of President Obama's famed Blackberry, rather special therapy was applied to a single known patient. Perhaps Obama's therapy cannot be scaled up; perhaps it relies on its obscurity to provide some of its security. But a cyber security solution for a high-value target may well have value to others and some economic mechanism to get that solution to an increasing number of high-value targets would certainly be a net positive.

INCENTIVES: ADDRESSING THE BALANCE OF POWER

All cyber security technologies are dual use – usable for either defense or offense. Some products lean more toward offense – platforms for developing attack tools to be used for legitimate penetration testing (Metasploit, Canvas, Core Impact, etc.) – but purely defensive products can readily be repurposed for offense, e.g., a successful attack on a security surveillance product will generally lead to great power for the attacker. Not all security technologies can be of dual use, but while the opportunity for any ordinary commercial cyber security product is defense, that does not mean that that product cannot be expanded toward other uses which may interest the U.S. government (and other governments). It does mean that conversions from defense to offense are much more likely than conversions from offense to defense because the commercial world tends always to advertise its (defensive) capabilities whereas states tend always to hide their (offensive) capabilities. Private actors are increasingly taking "law enforcement" into their own hands by taking offensive measures to disable threats instead of reactively defending against them.[5]

There has been a considerable shift in the balance of power between attackers and defenders. Prior to 2007 or so, attackers were mainly amateurs seeking notoriety; they made their work public as a prerequisite to being praised. Embarrassed, the software industry improved the security of its products just enough to make the braggarts go away. Discovering exploitable vulnerabilities got harder; and because it could no longer be a hobby, it became a job. When this changed around 2007, the main drivers of the attack space moved from braggarts to brigands, people who could treat finding vulnerabilities as a paying job. Because brigands do not make their findings public, the fraction of exploitable vulnerabilities that are publicly known (rather than privately held) began an unstoppable decline. Brigands live in a differentiated black

economy and, most importantly, fund their own research and development out of revenue. Another shift occurred in 2010 or so when the main attackers moved from brigands to brigades (including irregular armies with geopolitical ends).[6] Because brigades stockpile weapons, the fraction of deployable weaponry that is publicly known (rather than privately stockpiled) began an unstoppable decline. One can observe that the more cyber security matters, the less complete our knowledge.

Because an increasing knowledge gap between attackers and defenders is inevitable absent meaningful correction, investment in discovering exploitable vulnerabilities advances national security goals. Perhaps a response is the National Cyber Range (NCR) under development by the Defense Advanced Research Projects Agency (DARPA), an agency of the Department of Defense (DOD) responsible for the development of new military technology for use by the military.[7] According to its program manager, the NCR will test and validate cyber research and technologies and will help identify promising new avenues of research. Consistent with the idea that all cyber security products are dual use, the NCR work product is likely to include both defensive and offensive results. At the very least, the defensive technology should be shared with industry so that technology can appear in products that the U.S. government buys, rather than having to be retrofitted to those products under some procedural cover of darkness.

Those defenders that can and do best contain, if not address, the knowledge gap between themselves and the offenders are at an advantage relative to those defenders who fail to do so.

Taking both the post-2007 reality – that exploitable vulnerabilities are trade goods – and the post-2010 reality – that exploit tools are now trade goods as well – raises a question: Would it not be possible for the U.S. government to corner the market? Would it be possible for the government to just buy up all the vulnerabilities? Retired U.S. Air Force Gen Michael Hayden, a former director of the CIA and National Security Agency (NSA), is already on record that software vulnerabilities held by the U.S. government should be declassified, so the government buying program and declassification would be of great value to the software market that, in due course, would benefit the government as a customer of the software market.

There are existing vulnerability purchase programs already in place. One example is the company iDefense that pays 15,000 dollars per previously unknown vulnerability.[8] It is widely understood that other buyers are not so open. Whatever prices paid for those exploitable vulnerabilities by whatever buyer, the vulnerabilities themselves should be considered trade goods. Prices like iDefense's 15,000 dollars per vulnerability may be meaningful to the seller, but they are budget lint to the U.S. government. Cornering that market is certainly within the U.S. government's budgetary power. Some sellers will be reluctant because to sell is to announce oneself, so intermediaries would likely be involved and would naturally require assurances of safe passage, just as we do for bounty hunters (bail enforcers). The United States has spent nation-state adversaries under the table before and can do it in cyberspace.

It is possible to calibrate the value of newly acquired vulnerabilities. There are commercial entities whose products record all traffic, such as Netwitness.[9] So it is feasible to compare the vulnerabilities being sold to what network traffic has been observed in the wild. Recording all network traffic indirectly establishes a freshness date for what is being offered in the cyber vulnerability bazaar: If an attack can be mounted against a newly obtained vulnerability, then one must ask if that attack has already been used in the field before the defender became aware that the vulnerability existed. If it was previously used, then the telltale signs of that use will have appeared in those full-catchment network logs.

Formally, the null hypothesis (the conservative assumption) in vulnerability research is that any seemingly fresh vulnerability discovery was, in fact, already found elsewhere. If we assume that a vulnerability when found is soon exploited, then that null hypothesis can be tested by examining full-catchment network logs. If there is evidence of the vulnerability having been exploited (now that we know what to look for), then the person offering to sell that vulnerability to the U.S. government is not, in fact, offering fresh goods. If there is no evidence that it has been used, then the seller can be rewarded commensurate with the vulnerability having been shown to fresh.

The relationship between the buyer (the "U.S. Department of Market Cornering") and the seller (the vulnerability researcher as represented by a broker) is that the buyer can ascertain whether or not what the seller claims is indeed the case. In other words, the U.S. government can know whether or not the seller offered it first refusal for a previously unknown vulnerability. On that basis, an orderly market with tiered pricing can be developed. With classified human intelligence, the U.S. government pays out-of-country informants in proportion to the unobtainability of the information; treating cyberspace as an out-of-country locale with which the United States has no diplomatic relations seems apt.

A U.S. government-dominated market for fresh vulnerabilities is quite obviously of dual use. Some of the vulnerabilities bought would find immediate use by defenders; some would lead to new offensive capabilities. The commercial market's near absolute preference for making defensive tools has been an insufficient response to the increasing availability of offensive weaponry. The observable overall threat level continues to rise despite the availability of those defensive tools.[10] Too often the existence of offensive tools is discovered by being on the receiving end of them; better to develop them at least far enough to allow the makers of defensive tools to have realistic test pressure.

It is my judgment that the situation does indeed warrant the employment of novel incentives to meaningfully address this issue; the U.S. risk to cyber attack is due to its relative wealth, hence deploying that wealth as a counter to attacks on it is an adroit judo move. More of the same old same old will yield more of the same old same old – continuous surprise for the defenders. Making it clear to non-state-sponsored attack developers that it is possible to earn a good, legal living finding vulnerabilities might be the single most cost-effective strategy for broadening defensive power.

It is frequently claimed that if government procurement simply required secure cyber products, then the Age of Aquarius would soon follow. Would that it were so simple or that the mass of government's installed base was not such an enormous legacy drag. There was indeed a time when the U.S. government's buying power did steer the computer market, *per se*, but that ended somewhere in the interval from 1981 (IBM personal computer) to 1982 (SUN Workstation) to 1984 (Apple Macintosh).[11] While the U.S. government's buying power will never be relevant to general-purpose consumer electronics, that buying power can be entirely relevant to innovative security products, and especially in their formative stage.

The major intellectual advance in cyber security occurs in small firms plus that part of academia related to those small firms, including spinoffs. That the innovation is in the small firms is directly observable and corroborated by the constant flux of large security firms acquiring the small ones so as to get an exclusionary lock on their innovations. Many of these small firms sell about the time they exhaust the supply of early adopters. They sell rather than try to "cross the chasm" on their own revenue power. That is to say that they sell their company to someone larger because it is too hard to make the transition from early customers (the visionaries) to mainstream

If it were easier to sell innovation to the U.S. government, then either the supply of innovation on offer to the government would increase, the innovation would be offered to the government earlier in its life cycle, or both.

buyers (the pragmatists). Little companies run out of cash if they run out of visionary customers before they get traction with pragmatist customers. It is a well-known, well-studied phenomenon of high tech startups.[12]

U.S. government procurement is notorious for its slowness and the costs it imposes on suppliers such that small firms not headed by former government executives simply make no attempt to sell to the government – the opportunity is too opaque, the sales cycles are too long, the price requirements too onerous and the compliance details too draining of potential profit margins. While it is generally true of good ideas that "If you build it, they will come," this is not true when the seller is small and running on fumes while the buyer (the U.S. government) acts as if time is of no essence. Put differently, if the cost of anything is the foregone alternative, then selling to the government just looks to the small firm like too many foregone alternatives.

Modifying procurement is not my jihad, but let me be clear: If it were easier to sell innovation to the U.S. government, then either the supply of innovation on offer to the government would increase, the innovation would be offered to the government earlier in its life cycle, or both. As it is – and putting aside so-called "black" contracts from the intelligence community – what is on offer to the government represents technology that has either already been widely adopted or already turned down by everyone else. This is of unique importance in the cyber security sphere; the rate of change is so high because the opponents move on to new targets and methods whenever old ones become well defended.

That modifying procurement is so well studied and so thickly documented implies that it may be an immovable object, yet as the U.S. government becomes ever more dependent on the Internet, the threat from cyber insecurity may become an irresistible force. It would certainly be ironic if cyber criminals succeeded in forcing the U.S. government to reform its procurement processes when U.S. companies and taxpayers have failed to do so.

Along similar lines, it should be noted that while small firms have difficulty accessing to U.S. government markets, they also face continual difficulties with the U.S. government's favored systems integrators (SI). The SIs function as gatekeepers between the government and the small firms in ways that both inflate what the government pays and deflate what small firms receive. In addition, where SIs have acquired competing technology, their gatekeeping power transmutes to a blocking power.

INCENTIVES: INVESTMENT

Procurement is often so slow that by the time an innovative technology can be bought, it is obsolete or otherwise inferior, but in the long meantime before procurement overhaul, the U.S. government can use market-based incentives in other ways. I work at In-Q-Tel, the strategic investment arm of the U.S. intelligence community. While it is true for most people that where they sit determines where they stand, the reverse is true in this case.

Investment nuances in small firms so very often determine their outcome. Small firms that are wise do not choose investors based on who offers the most money but rather on who offers the most opportunity. Generally, this is the talent and oversight that comes with the money. For investors who are profit motivated, they invest first in the management team; second, the addressable market opportunity and third, the technology in hand. In other words, the act of giving investment and receiving investment alike is to choose amongst possible futures, to lay track toward a goal state.

Unlike a venture capital (financial) investor, the U.S. government need is not a "liquidity event" (a favorable financial cash-out for entrepreneur and investor alike), but an "availability event" where the tools of cyber security can be procured by the U.S. government at the earliest possible time. It is not in the government's interest to own a majority share of any cyber security firm; it is not even necessary to own, in the equity sense, any share. What is necessary is for the government to be willing to say what it needs, to figuratively own a share of the overall market opportunity, and to midwife the birth of those technologies it needs. In engineering, the inspiration is all but entirely in getting the problem statement right; the perspiration then follows. For that inspiration to be pregnant, it has to be forward-looking and fact-based. The more open the relationship between the U.S. government and the entrepreneur(s) in setting the problem statement, the more likely it is that if the entrepreneurs say, "This is possible," that it is, in fact, possible.

But in the end, just because something is possible does not mean that it deserves to be done. What matters is whether the proposed course of action would not only be possible, but efficacious. If investors are more certain that a market exists for an innovation, the less the risk premium that investors will demand from the innovators. If the U.S. government were openly laying out problem statements that do not amount to boiling the ocean, the more likely it would be that innovators would step forward.

The best way to incentivize investment is to be an investment partner to other investors.

Because the U.S. government's interests are not to make money but to create solutions to problems that the government will admit that it has, then the government as an investor and probable buyer multiplies its impact well beyond the dollar size of its investment. Political leaders very often use the word "investment" to verbally ennoble some vague social purpose. That is all well and good, but I am talking about something far more concrete and that is financial investment in – and market promise for – finding solutions to problems that the government faces.

