JUNE
2011

America's Cyber Future

Security and Prosperity in the Information Age

VOLUME I

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 Peter Bloom, Steve Bucci, Michael Chertoff, Gary McGraw, James Mulvenon, Michael Nacht, John Nagengast, Greg Rattray, Eric Rosenbach, Bill Smith and several anonymous reviewers, who all provided excellent comments on drafts of this report. 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 I

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

VOLUME I

America's Cyber Future: Security and Prosperity in the Information Age
By Kristin M. Lord and Travis Sharp

VOLUME II

JUNE 2011

America's Cyber Future

Security and Prosperity in the Information Age

AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE

By Kristin M. Lord and Travis Sharp

I. EXECUTIVE SUMMARY

By Kristin M. Lord and Travis Sharp

Cyber threats imperil America, now and for the foreseeable future. They endanger the enormous economic, social and military advances enabled by cyberspace, not only for the United States but also for the world. While a "cyber Armageddon" does not appear imminent, cyber attacks are more than a nuisance and more than criminal activity. They constitute a serious challenge to U.S. national security and demand greater attention from American leaders.

Cyber attacks can cause economic damage, physical destruction and even the loss of human life. The economic price of cyber crime, and especially the loss of intellectual property is startling, costing companies worldwide billions of dollars each year. U.S. government networks are vulnerable, with approximately 1.8 billion cyber attacks of varying sophistication targeting Congress and federal agencies each month. Foreign cyber intruders have penetrated America's power grid, and while their intentions are unclear, the potential for harm is considerable. U.S. military planners already must guard against a range of cyber attacks on their communications, weapons, logistics and navigation systems, and the threat to military networks is growing. Cyber attacks could disable critical equipment and even turn it against its users.

Despite productive efforts by the U.S. government and the private sector to strengthen cyber security, the increasing sophistication of cyber threats continues to outpace progress. The stakes are high and the need to find solutions is urgent.

Will America rise to the challenge?

Based on extensive research and consultations with individuals in government, the military, the private sector and non-profit organizations, our answer is, optimistically, yes. But success requires stronger and more proactive leadership by the U.S. government. It requires companies and researchers to innovate faster than criminals and spies. And it requires organizations and individuals across America and around the world to take responsibility for their own security. We must not wait for a digital disaster, intentional or otherwise, to reverse the growing trend of cyber insecurity.

Sobriety is in order. Terms such as "cyber war" conjure images of dystopian futures and limitless vulnerabilities, unconstrained by physical geography and prowled by hackers and hooligans. While cyber insecurity is all too real, these images fuel hype that is often unproductive. We must not allow hype to provoke panic, and we should not overspend. We must accept that a certain level of risk will persist, just as it does in the physical world.

To help American policymakers lead national and international efforts to address cyber insecurity, this report offers detailed recommendations, which are summarized below.

Adopt a Comprehensive Strategy for a Safe and Secure Cyberspace: The U.S. government should aim to keep malicious activity in cyberspace below a threshold at which it might imperil general confidence in the security of the Internet. To do this, the Department of Homeland Security (DHS) should strengthen its capacity for risk assessment and incident response. Congress should pass legislation that creates a new quasi-governmental "fusion" center to improve information sharing, clarifies DHS's legal authority to monitor U.S. government networks, enables Internet service providers to better cooperate with the U.S. government, and bolsters cyber security education and recruitment programs.

Forge an International Agenda for Cyber Security: The U.S. government should strengthen its international agenda for cyber security. In the near-term, it should foster greater cooperation with U.S. treaty partners to enhance information sharing, crisis response and joint military exercises. In the medium to long term, it should strengthen law enforcement by engaging a variety of international stakeholders to produce multilateral agreements and codes of conduct. The U.S. government should promote key norms in international fora, including protecting innocent civilians and minimizing collateral damage, upholding Internet freedom, and exercising proportionality and restraint in response to cyber attack. Finally, the U.S. government should address cyber security more directly, and if necessary more publicly, with China and Russia; initiate a coordinated cyber security foreign assistance plan; and encourage American companies to participate in international standard-setting organizations related to cyber security.

Establish U.S. Declaratory Policy on Cyber Security: The U.S. government should outline the broad contours of a declaratory policy for cyberspace. Doing so will help deter the most threatening actions and strengthen America's role as a shaper, not a victim, of developments in cyberspace. While the policy should remain ambiguous about how the United States might respond in specific situations, it should communicate America's view of which behaviors are acceptable and which behaviors are intolerable.

Raise Costs for Cyber Attackers: The U.S. government should increase the economic, political and military costs for cyber attackers while defending against them more effectively. To do this, it should clarify legal authorities related to military and intelligence cyber operations, improve cyber defenses, sustain America's offensive military advantage in cyberspace, implement a cross-domain prevention strategy, ensure that the U.S. military can operate in a command and control environment degraded by cyber attacks, and tap into the National Guard and Reserves for high-tech cyber skills.

Prepare for the Future of the Internet: The U.S. government should launch a national commission on the future of the Internet that provides recommendations to the president. It should evaluate the feasibility of changing the underlying architecture of the Internet to increase security and forming separate networks with higher levels of security. The commission should include the science and technology community, private companies and U.S. government representatives.

Build the Institutional Capacity Necessary to Coordinate U.S. Government Responsibilities for Cyberspace: The U.S. government should create an Office of Cyber Security Policy, within the Executive Office of the President, headed by a Senate-confirmed chief cyber security advisor to the president and director of cyber security policy. The office should remain small and nimble, maintain close links to the National Security Council (NSC) and National Economic Council, and avoid duplicating functions already performed by other agencies. The U.S. government also should continue to strengthen DHS's cyber security efforts, which are increasingly respected (if still far from sufficient) according to experts in the government, military and private sector.

Enhance Oversight of U.S. Government Cyber Security Activities: The U.S. government, particularly Congress, should conduct stronger and more comprehensive oversight of cyber security activities. The U.S. government should maintian command and control procedures for cyber operations by the U.S. military and intelligence community to ensure that senior civilian leaders retain the ability to review and approve significant activities; appoint two separate leaders for U.S. Cyber Command and the National Security Agency (NSA); create a President's Cyber Security Advisory Board to provide independent advice directly to the president; form a high-level joint contact group for DHS, the Department of Defense (DOD) and the intelligence community; establish a bipartisan, bicameral Cyber Security Task Force in Congress; and create objective cyber security performance metrics.

Protect the Nation's Most Critical Infrastructure: The U.S. government should remain proactively and consistently involved in protecting America's critical infrastructure, which includes vital assets such as energy, financial and transportation systems. Government involvement should not be heavy-handed or excessively regulatory, and should favor market solutions whenever possible. Congress should pass legislation that provides DHS with more explicit authority to coordinate the protection of U.S. critical infrastructure in cyberspace, offers tailored regulatory strategies that comport with the needs of specific infrastructure sectors, strengthens the authority and capacity of the Federal Energy Regulatory Commission and DHS, and uses military bases as test beds for cyber security innovation related to the smart grid.

Harness the Private Sector's Innovative Power for Cyber Security: The U.S. government should streamline government classification guides to enable better information sharing, protect private companies that cooperate with the U.S. government, extend liability protection to providers of innovative cyber security products and services, prioritize security when writing requirements and awarding contracts for information technology, fund new research on cyber security business models, assign foreign service officers to help U.S. companies partner with responsible cyber security stakeholders abroad, and clarify what support the private sector can and cannot expect from the U.S. government.

Guide to Key Terms*

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital that their incapacitation or destruction may have a debilitating impact on the security, economy, public health or environment of a nation. Examples include infrastructure that supports banking and finance, communications, energy and transportation.

Cyber: Broadly defined, a prefix referring to anything related to computers, electronic information and/or digital networks.

Cyber Attack: A hostile act using computers, electronic information and/or digital networks that is intended to manipulate, steal, disrupt, deny, degrade or destroy critical systems, assets, information or functions.

Cyber Defense: Activities that, through the use of cyberspace, seek to detect, analyze, mitigate and prevent vulnerabilities in order to protect computers, electronic information and/or digital networks.

Cyber Exploit: Enabling operations and intelligence collection activities conducted through the use of computers, electronic information and/ or digital networks to gather data about the critical systems, assets, information or functions of a target or adversary.

Cyber Incident: A cyber attack, exploit or intrusion that causes harm to critical systems, assets, information or functions across the public and private sectors by impairing the confidentiality, integrity or availability of computers, electronic information and/or digital networks.

Cyber Intrusion: Unauthorized act of bypassing the security mechanisms of computers, electronic information and/or digital networks.

Cyber Offense: Activities that, through the use of cyberspace, seek to manipulate, steal, disrupt, deny, degrade or destroy the critical systems, assets, information or functions of a target or adversary.

Cyber Operations: The employment of cyber capabilities with the intent to achieve objectives in or through cyberspace.

Cyber Security: The protection of computers, electronic information and/or digital networks against unauthorized disclosure, transfer, denial, modification or destruction, whether accidental or intentional.

Cyberspace: The impression of space and community formed by computers, electronic information and devices, digital networks, and their users.

Internet: A global information system, based on the use of Internet Protocols, that enables different components such as networks, computational facilities and devices to intercommunicate. The individual components are operated by governments, industry, academia and private parties.

Network: A distributed system of interlocking communications links.

Norms: A set of shared beliefs that help define and govern behavior and conduct by state and non-state actors.

* Definitions based on DOD's "Joint Terminology for Cyberspace Operations" and the Institute for Telecommunications Sciences' "Telecom Glossary."

II. INTRODUCTION

Over the past 20 years, the Internet has become integral to American life. Nearly 80 percent of American adults now use the Internet. Of those users, 94 percent access email, 75 percent seek news and 67 percent visit a government website – activities that bolster social ties and civic participation.[1] The economic importance of the Internet is enormous, contributing 6,500 dollars per capita to America's gross domestic product each year.[2] The centrality of the Internet is also growing globally, with the number of users worldwide topping two billion as of December 2010.[3]

Regrettably, the very openness that allowed the Internet to spread into almost every arena of human activity also has spawned countless vulnerabilities. "It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation," declared President Obama in 2009.[4] The president's view is shared widely. For years, the U.S. government has produced national security strategy documents that emphasize the grave risk posed by cyber threats and their interrelationships with crime, espionage and warfare.[5]

Cyber threats pose serious challenges to the United States. They blur traditional lines between peace and war, government and private sector, and strategy and tactics. As such, they present daunting obstacles that are legal, institutional, technical and cultural in nature. Overcoming these obstacles will require new ways of thinking and new means of governance, involving new actors and a level of agility to which the U.S. government is unaccustomed.

To help Americans and their government better understand the growing risks posed by cyber threats, the Center for a New American Security (CNAS) conducted a year-long study co-chaired by Robert Kahn, Mike McConnell, Joseph Nye and Peter Schwartz – four esteemed leaders who contributed a wealth of experience and knowledge. We conducted extensive research and commissioned 13 chapters (published in Volume II of this report) from a wide array of experts. We also convened eight working group sessions and interviewed senior leaders from the private sector, academia, civil society, and the U.S. government and military – a total of more than 200 experts.

Within the U.S. government, we interviewed representatives from the NSC, DHS, Department of State, Department of Commerce, DOD (including the NSA, Cyber Command, Joint Chiefs of Staff, Office of the Secretary of Defense and the military services), the intelligence community, Federal Communications Commission (FCC), FBI, House of Representatives, and Senate.

Within the private sector, we met with representatives from Internet service providers, large and small technology companies, critical infrastructure providers (including from the energy, financial services and defense sectors), Internet entrepreneurs, venture capitalists, and military and intelligence consulting firms. To hear perspectives from outside Washington, we traveled to California in February 2011 to meet with business and technology leaders from Silicon Valley.

The intent of this study is threefold. First, we seek to educate the broader national security policy community about cyber security, an issue that is often still relegated to technical experts and highly classified discussions.[6] It is now too entwined with America's national interests and economic future to be a niche issue. All those who seek to promote American security now must confront the challenge of cyber security. Though many details and operational plans should remain classified, an open national conversation is sorely needed.

Second, we seek to advance conceptual understanding of cyber security to aid the United States' decision makers. Cyber threats are evolving faster than our understanding of them, a frightening circumstance given the consequences of either inaction or mistakes. Cyber security seems so hard to grasp that it is compared endlessly to something else, whether nuclear weapons policy in the 1950s, guerilla warfare or epidemiology.[7] There are few case studies of cyber conflict, and those that do exist – most notably the cyber attacks against Estonia in 2007 and Georgia in 2008 – are often hyped.[8] Used excessively, improper comparisons and exaggerated case studies can cloud understanding and oversimplify decision-making rather than clarifying complex issues.[9]

Third, we offer policy recommendations to those who must protect the United States from the many emerging threats in cyberspace. While many actors must contribute to cyber security, this report's recommendations focus on the U.S. federal government. We provide actionable recommendations that, we believe, are in line with CNAS' mission to provide strong, pragmatic and principled national security policies that advance American interests and protect American values.

III. U.S. NATIONAL INTERESTS IN CYBERSPACE

Cyber security is vital to protecting and advancing America's national interests. As articulated in the 2010 U.S. National Security Strategy, which reaffirmed long-standing priorities in American foreign policy, these interests include:

- The security of the United States, its citizens, and its allies and partners.
- A strong, innovative and growing U.S. economy in an open international economic system that promotes opportunity and prosperity.
- Respect for universal values at home and around the world.[10]

Increasingly, America's ability to achieve these interests depends on reliable and secure access to the Internet, which is "a network that magnifies the power and potential of all others," according to Secretary of State Hillary Rodham Clinton.[11] If confidence in the reliability of the Internet, the security of systems connected to it, and the trust of its many users persists, America's ability to achieve these interests will grow. But the persistence of a safe and secure Internet is threatened and policymakers cannot take it for granted.

Protecting U.S. Security

Information technology is an enormous force multiplier for U.S. military and intelligence activities around the world.[12] For this reason, DOD now operates 15,000 networks and seven million computing devices across 4,000 installations in 88 countries.[13] This advanced information infrastructure helps the United States anticipate, detect and respond to national security threats with remarkable precision and effectiveness.