As to cyber security, the very nature of the cyber security lifecycle is the appearance of a problem, a scramble to find a solution, a scramble to ensure that the cure is not worse than the disease, another scramble to get that solution to edge nodes however defined, and the hope that the winner of the race will receive some reward commensurate with the exertion it takes to make this look simple. Because each new problem will be narrow in and of itself, the solutions will tend to be similarly narrow. The provider of a narrow solution in a volatile market has a narrow window of commercial opportunity, and so the point: Perhaps in no other field is the issue of market timing as brutal as it is in cyber security. Too early and you die. Too late and you die. Just in time and you may win, but the more serious the problem the more work that is required to counter it, more work means a longer runway before launch, and a longer runway consumes more investment dollars. For entrepreneurs, this is, generally, as it should be – but for cyber security, the windows of opportunity may be so narrow that they may discourage entrepreneurs from developing products in the first place.

While success as an entrepreneur in cyber security is particularly difficult, the need for good cyber security tools ratchets upward. What the U.S. government can do with investment is to 1. make starting earlier more plausible, and 2. make the window of market opportunity less narrow. Put differently, the cyber security entrepreneur has such a narrow window of opportunity that any help from the U.S. government in broadening that window would likely increase the supply of cyber security startups. At present, it is very much that one will be either too early or too late. By going in with private-sector investors, the U.S. government can both magnify its impact and avoid having to become an investment specialist itself.

INCENTIVES: COLLATERAL ENCOURAGEMENT

Sometimes markets need to exist before entrepreneurs can address them. Sometimes entrepreneurs spend their first two or three years actually creating the market they want to address. Sometimes, by the time a market develops, the entrepreneur has run out of money or better-funded competitors arise simply to take the market away from the entrepreneur who created it. In all of that, the entrepreneur is battling a clock ticking down to a zero bank balance, and probably diverting management time from building product to building market, and it does not always end well. To the extent that the U.S. government can gain greater access to innovation by accelerating market development for that innovation, the usual method is some mechanism of subsidy. The arena of "green technology" strongly reflects this in, to take an example, the subsidy to buy a clean diesel truck rather than a gasoline truck. Because subsidies are, by definition, market distorting, any subsidy must be designed to advance the availability of product, not to provide a kind of back-door price control the way, for example, ethanol production is so damagingly unsustainable.[13]

Better than subsidy, however, is to be a green technology market maker as, for example, the U.S. military intends to be as it drives to reduce operational dependence on fuel convoys.

Cyber security focal points where some combination of subsidy and market making may be sufficiently early to steer all players might be in regard to the cyber security of endpoint devices in the so-called "Internet of Things," especially if the last yard network transport for those devices involves smartphones.

As reported in *The Financial Times*, personal computer (PC) shipments have now been eclipsed by the smartphone.[14] The capabilities of these phones continue to grow, and they obviously are already small computers that happen to also make phone calls. The cyber security point, however, is not about market share or available tools, but rather the degree to which the smartphone is controlled by the end user. The more the smartphone endpoint is controlled by its owner, the more absolute the death of perimeter control as a meaningful cyber security strategy overall. That an owner can render a smartphone insecure matters because it could well contain business data or other information that needs to remain secure. Furthermore, owners pull down applications at any time. Even if all of them are spotless that does not mean that they are secure in combination with each other – it is entirely possible to get an insecure result by combining two secure components.

The differences between the Apple model (applications are forbidden until permitted by Apple) and the Google model (applications are permitted until forbidden by Google) are germane with respect to security, innovation, liability and profit margins. There may be only limited distinction between U.S. government civilian buyers and the public at large, but for U.S. military buyers, it seems difficult to reconcile the capabilities of a smartphone on a public network with the limitations under which

military users operate, such as to avoid being tracked and to not handle classified data outside of a security facility. Put differently, it is one thing to set up the SIPRnet vs. NIPRnet distinction (two secure networks operated by DOD) for fixed desktops in known locations, but another thing altogether to do this kind of walled garden for end-user owned consumer devices that automatically switch between access methods (cellular radio, 802.11 , etc.) on an as available basis. Advances in network technology (such as IPv6) are helping to make perimeter definition itself difficult, and you cannot defend a perimeter you cannot even define.[15]

For U.S. government personnel to be able to use smartphones in support of their respective missions is both approximately necessary and approximately unpoliceable. This issue, which is also faced by large corporations to many degrees, is an area where market driving by adroit purchases of security technology seems all but essential. The world market for smartphones certainly will not notice the objections of any individual company, but a common cause between the U.S. government and major U.S. industries for a partitioning model (where some parts of what is running on a given machine are prevented from interacting with other parts) with respect to individually owned smartphones would get notice. The various experiments that U.S. companies are already engaged in under the "bring your PC to work" rubric are exactly along these lines. These companies are trying to come to terms with the reality of what their employees have already, any products available in the market to ease this transition and the attractiveness to any organization of having its employees capitalize the end point in the corporate computing plant.

This goal of partitioning is precisely what was meant by "user security" in the timesharing world, so there is a considerable literature upon which to draw. While not using computer security terminology, financial regulatory compliance requirements for "separation of duties" are entirely parallel. In this arena, 1. the U.S. government knows what it wants (with the literature to back it up); 2. what the government wants is aligned with what large firms want; and 3. the opportunity to be a market maker is now. The necessary innovation is already well underway at such companies as Verdasys.[16] It is the government's choice whether to lead, to follow or to get out of the way.

Risk Absorption

Security, being a means and not an end, is subject to the laws of diminishing return. No one wants a police state, even if a police state requires the fewest policemen. At some point, risk and cost curves inevitably cross and investment in security gives way to acceptance of risk. At the same time and in U.S. government-speak, the Federal Information Security Management Act (FISMA) construct of "security commensurate with risk"[17] seems often to be met by accepting risk that is not understood. The divide between civilian and military agencies around what risks to accept is widening as the chief information officer at the White House pushes the adoption of new technology in civilian agencies without apparent concern for the security of those adoptions.

RISK ABSORPTION – WHY?

The root source of risk is dependence – you are not at risk from the loss of something you do not depend on. My definition of security itself has co-evolved with my understanding of risk and risk's source to where I today define security as the absence of unmitigatable surprise. It thus follows that increasing dependence means ever more difficulty in crafting mitigations, and that increasing complexity embeds dependencies out of view such that while surprises may grow less frequent, they will be all the more unexpected when they do come.

That is the crux of the matter: The U.S. government's dependence on cyber is inestimably irreversible and irreversibly inestimable. This leads to a conclusion: The U.S. government's paramount aim cannot be risk avoidance but rather risk absorption – the ability to operate in degraded states both in the micro and macro spheres, to take as an axiom that "our opponents have and will penetrate our systems at all levels" and "we will have to work around this in some way."

RISK ABSORPTION – WHAT?

To operationalize "the absence of unmitigatable surprise," the U.S. government must focus its investment attention on deploying technology that either lessens surprise or improves the ability to mitigate to the point that the residual risk is rationally absorbable. Expressing these in the language of engineering design constraints mean:

- No silent failure.
- No unwitting dependencies in critical paths.

These are cruel gods, but sacrifice to them is unquestionably necessary.

Some parts of the U.S. government need little instruction in what "no silent failure" means (and others need a beginner's guide. The dynamic range is great). Nevertheless, the topic at hand is how the government gains access to innovative technology that reduces the chance of silent failure.

One can say with assurance that from 1990-2005, the commercial world caught up with the military world in the application of cryptography. With slightly less assurance, it can be said that from 2000 onward, the commercial world has been making steady progress in traffic analysis including data fusion of multiple sources of passive collection. As firms in a position to see substantial slices of traffic improve their ability to make analytic sense of it, commerce will soon be in substantial parity with the military world in skill and have a far superior position to that of the military in terms of the sheer numbers of points of data acquisition, though the military may retain superiority in the quality of its points of data acquisition and its out-of-band knowledge of context. With respect to quantity, raw transmission (such as would be seen by an Internet service provider like Verizon or a content provider like Akamai) and behavioral usage patterns (such as would be seen by a search engine like Google or a social network like Facebook) can help clarify what risk the U.S. government is absorbing without even knowing it.

RISK ABSORPTION – HOW?

A question for the U.S. government is to what degree it wants access to technology that delivers the means to avoid unmitigatable surprise and to what degree it wants access to the results of using technology that delivers the means to avoid unmitigatable surprise. Is it a technology buy or a services buy? While this chapter does not debate the wisdom of CALEA (the Communications Assistance for Law Enforcement Act, which requires the technical possibility of wiretaps) or the legality of "warrantless wiretaps," they illustrate the point: The U.S. government may wish to have the results of innovative technology more than it wishes to own and operate that innovative technology.

Characterizing the choice as a simple build vs. buy decision is facile and wrong.

Acquired data is far more valuable than the technology that acquires it, an idea that is as venerable as ADM Grace Hopper's 1987 retirement speech:

> Some day on the corporate balance sheet there will be an entry which reads, "Information;" for in most cases the information is more valuable than the hardware which processes it.[18]

Put differently, the U.S. government wants important data that can only be derived by the most innovative technology when it is not, nor will it be,

the innovator. That innovator may not even be a U.S. company, thus the point of this section: How is the U.S. government to have access to innovation that manages the risk of unmitigatable surprise at a level where the residual risk (of events that are surprising, unmitigatable or both) can be absorbed without national consequence? The answer is probably to hire it, if only to corroborate the U.S. government's other sources and capabilities.

Minimizing Delays in Adoption

Without debating existing federal procurement rules, the probability that the U.S. government can buy innovative technology while it is still freshly innovative is near zero, at least outside of black budgets. Buying the output of such innovative technology is faster. This approximately "rent-to-buy" strategy would nurture small firms while permitting the U.S. government to gain access when the technology is still freshly innovative.

The economic reality within small firms is that their early customers are unavoidably part of the firms' design teams – those early customers have a level of influence early on that they will never again enjoy. All small firms are willing to accept fact-based mid-course corrections to their technology trajectory from their early customers. This may well imply that the U.S. government needs to be a frequent, easily recruited beta-tester, i.e., an evaluative user prior to general availability of the product, so as to give the kind of feedback that a beta-tester is obligated to provided in exchange for its early access to the product. Diligent beta-testers are very valuable to small firms pushing the envelope of what is possible, and being diligent is certainly what some U.S. government agencies know how to do well. Stronger still, if the government was to be a strategic investor (an investor who also uses the product), then this power to steer development would be even more effective. Being close to the design process tends also to clarify what failure modes the technology has, thus avoiding surprise.

Because the cyber threat is in no way limited to government, the twin constraints of matching funds and commercial viability are valuable to the country at large, not just the government.

This steering by way of early adoption plus investment does require finesse lest the product become useful to government only. There are far too many firms whose only market is the government, including firms that do nothing but live on grants from the government's Small Business Innovation Research (SBIR) program or which happily manufacture carpenter's hammers made to military specifications. To avoid the temptations of this sort, it is better for government investment to be of the sort that rarely leads investment rounds but rather matches private investment, while only buying from those firms whose products have commercial appeal outside of the government procurement. Because the cyber threat is in no way limited to government, the twin constraints of matching funds and commercial viability are valuable to the country at large, not just the government.

The U.S. government already uses open source software and both agencies, such as the NSA, and private sector firms, such as Veracode,[19] are regularly working on the security of open source software. As independent data shows, proprietary software tends to be more secure at the time of first release whereas open source software tends to have quicker reaction time when vulnerabilities are discovered. In the terms used here, whether to deploy generally equivalent

closed versus open source software is to ask if one prefers fewer surprises but slower mitigation or toward more numerous surprises but faster mitigation. Wisdom and skill in making this choice will matter.

An M.I.T./Lincoln Labs study demonstrated that the security of a representative open source code base (Open BSD) monotonically improved over time as security errors were eradicated faster than new ones were introduced. If that well-researched result[20] can be generalized, then it suggests that because version-to-version code differences are transparent in open source but opaque in closed source, the U.S. government would gain a degree of control over the probability of surprise if it chose open source, all other things being equal. Ironically, the mistrust of American products by other governments is hastening the adoption of open source by those other governments. ("Open source" means neither "amateur" nor "antibusiness" as the biggest contributor of open source software has been SUN Microsystems.)

Possible Futures

Perhaps the most fog-bound decision to make is whether the U.S. government wants a centralized approach to encouraging government access to innovative cyber security technology or a decentralized one. Arguing for centralization is that strategic targeting garners more cost effective return than does a scattershot approach, in large part because centralization pays the price of the investment learning curve only once, removes the chance of supplicants to venue-shop, has enough knowledge to play the winner,[21] and makes possible strong accountability. Arguing for decentralization is that all persistent central entities are subject to the corruption of power and the tendency to become incestuous with their clientele, which is why some private sector grant agencies have the rule that a given recipient gets one grant only in its lifetime.