America's military has excelled at developing new offensive cyber capabilities, drawing talent from the United States' preeminent technology sector.[14] These tools can create effects that are highly precise or broadly dispersed, effectively untraceable or widely publicized. They also can achieve things that kinetic force cannot. Offensive cyber capabilities are attractive in many ways, but also present challenges. The processes and authorities for using them are fraught with challenges. It is unclear how target countries will perceive and respond to them. There is the potential for negative unintended consequences, including the rapid spread or reverse engineering of destructive code once it is "out in the wild."

Military applications for cyber technology can promote American interests, but they also create vulnerabilities. The U.S. military relies extensively, though not exclusively, on access to civilian networks.[15] Even when military and civilian networks are separated, the movement of data and users between them can create unforeseen dangers.[16] Every day, America's armed forces face millions of cyber attacks and intrusions of varying sophistication. Every hour, U.S. military networks are probed or scanned approximately 250,000 times.[17] More than 100 intelligence agencies and foreign militaries are actively trying to penetrate U.S. systems.[18] While American cyber defenses typically repulse these advances, which are often unsophisticated, it only takes one breach for an attacker to compromise sensitive information.[19]

On the battlefield, cyber attacks could misdirect surveillance equipment, ships and people, or compromise information in ways that jeopardize America's military or citizens. Such tactics are not confined to sophisticated states: In 2009, Iraq-based militants used software that cost 26 dollars to access unencrypted imagery from U.S. military drones.[20]

Though cyber threats are present now, the most dangerous threats are still to come. Glimmers of that future are visible today. The computer worm known as Stuxnet ostensibly sent Iranian nuclear centrifuges spinning in ways that ultimately disabled them. Based on media reports, it appears to be a clear example of a cyber attack with a kinetic effect.[21] While this attack was targeted relatively precisely, future attacks could use similar technology far less discriminately.

A Strong, Innovative and Growing U.S. Economy

Access to cyberspace has created new opportunities for Americans to prosper. According to the Information Technology and Innovation Foundation, the information technology revolution allowed the U.S. annual gross domestic product to grow 2 trillion dollars larger than it would have otherwise.[22] Numerous studies have concluded that the Internet improves efficiency, lowers prices, expands consumer choices, boosts productivity, gives small businesses greater market access, stimulates innovation and increases wage growth.[23] Opportunities provided by the Internet also extend internationally. The Internet has generated an increase in labor productivity and corresponding economic growth worldwide.[24] There is no indication that these efficiencies have peaked.

The economic gains enabled by the Internet are not irreversible, however. Cyber crime and espionage endanger America's classified information, trade secrets and intellectual property, the drivers of U.S. military power and global competitiveness in this digital century. If the United States and U.S.-based companies become known as less reliable economic partners due to the corrosive effects of cyber attacks, American influence will wane, putting the nation's security at risk.

Even the most sophisticated organizations – whether technology companies or financial institutions – remain vulnerable to cyber threats. If they were seriously compromised, the harmful effects could spread far and wide. In 2011, two cyber attacks against sophisticated firms could have become what technology advisor Peter Bloom called "five alarm fires" for the cyber security community.[25] The first targeted RSA Security, the largest provider of cyber security authentication devices to the federal government and Fortune 500 companies. The attack used email-based malware to extract vital intellectual property that could compromise system integrity for most, if not all, of the company's customers.[26] The second targeted the Comodo Group, which provides digital certificates that confirm websites' authenticity. The attacker infiltrated an Italian computer company and used its access to Comodo's systems to create fake certificates for popular websites such as Google, Yahoo and Skype.[27] While Comodo and the websites responded quickly, such breaches could undermine confidence in the Internet if not immediately remediated because users would not know whether they were giving their information to a legitimate website or not.

The nation's critical infrastructure, which enables the dynamic U.S. economy to function properly, also remains insufficiently protected. Critical infrastructure providers are still coming to terms with the extent of their vulnerabilities to cyber threats. For example, a large water provider in southern California hired a computer hacker to probe the vulnerabilities of its computer networks – which he and his team did in a single day, seizing control of equipment that adds chemical treatments to Californians' drinking water.[28] According to a 2010 survey by the Enterprise Strategy Group, critical infrastructure providers did not perform security audits of their supply chains consistently or thoroughly enough. Nor did they provide sufficient opportunities for their software developers to receive the latest security training. The survey also found that 71 percent of providers believed that the U.S. federal government should participate more actively in strengthening cyber security for U.S. critical infrastructure.[29]

Respect for Universal Values

Access to the Internet promotes respect for universal values that Americans hold dear, such as freedom of speech and assembly. The Internet provides defenders of those values with new tools to advance their causes. It gives dissidents a voice, oppressed publics a means to organize and otherwise powerless individuals the opportunity for a global platform. While observers dispute the precise impact of the Internet on the 2011 revolutions in the Middle East and North Africa, few question that social networking websites like Twitter and Facebook played a significant role.

Because of the power of the Internet and the efforts of authoritarian regimes to thwart its free use, the Obama and Bush administrations have underscored America's commitment to Internet freedom. They have backed this commitment with dollars, investing increased sums in circumvention technologies that help individuals evade government censors. Building on President Franklin Delano Roosevelt's 1941 "Four Freedoms" speech, Secretary Clinton has articulated a "freedom to connect – the idea that governments should not prevent people from connecting to the Internet, to websites, or to each other."[30] She also has emphasized America's "global commitment to Internet freedom, to protect human rights online as we do offline," including the freedoms of expression, assembly and association.[31] (For a detailed discussion of Internet freedom and cyber security, see the chapter by Richard Fontaine and Will Rogers in Volume II.)

While widespread access to the Internet can play an important role in promoting human rights and advancing more representative political systems, the Internet also can aid dictators and terrorists.[32] Democracy-aspiring dissidents may use social networking and mobile technologies to organize peaceful protests, but oppressive regimes use those same tools to track them. Human rights advocates may use the Internet to inform global audiences and shame governments into upholding universal values, but violent extremists use the Internet to spread vicious ideologies and recruit new members. In sum, the Internet is a vast network that facilitates communication for good and ill alike. The challenge is to maximize the benefits of openness while mitigating the risks.[33]

U.S. Strategic Objectives in Cyberspace

CONNECTIVITY

- Maintain an open and secure Internet – despite the vulnerability inherent in such openness – to facilitate economic growth, innovation, scientific progress, and social and cultural interaction.
- Fight cyber crime and low-level security threats in order to keep them below a threshold where they would imperil widespread faith in the reliability of online transactions with trusted entities and, as a result, general confidence in the security of the Internet.
- Ensure that the Internet is resilient and trustworthy enough to serve America's enduring national interests.

SECURITY

- Deter cyber attacks by preventing nascent attacks, increasing the resilience of systems and networks through proper engineering, establishing layered "defense in depth," maintaining agility and capabilities for full-spectrum operations in cyberspace, and retaliating as appropriate.
- Cultivate strategic stability by establishing U.S. declaratory policy, building global norms regarding acceptable behavior for state and non-state actors, protecting innocent civilians, and suppressing cyber arms races and the inadvertent escalation of cyber conflict.
- Develop checks and balances within the U.S. government and maintain civilian oversight of military and intelligence cyber operations to ensure the proper use of cyber power as a means to advance U.S. national interests.

STRENGTH

- Sustain America's offensive military advantage in cyberspace in order to enhance non-cyber military operations and deter attacks during both peacetime and war.
- Protect against the loss of classified information, trade secrets and intellectual property via cyber crime and espionage, which sap America's competitiveness in the global economy.
- Build America's human and technological capital in order to enhance America's competitive advantage in the productive use of cyberspace.

Beyond these three core American interests of security, economic vitality and promoting universal values, open and secure access to cyberspace facilitates a wealth of interactions that benefit Americans and humanity writ large. It enables better health care, education, philanthropy and good governance. It bolsters innovation, scientific progress and communication among different peoples.[34] These social benefits cannot always be quantified, but they are essential to the advancement of American interests as well as the global good.

Guiding Principles

While the U.S. government and its partners must counter cyber threats, policymakers also must ensure that cyber security policies uphold core American rights and values and do not jeopardize the very gains the Internet has provided. The following principles should guide American efforts to achieve its strategic objectives in cyberspace.

The U.S. government's cyber security strategy should embrace the principle of risk management.

Countering every possible cyber threat is neither possible nor cost effective.

Because of the potentially severe consequences of cyber attacks, policymakers feel pressure to expend greater resources to defend against them. However, the number of potential targets in cyberspace is nearly boundless, and it is impossible to protect them all. Decision makers should recognize that perfect security does not exist in cyberspace, just as it does not exist in the physical world. As a result, U.S. policymakers should adopt a risk management approach that endeavors to reduce aggregate cyber security risk through closely scrutinized investments in areas where the United States is most vulnerable and the consequences of inaction are most grave. Since attacks will persist and networks will be penetrated, U.S. strategy cannot consist solely or even primarily of perimeter defenses. The U.S. government should invest in strengthening resiliency (the ability to continue operations during and after an attack), reducing the time intruders can spend undetected in networks, curtailing the ability of intruders to steal, leak or alter data, and limiting the damage attackers can inflict. It should invest in less vulnerable software, and in utilizing the full capacity of existing processes and technologies, which can address many existing threats.

The United States should lead a broad, multi-stakeholder international cyber security coalition that supplements U.S. freedom of action in cyberspace with global norms that will help protect its interests.

The United States must play a greater leadership role within a range of existing and emerging international coalitions if it wishes to shape the future of cyberspace and how it is governed.[35] Exercising leadership may, in some circumstances, require the United States to curtail some freedom of action internationally in order to shape the behavior of others. It does this already by adhering to existing norms and agreements, such as the Law of Armed Conflict and World Trade Organization. As long as such tradeoffs remain consistent with American interests and values, this cooperative leadership model offers the best way for the United States to strengthen its cyber security.

Since the United States pursues competing interests and values in cyberspace, it must develop policies that balance those interests and values.

An effective cyber security strategy requires American policymakers to balance competing interests and values in a way that defends the nation without subverting what it stands for. The United States should protect its national security interests in cyberspace by combating cyber crime and low-level security threats, countering violent extremism that metastasizes online and maintaining a strong defensive posture against potential adversaries. The United States also should uphold important values in cyberspace that are less directly related to its national security but are fundamental to its political identity, such as freedom of expression, the protection of innocent civilians, privacy and anonymity, freedom of assembly, and open access to information, ideas and opportunities.

Because cyber security is complex, it will require multidimensional solutions.

The complexity of cyberspace means that leaders must pursue cyber security policies through multiple channels. No single policy prescription will provide complete cyber security, just as no single U.S. government agency on its own can protect the nation.[36] Technological or organizational "silver bullets" do not exist and efforts to find them will be impractical at best and counterproductive at worst. The U.S. government should employ multidimensional strategies to strengthen its cyber security, including the use of domestic and international law, international diplomacy and cooperation, declaratory policy, strategic research and development, technological advancement, governmental organization and oversight, information sharing, military preparedness and close collaboration with the private sector.

Cyber Threats: Crime, Espionage, Agitation and War

While cyber threats are relatively new, the purposes for which they are used have deep roots in human history. Cyberspace simply provides a new means to achieve old ends, whether crime, espionage, activities that we collectively call agitation, or war.[37] In practice, these cyber threats are not mutually exclusive and frequently overlap.

CYBER CRIME

Cyber crime uses computer or related systems to steal or compromise confidential information for criminal purposes, most often for financial gain.[38] The aggregate cost of cyber crime can have strategic effects, but the victims are typically individuals or organizations.

Through the use of widespread attacks, cyber criminals are succeeding in their quest to reap undeserved financial benefits from today's prosperous digital economy. Though experts have attempted to estimate the exact damage done by cyber crime, it remains difficult to measure. Companies hesitate to report their actual losses, which they consider proprietary and a threat to public and investor confidence. The broad economic effects of cyber crime, such as the loss of customers and opportunity costs, are also difficult to quantify.[39] Nevertheless, McAfee estimated that the global economy lost at least 1 trillion dollars in intellectual property in 2008 due to cyber crime and deliberate or accidental loss by employees.[40]

While inadvertent losses are a normal part of doing business, economic losses due to cyber crime are likely to increase as cyber criminals grow increasingly sophisticated. For example, cyber criminals are enhancing their intelligence gathering activities by creating fake profiles on social networking sites in order to gather personal information that they can use to target selected users.[41] Such advances can enable more effective heists of companies' most closely guarded intellectual property.

CYBER ESPIONAGE

Cyber espionage uses computer or related systems to collect intelligence or enable certain operations, whether in cyberspace or the real world. Unlike cyber crime, in which incidents typically are financially motivated, cyber espionage is more likely to have strategic effects that threaten broader swaths of society. Motivations for cyber espionage vary, but include attaining military, political, industrial or technological advantages.

Spying is as old as human history, but cyber espionage presents a far less expensive way for both state and non-state actors, including private companies, to construct detailed informational mosaics on competitors and adversaries.[42] Cyber spies can use stolen information for any number of purposes, including intimidation, extortion or efforts to anticipate or disrupt the maneuvering of political opponents. During the 2008 U.S. presidential election campaign, for instance, then-Senator Barack Obama's and Senator John McCain's campaign computer networks were breached by cyber attackers seeking sensitive information about the candidates' plans.[43]

Armed with information stolen through cyber espionage, state or non-state actors could gain unparalleled insight into the plans, operations and vulnerabilities of the armed forces of the United States and its allies. Cyber espionage threatens the cutting edge technology produced in the U.S. defense industrial base. Cyber spies stole data from companies working on the F-35 Joint Strike Fighter aircraft, which relies on millions of lines of software code and is the most expensive weapons program in U.S. history.[44] Deputy Secretary of Defense William Lynn revealed in *Foreign Affairs* that an infected flash drive inserted into a U.S. military laptop in 2008 established a "digital beachhead, from which data could be transferred to servers under foreign control." The code spread undetected and was "poised to deliver operational plans into the hands of an unknown adversary."[45]

Like cyber crime, cyber espionage occurs all over the world. In 2009, for example, Canadian researchers uncovered GhostNet, a network of 1,295 infected host systems targeting foreign affairs ministries, embassies and multilateral organizations located in Iran, India, South Korea, Germany, Pakistan and many more.[46] Interestingly, GhostNet allowed its operators to activate computer cameras and audio devices on the infected Windows-based computers in order to monitor the users – an example of cyber espionage that enabled real world spying.