Of all the steps between a good idea and wide deployment, the most difficult to encourage is that of nurturing the bringing to market of germane products. As such, it is my judgment that the correct number of entities to orchestrate this game for cyber security is one. Other specialty topic areas, like the aforementioned green tech, deserve a separate orchestrating entity. Capping the number of such orchestrating entities at no more than a half-dozen is consistent with the U.S. government having to choose what topic areas are strategically important enough to matter. Cyber security is strategically important; therefore cyber security needs one, and one only, investor to partner with other U.S. government entities and the private sector in bringing in products that are matched to government needs.

A steering decision for the cyber security investment entity is whether to favor avoiding surprise or accelerating mitigation. In the language of engineering, this asks whether to prioritize increases in the mean time between failures (MTBF) or decreases in the mean time to repair (MTTR). At the limit, an MTBF of infinity and an MTTR of zero are equivalent. It is my judgment that the encouragement of cyber security within mature, critical (not merely desirable) infrastructures should largely concentrate on reducing MTTR.

It is likewise my judgment that the encouraging cyber security around new or quickly evolving cyber technology should largely concentrate on increasing MTBF.

Success in gaining better government access to innovative technology begins with detecting that technology's birth. Where it is natural for announcement to be made, a facility to gather such announcement is indicated, i.e., the cyber security entity must monitor academic journals and conferences as well as new product announcements (such as on the PR Newswire). Formation of companies is sometimes visible but

generally not. More typically, the narrow window of opportunity and the general irrelevance of patents for cyber security cause startups to stay in stealth mode until they have a product at the beta stage (ready for public testing). The counter to the startup's (prudent) tendency to stealth is for the U.S. government to be an investor and to have good relations with conventional investors such that invitations to look at new investment opportunities come to the government at the earliest practicable time. In my judgment, this implies an In-Q-Tel would have to be created if did it not already exist. Obama campaign literature suggested exactly this same approach for U.S. government access to innovative energy technology. The Department of Health & Human Services is reportedly thinking along these lines for health care technology as well.

Having private firms prioritize meeting government needs requires investment to that effect and some degree of an assured market worth addressing at the early stages of private company growth. In turn, this implies that these firms will need to hear clear problem statements for real government needs. Getting these problem statements is (and has been) a problem because coaxing them out of the agencies with the greatest downside risk has meant a kind of public acknowledgment of known weakness on the part of the agency. In my judgment, this underscores the value of one or a small number of centralized interfaces to the startup community so that an agency with a risk need not be *prima facie* identifiable in the early stages of negotiation with the prospective investee. Nothing is quiet for long, but any help is still help.

Cyber security issues are to a first approximation identical worldwide, such that a threat to one tends to be a threat to all and a solution for one tends to be a solution for all. While that cannot be altogether counted upon, it does mean that a solution that is worth having does not necessarily appear first in the United States. One can hardly argue with the U.S. government preference for U.S. firms, but all governments will have similar preferences for their own cyber security industry if they have one. In my judgment, the interface between the U.S. government and potential sources of worthwhile innovation cannot limit itself to U.S. firms even if that self-limitation operationally means that the interface entity acts only to stay informed where it cannot perform the rest of the functions recommended here.

Much ink has been spilled on whether security and privacy are in direct opposition, whether security and privacy are a zero sum game, and whether security and privacy technologies are either/or. In paragraphs above, it was stressed that the acquisition of security-relevant data was valuable and unlikely to be something that the U.S. government can do on its own.

While ordinarily the reaction of government is to demand data that it needs from those who are in a position to provide it, this is not the only mechanism of doing so.[22] The same, only more so, is true for the discovery of flaws in the installed base of U.S. government and critical infrastructure entities because those flaws are still regularly found by independent third parties. In my judgment, rather than demanding such sources cooperate it would be more straightforward to pay for it, and to pay well enough that the U.S. government's world-leading capacity to pay was treated as a strategic asset.

It is the position of leading parts of the public health community that the battle against obesity has been lost and with finality. That grouping calls for forgetting about obesity reduction and to instead put available research dollars into drugs that make obesity a source of neither morbidity nor mortality.[23] If one were to substitute "cyber insecurity" for "obesity," one would be repeating what Nat Howard said at the Advanced Computing Systems Association (USENIX) conference in 2001, "Security will always be as bad

as it can possibly get and still allow us to survive." Along those lines, it is my judgment that of all the point investments that might be made or compelled, intrusion tolerance is the most congruent with the situation on the ground. We must assume that intrusions have happened and will happen. We must maximize the probability that we can tolerate the direct effect of those intrusions, and that whatever damage is done by the intruder, the system can continue to do its job to the extent possible. This is an issue of survivability.

While the message that "complexity breeds insecurity" has been heard, understood and acknowledged by sophisticated cyber security professionals at all levels, the trend of cyber space complexity is accelerating. In my judgment, the U.S. government would dampen its need for innovative cyber security technology were it to decline to adopt new cyber technologies that increase complexity. In other words, to maximize the defendability of its cyber assets, the U.S. government may want to favor simple systems because simple systems are easier to defend, a kind of Pareto constraint.[24] This goes for both civilian and military compartments. Where this strategy is thought infeasible for whatever reason, avoiding unmitigatable surprise will necessarily mean retaining the capability to fall back to prior methods of the work of government. Only a few commercial firms still drill themselves with occasional "paper days" (days on which working with paper alone is practiced lest it be forgotten how). It is impractical to imagine that the U.S. government should have the occasional "paper day." At the same time, the government must not lose the ability to operate its critical functions if they suffer irremediable cyber damage whether by hostile action or plain bad luck. This is the "intrusion tolerance" we spoke of earlier at the limit; the intentional capacity to work under degraded conditions. Knowing what those limits are in advance seems essential to crafting actual operational plans.

Our dependence on cyber technologies is great, therefore our risk from them is also great. In the spirit of mitigating that risk, we need to know what we can do under the stress of not having all of our dependence satisfied.

While this essay is not about the U.S. economy, but let us be clear about something. Cyber security is a worldwide demand. If Americans want a domestic cyber security industry, it will not happen without investment whose purpose is to ensure not only that the U.S. government has access to innovative cyber security technology, but that U.S. cyber security innovators are able to compete. It will not happen without policies rather more meaningful than some sort of "Buy American." It requires nurturing, perhaps even creating, the market that those innovators can address. Procurement set asides are not the answer; investment in the companies either directly or by helping them develop products of direct value to the government might be. Whether to encourage American entrepreneurs is a choice. It will not be recoverable much longer. We do not have sheer numbers on our side (there appear to be more Chinese working on finding flaws in open source software than there are Americans writing it), but we do have investment capacity and we do have a need greater than any other entity less dependent on cyber technology.

Conclusion

While there is no ready way to "force" more good ideas to appear per unit time, incentives can meaningfully reorder who has the earliest access to evolving cyber security realities just as nothing can limit who ultimately has access. Quality cyber security information is better bought than seized. Dependency on any cyber technology leads to risks unless they are purposefully checked. Unless purposefully checked, dependence on any cyber technology progresses to risk from it, so for mature cyber technology, the U.S. government's goal should be to reduce the mean time to repair,

whereas for new or quickly evolving cyber technology, the U.S. government's goal should be to increase the mean time between failures. In all things, investment and market-making trump all other approaches and are proven. In doing anything that is outlined here, the U.S. government cannot limit itself to U.S. cyber security technology and still keep up with the pace of advancements. Where for whatever reason the U.S. government cannot accelerate the deployment of cyber security technology, it must decelerate the deployment of other cyber technologies that increase complexity and, where feasible, have as clear a capacity to operate without its cyber assets as it is possible to have. As the bottom line, the private sector will provide nearly everything the public sector lacks, but only if the public sector cultivates a meritocracy as, like it or not, cyber security is fundamentally Darwinian.

ENDNOTES

1. Metcalfe's Law states that the value of a network is proportional to the number of possible conversations that can take place on it, which is to say the value of a network rises as does the square of the number of parties (N^2) on that network. It first appeared in a slide in 1980, but George Gilder gave it name; see George Gilder, "Metcalfe's Law and Legacy," *Forbes ASAP* (13 September 1993).

2. Reed's Law states that the number of possible interactions on a network is not the number of two-way conversations that might take place, but rather the number of groups that can form in that network, which is to say the number of combinations of parties (2N) possible on that network. See David Reed, "The Law of the Pack," *Harvard Business Review* (February 2001): 23-24.

3. Daniel Geer Jr., "Does a Rising Tide Lift All Boats?" *IEEE Security & Privacy*, Vol. 9, No. 1 (January/February 2011): 86-87.

4. These costs include detection, capture, analysis, crafting a signature, testing for efficacy, and safety, packaging, documentation and distribution.

5. There is no definitive work on cyber vigilantism, nor would a definitive work be definitive for long, but social networks with digital guns have low assembly costs and little risk.

6. U.S. Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

7. The planned National Cyber Range is an artificial, sealed-off Internet inhabited by simulated nodes, computers, system administrators, users, and others, in which the United States can test-fire cyber weapons and practice cyber combat. DARPA has announced that it is planned to reach demonstration status by July 2011. The National Cyber Range is outlined in DARPA-BAA-08-43.

8. For more information on the iDefense "Vulnerability Contributor Program," see http://labs.idefense.com/vcp/.

9. Netwitness captures all network flow and then stores and indexes it such that reconstruction is possible. Analysis is not a lightweight activity and requires skill; the point here is that it is possible.

10. Several regular reports on cyber security threats include Verizon's "Data Breach Investigations Report," Akamai's "State of the Internet," Symantec's "Internet Security Threat Report," and the "For Good Measure" column in *IEEE Security & Privacy*.

11. From 1984 to 2011, Moore's Law alone delivered 250,000 times more computing power for the same dollars; a 1984 computer market driven by rich buyers like the U.S. government became a 2011 mass consumer electronics market.

12. Geoffrey Moore, *Crossing the Chasm*, Rev. ed. (New York: HarperBusiness, 1999).

13. The Congressional Budget Office calculates that the ethanol program costs 750 dollars per metric ton of carbon reduction whereas Terrapass, a carbon-offset trader, values the same reduction at less than 15 dollars. See Congressional Budget Office, "Using Biofuel Tax Credits to Achieve Energy and Environmental Policy Goals," Publication Number 4044 (July 2010), http://www.cbo.gov/ftpdocs/114xx/doc11477/07-14-Biofuels.pdf; and Matt Kibbe, "Let Ethanol Subsidies Expire for Good," Forbes.com (9 December 2010), http://www.forbes.com/2010/12/08/ethanol-subsidies-energy-opinions-contributors-matt-kibbe.html.

14. According to this article, "Makers of mobile devices distributed a total of 101 m[illion] smartphones in the last three months of [2010], up 87 per cent from the same period a year earlier, according to International Data Corp, the market researcher. IDC had earlier said that personal computer shipments reached 92 m[illion] units in the fourth quarter, up less than 3 per cent." See Joseph Menn, "Smartphone shipments surpass PCs," *Financial Times* (8 February 2011).

15. For example, "privacy enhancements" in the IPv6 protocol include address hopping and multi-homing for the endpoint via the Extended Unique Identifier (EUI) portion of the IPv6 address.

16. For example, Verdasys' Digital Guardian is a commercial version of the U.S. government's Trusted Computer System Evaluation Criteria (Orange Book), combined with a distributed log engine.

17. Public Law 107-347, Title III, Sub-Chapter III, Section 3544.

18. Andrew Blyth and Gerald L. Kovacich, *Information assurance: security in the information environment*, 2nd edition (London: Springer, 2006): 92.

19. NSA's Security-Enhanced Linux and Veracode's Error Logging Modules and Handlers (ELMAH) are both open source databases.

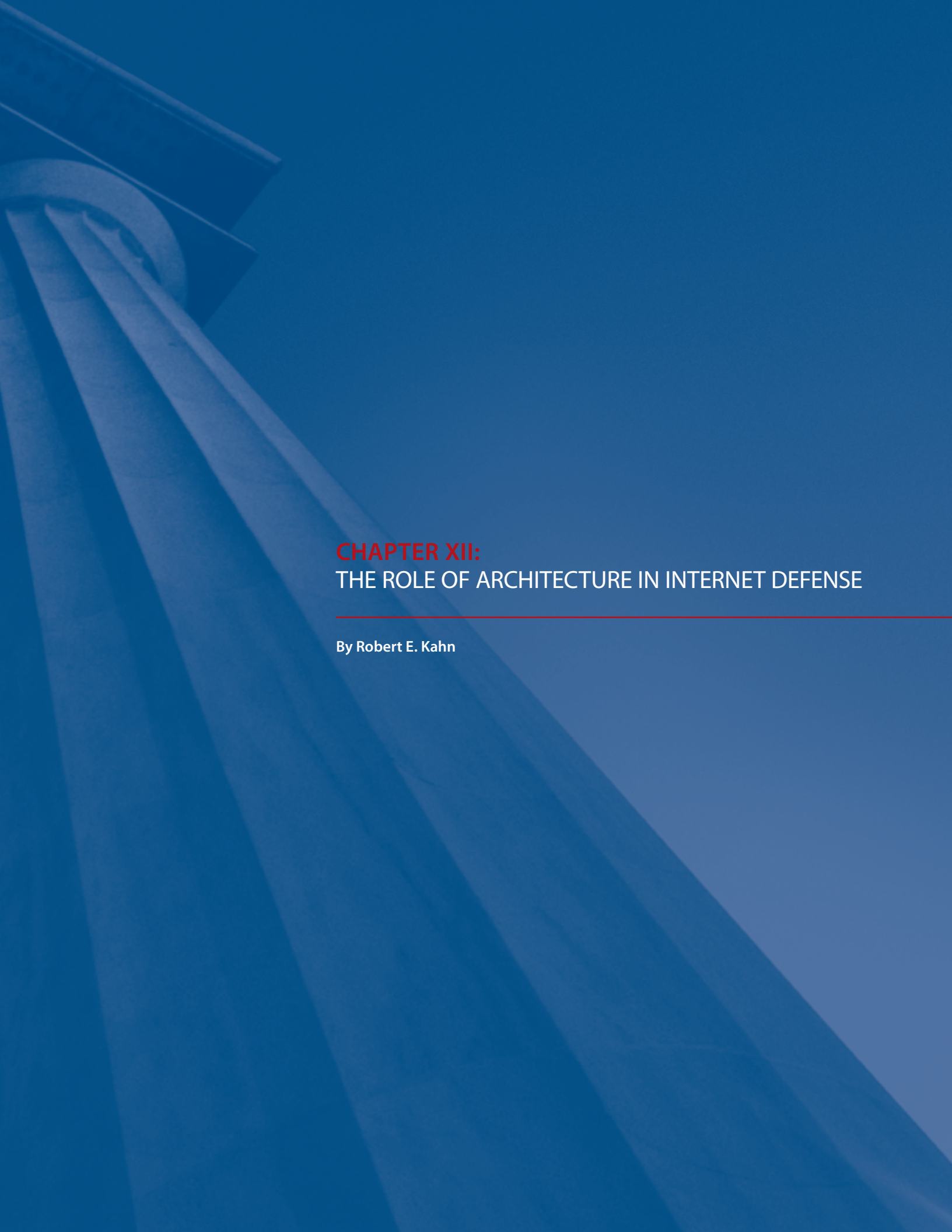
20. Andy Ozment and Stuart Schechter, "Milk or Wine: Does Software Security Improve with Age?" paper presented at USENIX Security 2006, http://www.ll.mit.edu/mission/communications/ist/publications/060731_Schechter.pdf.

21. The term "play the winner" means to use the approach that has proven most effective in the past. In clinical drug trials, it means that if an experimental drug worked on the first patient, then the second patient should receive it as well. If it did not work, then the second patient should receive a different experimental drug, and so on. In this context, "playing the winner" means that if one supported entity produces something valuable, then the government should ask it to address the next problem. If that entity does not produce something valuable, then the government should ask a different supported entity to address the next problem.

22. Such government demands may reduce firms' willingness to acquire or to keep data. Instead, the government could purchase the information it needs, which would give companies a strong incentive to make their data available.

23. "Shrinking the Effects of the Obesity Epidemic," *Harvard Public Health Review* (Winter 2011): 14-19.

24. A Pareto constraint means a proposed change will only be adopted when it harms no one and helps at least one actor. Economic theory suggests that Pareto improvements add to an economy until that economy achieves "Pareto efficiency," namely, where no more Pareto improvements can be made.



CHAPTER XII:
THE ROLE OF ARCHITECTURE IN INTERNET DEFENSE

By Robert E. Kahn

America's Cyber Future

Security and Prosperity in the Information Age

THE ROLE OF ARCHITECTURE IN INTERNET DEFENSE

By Robert E. Kahn

Since it was first introduced in the early 1970s, the Internet has met the growing needs of an ever-widening community of users with great benefits to individuals, organizations, governments and their associated disciplines. Yet, along with that growth and evolution has come an increasing downside, namely traffic that intrudes and may disrupt productive uses of the Internet. Worse yet, concerns exist that such unwanted and unwarranted intrusions may cause more extensive damage in the future. Managers of information systems and resources attempt to find ways to ensure that access controls are not breached, or that intrusions or disruptions have little likelihood of success: There are no guarantees, however, that a resourceful adversary will not find ways to subvert existing techniques to their own benefit. Since cyber insecurity is likely to persist, a rethinking of the architecture of the Internet, and how it might evolve to become more secure, is warranted.

This chapter explores the interplay between Internet architecture and the ability of users, network operators and application service providers to adequately defend against threats posed by others on the Internet. It introduces the digital object (DO) architecture and suggests a way of integrating certain defined functionality into the Internet based on the use of digital objects. This approach is compatible with existing Internet capabilities and has the potential to substantially improve our ability to detect and deal with intentional hostile actions. It would also deal with actions that are simply accidental or naively misguided, but which may have serious consequences.

Today's Internet subsumes a wide range of networks, devices and other computational facilities, as well as diverse services, processes and applications. In order to protect against real and potential threats, technical capabilities are required to understand what is transpiring within the Internet and its various constituent components, and to take steps to deal with emergent

situations that may require action. For example, most laptop users have little or no idea what is transpiring on their computers, and no effective way to find out in real time. They may only know that something is not working properly, or that the machine is running more slowly than usual. At present, the Internet landscape is sufficiently complex that the myriad exchanges of bits over the Internet cannot easily be differentiated by intent or function. Certain architectural changes to the Internet, which primarily affect the way the Internet is used, can help in mitigating these situations. Specifically, the DO architecture can help remediate this situation.[1]

There are no guarantees that future threats, which require reconsideration of various architectural and design choices in the future, will not materialize; nor does use of the DO architecture guarantee that those who ignore or do not otherwise choose to take advantage of new architectural approaches will necessarily be harmed by that choice. At present, the Internet environment is tilted in favor of those with adverse motives, while the rest of the community must be on constant vigil to defend against harmful interference. However, over time, architectural changes become more pervasive. The assertion of this chapter is that the playing field will become more level in a way that provides architectural advantages for the defense of the Internet.

In the DO architecture, all system interactions involve the exchange of structured information in the form of digital objects, each of which has a unique identifier that can be resolved by a resolution system to state information about the object. Information, structured as a digital object, can be accessed and used by resources on the Internet based on its identifier, and is subject to any stated access controls or permissions associated with such objects. Even user commands, where invoked, can be converted into digital objects before being sent. This enables interoperability of the systems that embrace the protocol.

Digital Objects

A digital object consists of a data structure that is flexible, scalable and extensible. This data structure has a unique persistent identifier and may have one or more of the following:

- A set of type-value attributes that describe the object (one of which is the above mentioned object's identifier, which is mandatory).
- A set of named "data elements" that hold potentially large byte sequences (analogous perhaps to one or more data files).
- A set of type-value attributes for each of the data elements.

The elements of a digital object consist of "type-value pairs" that software at the destination and other locations can interpret for further processing. A protocol, known as the DO protocol, is responsible for managing the interactions between systems, services and other resources.[2] This protocol enables actions to be taken based on the use of identifiers. The actions to be taken, and the targets of those actions, are specified by identifiers, which relate to digital objects that prescribe the actions or enable access to the target information. This approach also enables verification of resources by clients/users, and clients/users by resources, since each client/user and resource also has at least one unique identifier. Indeed, a user may have multiple identifiers depending on the particular role the individual is playing at the moment (for instance, whether they are representing their employer or acting as an individual).

While many, if not most, interactions on the Internet are likely to be reasonable and legitimate, intrusions or hostile actions need to be flagged. Action must be taken to prevent damage, or other steps must be taken to quickly isolate matters. Even with the more structured view of the Internet provided by the DO architecture, the task is extremely challenging. Without such a view, the task is close to daunting, and would likely require semantic

interpretation of unstructured interactions, even if decrypted on the user's machine, that may be beyond the state of the art.

In the future, if arbitrary information arrives, the type of information will need to be understood from the structure of the information itself to enable further processing. Further, the environment into which the information arrives or is ultimately processed will require some degree of structuring, such as the structuring provided by the DO architecture, to determine with more specificity how best to deal with the information. In some cases, manual intervention may still be called for. In many other cases, however, automated processing may be possible based on interpretation of the structure of the actual information. For example, a medical reading sent by a remote wireless device might be understood from the structured information itself and placed in the user's medical record. Likewise, a remote financial transaction may be received and inserted automatically into a record of the user's daily transactions. Information collected in real time from remote sensors and appropriately identified can also be managed according to general rules and procedures adopted for such types of sensor information.

Overview of the Existing Internet Architecture

The existing Internet architecture was designed to enable the interconnection of multiple networks, devices and other computational facilities. Each potentially had a different design and performance, such that computers on different networks could communicate seamlessly and reliably with each other without having to know the location of the facilities, the intervening networks or how to actually route the information. More specifically, it enabled information in the form of packets of digital information to be communicated between computers without the need to first establish communication pathways between the computers. As a result, the Internet has become a standard means of communication worldwide, not only for traditional computer facilities, but also increasingly for digital representations of voice, video and sensor data managed by computers.[3]

At present, the Internet environment is tilted in favor of those with adverse motives, while the rest of the community must be on constant vigil to defend against harmful interference.

The Internet's creators based the existing architecture on two relatively simple notions. One was connecting networks with routers, which forward received packets by a process in which the routers act as relays with each step hopefully moving the packet closer to the eventual destination. The destination is specified by a globally unique identification known as an Internet protocol (IP) address that distinguishes the destination machine from all other destination machines on the Internet. The routers interpret the IP address to determine how best to route the packet. The process of communicating packets does not require the user to specify how to route the packets, which combination of networks to use, or even where the destination machine is located. Indeed, except for certain control information (such as the IP address) the contents of the packet may be encrypted. A dynamic routing protocol is used to adapt to changes in the underlying network components, such that if the packet can be routed to the eventual destination, it can be delivered in a timely fashion.

The second notion was the use of a host protocol, originally known only as the Transmission

Control Protocol (TCP), to enable the components to intercommunicate. TCP was later separated into two parts, one of which is IP, and the remaining part remained TCP. At the destination computer, TCP checks the validity of the arriving packets, discards duplicates that may have been generated along the way, reconfigures the data as appropriate and takes the necessary next steps in furthering the processing of the packets at the destination. In 1995, to clarify what the Internet actually was, the U.S. Federal Networking Council provided a definition of the Internet as a global information system that enables information resources of all kinds to intercommunicate by use of certain defined protocols (including IP) or their logical follow-ons and extensions.[4]

We note here that the overall objective of today's Internet is to ensure that global connectivity is achieved with low latency and reliable communication. While attacks on the network components of the Internet are possible, the Internet is far from completely defensible. Operators can take many types of precautions to ensure that traffic originating from users on their networks – and transit traffic from other networks – cannot directly cause actions within their networks (adverse or otherwise) other than to forward packets to their intended destination. However, although network operators can play a central role in helping to understand what is happening within their networks when adverse actions are reported or detected elsewhere, much of the concern still centers on vulnerabilities of the application service providers, their users and the underlying information systems they employ.

Vulnerabilities in Today's Internet

Various characteristics of the existing Internet make it especially vulnerable to harmful interference. One is the lack of overt security, which makes communications vulnerable to interference. Second is lack of identity management, which makes verification less secure than perhaps may be desired or necessary. Password protection is often used, but public key systems offer greater protection assuming the private keys are not communicated over the Internet. Passwords, which are communicated, may travel in the clear or be included in email messages (or perhaps accessible files), and can be used by anyone to access a password controlled system if they know the account name. Third is freedom of communication without prior arrangement that can include desirable or essential communication; however, this also enables undesirable communications, which may range from simply annoying to potentially harmful. There is a role for anonymous and non-pre-arranged communication in the Internet. But, at present, all communications are treated basically with equal significance, thus making it difficult to differentiate between those that are known and acceptable, versus those that are unknown and possibly undesirable. The key to addressing this issue lies with architectural changes in how information is managed in the Internet, including, in particular, in the devices and other computational facilities that provide the application services.