There is a fine line between espionage and attack in cyberspace.[47] Nations have long accepted that they spy on each other and have developed informal codes of conduct to keep such activities below the threshold of conflict. However, the line between espionage and attacks that could disable an entire power grid – an act of sabotage that would have required a sizable kinetic strike in the past – is now just a matter of keystrokes. Because malicious code can go undetected on networks for long periods of time, years could elapse between intrusion and attack.

U.S. Air Force Senior Airman Julia Richardson, a 10th Intelligence Squadron cyber transport technician, analyzes computer imagery.

(U.S. Air Force illustration by Senior Airman Dana Hill)

CYBER AGITATION

Cyber agitation uses computer or related systems to harass, distract, influence, intimidate or mislead a target or adversary. It is typically motivated by either political or ideological goals and uses means considered illegitimate by law, practice and/or custom.[48] Nihilist and anarchist hacker groups practice cyber agitation; for instance, the loosely connected "Anonymous" organization conducted several high profile cyber attacks in response to the imprisonment of WikiLeaks leader Julian Assange.[49] In contrast to cyber crime and cyber espionage, which seek to steal or alter data, cyber agitation attempts to punish or influence the beliefs and behavior of a targeted actor. Data may be stolen or altered in the process, and large sums of money may be lost due to network shutdowns, but cyber agitation's aim is to harm or persuade.[50]

The severity of cyber agitation can vary greatly. It can consist of little more than digital graffiti sprayed across an adversary's website in order to publicize a grievance to a wider audience. Such incidents pose an inconvenience but are typically less damaging than cyber crime or cyber espionage. More seriously, cyber agitation could sow mass confusion or undermine confidence in the effectiveness of important institutions such as national governments, multilateral organizations or financial institutions.

WikiLeaks' publication of 250,000 confidential U.S. government documents is an example of cyber agitation. While the original security breach was allegedly perpetrated by someone within the U.S. military, WikiLeaks' decision to publish the stolen documents was motivated by a political agenda bent on discrediting countries seen as practicing excessive secrecy.[51] The revelations heightened political tension between the United States and its allies, and damaged the reputations of several American officials.[52] The incident demonstrated the strategic threat posed by cyber agitation to a nation like the United States that must delicately cultivate international relationships in order to advance its wide ranging global political interests.

Cyber agitation offers a powerful but unpredictable way for actors to shape international perceptions to suit their ends and discredit their adversaries.[53] Both state and non-state actors can use these means, but to date cyber agitation has been conducted primarily by so-called "hacktivists," individuals who are loosely connected and hack computer systems and networks for political purposes. (Hackers who are not politically motivated – such as teenagers who hack for fun – engage in cyber crime, not cyber agitation, when they steal or compromise confidential information). Since malware and automated attack tools are widely available on the Internet, hacktivists today do not need to possess advanced computer skills.[54] All they need is the inclination to act.

Cyber terrorism, the use of cyber means to create fear or panic in a society, is a variant of cyber agitation. It may or may not result in physical destruction – the objective is ultimately psychological – but it is always perpetrated to accomplish a political, religious or ideological goal.[55] To date, acts of cyber terrorism have remained largely unsophisticated, consisting of modest efforts like overloading ideological opponents with email messages, conducting distributed denial of service attacks or defacing websites.[56] However, the U.S. government is increasingly concerned about the possibility of more advanced threats since cyberspace offers a natural safe haven for terrorists. The FBI has investigated individuals affiliated with or sympathetic to al Qaeda who have expressed interest in conducting cyber attacks against U.S. critical infrastructure and acquiring more sophisticated cyber capabilities from outside sources.[57] The United States should anticipate that terrorist groups can and will find ways to employ cyber means in the future.

CYBER WAR

Cyber war consists of military operations conducted within cyberspace to deny an adversary, whether a state or non-state actor, the effective use of information systems and weapons, or systems controlled by information technology, in order to achieve a political end. Cyber war can occur in a "regular" manner between the official military forces of states or in an "irregular" manner among the official and unofficial forces of state and non-state actors engaged in a struggle for legitimacy and influence.[58] It can constitute the entirety of a conflict, or occur as part of a wider war that includes ground, maritime, air or other military forces.[59] The former transpires only in cyberspace, even if it produces real-world effects, while the latter takes place in cyberspace and the physical world simultaneously.[60]

Cyber war is far easier to define in theory than in practice – particularly because a known cyber war has not yet occurred. Cyber attacks can have kinetic effects, but they have not yet caused the type of destruction or bloodshed traditionally associated with warfare in the physical world. The bits of information comprising cyber attacks do not kill people directly, even though they may destroy or reprogram digital systems in ways that result in the loss of life. Cyber attacks may inflict significant damage but still fall below the threshold of cyber war, often because the attacked entity is unable or unwilling to admit or respond to the attack. (War involves dynamic interaction between at least two entities. A cyber attack launched against an entity with no willingness or capability to defend itself or retaliate is undoubtedly a significant event, but it is not war).[61]

The line between an act of cyber war and an act that falls short of that designation will remain blurry. It will depend on whether the attacked entity considers itself a victim of an act of war, and the conclusions drawn by third parties. While legal experts increasingly believe that states should define cyber war more narrowly to encompass only acts that result in a significant level of damage, uncertainty and subjectivity will continue to exist, much as they do in other forms of conflict.[62]

IV. THE NATURE OF CYBER THREATS

The ability to leverage cyberspace is one of the 21st century's most important sources of power. State and non-state actors can use this power to achieve financial, military, political, ideological or social objectives in cyberspace or the physical world. These objectives can be positive and contribute to the greater good, or they can be nefarious and harm innocent people. Like most technologies, cyberspace is agnostic to politics and ideology.

Cyber power is attractive to powerful and less powerful actors alike because of its low relative cost, high potential impact and general lack of transparency. Powerful actors such as the United States can combine cyber power with existing military capabilities, economic assets and soft power networks. Less powerful actors – states, organizations, individuals or any combination thereof – can gain asymmetrically in cyberspace by inflicting extensive damage on vulnerable targets. For a relatively small investment, they can cripple networks and steal valuable personal and proprietary information. Americans already spend billions of dollars trying to defend themselves, but even investments this large are insufficient.

The virtual terrain of cyberspace strongly favors offense because cyber attacks are inexpensive and conducting them rarely brings consequences. Cyber attacks against the United States are nearly constant, with approximately 1.8 billion cyber attacks targeting the computer systems of Congress and executive branch agencies each month.[63] While the vast majority of these attacks fail, some incursions by both state and non-state actors have succeeded – mostly on unclassified networks, but on classified networks as well.[64] "This threat is increasing in scope and scale, and its impact is difficult to overstate," concluded Director of National Intelligence James Clapper during recent congressional testimony.[65] Steven Chabinsky, Deputy Assistant Director of the FBI's Cyber Division, told us, "The threat is increasing at a scale far greater than our resources to respond can handle."[66]

Underlying Causes of Cyber Insecurity

Three conditions distinguish cyberspace from other domains of activity and fundamentally shape the nature of cyber threats: the architecture of the Internet, exponential innovation and the Internet's widespread integration into America's military, economy and society.

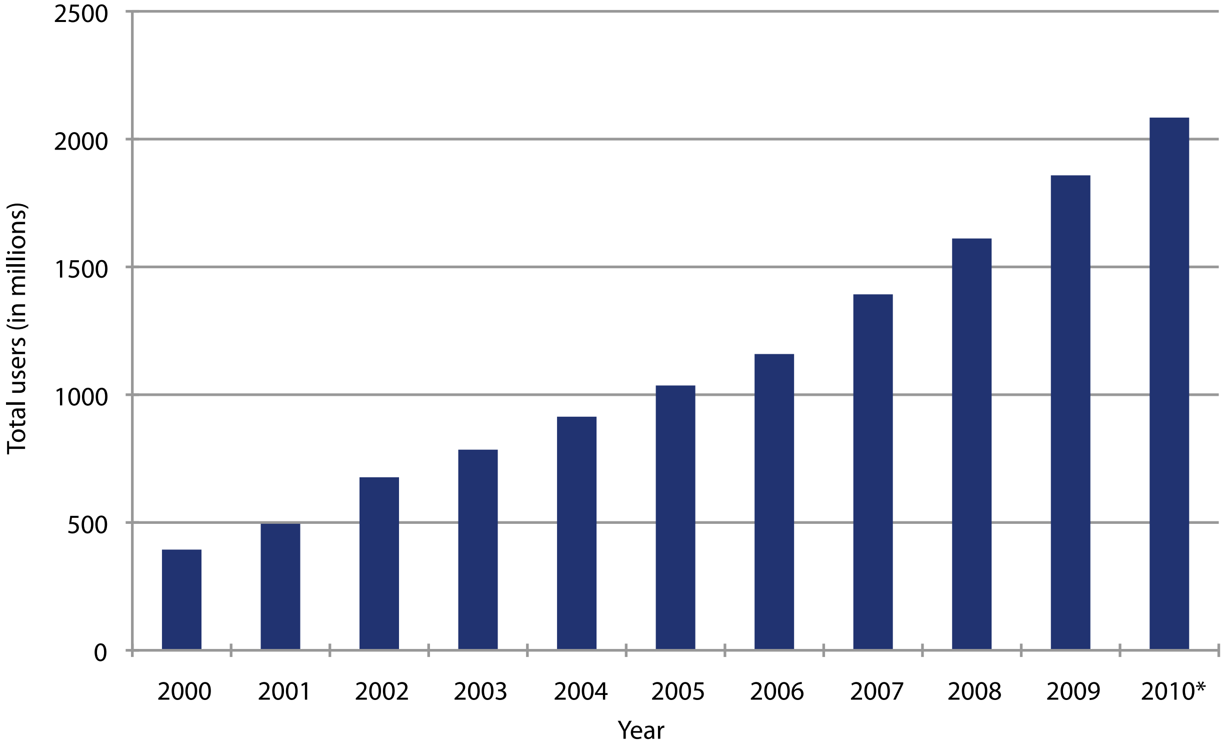
ARCHITECTURE OF THE INTERNET

The Internet was built with ingenious flexibility and reach, which have facilitated an endless stream of innovations. Its architecture enables nearly instant movement of information globally at an extremely low cost. A small group of designers engineered the Internet to connect multiple networks, computational facilities and trusted institutions seamlessly and reliably – a goal they largely accomplished.[67]

Yet it was hard to foresee the vulnerabilities that would emerge as the Internet blossomed from a Pentagon-sponsored research project into a global communications network that pervades modern life. The Internet's very openness carries downsides; namely, it makes it easier to attack applications and operating systems that are not adequately defended.[68]

The architecture of the Internet presents a number of fundamental security challenges. The Internet was designed as a decentralized system and its users are functionally anonymous. They generate information that travels in undifferentiated packets that can be encrypted to disguise the origin.[69] Taken together, the anonymity provided by the Internet's architecture leads to an attribution challenge (in the security context) that makes some significant cyber attacks untraceable. Establishing, let alone authenticating, identity is challenging if it is possible at all.[70]

CHART 1: WORLDWIDE INTERNET USERS



* Data for 2010 are estimates.

Source: International Telecommunication Union

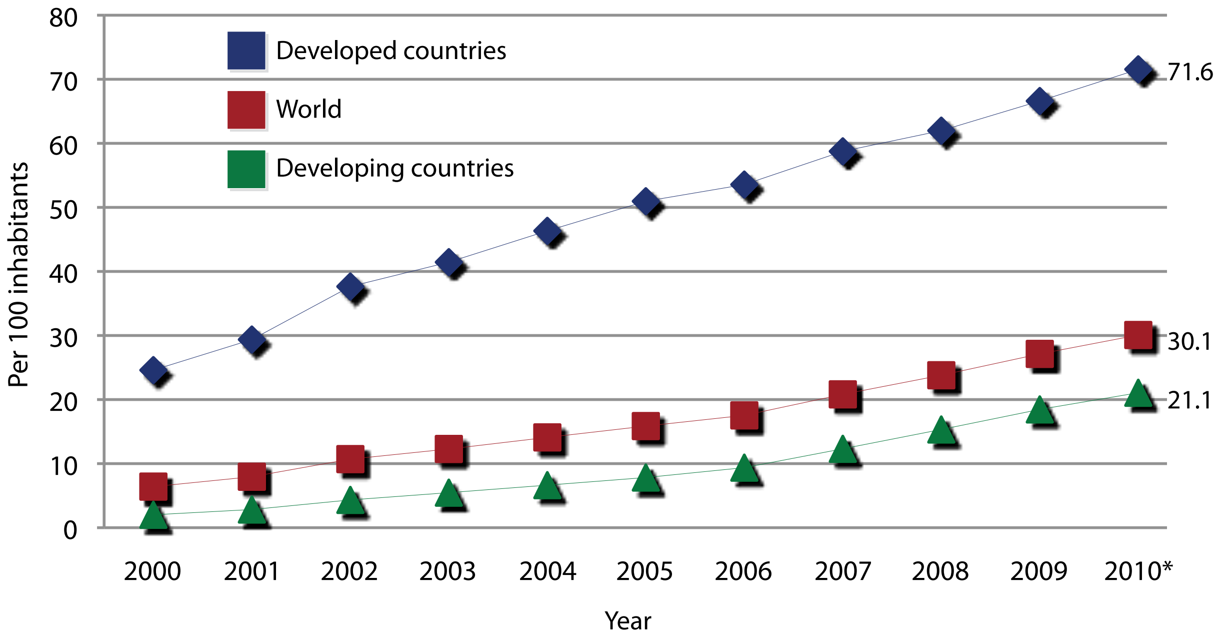
The attribution challenge empowers both strong and weak actors who benefit from having their identities disguised. Online anonymity can hide political activists from dictators, but it also makes identifying – and punishing – cyber attackers extremely difficult. Interlinked individuals operating from globally dispersed locales can, with no warning and only milliseconds between decision and impact, attack scores of digital targets simultaneously without revealing their identities. Those who try to locate attackers often find themselves chasing ghosts when the attacks originate from computers and servers in multiple countries.