At present, all communications are treated basically with equal significance, thus making it difficult to differentiate between those that are known and acceptable, versus those that are unknown and possibly undesirable.

Much has been done to protect the various networks that comprise the communications portion of the Internet, and serious ongoing efforts exist to build ever more robust and reliable computational facilities. But, for the most part, the most severe

vulnerabilities in today's Internet exist in those applications – in operating systems and in other resources – that cannot adequately defend themselves. The extent of the threat possibility is still unfolding, but the earliest examples of intrusive action are by now well known. For example, spam is unwanted email that consumes communications capacity and can overwhelm user systems. But spam is increasingly being filtered out with the help of commercially available software designed to distinguish between spam and non-spam communications. Generally speaking, these software packages are not perfect, but they do reduce the nuisance significantly. Since most spammers rely on the dissemination of lots of similar traffic relatively indiscriminately, certain charging schemes could mitigate the spam traffic. However, most spam is not intended to cause damage, and some unwanted advertising might actually be of interest to some. In most cases, however, it represents an intrusion upon an unwilling recipient.

Other actions can actually cause damage in some form. Intrusions that penetrate user systems can collect private information, can harm or degrade the operation of the user's system and in extreme cases can render it unusable. These harmful actions are usually achieved by exploiting vulnerabilities in the operating system or in one or more applications that run on the machine. These actions result from incoming traffic generated by usually unknown sources that may have immediate effect, or may be the result of implants which arrived over the Internet much earlier. Indeed, one of the loopholes that many users are unaware of is that such intrusive software and implants may result from devices such as memory sticks that transmit them when inserted into the user's machine. Any individual whose memory stick has been compromised can (in principle) compromise any system to which it comes into contact. If you change the word "compromise" to "infect," the analogy with epidemiology becomes clear.

Finally, every network capability can be compromised by what are known as distributed denial-of-service attacks. These generally require coordinated actions by lots of machines on the Internet; and certain known types of attack can be mitigated or denied by the network operators who detect or are otherwise made aware of them. The first line of defense here must be the network operators.

How Best to Deal with These Vulnerabilities?

What can be done to deal with this situation going forward? Three assertions are made in this chapter, each of which is discussed further below. First, the DO architecture will help to achieve increased visibility and awareness into the possibility of actions that threaten systems that are part of the Internet. Second, a greater use of identity-based transactions on the Internet will ensure that – with the user's concurrence – the parties and perhaps devices and systems/resources involved in the transactions can be determined from the transactions, while still supporting privacy and allowing anonymous operations, if desired. Third, the use of an identifier-based mode of interaction with Internet resources may help to circumscribe the kinds of actions that can be taken and thus help to clarify the landscape whereby intrusions may occur. None of these steps, by themselves, will prevent clever individuals from seeking workarounds; but the architectural constraints can help to make the commission of unwanted actions more visible and harder to accomplish.

INCREASING VISIBILITY AND AWARENESS

When we drive a car, we have a general idea of what the car is and what is normal and abnormal behavior. We can determine if a tire is flat, or a headlight is out by direct inspection. By other clues we know that gas is required to power the engine and can sense when the tank may be empty, and can see the tank level from the gauges on the dashboard. In general, we have a degree of visibility into the current operation of our car. Similar statements can be made for many other things we come into contact with and depend on. No such statement

can be made about the computational facilities on which we depend or, for that matter, about the Internet itself.

Internet operators may know quite a bit about their networks and other computational facilities from information accessible in their control centers, and they are in a position to readily respond to many types of outages and disruptions. In general, they tend to have visibility into their networks and are aware of their current state and what may go wrong. While there will always be new situations they have not encountered before and situations in which they have no idea what is happening, their forensic staffs will undoubtedly be engaged to deal with these situations quickly. No such thing can be said if the situation is such that significant parts of the Internet are compromised. Remedial action by one network operator may only solve a piece of a more complex problem. While a global means of responding to a widespread threat is needed, this is largely a matter for policymakers from multiple nations to address in a political arena.

Users are generally in the worst position to respond to attacks and would have to rely on Internet defenses provided by others or contained in the software they use. Users typically rely on their computational facilities to carry out well-known tasks, and are usually much less knowledgeable than technical staff working for the organizations providing Internet services. For example, there is no serious equivalent of a user dashboard that portrays for the user the most important aspects of its computer in such a way that the user will know when something unwanted has happened, or makes it possible for the user to take action to repair the problem. Turning a machine off and then back on does nothing to deal with an implanted and potentially harmful virus, for example. Virus checking programs can help to prevent such unwanted intrusions, but, with today's operating systems and applications, clever perpetrators will easily find ways around commercial virus checkers and even hide the presence of harmful actors on a user's machine from subsequent detection.

Users should be able to inspect their computers with as much facility as they can inspect their cars. What might they like to know? Perhaps some would like to visualize the "actual" memory map of their computer to know what is stored in the various parts of memory – "actual" meaning what is really there, rather than what a program may be fooled to think is there. In addition, a user might like to know when traffic that makes it into or out of his or her machine is notable for some reason. A user might like to know about information flow that is unauthorized and to locate (and remove) programs that may be extracting information and shipping it elsewhere without permission or authorization. Further, users may want to access audit trails that provide information about how the unauthorized program was put on their machines, along with certain information that may already be available such as the time it was created on the machine.

With the DO architecture, a basis would be in place for better understanding what is transpiring within the Internet, thus yielding greater visibility into and awareness of potential threats. In this mode of operation, all operations are explicit and, with authorization, can be logged and diagnosed. In addition, the same can be done for entire sessions consisting of many transactions in series. Programs and users will have a smaller set of well defined primitives to invoke in their instrumentation; and presentations of results can be more succinctly prepared along with more detailed semantic interpretation.

While much of this area is still likely to be the subject of research and development for many years, some aspects can be addressed immediately. It remains to be seen, however, just how much information the average user will need or want in order to be a more informed Internet user in the future.

IDENTITY-BASED OPERATIONS

Critical information about users and their intended actions on the Internet today is largely unavailable

Users are generally in the worst position to respond to attacks and would have to rely on Internet defenses provided by others or contained in the software they use.

from or not visible from the information communicated. Further, such information may be encrypted and, thus, the intent would be purposely hidden while the information is in transit. The communications are from one machine with an IP address to another and otherwise consist of a flow of undifferentiated packets. Authorized users who wish to make use of remote machines are usually required to log into the remote machine and supply a password of some kind. Some systems allow anonymous usage (e.g. most search engines), but take steps (usually by severely limiting the number of possible actions) to ensure that users cannot harm their systems.

Let us postulate that every user has the ability to obtain one or more unique identifiers from one of potentially many bodies, each of which is known and trusted to authenticate assertions in digital form about individuals, including the mapping between such assertions and their unique identifiers. Efforts are underway in several quarters to formalize this mapping process, but such formal processes may not be required in many customary cases. The most convenient way to handle this is via individual actions involving parties that know and trust each other. For example, if a patient has an identifier he is comfortable providing to his doctor, the doctor can rely on that identifier for the purpose of providing information to that patient, since the patient would have authorized use of that identifier in the first place. If the identifier has associated with it a public/private key pair, and if the public key is accessible by use of the identifier, then a public key authentication can be invoked at any point the doctor or the doctor's information management system wishes to validate the patient. Similarly, if the patient contracts with a company to manage his or her health records, that company would have the obligation to make the connection between user and identifier.

An assertion about an individual that has a unique identifier acquired in connection with a desired task, process or service can be used to authenticate the user to a resource on the Internet. This provides a uniform way of validating the assertions. A similar process can be used to authenticate assertions about services, physical objects, organizations and other entities. When the service is remote, and the user learns of its identity from a third party, the user may elect to trust the third party (although this is not without its potential pitfalls) or to rely on bodies that maintain trusted information about such services.

However, users that do not wish to use their identifiers, or do not have identifiers, may still use Internet resources that permit such anonymous access. However, taking the route of anonymity may still allow services to be controlled in some situations where such control is deemed important or necessary. The main concern here is the provision of bogus identifiers by trust authorities or other entities. Using the term bogus does not mean that the identifiers are invalid, although that may be the case, but rather that the mapping of the identifier to assertions about the individual is not accurate or perhaps simply not known. These cases represent a kind of anonymity, but identifiers known to be linked to specific individuals may be unimportant in many cases, such as where payments are properly made or where accurate checking of identity is not critical. If problems were to arise here, one will know which identifiers were involved and perhaps who issued them in the first

place. Some regulation of the issuance of identifiers and the coupling of them to key pairs will be important, as is regulation of other trusted entities in society (such as banks).

Once a means of obtaining identifiers for individuals and organizations becomes routine, similar steps can be taken for Internet resources of all kinds. Systems and services can be given identifiers and users can validate them as easily as they can validate the users. Although accurate audits of information requested and disseminated can be enabled in this fashion, it also has the downside of enabling unauthorized accounts of such activity. In a free society, the balance of privacy versus security comes squarely into play here and requires careful examination from both regulatory and political perspectives.

Assuming all Internet information systems and other resources (including users, networks and devices, as well as the actual information or services being provided) have associated unique persistent identifiers, how would the operation of the Internet actually function in this context? How would informational resources be accessed in this manner? And why would it matter for Internet defense?

Circumscribing the Operations

If the main vulnerability of today's information systems comes from the operating systems and the applications that make use of them, an important first question is whether either or both of them can be avoided or if it is possible to otherwise constrain the vulnerabilities in some fashion. For some applications, the answer is clearly no, since they are essential to providing the desired user functionality. Most applications currently depend on underlying operating systems for many tasks such as storing files, scheduling multiple tasks and handling security and network functions. Vulnerabilities in the operating system pose direct threats to the application, yet many operating system functions will still be required. If some of the operating system functions are not really needed, however, perhaps that software can be simplified and made less vulnerable to attack.

Most of today's workstations, desktop and laptop computers are installed with a suite of application software, including office-related software for document preparation, spreadsheets and more. Downloads from trusted vendors are the norm, but subject to the vagaries of the user's system. Access to remote sites, such as those on the Web, are typically enabled via a Web browser, where each website complies with standard Web protocols and vulnerabilities in the browser protocols can have repercussions for users of the websites visited.

Reliance on structured information in the form of digital objects is another way to circumscribe the operations, since one knows both the nature of the operations to be performed and the targets of those operations. Digital objects, whether embodying what is traditionally viewed as "content" or actions to be taken on that content (perhaps in the form of executable code for which trust mechanisms can be invoked) can easily be incorporated within the DO architecture to enable a scalable and evolvable system going forward.

The largest growth in computational facilities has recently been with wireless devices, such as smartphones and tablets, where the devices may not be intended for use as general purpose computing platforms; and user desired functions that are not already installed on these devices are enabled by obtaining vetted computer programs (applications or "apps") usually written by others. Such apps can provide services of their own, or enable access to other resources on the Internet. Users typically activate these apps by touching the screen on their wireless device or taking an equivalent action. These apps can be customized by their providers to give a unique experience either using the device or in connection with a remote service or interaction. Thus, suppliers of such apps are usually not constrained by the technology to

any single set of application protocols or means of presentation, but those made available with the user's device are often the most convenient to use. By this measure, the Web, along with the Web browser, is but one very pervasive app.

Apps, in general, may not require many services typically provided by an operating system. In this chapter, it is assumed that the operating system may be viewed as a mini-version of a combined traditional operating system with a high-level programming language, which we call "MyOp" for short. MyOp is assumed to provide a well known programming language execution environment, network access, maintenance of address books and/or mailing lists, the ability to select and schedule resources for execution and the ability to execute public/private key encryption and decryption. It is assumed that usual file and folder operations are replaced by use of a special purpose app that provides repository functions and uses either internal storage (if necessary), external storage (if available) and possibly both under certain conditions. Synchronization functions are not discussed here, but these could be embedded in MyOp or combined in the repository app.