EXPONENTIAL INNOVATION

In 1965, Intel co-founder Gordon Moore proposed what has become known as Moore's Law. It states that the number of transistors on a computer chip will double roughly every two years, resulting in constantly increasing computing power at decreasing cost. The prediction has proven remarkably accurate.[71] In fact, the silicon transistors on today's computer chips are 1,000 times thinner than a human hair and cost about as much as a single alphabetic letter printed in a newspaper.[72] This exponential innovation has allowed cyberspace, and its uses, to evolve faster than many ever imagined.[73]

Innovation has expanded the availability, use and functionality of the Internet at a remarkable rate. Today, there are approximately two billion global Internet users, a vast increase from the 361 million users online in 2000.[74] The spread of mobile devices, which surpassed five billion subscriptions worldwide in 2010, will give an even greater number of people in the developing world access to the

CHART 2: INTERNET USERS PER 100 INHABITANTS



* Data for 2010 are estimates.

Source: International Telecommunication Union

Internet, especially as mobile devices continue to offer better functionality.[75] Ever-increasing processor speeds and improved algorithms continue to facilitate greater reliance on the Internet, which adds trillions of dollars to the global economy each year.[76] Global e-commerce activity totaled 10 trillion dollars in 2010, and is expected to reach 24 trillion dollars by 2020.[77] Internet startup companies add enormous entrepreneurial vibrancy to the global economy, offering customers better products while challenging more traditional businesses to keep up or get out of the way.

While continued innovation offers growing opportunities for productive use of the Internet, it also aids those individuals with malicious intent by offering more targets and tools for attack. Cyber security is time consuming and expensive, and the pressure companies feel to unveil innovative products quickly – and thus capture greater market share – leads to the introduction of technologies that are less secure than they would be if more time was spent bolstering their security.[78]

McAfee identified more than 20 million new pieces of malware in 2010, or an average of nearly 55,000 per day. Each one represents a new weapon for cyber attackers.[79] McAfee also reported "increases in targeted attacks, increases in sophistication and increases in the number of attacks on the new classes of devices" in 2010.[80] Identity theft reportedly affected 600,000 to 700,000 Americans in 2000. In 2009, however, 11.1 million Americans were victims of identity theft, with much of the increase attributed to online fraud.[81]

WIDESPREAD INTEGRATION

The Internet's architecture has facilitated its integration into almost every aspect of modern life. This integration has yielded incredible advances in productivity and efficiency. However, it also has created vulnerabilities that exceed understanding of the potential consequences.

The integrated nature of cyberspace increases the chances that any disruption will ripple far beyond the original incident. As the 2009 U.S. National Infrastructure Protection Plan concluded, "Network disruptions resulting from cyber attacks can lead to loss of money, time, products, reputation, sensitive information or even potential loss of life through cascading effects on critical systems and infrastructure."[82] The diverse and distributed ownership of cyber infrastructure presents enormous security challenges because it is impossible to homogenize policies or best practices.[83] Today's global supply chains mean that vulnerabilities exist not only within U.S. borders.

Critical infrastructure such as financial, electrical and telecommunications networks are increasingly vulnerable to cyber attacks. The private sector controls 85 to 90 percent of U.S. critical infrastructure, and these providers use cyberspace to communicate and control sensitive processes, such as balancing levels of chlorination in water, opening and closing valves, controlling the flow of oil, executing financial transactions and regulating temperatures.[84] If disrupted by a cyber attack, even for only a short period of time, the effects could destroy property and potentially kill innocent civilians.[85]

Critical infrastructure systems are more vulnerable today than in the past because standardized technologies create systemic vulnerabilities and technical information is publicized widely.[86] According to a 2011 survey, over 80 percent of critical infrastructure providers reported being the victim of large-scale cyber attacks or infiltrations.[87] While some attacks on critical infrastructure are minor, the work of hackers seeking an adrenaline rush or bragging rights, others are more serious. In 2009, *The Wall Street Journal* reported that cyber spies based in China and Russia had infiltrated, mapped and deposited software tools in the U.S. electrical grid that could steal and damage data or even control facilities' operations remotely.[88]

Critical Infrastructure and Key Sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

Source: Department of Homeland Security

The integrated nature of cyberspace blurs the line between military and civilian operations, complicating both offense and defense. "Surgical" cyber attacks, in which little intended collateral damage is wrought on civilians or infrastructure, are difficult to model and execute because cyberspace is so tightly integrated.[89] While the most advanced actors, including the United States, can execute precise strikes, the possibility of unintended consequences is great, particularly as more everyday devices and appliances gain Internet connectivity and thus become vulnerable.[90] Even the sophisticated Stuxnet worm, which ostensibly targeted specific industrial control systems in Iran, infected 100,000 systems in 155 countries because of its aggressive propagation techniques. Symantec concluded that "These additional infections are likely to be 'collateral damage' – unintentional side-effects of the promiscuous initial propagation methodology utilized by Stuxnet."[91]

The risk of collateral damage should weigh heavily on responsible decision makers contemplating the use of cyber attacks. They must consider how important a target is to their objectives, if using a cyber attack could lead other actors to retaliate, and whether any other option might accomplish their goals more effectively. The United States decided early in the Iraq War that it would not launch a cyber attack against Iraq's financial system because senior U.S. officials thought the risk of unintended consequences was too great.[92] Of course, America's conventional military superiority meant that a cyber attack was not required to invade Iraq successfully. Lacking similar options, less powerful actors may see cyber attacks as an attractive course of action. Indeed, terrorist organizations have demonstrated an interest in cyber capabilities, and the FBI has investigated individuals affiliated with or sympathetic to al Qaeda who have discussed conducting cyber attacks against U.S. critical infrastructure.[93]

Implications for Cyber Security

These three underlying causes of cyber insecurity carry implications that American leaders must grapple with in order to craft effective policies. The most significant of these implications are analyzed next.

SPEED AND THE COLLAPSE OF DISTANCE

When combined with the attribution challenge, cyberspace's speed and collapse of distance present a formidable security challenge to the United States. Geographic distance imposes significant time and maneuverability constraints on military operations on land, in the air, at sea and in outer space. In these domains, temporal and physical distance often enables a target to prepare and/or preempt when it sees an attack coming. Detectable actions, such as mobilizing an army, testing a new weapons system or even declaring one's intentions publicly, often precede an attack. Targets therefore have time to prepare countermeasures that will mitigate or prevent damage.

> *The United States is under constant assault in cyberspace, and as these attacks grow in magnitude and intensity, the risk of a catastrophic incident with cascading social effects increases.*

In cyberspace, foreknowledge is limited because information moves from origin to destination almost instantaneously.[94] As a result, cyber attacks are not constrained by geographic location or distance (though the manmade infrastructure supporting cyberspace is so constrained). Targets will remain constantly vulnerable to attacks that they may not detect or have time to prepare for. However, speed works both ways in cyberspace. Because targets can shift or flee extremely quickly, attackers must constantly reorient and update their plans.

MAGNITUDE AND INTENSITY

The reach and importance of the Internet mean that small actions can have enormous effects. The United States is under constant assault in cyberspace, and as these attacks grow in magnitude and intensity, the risk of a catastrophic incident with cascading social effects increases.

Three examples hint at the potential magnitude of future cyber attacks. In 2000, a disgruntled employee at a water-treatment plant in Australia sabotaged a computerized control system, releasing more than 200,000 gallons of sewage into parks, rivers and a nearby hotel.[95] An international cyber crime network used malware known as Zeus to capture online banking data from medium-sized companies, towns and churches. Before the FBI and other law enforcement agencies thwarted the operation in 2010, the network managed to steal 70 million dollars.[96] Finally, in Wall Street's May 2010 "flash crash," complex automated trades created enough market volatility to hemorrhage approximately 1 trillion dollars in only minutes, with some stocks dropping more than 90 percent in value.[97] While the volatility was unintentional and the stocks recovered, the crash illustrates the potential consequences of sophisticated cyber attacks against a financial system that relies increasingly on automated high-frequency trading.[98]

The magnitude and intensity of cyber attacks make them ideal instruments of coercion. Since a cyber attack on critical infrastructure could inflict tremendous damage, merely threatening to attack can compel the behavior of others.

Because cyber attacks can cause severe disruption without harming people physically, groups that would most likely never undertake protests, crime or violence in the real world may still use cyber attacks. A recent example of this phenomenon is the response by Anonymous, the loosely connected hacking collective, to PFC Bradley Manning's imprisonment on charges of providing classified information to WikiLeaks. Anonymous launched distributed denial of service attacks against major companies, and according to news reports it aspired to "harass staff at [Marine Corps Base] Quantico Brig to the point of frustration" and planned a "complete communications shutdown" of the base's Internet pages and phone links.[99] Anonymous allegedly also stole and then distributed thousands of internal emails from a U.S. security firm, HBGary Federal, after the firm claimed to have infiltrated the group and identified key members.[100] It is hard to envision members of Anonymous pursuing such criminal activities if they did not have easy access to cyberspace.

LOW BARRIERS TO ENTRY

Cyberspace's barriers to entry are extraordinarily low, even though many resources were expended to develop it and are still needed to maintain its physical infrastructure. To launch a cyber attack today, all a person needs is a computer, which costs less than 400 dollars in the United States, an Internet connection and limited technical knowhow. As a result, cyberspace enables greater malicious potential at lower cost than other domains, although the most sophisticated cyber attacks will still be quite expensive and the most advanced kinetic attacks will still inflict greater damage than cyber attacks.[101]

Like any sophisticated attack, cyber attacks require capability, skill and will. However, these traits increasingly need not be found together. With downloadable malware and automated tools widely available on the Internet, cyber attackers today do not need to spend the time or money previously required to acquire attack capabilities.[106] As cyber security expert Gary McGraw notes, "The most impressive tool in the attackers' arsenal is Google," because it is relatively easy to find these capabilities online.[107] Attackers can develop the necessary knowledge and skill without calling much attention to themselves (unlike nuclear weapons scientists, for example, who attend college for years and then often work in government-funded organizations).

The growing professionalization of cyber crime demonstrates how cyberspace's low barriers to entry can intensify security threats. Cyber criminals increasingly are disassociating themselves from any specific cause. Instead, they make their services available to the highest bidder on the black market.[108] Non-specialists can download cyber attack capabilities online for free, or spend anywhere from 500 dollars to 250,000 dollars (or more) for an advanced capability.[109] Cyber attack scripts are now sold online in a customizable format; customers select their desired capabilities from a checklist and computer programmers write the code accordingly. With such customization available for a relatively modest fee, cyber attack capabilities are now available for an unlimited number of malicious causes.

It is becoming more difficult to disaggregate the interrelationships among cyber criminals, states, terrorists, traditional organized crime syndicates, drug traffickers and others.[110] As a result of these so-called "unholy alliances," the odds are increasing that the most malicious actors will collaborate with those who possess the most advanced capabilities.[111] Such collaboration ostensibly transpired between Russia and loosely affiliated hackers during the cyber attacks against Estonia in 2007 and Georgia in 2008. This type of arrangement allows states to reap the benefits of cyber attacks without having to risk the political consequences of undertaking such action directly.[112]

Goliath in Cyberspace

Though cyberspace's low barriers to entry favor attackers and the less powerful, more powerful actors still retain significant advantages. As strategist Thomas Mahnken argues in his chapter in Volume II, cyber capabilities alone do not compensate for weakness in other instruments of power such as conventional military strength, economic leverage, political influence and sophisticated intelligence collection. More powerful actors will continue to possess these qualities and use them to achieve their objectives internationally, often at the expense of the less powerful. While cyber attacks can inflict significant damage, their effects still pale in comparison to the destruction wrought by nuclear weapons, precision-guided munitions, battle tanks, armed drones and the other tools of modern warfare possessed by the most powerful states.

While experts debate whether non-state actors can acquire cyber attack technologies comparable to those possessed by states, many of the things that make a cyber attack successful are not technical in nature. For example, though the Stuxnet code itself was technically advanced, the attack's true sophistication came from its relatively precise targeting of a specific configuration of devices found only in a handful of locations worldwide. Significant resources were probably expended beforehand to test the code against a trial set of identical centrifuges.[102] In other words, it was the intelligence and tests enabling Stuxnet, not just the worm itself, that made the attack effective.[103] In general, states will continue to have greater access than non-state actors to the resources needed for intelligence gathering and related enabling activities.

If targeted by cyber attacks, states have no reason to limit their response options only to cyberspace. Though cyberspace is a unique domain with vastly increased scale and uncertainty, it also depends on physical infrastructure, whether computers or network servers, that is vulnerable to kinetic attacks by conventional weapons typically possessed only by states. Furthermore, cyber attacks do not occur naturally like earthquakes or bad weather, as Google's Eric Davis told us.[104] Though the specifics may be difficult to determine, somebody, somewhere usually must push a button for a cyber attack to occur. As strategist Colin Gray wrote, "Human beings, unlike cyberspace, are not placeless – they act within geography."[105] These human beings are vulnerable to kinetic weapons, law enforcement and other security instruments that are the comparative advantage of states.

LACK OF TRANSPARENCY

Though the Internet disseminates information faster, more broadly and less expensively than ever before, discrete activities in cyberspace are difficult to detect. There is less chance of being caught or punished for malicious acts in cyberspace, which lowers the cost of committing them. As a result, actors will consider them less risky and thus more attractive than alternative non-cyber options. Momentum will build for more sophisticated attacks as actors push the boundaries in order to maximize their gains.