MyOp is assumed not to be programmable by third party computer programs, and since apps cannot directly interact with other apps except by communicating with them via information structured as digital objects, this should limit the vulnerability from external threats to manifest themselves through unknown installed "hooks." It remains to be seen whether it will be possible to inhibit apps from permitting the execution of third party digital objects that are executable programs. If not, the use of specialized sentinel programs called "bastion objects" that cordon off the range of operations of such apps may be required. If a user can be aware of all the downloaded apps on his device, he can be made aware if an unwanted app were somehow to arrive. In any event, since he would have taken no action to cause it to be downloaded (of which he was aware), either his system would detect it to be unwanted and take appropriate action or, somehow, his system would have had to be fooled into making such a request (or getting his system to think such a request had been made). All this is to explain how the discourse of dealing with threats and defense against such threats would shift from a wide unknown range of possibilities to a situation in which various types of attack scenarios can be better described and thus dealt with both before, during and after the fact.

No other actions are allowed by any app relative to MyOp, and further no app is permitted to interact with any other app except by passing identified information, referred to here as digital objects. So, temporary or permanent storage of digital objects takes place via the internal repository app or by passing the information to an external repository. Digital objects are constructed by the repository app, or by APIs (application programming interfaces) that make use of it, according to a meta-level standard and parsable structure understandable by apps throughout the Internet; a unique persistent identifier is also associated with each such digital object. Thus, all arriving and departing information is in the form of digital objects, and internally generated information that does not leave the local computational environment is also stored as one or more digital objects.

Information in the form of digital objects flowing over the component networks of the Internet can thus be individually identified along with all incoming and outgoing information from any device or other computational facility. Although there is no requirement that any part of this information, including its associated identifier, be made visible in the network, users may wish to make the identifier part of a given digital object visible for any of several reasons. One is that the provenance of the information can be made available when the information becomes available. Another is that users can require that references to responses from their systems include the identifier of each digital object being responded to for cross-correlation or validation on receipt. Coupled with

timestamps and use of public key encryption, this approach can also be used to validate individual steps in a series of transactions or other operations taking place during a single session.

Large server farms will have very different needs than an individual user's computational devices, but their level of expertise can be expected to be much higher as well. No matter what the level of expertise, however, if such server farms require more sophisticated operating systems and related services to support distributed computing (sometimes referred to as "cloud computing") within and among the servers in the farm, care will have to be taken to identify, isolate and hopefully remove latent system vulnerabilities. Internet-based server farms, particularly if they store large amounts of data, provide specific targets for potential attackers. Thus, a combination of local storage and remote storage might provide a reliable approach in the event of sabotage or denial-of-service. Normally, one might rely on remote storage for day-to-day operations and only use the then-current local storage choice in those cases for which the remote storage is unavailable. If the remote storage is disabled or destroyed, or cannot otherwise be brought back up for days, weeks or months (or longer), a user can temporarily resort to the user's local storage capability.

It is assumed these server farms can be operated both reliably and securely. However, users may wish to store their digital objects in encrypted form, with the keys kept separate from the remote storage site. In this case, operations with the remote storage site will likely be of the warehousing variety with entire digital objects being passed back and forth. When encryption is not required or is not invoked, operations with the remote storage can be more fine-grained, and specific elements of the digital object may be accessed directly or after performing one or more remote operations without the need to retrieve the entire object. Recent developments have shown that remote interactions with encrypted objects are also possible in certain cases, but this aspect is not explored further in this chapter. In cases of very large objects, which would consume bandwidth and take time to transport, the ability to access directly specified parts of the object would have obvious appeal.

In each of these cases, the potential number of digital objects can be quite large and users cannot, and indeed will not, be able to remember their identifiers, even if they can recall attributes of the digital objects to which they were assigned. Software known as registries serves the purpose of allowing users to register such objects, presumably automatically in most cases and manually (if desired) in others. These registries can be installed as separate apps on the user devices, or provided by server farms over the Internet. In both cases, the registry metadata will be produced either manually by the user or automatically at the time the original digital object is created. Indeed, the user should be able to annotate such metadata and have it apply to the metadata pertaining to a specified range of digital objects.

If a user's device is lost, he may lose the apps that were available on it, but some vendor implementations should permit the user to access such programs over the Internet at no additional cost and inhibit the operation of that app on the lost device. At a minimum, this capability would seem to require each such computational device to have its own unique identifier, and perhaps be able to hear about such loss via MyOp; however, other means of disabling such apps are also possible.

In this model, the role of IP addresses would remain unchanged, along with the role of routers and networks that interpret them. In addition, those components would have the added advantage of using the digital object identifiers to meet stated objectives as well. The DO architecture can thus be integrated into the existing Internet as well as working in other communication systems. To clarify this point, in a proposed modification to the 1995 Federal Networking Council definition,

the Corporation for National Research Initiatives (CNRI) recommended adding the words "or integrated with" to the section that talked about applications layered on the underlying protocols.[5]

In an architectural environment where all accesses to systems, services and other resources are managed using identifiers for each such resource, and all information is structured in the form of digital objects, the task of Internet defense is altered in several fundamental ways. When operations in the Internet can be made more structured, one no longer has to be on the lookout for bit patterns whose purpose and intent cannot easily be determined. If, as a result, most actions consist of a more limited set of types of basic operations (which the author refers to as "meta-level operations" to reflect the fact that they indirectly reference the actions to be taken and their targets), it may be possible to develop protective steps that are more effective. This is definitely not the case today. If the digital object architecture were integrated within the Internet, its operations and targets would be separately identifiable so that, from these identifiers, the digital objects that were involved could be determined from the metadata, and the users could (if they choose) retain all the associated digital objects for later analysis (if desired). Many other properties of the communication could also be acquired, such as timing data for each digital object (e.g., creation, dispatch and arrival) should that be of interest. This is particularly important in connection with emerging Internet capabilities that relate information about "things" to other information in the Internet.

A user who is well aware of what is happening on his device will ordinarily be in a position to take manual action if necessary. First, he has to be paying attention, which may not always be the case. Second, an attack may have significant negative impact within seconds, or even microseconds. Thus, the ability of a system to respond in kind would seem to be essential. Efforts to develop cognitive systems that understand their environment, their own capabilities and modes of behavior, and threats to their operation have been undertaken in the past; but the task has remained daunting by virtue of the many degrees of freedom posed by the general problem. In other words, there are just too many things to have to know about, look for and react to. With the digital object architecture, the number of possibilities is greatly reduced and, thus, the likelihood of success is potentially much higher. An environment where threats could be internalized within a system, and where the system can defend itself with mobile programs specifically tasked and authorized to take actions against fast moving attacks, would provide an immediate benefit to the user by defusing the attack in real time. It could also serve to provide data for a post-mortem report on the attack.

As a matter of policy, it would be useful if users can work with the involved carriers or other relevant service providers when such problems arise to determine what happened. This can be helpful in determining what networks, proxy servers or other related infrastructure or resources may have been compromised, and how best to thwart any such ongoing incidents. This would potentially have the effect of enabling legitimate backpressure or other corrective action wherever required in the Internet.

Conclusion

The digital object architecture would impact the nature of many Internet activities by making them more explicit and, thus, potentially more defensible against attack. It would help to support an informed discourse about implementation of effective Internet defense strategies that are difficult to achieve today. The continuing transition to the DO architecture is an incremental process that may take years to complete. In the meantime, considerable progress could be achieved (especially for users) in understanding what is transpiring on the Internet (including on their machines and devices), and working with Internet service providers to ensure that undesirable events can be more easily diagnosed and prevented, or at least detected and hopefully defused before they cause substantial damage.

ENDNOTES

1. Peter J. Denning and Robert E. Kahn, "The Long Quest for Universal Information Access," *Communication of the ACM*, Vol. 53, Issue 12 (December 2010): 34-36, http://dx.doi.org/10.1145/1859204.1859218. See also Corporation for National Research Initiatives, "A Brief Summary of the Digital Object Architecture" (1 June 2010), http://hdl.handle.net/4263537/5041.

2. Sean Reilly, "Digital Object Protocol Specification," Corporation for National Research Initiatives (12 November 2009), http://dorepository.org/documentation/Protocol_Specification.pdf.

3. See Robert E. Kahn and Vinton G. Cerf, "What is the Internet (And What Makes It Work)," Corporation for National Research Initiatives (December 1999), http://www.cnri.reston.va.us/what_is_internet.html; and Robert E. Kahn, "The Architectural Evolution of the Internet" (17 November 2010), http://hdl.handle.net/4263537/5044.

4. U.S. National Coordination Office for Networking and Information Technology Research and Development, "FNC Resolution: Definition of Internet" (24 October 1995), http://www.nitrd.gov/fnc/Internet_res.html.

5. Patrice A. Lyons, "The End-End Principle and the Definition of Internet," Corporation for National Research Initiatives (10 November 2004), http://www.wgig.org/docs/CNRInovember.pdf.

CHAPTER XIII:
SCENARIOS FOR THE FUTURE OF CYBER SECURITY

By Peter Schwartz

America's Cyber Future

Security and Prosperity in the Information Age

SCENARIOS FOR THE FUTURE OF CYBER SECURITY

By Peter Schwartz

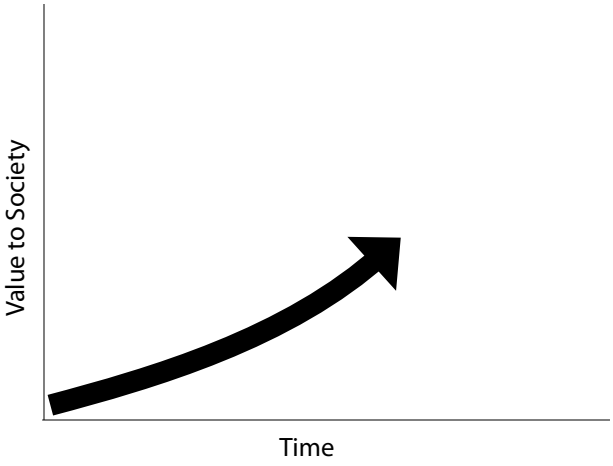
The Increasing Value of Cyberspace

The value of cyberspace has the capacity to continue to grow at least as fast as it has over the last 40 years, becoming an ever more vital part of society's infrastructure. This assumes, however, that information networks, and particularly the Internet,[1] will become more efficient, economic, reliable and secure – and that we do not act to undermine its value. Its future growth and value depends on our ability to apply to it the rule of law, better technology and appropriate social norms.

Cyberspace has become increasingly valuable since 1967, which marked the beginning of dial-up access. I first accessed the Advanced Research Projects Agency Network (ARPANET) – the precursor to the Internet – in 1973 with a TI Silent-700, a portable computer terminal manufactured by Texas Instruments, which was about the size of a suitcase with an acoustic coupler for telephone connection. Through the 1990s, the value of cyberspace rose steadily – but mostly within the computer and academic subcultures. Then, in 1995, the World Wide Web became an effective communication and business platform, with Amazon, eBay, Google and others leading the way. The Internet moved from an esoteric, small phenomenon to an increasingly global phenomenon. More and more businesses, services and government institutions connected to the Internet for one reason or another. As a result, the value of the Internet rose rapidly in the last decade and a half (see Figure 1).

As long as cyberspace remains relatively secure, it will continue to grow in value as fast as it has in the past, or faster, because connections increase exponentially as more people are involved and technology advances. A great example of the evolutionary dynamics at work in cyberspace is the introduction of Apple Inc.'s iPhone application platform. Hundreds of thousands of applications quickly developed to use that platform in novel ways. The Internet is expected to only get faster,

FIGURE 1: VALUE OF INTERNET TO SOCIETY OVER TIME



less expensive and more accessible around the world. As a result of endemic human use of the Internet, society will depend on it ever more. The Internet will be, if it is not already, a significant, critical part of global infrastructure. For example, on a recent visit to rural Rajasthan, India I encountered a young, extremely poor woman coming down a hillside having illegally harvested 100 kilograms of firewood she was carrying on her head – while checking her smartphone on which local village had the best price for firewood.

However, cyber insecurity and its related challenges could cause the value of cyberspace to decline. This chapter examines how that might happen, and identifies several factors that might help indicate whether cyberspace is evolving in ways that will promote its ever-increasing value, or whether security concerns, conflicts and poor management will diminish its value.

The Architecture of the Internet Today

In their 2010 book *Cyber War*, Richard Clarke and Robert Knake outline certain basic principles of the Internet: Because networks have to stand on their own, each network is a self-organizing, bottom-up system as opposed to a controlled, top-down system.[2] On the one hand, this characteristic makes it extremely difficult to modify architectures; on the other, it dramatically reduces vulnerabilities. If part of the system breaks down, this does not interrupt the system as a whole.