Cyberspace's lack of transparency hinders strategies that could mitigate conflict escalation. Arms control in cyberspace is challenging because verification – the bedrock of strategic stability – is exceedingly difficult due to the attribution challenge.[113] In contrast, consider nuclear missiles: they are physically large and their effects fairly predictable, giving actors enough confidence to negotiate arms control agreements based on observable verification. Cyber weapons, on the other hand, are difficult to detect and can produce unintended effects. As a result, perceptions of insecurity are likely to remain acute in cyberspace, and verification-based strategies will inspire little confidence.

Lack of transparency in cyberspace also complicates oversight of government activities. The time available for careful decision-making is far shorter in cyberspace due to the dramatic increase in the breadth, source and speed of threatening activities. This volatile reality challenges fundamental principles of U.S. national security by creating pressure to decentralize decision-making and provide pre-delegated authority to more junior military commanders. Were this to happen, senior civilian leaders might exercise less control over cyber operations, which could potentially erode civilian control of the military, a central tenet of American government.

Cyberspace's lack of transparency impedes policymakers' ability to muster the political support needed to defend against cyber threats. Cyber attacks need not be spectacular to have serious consequences. "One of my greatest concerns is the attacks that we don't note and we don't notice," said Debora Plunkett, a senior NSA official. "The most sophisticated adversaries are going to go unnoticed on our networks," she added.[114] Because the effects of cyber attacks are hard to detect and quantify, it is difficult to generate the political will required for effective solutions – especially since such solutions require high-level attention and resources.[115] As former Secretary of Homeland Security Michael Chertoff told us, "I hope we don't need a catastrophe to mobilize the United States."[116] Short of a catastrophe, however, efforts to mobilize action will be an uphill fight because governments historically have required forcing functions to undertake sweeping reform.

UNCLEAR NORMS OF BEHAVIOR

Acceptable norms of behavior are often unclear in cyberspace. This lack of agreed-upon norms means that actors cannot reliably anticipate the likely consequences of their actions. With unclear expectations about acceptable behavior and likely consequences, cyberspace cloaks malicious actors in enough ambiguity to enable their use of crime, espionage, agitation and warfare.

One of the most challenging aspects of cyber security is that attackers can cause significant damage without crossing a threshold into the type of physical violence associated with armed conflict. Laws and customs have developed in the ground, maritime and air domains regarding what is, and is not, an aggressive act. But cyber attackers can operate below the threshold of conflict without necessarily eliciting a strong response. One example is Stuxnet, which ostensibly damaged an Iranian nuclear centrifuge cascade without using the type of kinetic force that likely would have provoked a harsher response from Iran.

Long-established norms of behavior and widely shared expectations dictate that committing or threatening physical violence against a powerful country like the United States will elicit a response that may include armed force. Self-defense is widely enshrined as a legitimate justification for preemption or retaliation with military force. To date, however, the point at which a cyber attack would trigger a kinetic response remains unclear. This uncertainty heightens the appeal of cyber attacks as an asymmetric tool to use against the more powerful.

The fact that cyberspace appears to be a virtual world without "real" effects has clear implications for norms of behavior. Protecting innocent civilians, respecting neutrality during wartime and responding proportionally to attack are not accepted consistently in cyberspace, even though states have respected such norms for decades in the ground, maritime and air domains.[117] Moreover, because cyberspace empowers individual users, not just states, norms of behavior for individuals have broad implications for cyber security. If people in general see cyber attacks as more acceptable, attacks will become more widespread and sophisticated. This would endanger a nation like the United States that depends heavily on cyberspace for its security and prosperity.

OFFENSIVE DOMINANCE

Offense dominates in cyberspace, which is far more conducive to attackers than defenders. In numerous war games and exercises, U.S. officials have found that cyber offense has the upper hand.[118] Actors' persistent vulnerability to attack hinders the emergence of stability, predictability and trust, and creates incentives for preventive and preemptive action, whether in cyberspace or the physical world.

The relative cost of offense is extremely low in cyberspace. Untraceable attackers spending hundreds, thousands or millions of dollars possess a clear advantage over defenders spending billions of dollars on cyber defenses that do not offer reliable protection. One specialist, for example, calculated that a high-end "cyber army" capable of overcoming U.S. government defenses could be developed in two years for 100 million dollars, a fraction of the amount that the United States spends on cyber security each year.[119]

In addition to a favorable cost ratio, attackers also possess advantages in the required levels of effort and complexity. According to the Defense Advanced Research Project Agency (DARPA), the number of lines of code included in security software increased from several thousand 20 years ago to nearly 10 million today. Over the same period, the number of lines of code included in malware remained constant at approximately 125.[120] In other words, cyber defenses have grown exponentially in effort and complexity, but they continue to be defeated by offenses that require far less investment by the attacker.

Offensive dominance creates a great risk of cyber arms races. State and non-state actors are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fueling an action-reaction dynamic of iterative arming. Experts believe that at least 20 nations are engaged in a cyber arms competition and possess the type of advanced capabilities needed to wage cyber war against the United States.[121] As Michael Nacht, Former Assistant Secretary of Defense for Global Strategic Affairs, told us, "An arms race is already going on in cyberspace and it is very intense."[122]

Conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities. Actors are more likely to misperceive or miscalculate actions in cyberspace, where there is no widely understood strategic language

U.S. Cyber Power in Context

The current leaders in cyber offense are the United States, the United Kingdom, France, Israel, Russia and China.[125] However, many other states are working to develop their capabilities. "Most of the modern nations have capabilities that, I think, many could argue are near to [the United States] and, in some cases, may beat our capabilities," said GEN Keith Alexander, head of U.S. Cyber Command, in 2010.[126]

Recent moves by Russia, China and the United States illustrate how cyber offenses and defenses may evolve in the years ahead.

Russia's cyber offense serves as a force multiplier for its military. Russian strategy calls for cyber attacks against information, communications and other parts of an adversary's critical infrastructure before military operations commence in the real world. Indeed, this is how events in Georgia unfolded during the 2008 conflict, albeit with hacktivists, not official Russian government personnel, launching the attacks. Russian strategy delineates sophisticated attack sequencing that includes denying an adversary any access to external information, disrupting credit and monetary circulation, and waging a widespread disinformation and propaganda campaign against the target population.[127]

China is increasingly developing and fielding advanced capabilities in cyberspace. It is focused not only on collecting sensitive information, but also on developing the capabilities of the People's Liberation Army (PLA) to cause economic harm, damaging critical infrastructure and influencing the outcome of conventional armed conflicts.[128] According to the Pentagon, the PLA is also preparing to wage cyber attacks "against civilian and military networks – especially against communications and logistics nodes."[129] In a future conflict with another major power, for instance against the United States during a dispute over Taiwan, Chinese defense strategists would likely see cyber attacks as an attractive option.[130]

These capabilities are cause for concern, but U.S. policymakers also should understand the broader context.

The most sophisticated actors, including the United States, are constantly preparing for conflict in cyberspace and probing one another's weaknesses. An American official once asked a Chinese military leader why his country launched so many cyber attacks and intrusions against U.S. networks. He replied: "Do you know how much we are attacked in cyberspace by the United States every day?"[131]

The U.S. military and intelligence community have invested heavily in highly classified offensive cyber tools designed to deter and disable potential threats.[132] Right now, experts consider these capabilities more advanced than those possessed by potential adversaries. "Whatever the Chinese can do to us, we can do better," a former National Security Agency watch officer observed. "Our offensive cyber capabilities are far more advanced," he added.[133] The 2006 U.S. National Military Strategy for Cyberspace Operations offered a similar assessment, but warned:

> Although the United States currently enjoys technological advantages in cyberspace, these advantages are eroding. The United States will not continue to enjoy an advantage in how this technology is developed and employed. The United States increasingly depends on technology designed and manufactured by entities that reside outside the United States who may become adversaries. Unlike the other warfighting domains, the United States risks parity with adversaries.[134]

Though this conclusion was reached in 2006, the judgment is still widely shared today. Despite offensive advantages, the United States has immense vulnerabilities. As a senior U.S. military official told us, "We're already very good at offense, but we're just as bad at defense."[135]

for signaling intent, capability and resolve.[123] Uncertainty will encourage states to prepare for worst-case contingencies, a condition that could fuel escalation. Furthermore, "false flag" attacks, in which an actor purposefully makes an attack look like it came from a third party, could also ignite a conflict.[124]

The Future of Cyber Threats

Since cyber threats are evolving rapidly, cyber security policies based only on present conditions will leave the United States vulnerable to future attacks. This section identifies several trends that could shape future cyber threats.

CLOUD COMPUTING

Cloud computing, information technology systems that are physically removed from the computers and other devices that access them, presents enormous risks and opportunities for cyber security.[136] Indeed, it is the most important emerging trend affecting cyber security. On the one hand, concentrated data in large server farms presents an enticing target for malicious actors who have demonstrated the ability to penetrate the most sophisticated defenses. On the other hand, placing data in the hands of highly trusted and sophisticated actors would eliminate the use of many devices with weak security. As a more centralized arrangement, cloud computing could offer stricter access and quicker responses to cyber security breaches.[137] Cloud computing may also allow smaller businesses with limited resources to better protect their information against sophisticated attacks.

AUTOMATION AND ARTIFICIAL INTELLIGENCE

Automation and artificial intelligence will accelerate the complexity of cyber threats. On the one hand, automation can enhance cyber security dramatically by increasing the speed, reliability and accuracy of defensive systems. On the other hand, it will become harder to control the initiation, conduct and termination of cyber operations as human beings become increasingly divorced from direct operational involvement. Artificial intelligence will further exacerbate these trends. If drones, for instance, could fly using closed-loop artificial intelligence, cyber attackers would have fewer chances to intercept communications. More negatively, artificial intelligence could erode traditional notions of military command and control.

MOBILE DEVICES

The spread of mobile devices will further complicate cyber security. Mobile devices provide more targets for cyber attackers to exploit. However, the devices also belong to specific individuals – a fact that may make identification, attribution and security more practical than with personal computers. Advanced mobile devices offer new opportunities for cyber attack, exploit and defense that could aid the U.S. military. But they also create new vulnerabilities. For instance, Symantec identified 163 vulnerabilities in mobile device operating systems in 2010, a 42 percent increase over the previous year.[138] Mobile devices with sensory capabilities that detect the external environment provide cyber attackers with more detailed information about a target's location and behavior, thus enabling more sophisticated attacks.

ARCHITECTURE OF THE INTERNET

The evolving architecture of the Internet may transform the range and type of cyber threats. Two potential architectural changes could redefine cyber security: 1. Reengineering the Internet to structure the cyber landscape more uniformly, including with greater identification, security, privacy and/or anonymity where desired, and 2. Layering new networks onto the Internet to provide greater security for data exchanges that do not require anonymity and privacy (such as financial transactions or military communications). These changes will inevitably introduce new challenges, and policymakers must consider the unanticipated and perhaps negative consequences.

HIGH SPEED BROADBAND, WIRELESS INTERNET ACCESS AND FIBER OPTIC CABLES

The continued spread of high speed broadband, wireless Internet access and fiber optic cables will permit new Internet users to access cyberspace faster than law enforcement or governance structures can keep up. These new stakeholders entering cyberspace will challenge social, political and economic norms of behavior. The range of potential targets for cyber attackers will grow, and conflicts will erupt as actors jostle to ensure their security. U.S. leadership is not guaranteed in this environment, particularly as cyber expertise continues to diffuse globally and America's share of global spending on information technology shrinks, thereby reducing its ability to influence international market trends.[139]

INSIDER THREATS

Insider threats will persist no matter how sophisticated or effective cyber security becomes. As long as humans are able to access information, no level of biometric authentication or encryption will prevent them from accessing – or being coerced or bribed to access – important data. Nonetheless, sophisticated monitoring systems can help by flagging unusual behavior and triggering intervention by a human overseer.

V. CURRENT U.S. GOVERNMENT EFFORTS TO PROMOTE CYBER SECURITY

Building on the work of the Bush and Clinton administrations, the Obama administration has stressed the severity of cyber threats and worked diligently to strengthen America's cyber security. Its notable achievements include conducting a 60-day Cyberspace Policy Review, creating U.S. Cyber Command, elevating the role of DHS, increasing funding for key programs, and unveiling the National Strategy for Trusted Identities in Cyberspace and an international cyberspace strategy. The administration also appointed a White House cybersecurity coordinator who has regular access to the president and works closely with the economic and national security teams.

Despite this progress, the U.S. government must do much more to outpace the growing threats in cyberspace. As President Obama said about cyber security in 2009, "We're not as prepared as we should be, as a government or as a country."[140]

Cyber security is far too complex to be managed by a single agency or organization. It has too many dimensions and there are too many stakeholders. This section analyzes the strengths and weaknesses of several key U.S. government entities.

White House

The White House has devoted considerable attention to cyber security. In April 2011, the White House released the National Strategy for Trusted Identities in Cyberspace (NSTIC), which the administration refers to as an online "Identity Ecosystem."[141] The National Strategy for Trusted Identities in Cyberspace calls for authoritative entities, preferably from the private sector, to create a system for authenticating secure digital identities. If Internet users choose to participate in the system, they will no longer need to use – or most likely reuse, given common Internet browsing habits – log-in information for the various transactions now regularly completed online.[142] In May 2011, the White House published its international cyberspace strategy, which provides a single unifying framework for numerous cyber security issues. Foreign governments are extremely interested in the development of the strategy, and it is expected to influence cyber security policies all over the world.[143]

Despite these achievements, the White House still faces problems providing sufficient leadership and coordination. Cyber security is a multidimensional problem, the workload is immense and the White House's staff is small relative to the enormity of the task. The White House has not yet fully addressed many issues identified in the 60-day Cyberspace Policy Review, such as articulating well-defined roles within federal government agencies, bolstering information sharing and establishing a strong public-private architecture to facilitate responses to cyber attacks.[144] Numerous observers have concluded that the U.S. government has not unified its disparate cyber security programs under a comprehensive strategy.[145]

Our interviews with private sector and congressional representatives revealed ongoing concern that the White House's leadership is not yet strong or timely enough. Based on our research, this judgment largely reflects structural challenges and the difficulty of the task, not any particular failings on the part of White House staff.