While the Internet's distributed structure persists, there are many who believe it should be transformed to concentrate more power and control at the top. Most cyber-related policy discussions revolve around this struggle: Should we empower individuals to secure themselves, for example, through software on their laptops; or should we build walled gardens, very secure networks that are cut off from their surroundings and controlled from the top down?

This issue is currently playing out in the "Apple world." There, Apple Inc. CEO and co-founder Steve Jobs can prevent a software company like Adobe Systems Incorporated from running its software on an Apple device such as the iPhone – simply because he does not like the software, or because he does not think it fits Apple Inc.'s view of the desirable user experience. This argument, driven by the desire to control the experience, create perfect security, etc., is perfectly legitimate within the Steve Jobs-controlled universe. Indeed, downloading software or products from Apple Inc. is highly efficient, economic, effective and secure … as long as users are inside the Apple world.

In addition to corporate walled gardens like Apple Inc., there are also national walled gardens, a great example of which is the expanding great firewall of China. If more cross-border attacks continue of the Estonia-Georgia, Stuxnet or even the Google-China variety, nations may be inclined to say, "We want to opt out of a global Internet."

The Apple Inc. example and, to a certain extent, the China case, provide alternative models for the evolution of the Internet – and there are virtues associated with both the top-down model and the distributed structure. However, if walled gardens

Potential Power Resources of Actors in the Cyber Domain

MAJOR GOVERNMENTS

- Development and support of infrastructure, education, intellectual property.
- Legal and physical coercion of individuals and intermediaries located within borders.
- Size of market and control of access, e.g., EU, China, United States.
- Resources for cyber attack and defense: bureaucracy, budgets, intelligence agencies.
- Provision of public goods, e.g., regulations necessary for commerce.
- Reputation for legitimacy, benignity, competence that produces soft power.

Key Vulnerabilities: High dependence on easily disrupted complex systems, political stability, reputational losses.

ORGANIZATIONS AND HIGHLY STRUCTURED NETWORKS

- Large budgets and human resources; economies of scale.
- Transnational flexibility.
- Control of code and product development, generativity of applications.
- Brands and reputation.

Key Vulnerabilities: Legal, intellectual property theft, systems disruption, reputational loss.

INDIVIDUALS AND LIGHTLY STRUCTURED NETWORKS

- Low cost of investment for entry.
- Virtual anonymity and ease of exit.
- Asymmetrical vulnerability compared to governments and large organizations.

Key Vulnerabilities: Legal and illegal coercion or retaliation by governments and organizations if caught.

Source: Joseph S. Nye, Jr., "Cyber Power" Belfer Center for Science and International Affairs (Harvard Kennedy School, May 2010).

continue to persist, they may begin to break down the virtues of the Internet's bottom-up system, ultimately transforming the nature of its evolution, creating islands of disconnection.

ACTORS AND THEIR RELATIVE POWER RESOURCES

To understand who is doing what in cyberspace, I use scenarios based on a framework developed by Joseph S. Nye, Jr., in his 2010 paper "Cyber Power."[3] Nye introduces three critical actors in the cyber domain and describes each actor's relative power resources: 1. governments; 2. organizations and highly structured networks; and 3. individuals and lightly structured networks (see "Potential Power Resources of Actors in the Cyber Doman" text box).

- First, there is government, which created the Internet for two purposes: To facilitate connectivity among scientific research stations and to provide a backup communications infrastructure in case of a breakdown in fundamental communications. Since then, the role of government has come to encompass everything from development and support of cyber infrastructure, regulation, defense resources, etc., to controlling the Internet in terms of access and

TABLE 1: PHYSICAL AND VIRTUAL DIMENSIONS OF CYBER POWER

TARGETS OF CYBER POWER		
	WITHIN CYBERSPACE	**OUTSIDE CYBERSPACE**
Information instruments	**Hard:** Launch denial of service attacks. **Soft:** Set norms and standards.	**Hard:** Attack SCADA systems. **Soft:** Initiate public diplomacy campaign to sway opinion.
Physical instruments	**Hard:** Enforce governmental control over companies. **Soft:** Introduce software to help human rights activists.	**Hard:** Destroy routers or cut cables. **Soft:** Stage protests to name and shame cyber providers.

Source: Joseph S. Nye, Jr., "Cyber Power" Belfer Center for Science and International Affairs (Harvard Kennedy School, May 2010).

investment. For example, the U.S. government opposed Verizon's move to buy switch gears from Huawei, a Chinese company. In doing so, it implicitly informed China that it does not trust it enough to buy its hardware. The lack of mutual trust will only deepen friction between China and the United States. The risk of actually buying Chinese hardware may, in fact, be too great.

- Second, there are large organizations like telephone and media companies and Internet service providers (ISPs) that are users and/or providers of cyber infrastructure and systems. These highly sophisticated organizations, which can operate both domestically and globally, are governmental or quasi-governmental in many places where national governments play a larger role in telecommunications.
- Finally, there are individuals or small organizations with relatively limited resources, which can access the Internet at a fairly low cost. Given the nature of cyber systems, they can remain anonymous relatively easily, while having the potential to inflict massive damage.[4]

To begin thinking about different cyberspace scenarios and how they may evolve, we have to consider these three actors and the fundamental asymmetry of power that exists between them.

In addition to the targets of cyber power and types of cyber attacks, it is useful to think about the expression of force in cyberspace, in other words, the relationship between government, organizations and individuals. Again, Nye identifies three aspects of influence in cyberspace (see Table 1):

- **A induces B to do what B would initially otherwise not do.** This involves some form of coercion, by exercising hard and/or soft power. For example, the current WikiLeaks incident is intended to produce a change in the behavior of the United States and other governments through a radical act of transparency.
- **Agenda Control – A precludes B's choice by exclusion of B's strategies.** As an example, ISPs can influence the architecture of the Internet by monitoring and controlling access via filters, firewalls, the use of widely-accepted software standards, and through other means.

- **A shapes B's preference so some strategies are never considered.** The anonymity of the Internet has created an interesting new environment in which people and organizations reconsider doing things because of the implications of exposure through public dissemination of information. WikiLeaks, for example, has had a substantial effect on cyberspace power dynamics.

The Spectrum of Cyber Scenarios

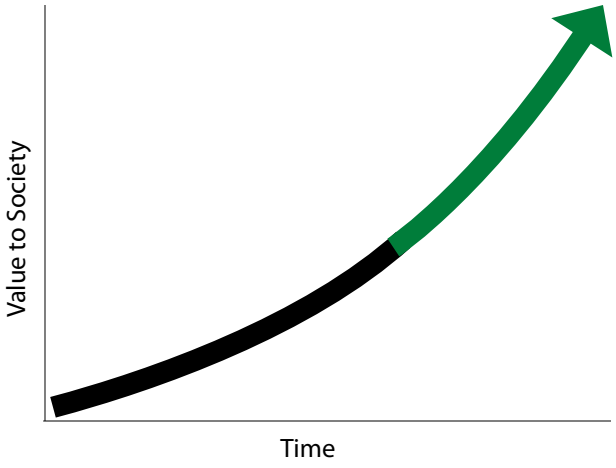
A very simple framework for thinking about cyber scenarios is based on the value of cyberspace to society, measured in dollars of business transactions, volume of activity on the Internet, number of firms providing services, number of people on the Web and so on. There is a spectrum of scenarios for the future of cyberspace, bounded by two extremes: the Ideal Scenario and the Worst Scenario.

THE IDEAL SCENARIO: OPENNESS AND SECURITY

In the Ideal Scenario, the upward trend moves forward such that the value of the Internet to society would continue to increase exponentially because the Internet is increasingly globalized and nearly universal (see Figure 2). In the third quarter of 2010, the number of installed Internet-capable devices reached 5 billion globally, and that number is expected to increase to 22 billion by 2020.[5] Cell phone networks, which are expanding faster than any other networks, have made the smartphone the platform of choice in much of the world – even in rural regions of the world and at the poorest levels of society. As a result, the Internet has evolved from a tool formerly only accessible to intellectual elites.

What might the Ideal Scenario look like? Fundamentally, if the Internet of today is a Wild West with very few rules and little visibility into what is going on in the networks, the idealized world is one in which a more civilized approach to Internet usage expands, understanding of and visibility into networks improves and the Wild West

FIGURE 2: THE IDEAL SCENARIO



becomes mostly tamed. While there will continue to be small islands of chaos – for example, individual countries where cyber crime persists and is largely tolerated – by and large, the cowboys will complain that "it's no more fun here out on the range now that the sheriff has arrived."

Some characteristics of this evolution would be:

- **Democratization of Internet access and applications.** There is a continued deepening and extension of all the applications that are currently leading to more effective uses of and access to the Internet in commerce, security, education, governance, health and other areas. This includes government 2.0 technology, applications in health care and education, etc. This is a world in which applications continue to proliferate and serve the majority of the world's population and organizations of all sizes and shapes.
- **Increased Internet security through public and private leadership.** Public and private organizations will lead the development of effective Internet defense and security, through both cyber and non-cyber approaches. National and regional governments develop more coordinated Internet governance institutions than currently exist, both domestically and internationally. We begin seeing more institutions like the

International Telecommunications Union (ITU), which is effective in telecommunications regulation, as opposed to inadequate structures like the Internet Corporation for Assigned Names and Numbers (ICANN). Effective private sector leadership may involve increased vigilance over network activity and robust infrastructure rollouts to secure network components. Both public and private actors invest substantial resources to defend critical infrastructure systems, particularly the telecommunications backbone, power grids and the Department of Defense. The defenses we put up are effective, not because they are perfect but because they are good enough to deter malicious action. We are able to create a very high workload for attackers, who realize that there are easier things to do than to act maliciously in cyberspace.

- **Deterrence for major countries through entanglement.** Part of the reason deterrence works is that major countries come to recognize the criticality of securing Internet infrastructure for their own sake. Even China's leaders realize that our systems are so entangled – the word "entangled" is correct in a literal sense – that they cannot be separated, and that what they do to us and to others will bounce back to hurt them.

  For example, it is interesting to observe there is very little hacker activity in India as compared with China, particularly given the sophisticated computer technology in India. This happened because India recognizes that its communications infrastructure is an empowering tool that is central to its success. It has become a kind of computer agent for the world, and it knows that if it undermines that infrastructure, it will really be hurting itself. The Indian case is a good example of what China and other countries may become, i.e., countries with acute self-awareness of their inherent entanglement and complete involvement with cyberspace.

- **Enhanced visibility and potential network redesign diminishes security threats.** Over the course of his career, Bob Kahn, inventor of the Transmission Control Protocol (TCP) and the Internet Protocol (IP) – the fundamental communication protocols at the heart of the Internet – and former director of the Defense Advanced Research Projects Agency (DARPA) when the ARPANET was created, has been asking himself, "How would we have architected the Internet in the beginning, if we knew then what we know now? If we were to re-architect the Internet today, given its current roles, what would we do? How would we migrate from the current state to the future state?" As Kahn notes in this volume, the initial objective of the Internet was ensuring connectivity and moving bits around, whereas there is now significantly more interest in managing the information itself. Indeed, Kahn says that one of the reasons people are so concerned with cyber security is because there is very little visibility into what is going on in the networks.

  So how can we ensure more visibility into the network? While there are likely additional methods of achieving visibility, Kahn proposes developing a "digital object architecture." This involves creating new categories called "digital objects," which are defined data structures (such as a file or a game) that are machine-independent. Digital objects would have a unique and persistent identification, instructions for storage in "cloud" repositories and associated properties and transaction records containing metadata and usage information. The digital objects would be accessed through metadata registries, which would essentially act as a firewall between modes of access and the specific content in a way that enables more inherent, higher-level security of content. Such a re-engineering of information infrastructure will diminish security threats.

  It should be noted that this model is nearly identical to the model my team developed for digital

preservation at the Library of Congress when it wanted to create secure access and protection of digital property, as well as structures that could accommodate evolution over time. Clay Shirky, a writer on the social and economic effects of Internet technologies, and the late Bob Spinrad, one of the inventors of Ethernet, came up with the model, which has since been used by the Library of Congress. Several different pathways could lead to similar models of data organization that facilitate both efficiency of access and security.