Department of Defense

The Department of Defense has elevated cyberspace to be the fifth domain of warfare, along with land, sea, air and outer space. It established a sub-unified command known as U.S. Cyber Command, which is subordinate to U.S. Strategic Command, to protect U.S. military networks (sometimes referred to as "dot mil"). Cyber Command centralizes the military's cyber security efforts, which until recently were an amalgamation of task forces. There also is ample space for collaboration between Cyber Command and non-military components of the government. For example, Deputy Secretary of Defense William Lynn said that in the case of a cyber attack, "The military's cyber capabilities will be available to civilian leaders to help protect the networks that support government operations and critical infrastructure."[146]

To address the vulnerabilities created by the Pentagon's glacial acquisition procedures, DOD is seeking to accelerate its procurement process for information technology.

During congressional testimony in March 2011, GEN Keith Alexander raised concerns about Cyber Command's lack of authority to respond to a cyber attack on critical infrastructure. Though DHS is designated as the primary coordinator for response, Cyber Command and the NSA possess technical capabilities that are vastly superior.[147] The U.S. government is working to address this mismatch between authority and capability. For instance, a September 2010 DHS-DOD memorandum of understanding codified plans "to enhance operational coordination and joint program planning" for cyber security.[148]

All the military services are realigning their cyber operations, which will be integrated into Cyber Command. The 24th Air Force, created in August 2009, is the war fighting organization that establishes, operates, maintains and defends Air Force networks and conducts full-spectrum operations in cyberspace.[149] In 2010, the Air Force published its foundational doctrine for activities in cyberspace.[150] In January of the same year, the Navy created U.S. Fleet Cyber Command and recommissioned the 10th Fleet to provide operational control of Navy cyber forces and to execute full-spectrum cyber operations.[151] That same month, the Marine Corps established Marine Forces Cyber Command to coordinate its own cyber efforts.[152] In 2011, Marine Forces Cyber Command plans to release a capabilities-based assessment that will recommend doctrine, training, personnel and materiel required for its cyber operations.[153] Finally, the Army activated Army Cyber Command/2nd Army in October 2010 to unify its cyberspace activities. The Army also published Cyberspace Operations Concept Capability Plan 2016-2028, which outlines how the Army should leverage and integrate cyberspace into its operations.[154]

In order to prepare for current and future conflicts, the U.S. military is further integrating cyber scenarios into its doctrine and training exercises. National Security Agency "red teams" now work with military commanders to inject cyber threats into exercises in order to test plans and responses.[155] In spring 2010, U.S. Pacific Command's annual exercise included a cyber component for the very first time.[156] A Cyberspace Joint Operating Concept is slated for publication this year. Despite this progress, however, senior officials told us that the U.S. government must do more to ensure that cyber offense and defense are fully integrated into military plans.

To address the vulnerabilities created by the Pentagon's glacial acquisition procedures, DOD is seeking to accelerate its procurement process for information technology. In February 2011, Deputy Secretary of Defense Lynn stated that it takes DOD 81 months to field a new computer system. By contrast, Apple's iPhone was developed in only 24 months.[157] In March 2011, Principal Deputy Under Secretary of Defense for Policy James Miller told Congress that DOD's acquisition process must operate on 12- to 36-month cycles to reflect information technology's rapid rate of innovation.[158]

The Department of Defense's acquisition of technology can influence certain segments of the cyber security market, especially for large enterprise companies that work frequently with the U.S. federal government. However, this influence is not as great as is often assumed. The Department of Defense accounts for only slightly more than 0.1 percent of all information technology expenditures worldwide, and DOD's average information technology contract action shrank from 2.5 million dollars in 2000 to only 204,000 dollars in 2007 due to the decentralization of buying activities.[159]

National Security Agency

As part of DOD and the U.S. government's intelligence community, the NSA collects and disseminates signals intelligence and supports military and intelligence operations. By nearly all accounts, its cyber security capabilities are formidable. As a result, some have suggested that the agency should lead cyber security efforts across the U.S. government. However, others have argued that its highly secretive nature would result in less transparency, less trust and less corporate and public participation, which collectively would undermine cyber security.[160] The Obama administration has pursued a middle course by keeping DHS as the lead agency for protecting the U.S. government's civilian networks while still seeking to utilize the NSA's advanced capabilities. This approach was codified in the recent memorandum of understanding between DHS and DOD.

The NSA operates under the U.S. Code's Title 50, which governs intelligence activities, and in a combat support role under Title 10, which governs military activities. It is intricately entwined (and currently shares a dual-hatted leader) with Cyber Command, which operates under Title 10.[161] While this arrangement increases efficiency by preventing

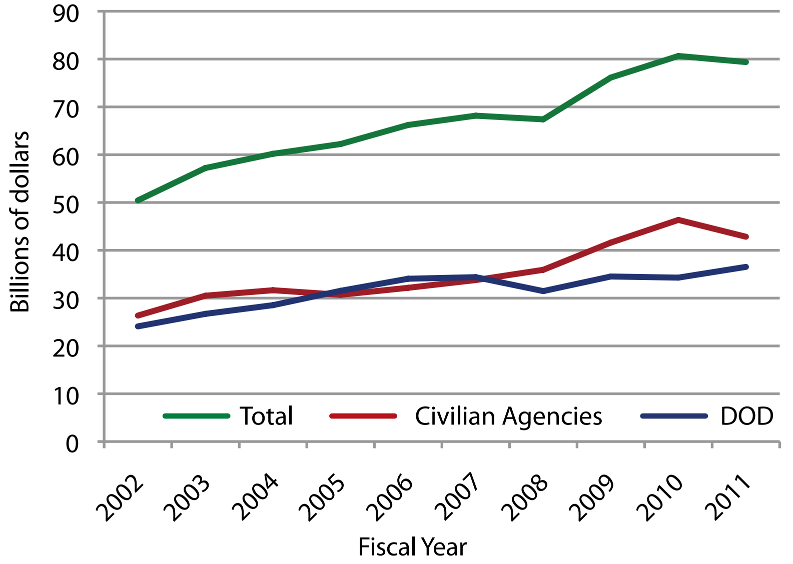
Tracking Federal Spending on Cyber Security

Despite the ballooning U.S. federal debt and increasing calls for fiscal austerity, information technology and cyber security will remain a growth industry in Washington for years to come. The U.S. government has spent almost 650 billion dollars on information technology since fiscal year (FY) 2002 – nearly one and a half times more than it has spent on the war in Afghanistan – and a growing portion of that spending is devoted to cyber security.[168]

In FY 2010, the most recent year for which data is available, major executive branch agencies reported 12 billion dollars in combined spending on cyber security.[169] This figure includes direct costs such as personnel, tools, testing and training, but excludes indirect costs that are difficult to measure such as system recoveries, architecture redesigns and security upgrades. On average, executive branch agencies devoted 15.6 percent of their total information technology budgets to cyber security. Personnel costs were by far the biggest cyber security expenditure and represented, on average, 74.4 percent of non-defense agencies' cyber security budgets.[170] Private contractors remain an integral part of the workforce, representing 32 percent of the Department of Defense's (DOD) cyber security personnel and 54 percent of non-defense agencies' cyber security personnel.

The Obama administration's FY 2012 budget request continues the trend of greater spending on cyber security. The request provides 548 million dollars for government-wide cyber security research, development and education – a 35 percent increase from the amount spent in FY 2010.[171] The president's budget also would provide additional cyber security resources to the Department of Homeland Security (DHS) and DOD (see text box, next page). For FY 2012, DOD's cyber security budget request is more than three times larger than DHS's request.

CHART 3: U.S. GOVERNMENT SPENDING ON INFORMATION TECHNOLOGY SINCE 2002



The FY 2012 request devotes 936 million dollars, a 30 percent increase over the amount enacted in FY 2010, to DHS's Infrastructure Protection and Information Security program, which administers many of the department's cyber security initiatives. This increase would drastically boost funding for U.S.-Computer Emergency Readiness Team, which would receive 391 million dollars in FY 2012 – more than double what it received in FY 2010.[172]

The administration requested 3.2 billion dollars for DOD's cyber security initiatives in FY 2012, a roughly 2 percent increase over FY 2011 spending levels.[173] The request funds continued efforts to strengthen Cyber Command and adds 500 million dollars for new cyber technology research focusing on cloud computing, virtualization and encrypted processing.[174]

In a sign of the ambiguity surrounding cyber security budgets, the Pentagon at first proposed spending only 2.3 billion dollars on cyber security when it released its FY 2012 budget in February 2011. But it later revised the figure upward to reflect the growing number of programs being re-categorized as cyber security-related.[175] Additionally, DOD has offered no public details about classified spending on cyber security within its so-called "black" budget, which totals at least 56 billion dollars in the FY 2012 request.[176]

duplication between the two organizations, it poses difficult challenges for effective oversight. In one example noted by the Senate Armed Services Committee, the close links between a military command (Cyber Command) and a large acquisition organization (NSA) may reduce the U.S. government's ability to oversee acquisitions appropriately. "It is necessary to ensure that self-perceived requirements do not emerge in U.S. Cyber Command and migrate under the radar screen of defense acquisition management processes directly to NSA for solutions," the committee warned.[162]

Department of Homeland Security

The Department of Homeland Security leads the effort to secure civilian U.S. government agencies' unclassified networks, commonly referred to as "dot gov." The 2010 Quadrennial Homeland Security Review codified cyber security as one of DHS's five core mission areas.[163] The Department of Homeland Security provides technical expertise to the private sector and critical infrastructure providers, raises awareness among the general public and coordinates national responses to major incidents.[164] It administers a national cyberspace response organization, the U.S.-Computer Emergency Readiness Team (US-CERT), to provide response support. Finally, DHS works with the private sector, international partners and state and local governments to share information and implement cyber security risk management programs.

While the success of the U.S. government's cyber security efforts depends on DHS, there are concerns about whether it can execute its responsibilities successfully. The Department of Homeland Security continues to suffer organizational challenges, including a sprawling bureaucracy and problems attracting and retaining experienced governmental personnel. In fact, one expert estimated that the U.S. government currently employs only three to ten percent of the cyber security professionals it actually needs.[165] The Department

Department of Homeland Security's Cyber Security Budget Request for Fiscal Year 2012 (in millions)

Identification and Analysis	84
Coordination and Information Sharing	48
Mitigation Programs	190
U.S.-Computer Emergency Readiness Team	391
Strategic Initiatives	65
Outreach & Programs	7
Priority Telecommunications Service	57
Programs to Enhance Telecommunications	13
Critical Infrastructure Protection Programs	11
Next Generation Networks	25
Office of Emergency Communications	43
Total	**936**

Notes: Figures are for Department of Homeland Security's (DHS) Infrastructure Protection and Information Security (IPIS) program. IPIS does not administer all DHS programs that devote resources to cyber security, but it nonetheless serves as a representative (if imperfect) measurement for department-wide efforts.

Source: Department of Homeland Security

Department of Defense's Cyber Security Budget Request for Fiscal Year 2012 (in millions)

Army	432
Navy	347
Air Force	440
Defense Agencies	1,600
Other (includes Cyber Command)	443
Total	**3,262**

Notes: Totals may not add due to rounding. Defense agencies include Defense Information Systems Agency, National Security Agency, Defense Advanced Research Projects Agency, Missile Defense Agency, Defense Logistics Agency, Defense Finance and Accounting Services and the Office of the Secretary of Defense.

Source: NextGov, "Cyber Spending at Defense" (29 March 2011).

of Homeland Security's mandate and priorities are constantly subject to intramural feuding and fractured congressional oversight, with more than 80 congressional committees and subcommittees claiming some jurisdiction over its operations.[166] Many DHS leaders believe that their authorities are inexact and require clarification, particularly on the issue of protecting critical infrastructure.[167]

Our research uncovered growing, if still guarded, confidence in DHS's cyber security capabilities … it has attracted talented personnel, cultivated relationships with the private sector, prioritized cyber security in its strategic planning and improved its ability to harness the strengths of other federal agencies.

Despite such concerns, our research uncovered growing, if still guarded, confidence in DHS's cyber security capabilities. High-level leaders in DOD, the State Department, Congress and the private sector agreed that while DHS still needs to increase its capacity, it has attracted talented personnel, cultivated relationships with the private sector, prioritized cyber security in its strategic planning and improved its ability to harness the strengths of other federal agencies. However, the same leaders noted that DHS still needed to do more in all these areas. They recommended strengthening DHS's existing capacities instead of adding organizational layers or undertaking more costly internal reorganizations.

Congress

From the corridors of federal agencies to the conference rooms of private companies, a struggle is underway to influence the U.S. government's cyber security efforts, which are well funded despite the climate of growing fiscal austerity. Yet the statutory, policy and oversight guidelines that help moderate such struggles are especially ill defined for cyber security. To address these challenges, Congress is currently working to pass comprehensive cyber security legislation.

Several major cyber security bills were introduced in the 111th Congress, but none were enacted. House and Senate leaders have prioritized passing a major bill during the 112th Congress, and several key members of Congress and their aides are working behind the scenes to negotiate key provisions.[177] Those involved expect to face a formidable challenge in educating members about the many complex issues. Ambiguity about who "owns" cyber security on the Hill – seven committees in the Senate alone claim jurisdiction – complicate matters further. Finally, political maneuvering between the Democratic-controlled Senate and Republican-controlled House will affect any legislation. Since passing a major cyber security bill will offer both parties an attractive talking point as the 2012 elections draw near, legislators are sure to jostle over who will get credit.

VI. POLICY RECOMMENDATIONS

The United States must capitalize on the opportunities and diminish the vulnerabilities presented by its growing reliance on cyberspace. This will require the U.S. government to exercise strong leadership, engage the private sector more effectively and develop new strategies, policies and capabilities. The U.S. government must lead internationally and domestically since solutions require focused cooperation among all relevant stakeholders. Based on our assessment of interests and threats, we recommend that the U.S. government implement the following policies.