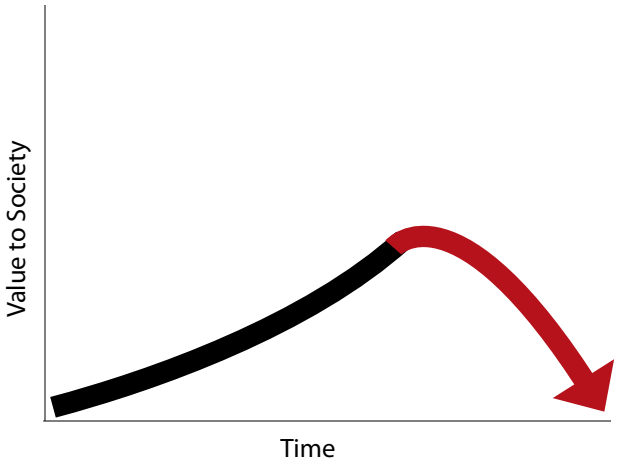
- **Constraining and changing social norms.** Constraining social norms in the cyber domain are becoming common. To make an analogy, in most countries today no one urinates on sidewalks (except sick and homeless people) – but they do the equivalent on the Internet. That is, people are willing to meddle with the Internet, not necessarily with malicious intent, but because they do not recognize how consequential their actions can be. In this scenario the Internet becomes like the sidewalks of modern societies, and most people in most places comply. One effect of this is that hacker culture changes because of the recognition by hackers that their behavior is no longer socially acceptable. As a result there is little malicious hacking or hacktivism, and few WikiLeaks-like incidents.

It is important to note that there would be little, if any, cyber war or terrorism in the Ideal Scenario, because we would successfully defend against it. The Ideal Scenario involves everything working out perfectly right, but recent history suggests that reality is unlikely to play out quite so benignly.

THE WORST SCENARIO: CONTINUAL ATTACKS AND CONFLICT

In the Worst Scenario, the value of cyberspace to society declines rather than continuing the upward trend of the last 40 years (see Figure 3). In this world, the sheriff does not show up, the rules do not develop and the only place the Indians do not

FIGURE 3: WORST SCENARIO



attack is within the boundaries of Fort Apache. It is a world in which the Wild West persists with islands of order. As cyber attacks (both physical and virtual) increase, the budget, time and energy of public and private actors are absorbed attempting to defend the network. Consequently, the economic and social value that the Internet might have created is wasted; cyberspace is no longer a tool for political participation, cultural expression, democratization of education, innovation or business optimization.

The costs of this scenario are very steep, characterized by:

- **Weak public and private leadership.** There are few effective government institutions and very little effort to enhance international governance structures. Government and companies are unable to collaborate, and as a result high levels of friction develop regarding cyberspace resources. Poor management of the "common pool resource" leads to decline in efficiency, reliability and security.
- **Persistent threat of cyber conflicts.** Cyber weapons are low-cost and extremely efficient, i.e., no lives are invested, no planes are required and identifying the attacker is astonishingly difficult. Cyber weaponry becomes the weapon of choice and there

is a persistent threat of cyber conflicts. These cyber conflicts may take the form of intra- and inter-country attacks, may come from both state and private actors and may remain in the cyber realm or spill over into the physical world. Such conflicts will run the gamut from distributed denial-of-service attacks on a country's utility infrastructure to coordinated harassment of political opponents (e.g., the recent cases in which vigilantes identified and urged harassment of abortion providers and undocumented illegal immigrants).

- **An increase in cyber terrorism and crime.** One can easily imagine an increase in cyber crime where people act as disruptors and spies who steal all manners of information. For example, foreign governments steal the intellectual property of American firms (and this is increasingly perceived to be both common and almost unstoppable). In effect, intellectual property becomes a major point of contention between nations.
- **Wholly insufficient cyber security.** Cyber security systems are so weak that the workload of the intruders is relatively low. Many people play "the bad guy," and a large population of hackers and hacktivists are able to develop new tools faster than the good guys. Governments increase insecurity by abusing privacy, and people come to see government as an enemy with whom they are unlikely to cooperate. WikiLeaks and the anti-government response from Anonymous, a loosely connected group of hackers, are perfect examples.

SCENARIOS THAT LIE IN BETWEEN

We may move toward the Ideal Scenario – if we do everything properly – in a smooth way and with foresight and leadership. However, the far more likely scenario is that we will face a set of crises to which we will respond imperfectly, but nonetheless in ways that enable us to move toward a world where the Internet is secure, efficient and reliable. Our transition will not be smooth, and will cost more than it would if we simply managed these crises effectively, for example, or if we did not face crises at all.

On the other hand, we may move toward the Worst Scenario. Basically, cyberspace could erode at the margins because we are not defending it effectively, even without a crisis. Or it could rapidly decline because we failed to respond effectively to a series of crises, such as cyber wars, cyber terrorism, accidents that break down information infrastructure or rampant crime on the Internet.

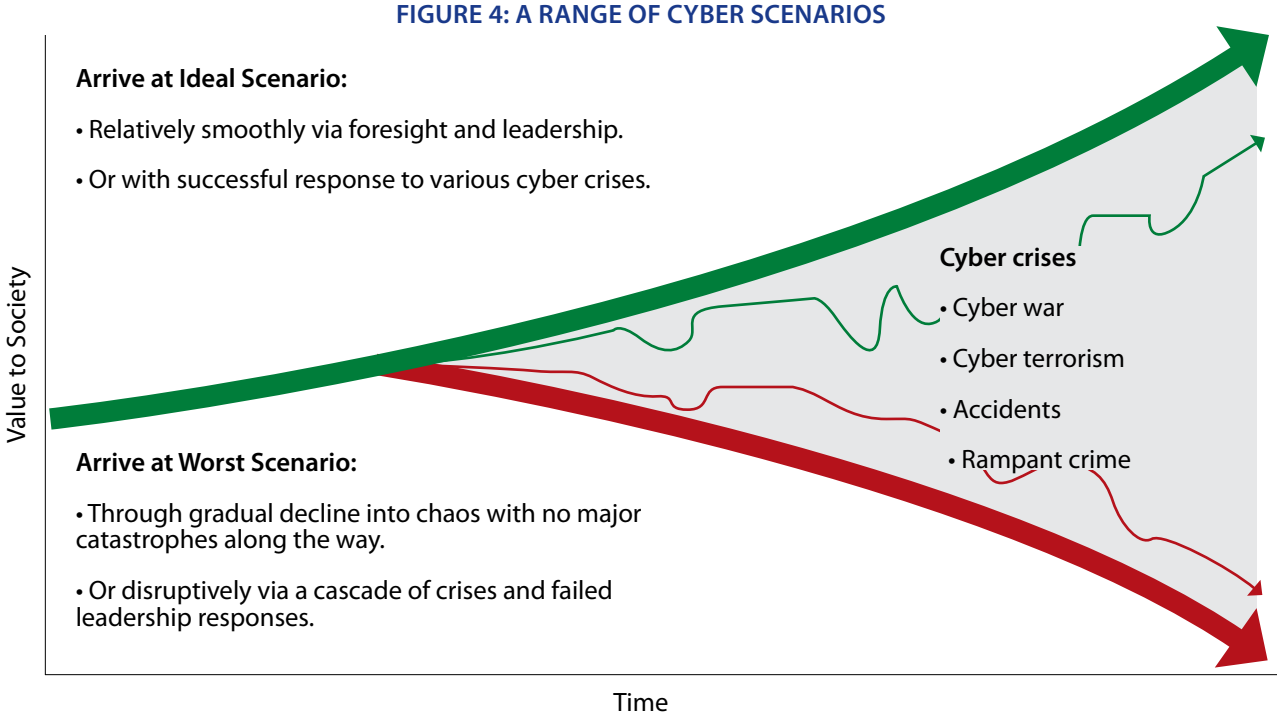
Thus, there are also two broad scenarios that lie between these extremes: A world moving in the right direction, but imperfectly and not smoothly; and a world moving in the wrong direction, but also imperfectly and not smoothly. The most likely outcome is somewhere in the middle, getting some things right and others wrong (see Figure 4).

Indicators to Watch

There are certain forces pushing us away from the Wild West toward a well-ordered world, and vice versa. Several trends may indicate which forces are prevailing and which scenarios are becoming more likely, including:

- **Pace and pattern of technological innovation.** Do the protectors and systems architects get ahead of the attackers in terms of innovation? Are better security systems, software, etc. deployed effectively? To what degree do major technological developments like ubiquitous sensors, smart cities and smart grids, cloud computing and authentication technologies affect the security of the Internet or complicate the job of those trying to defend it?
- **Punctuated equilibrium evolution, not revolution.** Is there a kind of steady – but radical – evolution, where the Internet may experience some growing pains but will remain fundamentally reliable and secure? Or will the network become plagued by hackers, cyber attacks,

FIGURE 4: A RANGE OF CYBER SCENARIOS



overburdened networks, costly security measures, etc., causing a fundamental break that will require reinventing the system?

- **Successful adoption of new layers.** Are the government, business and technology leaders who are constructing the Internet able to design and implement new technological layers that increase efficient access and security?
- **Rising social norms/declining international conflicts.** Is there an agreed-upon standard for appropriate online behavior? Do different countries adhere to this standard, or is cyberspace behavior contentious?
- **Increasing faith in our institutions.** Do people actually trust government institutions to manage cyberspace?

These forces affect the speed and effectiveness with which cyber attacks are deployed – as well as the defensive measures that are deployed against them. Unfortunately, people like Mike McConnell, former head of the National Security Agency, explain that while we are still talking and not acting, there will inevitably be some catastrophic event that will cause us to overreact, and that we will, in a sense, oscillate between not enough control and too much control.[6] Managing that is going to be difficult, and we are bound to get some of it wrong.

Progressing Toward the Ideal Scenario

If policymakers want to influence the ultimate outcome of these scenarios, what can they do?

Three key opportunities are:

- Leading efforts to enhance governance of the Internet, driving toward adoption of common rules and standards of civil behavior.
- Encouraging and supporting research into redesigning the architecture of the Internet to improve visibility into the network and diminish security threats.
- Supporting the extension and continued build-out of the Internet in both advanced and

emerging markets. As emerging markets increase Internet usage and broadband connections, their economic ambitions and continued strong growth will contribute to an increase in Internet-related products and services, productivity and global economic growth.

The United States will almost certainly have some cyber crises in the years ahead. The fundamental question to keep in mind, from a policy perspective, is whether the government is organizing the appropriate incentives to move the country toward the Ideal Scenario rather than the Worst Scenario. The actions and policy choices policymakers make today will significantly affect the evolution of cyberspace in the long term – which will affect the very future of the American society, economy and security.

ENDNOTES

1. As used here, the term Internet means more than just the World Wide Web; it encompasses all the ways in which information networks interconnect, including, for example, Skype running on the telephone network. Collectively, these networks make up what is known as "cyberspace."

2. Richard A. Clarke and Robert K. Knake, "Cyber War" (New York: Ecco, 2010).

3. Joseph S. Nye, Jr., "Cyber Power," Belfer Center for Science and International Affairs (Harvard Kennedy School, May 2010).

4. Joseph S. Nye, Jr., "Cyber Power," Belfer Center for Science and International Affairs (Harvard Kennedy School, May 2010): 7.

5. IMS Research, "Internet Connected Devices About to Pass 5 Billion Milestone" (19 August 2010).

6. Kim Zetter,"Cyberwar Issues Likely to Be Addressed Only After a Catastrophe," *Wired* (17 February 2011), http://www.wired.com/threatlevel/2011/02/cyberwar-issues-likely-to-be-addressed-only-after-a-catastrophe/

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic, and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS aims to engage policymakers, experts and the public with innovative fact-based research, ideas, and analysis to shape and elevate the national security debate. A key part of our mission is to help inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, D.C., and was established in February 2007 by Co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is nonpartisan; CNAS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

Center for a New American Security
1301 Pennsylvania Avenue, NW
Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Production Notes

Paper recycling is reprocessing waste paper fibers back into a usable paper product.

Soy ink is a helpful component in paper recycling. It helps in this process because the soy ink can be removed more easily than regular ink and can be taken out of paper during the de-inking process of recycling. This allows the recycled paper to have less damage to its paper fibers and have a brighter appearance. The waste that is left from the soy ink during the de-inking process is not hazardous and it can be treated easily through the development of modern processes.

STRONG, PRAGMATIC AND PRINCIPLED
NATIONAL SECURITY AND DEFENSE POLICIES

1301 Pennsylvania Avenue, NW
Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org

www.cnas.org

ISBN 978-1-935087-49-6

Printed on Post-Consumer Recycled paper with Soy Inks