Adopt a Comprehensive Strategy for a Safe and Secure Cyberspace

The U.S. government should adopt a strategy that promotes the safety and security of cyberspace and endeavors to stop malicious activity from imperiling general confidence in the security of the Internet.[179] The U.S. government should promote safety in cyberspace because, although individuals and organizations have an interest in maintaining security on their own computers and networks, their failure to do so carries risks for all other users.

To promote a safe and secure cyberspace, the U.S. government should adopt a "cyber hygiene" mindset akin to addressing public health challenges.[180] (For more on this approach, see the chapter in Volume II by Gregory Rattray and Jason Healey.) Though analogous paradigms should be used with caution, the public health model is useful for approaching cyber security because it implies a persistent level of "infection" that policymakers cannot cure and so must manage. It also links individual actions to the broader health of the Internet; emphasizes reporting, measurement, public education and prevention; demands cooperation among diverse actors; and places responsibility on individuals, private organizations and governments.

Timeline for Implementing Policy Recommendations

By December 2011

- The White House should create a President's Cyber Security Advisory Board.
- The Department of Homeland Security (DHS), Department of Defense and the intelligence community should create a Cyber Security Coordination Council.
- Congress should create a bicameral, bipartisan Cyber Security Task Force.
- Congress should pass comprehensive cyber security legislation.

By June 2012

- The White House should create an Office of Cyber Security Policy within the Executive Office of the President.
- The White House should direct agencies dealing with cyber security to review their classification guides.
- DHS should develop new disaster response plans for a major cyber attack.
- The U.S. government should outline its cyber security declaratory policy.
- The State Department should initiate a coordinated cyber security foreign assistance program for developing countries.

By June 2013

- The White House Office of Science and Technology Policy should lead a national commission on the future of the Internet.

Note: Many of our recommendations will require sustained effort over many years, and thus are not included in this timeline.

Cyber Security Guidance for Individuals and Organizations

By Jacqueline Koo
Joseph S. Nye, Jr. Intern

While this report focuses on the U.S. government's role in strengthening cyber security, individuals also have an important role to play. Cyber attackers have numerous points of entry into business and home networks, so it is crucial to take preventative measures.

To start, it is important to **create strong, unique passwords and make sure they are protected and changed often**. Strong passwords should contain more than ten characters of varying types and should be different for each account. Answers to "secret" or "challenge" questions should not be publicly searchable.

Based on recommendations from the National Security Agency, the guidelines below will help individuals protect themselves against cyber threats.[178] (For further explanation of these guidelines and additional information, visit the U.S.-Computer Emergency Readiness Team's tips website at www.us-cert.gov/cas/tips and the National Cyber Security Alliance at www.StaySafeOnline.org).

HOW TO PROTECT COMPUTERS

Switch to and maintain an up-to-date operating system to ensure that computers are equipped with the latest security enhancements. Windows users should have Windows 7 or Vista, and Mac users should configure the Mac OS X to notify them automatically about system updates.

Keep application software up to date, since attackers usually target applications that do not have automatic update features. This can be done using software that quickly surveys all the applications installed and identifies which ones need updates. Users should install a comprehensive suite of security software on their computers to provide added layers of protection.

Refrain from using the "administrator" account, since doing so can help attackers gain persistent access to a host computer. Instead, use a "user" account and only use the "administrator" account when downloading and updating software.

HOW TO PROTECT NETWORKS

Configure home networks to maximize control by setting up a separate routing device as the access point between the Internet service provider and a home network.

Set up a Wi-Fi Protected Access 2 (WPA2) network instead of Wired Equivalent Privacy (WEP), the WPA2's predecessor, to protect networks. WEP uses encryption that is much easier to infiltrate. If it is broken into, it will reveal to the attacker all the web traffic that has passed through the network.

HOW TO BE SAFE ONLINE

When using mobile devices such as cellular phones, laptops and tablets, avoid using public Wi-Fi hotspots whenever possible. Instead, use the mobile Wi-Fi, 3G or 4G connection on mobile devices, or a Virtual Private Network (VPN), which will encrypt information and provide added protection between the mobile device and the VPN gateway. If the Wi-Fi hotspot is the only option available, limit activities strictly to Internet browsing that does not include sharing personal or sensitive information.

When uploading and posting personal information online, be aware of the hosting sites' privacy settings. This is especially applicable to social networking sites. Users should periodically read the security policies of any sites they visit in order to stay abreast of any changes or new features that may enhance (or undermine) their security.

Treat unsolicited emails with attachments or links cautiously, and delete before opening whenever possible. In particular, do not answer emails disguised as commonly used web applications that ask for personal information. Also, in order to avoid targeted attacks, use different usernames for personal and work email accounts and be cautious about using out-of-office responses since doing so will verify to attackers that an email address is real.

At a time when security and privacy advocates often seem at odds, promoting a safe and secure cyberspace also suggests a productive common agenda. Improving cyber security helps to protect the personal information of individuals and also prevents its misuse. Privacy and cyber security are, in this way, complementary. (For further discussion, see James Lewis' chapter in Volume II.)

To implement a comprehensive strategy, the U.S. government should take the following actions.

- **The Department of Homeland Security, in close collaboration with DOD, the intelligence community, the private sector and other key stakeholders**, should strengthen its role as the U.S. government's lead provider and coordinator of cyber security risk assessment activities, which include monitoring, analysis, warning and response.[181] Strengthening DHS's risk assessment authorities and performance will promote a healthier cyber environment by raising shared awareness within the U.S. government, the private sector and the American public, thereby helping to generate the political will required for effective solutions. In particular, a more sophisticated understanding of risk will help the private sector develop business cases for investing in cyber security. It also will help the American public understand that improper cyber security behavior by individuals can, in the aggregate, have serious consequences for U.S. national security.
- **The Department of Homeland Security, in close collaboration with interagency partners, state and local governments, international allies, non-governmental organizations and the private sector**, should build on the recent National Cyber Incident Response Plan to develop new disaster response plans for a major cyber attack that disables government operations and critical infrastructure. The plans should include greater use of realistic exercises – such as the groundbreaking annual "Cyber Storm" exercises – that feature dynamic scenarios and involve cabinet-level U.S. government officials and the actors listed previously. The U.S. government has made progress in this area, but it takes time and money to coordinate complex plans. High-level officials report that many government agencies remain averse to investing their limited resources in incident response exercises. As a senior U.S. government official told us, "Some people think we should just show up for exercises, not waste time or resources preparing for them beforehand."[182] Regular high-level participation by government officials and industry leaders should lessen this institutional resistance by demonstrating that exercises are a top priority.
- **Congress** should bolster a comprehensive strategy by passing legislation that will:
  - » Create a new quasi-governmental operating or "fusion" center through which U.S. government agencies and private companies – in particular Internet service providers – can share, in real time, information about cyber threats. This organization will allow Internet service providers and government agencies to share information legally and quickly so they can take immediate action to respond to threats. It also will strengthen the U.S. government's ability to protect companies' proprietary information while placing a greater burden on the U.S. government to share actionable threat information in a timely manner. Privacy organizations should be part of the organization, with the responsibility to monitor cyber security activities and ensure that civil and privacy rights are protected.
  - » Clarify DHS's legal authority to monitor U.S. government networks for malicious activity, with adequate protections for privacy, in order to make it easier for DHS to conduct risk assessments and identify, prevent and/or mitigate threats to government networks in real time.

- » Enhance protections for Internet service providers to cooperate with the U.S. government on cyber security issues without risking violations of the Electronic Communications Privacy Act, antitrust investigations or lawsuits.
- » Update the Federal Information Security Management Act of 2002 to assign DHS the responsibility to develop, oversee and enforce cyber security policies throughout the U.S. government.[183]
- » Authorize increased funding for DHS’s cyber security professional development programs, the National Science Foundation’s Scholarship for Service program, DOD’s Information Assurance Scholarship Program and related initiatives.[184] Cyber security education is essential to developing qualified professionals, and these existing programs will help the U.S. government attract the next generation of talent.

Forge an International Agenda for Cyber Security

Since threats in cyberspace are a transnational problem, the United States should forge an international agenda for cyber security. The U.S. government should lead by example and build on America’s broader political, economic and military relationships with its partners around the world.[185]

To do this, the **State Department, in close collaboration with the White House, DOD, intelligence community, DHS and other key agencies**, should empower its new Office of the Coordinator for Cyber Issues to create a new Global Cyber Security Initiative. The **president** and **secretary of state** should provide high-level public support for the initiative, which should pursue the following activities.

- Conduct an “audit” to identify which international organizations and non-state actors, including from the private sector, possess the requisite expertise and jurisdiction to address specific cyber security issues – particularly the ability to develop, disseminate and enforce international norms and standards – and then reinvigorate U.S. government engagement with those organizations and actors. International standard-setting bodies should be a special area of emphasis. This approach will allow the U.S. government to layer cyber security onto existing agreements and institutions instead of investing in new ones.[186]
- In the near-term, pursue improved information sharing, crisis response and joint exercises (enabled by memorandums of understanding) with treaty partners, and undertake bilateral cyber security talks and, potentially, confidence building agreements – such as a cyberspace version of the Incidents at Sea agreement used to increase U.S.-Soviet stability during the Cold War – with non-treaty partners. The U.S. government should deepen its cyber security cooperation with the “Five Eyes” nations (United States, United Kingdom, Canada, Australia and New Zealand) that already share intelligence, and with NATO, Israel, Japan, South Korea, India, the European Union and others.
- Over the long-term, seek multilateral agreements to strengthen law enforcement related to cyber security and clarify international norms of behavior.[187] The most realistic agreements will likely come in the form of codes of conduct endorsed by multilateral coalitions.
- Support efforts by non-governmental organizations to cultivate international accountability for cyber crime and cyber espionage by using objective metrics to “name and shame” the worst offenders and their countries of origin. Since publishing such information would discourage foreign direct investment and trade, states would feel greater pressure to take responsibility for the illicit activity occurring on their networks.[188]

- Continue to address the issue of cyber security directly and, if necessary, more publicly with China and Russia, which are the source of many sophisticated attacks on U.S. companies, government agencies and NGOs. Chinese and Russian officials have largely refused to talk about curtailing cyber attacks, but American officials should continue to apply pressure and link cyber security to broader issues such as economic and military cooperation whenever possible. In return, the U.S. government should continue to use law enforcement to curb cyber attacks by American hackers against Chinese and Russian targets, and encourage greater collaboration on issues like cyber crime.
- Initiate a coordinated foreign assistance program to help developing countries build legal and technical expertise on cyber security. Just as the Nunn-Lugar Cooperative Threat Reduction program promotes the security of the United States by helping countries to rid themselves of vulnerable nuclear materials, this program would protect America by spreading basic cyber security practices and values more broadly.[189] The assistance program should connect legal and technical experts with leaders in host nations, and provide opportunities for follow-on training.
- Galvanize American companies to participate in international standard-setting organizations involving cyber security, such as the Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C). These organizations are increasingly dominated by foreign companies that could shape cyber security standards in ways detrimental to U.S. interests unless American companies play a more active role with support from the U.S. government.

America's international agenda should include forming widely accepted cyber security norms for state and non-state actors, including private sector companies. **The State Department, in close collaboration with the White House, DOD, DHS and other key agencies**, should focus on developing cyber security norms that uphold: 1. Protecting innocent civilians and minimizing collateral damage; 2. Internet freedom, defined as the inalienable right, consistent with the Universal Declaration of Human Rights, to receive and impart information without interference; and 3. Proportionality and restraint in response to cyber attack. (These three norms are explained further in the next section).

To develop these norms successfully, the **State Department** should adhere to the following principles. (For further discussion, see Martha Finnemore's chapter in Volume II.)

- Graft norms onto existing, well-established normative frameworks – including those related to human rights, law enforcement, trade, armed conflict and conduct in non-cyber domains (e.g. maritime) – in order to increase the chances of success.[190]
- Simultaneously cultivate norms in multiple venues – including through existing multistakeholder organizations and ad hoc coalitions of like-minded actors – in order to yield more timely progress than would occur by pursuing individual initiatives successively.
- Resist foreign governments' attempts to define cyber security in ways that would unduly restrict freedom of expression online, or set new standards that contradict or compete with internationally recognized standards.
- Pursue a comprehensive Internet freedom agenda that provides technological support for democracy and human rights activists, uses diplomacy to protest the imprisonment of dissidents and online authors, integrates Internet freedom into U.S. policies toward specific countries and regions, and reforms export controls.[191]
- Reinforce norms with applicable laws at the national, local and even international levels whenever possible.

- Provide technical assistance and funding to help key actors comply with emerging norms such as cleaning up networks and enforcing legal penalties for cyber crime.[192]

Establish U.S. Declaratory Policy on Cyber Security

The White House, State Department, DOD and DHS should outline the broad contours of a U.S. cyber security declaratory policy, which would establish the role of cyberspace in U.S. foreign and defense policies. While the declaratory policy should necessarily leave some strategic ambiguity about how the United States would respond to cyber attacks, it should communicate more clearly America's views of expected behavior by state and non-state actors, what acts are considered intolerable, allies' responsibility to respond to attacks, and areas where increased collaboration and understanding are required.[193] The U.S. government should craft its policies in consultation with international partners, federal agencies and the private sector. Specifically, the U.S. government should reaffirm and declare that:

- The Universal Declaration of Human Rights articulates, for all nations and all peoples, inalienable human rights to free expression, association and assembly. These freedoms apply to all human activities, including those in cyberspace.
- The United States will consider a cyber attack of sufficient magnitude to be an "armed attack" – thus justifying the right to legitimate self-defense, whether through cyber or non-cyber means, under Article 51 of the U.N. Charter.[194]
- The United States affirms, both to its allies and to those that would threaten them, that it shall respond to a cyber attack against an ally as it would to a non-cyber armed attack, and that existing collective defense provisions outlined in treaties encompass cyber attacks.
- The United States will respond to a cyber attack at a time and manner of its choosing and draw on a full range of instruments of national power. In choosing whether and how to respond to a cyber attack, the United States will not confine itself to cyber means.
- The United States, when deciding how to respond to a cyber attack, will adhere to the Law of Armed Conflict and seek to protect civilians, minimize collateral damage and exercise proportionality and restraint.
- The United States considers the peacetime placement of logic bombs (pieces of computer code designed to execute a malicious function when specified conditions are reached) or other mechanisms to disrupt critical infrastructure to be an unfriendly and potentially hostile act.[195]
- The United States adheres and expects other nations to adhere to the principles articulated in the Budapest Cybercrime Convention; namely, that the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right is a criminal offense and that nations should provide mutual assistance "to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[196]
- The United States believes that existing norms, laws and treaties governing the protection of property rights, including those that protect intellectual property, extend to cyberspace.

Raise Costs for Cyber Attackers

The *sine qua non* for strengthening U.S. cyber security is to change the incentive structure for both attackers and defenders so that it is more expensive to attack and less expensive to defend. In other words, the United States must increase the consequences – using financial, political, legal, technological and military tools – for cyber attackers while defending more effectively.

The Department of Defense, Congress and the White House should prioritize maintaining America's offensive military advantage in cyberspace.

To raise costs for cyber attackers, we recommend the following:

- **The Department of Defense, the intelligence community, the Department of Justice, Congress and the White House** should clarify legal authorities related to military and intelligence operations in cyberspace. GEN Alexander told Congress in March 2011 that the U.S. military does not yet possess the legal authorities it needs to respond to a cyber attack against the United States or its allies.[197] LtGen Robert Schmidle, Jr., deputy commander of Cyber Command, elaborated that "There is a real dearth of doctrine and policy in the world of cyberspace," pointing to the lack of coordination and guidance from civilian leadership.[198] This lack of clarity is understandable as cyber operations evolve faster than legal and political processes, but it could cause confusion and disorganization during a major cyber attack. By delineating the authorities granted to the military, the U.S. government will reduce uncertainty and thereby increase its ability to use the capabilities it has more effectively and without undue hesitation. This outcome will raise the retaliatory costs suffered by potential adversaries if they attack the United States and the attacks can be attributed to them, which will help deter them in the first place.
- **The White House, DHS, DOD, Department of Commerce, Cyber Command and the private sector** should improve cyber defenses, including through the aforementioned fusion center and greater use of more secure software. (For more information, see the chapter by Gary McGraw and Nathaniel Fick in Volume II.) The U.S. government also should prioritize the use of existing technologies and policies, which are often sufficient to address a large majority of cyber security threats. When making investments, DOD in particular should seek to maintain technological diversity in its networks and systems to prevent a single point of failure (even though doing so will create usability and interoperability challenges).[199]
- **The Department of Defense, the intelligence community, Congress and the White House** should prioritize maintaining America's offensive military advantage in cyberspace. While offensive capability will never lead to flawless security due to the attribution challenge, the prospect of U.S. retaliation using offensive cyber capabilities will induce caution in aspiring attackers and raise costs for potential adversaries. While the future protection of U.S. interests and projection of U.S. power requires such an investment, maintaining America's offensive advantage should be accompanied by strengthened oversight and the development of prearranged mechanisms – such as a cyberspace version of the Incidents at Sea agreement – to offer multilayered options to defuse escalatory tensions during a crisis.[200] Additionally, the U.S. government should develop ways to talk about its offensive capabilities without compromising sources and methods or being inordinately constrained by over-classification. Broadly communicating U.S. cyber offensive capabilities will inform adversaries that America possesses credible retaliatory options, which will help deter attacks.
- **The Department of Defense, the State Department, the Department of Justice, the Treasury Department and the intelligence community** should implement an integrated cross-domain prevention strategy to bring cyber

attackers to justice. Under this strategy, the U.S. government should use not only sophisticated defenses and the threat of retaliation to raise costs for attackers, but also rely on non-military tools such as intelligence, sanctions, law enforcement, travel bans and more.[201] U.S. government agencies must coordinate the integration of these options, which does not occur regularly today (although DOD has studied the issue with outside experts).[202] Though imperfect attribution in cyberspace will continue to hinder security strategies, the United States should seek recourse using diplomatic, economic and traditional military methods, not just cyber security tools.

- **The Department of Defense** should ensure that the U.S. military can operate in a command and control environment degraded by cyber attacks. As its 2010 Joint Operating Environment report concluded, "More sophisticated opponents of U.S. military forces will certainly attack American vulnerabilities. For instance, it is entirely possible that attacks on computers, space, and communications systems will severely degrade command and control of U.S. forces. Thus, those forces must possess the ability to operate effectively in degraded conditions."[203] To achieve this, the U.S. military should audit critical military systems and processes that depend on cyberspace to determine which ones require bolstered redundancy; further incorporate redundancy into its force plans; and require military personnel to learn and use non-cyber tactics, techniques and procedures. In a degraded command and control environment, U.S. troops may need to use techniques such as Morse code and celestial navigation to complete their missions, and may need to execute complicated logistics operations without access to the Pentagon's unclassified network. DOD should require all military personnel to receive regular instruction in non-cyber techniques, and conduct training exercises without the benefit of cyber tools, in order to ensure that the U.S. military can fight through cyber attacks – thereby raising costs for cyber attackers by increasing the odds that U.S. forces will be able to retaliate.
- **The Department of Defense** should tap into the high-tech skills contained in the National Guard and Reserves to help meet its growing demand for specialists who know how to raise costs for cyber attackers. Reserve component service members' civilian backgrounds and careers provide them with expertise, particularly in specialized and high-tech fields, that is generally difficult to locate, train and retain in the U.S. military's active component. For example, a Guardsman or Reservist who works in civilian life as a Google software engineer could fill a critical cyber security billet. A recent RAND Corporation assessment of the Air Force judged that Guardsmen and Reservists employed in high-tech fields such as information technology "can be tapped to provide the most current knowledge, tools, and techniques for network warfare operations."[204] Using Guardsmen and Reservists in this way "could offset additional staffing requirements that may be needed in the active component for these operations," RAND concluded in a separate report.[205] As Principal Deputy Under Secretary of Defense for Policy James Miller recently told Congress, "The type of people that we're looking for with the skills for cyber will span a wider range than the standard profile for military service."[206]

Prepare for the Future of the Internet

The White House Office of Science and Technology Policy (OSTP) should lead a national commission on the future of the Internet. The commission should involve the science and technology community, private companies and U.S. government representatives. It should grapple with the feasibility of issues such as changing the underlying architecture of the Internet to make it more secure (see Robert Kahn's chapter in Volume II), and forming separate networks with higher levels of security. The Office of Science and

Technology Policy's commission should result in recommendations to the president and ultimately feed into a new White House strategy. The National Academy of Sciences should participate by providing an objective assessment of the various future options, along with analysis of their costs and benefits.

The aforementioned National Strategy for Trusted Identities in Cyberspace (NSTIC) is an important initiative on the future of the Internet. To keep NSTIC moving forward, the U.S. government – and in particular the **Department of Commerce,** which has assumed a leading role in its advancement – should resolve the following issues.

- The National Strategy for Trusted Identities in Cyberspace should clarify private sector liability in the event that a digital identity fails so that companies fully understand their risk exposure and can develop sound business cases.[207]
- Because the Internet is transnational, NSTIC cannot succeed if it serves only American users. Thus, the U.S. government should engage with America's international partners to explain the purposes and benefits of the Identity Ecosystem. Many American privacy advocates and companies have supported the initiative, but foreign audiences may misunderstand NSTIC as a U.S. attempt to control the Internet if American leaders do not build international support for it.[208]
- The National Strategy for Trusted Identities in Cyberspace should undertake a public education campaign to raise awareness about the need for an Identity Ecosystem and explain how it will protect user privacy.[209] Otherwise, the odds of widespread public support and use will remain low.[210]
- The National Strategy for Trusted Identities in Cyberspace should develop regulations for the creation, management and use of digital identifiers in order to prevent fraud and abuse. Regulation of the Identity Ecosystem would mirror regulation of other generally trusted entities in American society, such as banks.
- The National Strategy for Trusted Identities in Cyberspace should consider options for creating different digital identity tiers – perhaps "High" and "Standard" – so that stringent security requirements well suited for high-value transactions do not create friction that inhibits low-value transactions.[211]

Build the Institutional Capacity Necessary to Coordinate U.S. Government Responsibilities for Cyberspace

Cyberspace is now too important to America's security and prosperity to be managed by an ad hoc collection of offices sprinkled across the U.S. government. While Americans may question any new government initiative during a time of fiscal austerity, a modest investment today will save money in the long run by preventing costly mistakes and reducing unnecessary redundancy.

To oversee and coordinate U.S. government efforts on cyber security, the **White House and Congress** should create an Office of Cyber Security Policy within the Executive Office of the President. It should resemble the Office of Science and Technology Policy, and be headed by a Senate-confirmed chief cyber security advisor to the president and director of cyber security policy. The office should remain small and nimble, maintain close links to both the NSC and National Economic Council, and avoid duplicating functions already performed by other agencies. It should serve as the hub of the U.S. government's cyber security policies, leaving operations to other government agencies.

The president should provide direct support for the new office, which should perform the functions below. The current cybersecurity coordinator already does many of these things, but the proposed Office of Cyber Security Policy would significantly increase the White House's capacity to:

- Develop cyber security strategies that prioritize national interests and communicate the U.S. government's intentions.
- Coordinate cyber security policies, their implementation across federal agencies, and the use of law enforcement, economic, financial, diplomatic, public engagement and military means to support them.
- Evaluate the potential need for a cabinet-level U.S. government agency whose sole responsibility would be to develop and implement cyber security policies.
- Liaise with domestic and international audiences so that the White House maintains a highly visible role as a proactive coordinator of government-wide cyber security efforts.
- Interact regularly with key stakeholders from the private sector, academia, multilateral organizations, civil society and elsewhere.
- Develop and share analysis of global trends and U.S. government investments – with the assistance of the intelligence community, other executive agencies, the Office of Management and Budget and federally funded research and development centers – in order to help frame cyber security policy choices for the president.
- Marshal the interagency use of non-cyber policy instruments to address cyber security. These instruments include economic policy, law enforcement, intelligence, military and commercial relationships, diplomacy, standards, regulations and public engagement.

Enhance Oversight of U.S. Government Cyber Security Activities

The U.S. government badly needs stronger and more comprehensive oversight of cyber security. This theme emerged repeatedly in interviews with both government and private sector leaders. As a senior Pentagon official told us, "We need better civilian control in this area."[212] A Senate staff member observed that "We have far more offensive capabilities than policies to regulate them."[213] Current policy initiatives are being undertaken in a climate of governmental disorganization, underdeveloped institutions and processes, high degrees of secrecy and enormous technical complexity. This climate puts the U.S. government at risk of making mistakes with substantial consequences for national security, civil liberties and the national purse.

The U.S. government badly needs stronger and more comprehensive oversight of cyber security. This theme emerged repeatedly in interviews with both government and private sector leaders.

To conduct stronger oversight of cyber security activities, the U.S. government should take the following steps.

- **The White House and DOD** should maintain command and control procedures for cyber operations by the U.S. military and intelligence community in order to preserve senior civilian leaders' ability to review and approve significant activities.[214] While the U.S. government has proceeded cautiously with cyber operations thus far, the urgent need to respond at "netspeed" may increasingly challenge senior leaders' ability to stay in the decision loop.[215] "Areas of hostility" and other blurry operating scenarios further complicate command and control.[216] A hybrid strategy likely offers the best practical solution. It should consist of command and control policies similar to those adopted for U.S. nuclear weapons, such as predetermined rules, preauthorization authority, fail safe mechanisms to prevent unauthorized actions, and positive control that ensures successful execution of any attack order.[217]

- **The White House** should appoint separate heads of the NSA and Cyber Command. A dual-hatted leader offered certain organizational benefits while Cyber Command was being established. Given the overlap between intelligence collection and military action in cyberspace, the NSA and Cyber Command should remain co-located, cooperate extensively and continue to share personnel. However, having the head of an intelligence agency also serve as the head of a U.S. military command is not the appropriate long-term solution. Such an arrangement makes it difficult to conduct effective oversight and blurs the important line between intelligence gathering and military operations.
- **The White House** should create a President's Cyber Security Advisory Board, modeled on the Defense Policy Board and Intelligence Advisory Board, to provide independent advice and oversight on cyber security issues directly to the president. Though a number of advisory boards already exist, the Cyber Security Advisory Board is needed to provide the president with concentrated cyber security expertise that is not accessible elsewhere. The board should include up to 16 non-governmental members with varied backgrounds, including those with experience in civil liberties protection and in the private sector. The proposed White House Office of Cyber Security Policy should administer the board.
- **The Department of Homeland Security, DOD and the intelligence community** should create a high-level joint contact group known as the Cyber Security Coordination Council (CSCC) to oversee and coordinate activities. Modeled on the Nuclear Weapons Council that includes DOD and the Department of Energy, the CSCC should craft joint strategies, resolve issues and report regularly to the president and Congress on cyber security initiatives. The three organizations do currently meet, but the CSCC would provide a more consistent and responsive structure for collaboration. The first objective of the CSCC should be to produce a memorandum of understanding that advances information sharing among the three agencies.
- **Congress** should constitute a bicameral and bipartisan Cyber Security Task Force to promote greater understanding of cyber security issues. While the task force need not necessarily become a permanent fixture on the Hill, it would provide a forum to convene for a few years – especially as Congress works to pass and oversee comprehensive cyber security legislation. By creating a forum to develop policy and educate lawmakers, the task force would improve bicameral coordination and strengthen Congress's ability to conduct vigorous oversight.
- **The White House** should commission OSTP or the National Academy of Sciences to produce a set of objective cyber security metrics to assess penetrations and attacks thwarted, along with attackers' so-called "dwell time" in government networks, ability to inflict damage, and ability to steal or alter data. U.S. policymakers should then use the metrics to evaluate performance and guide necessary adjustments.

Protect the Nation's Most Critical Infrastructure

Some critical infrastructure is so central to Americans' way of life that its protection requires proactive and consistent involvement by the U.S. government. There is a need for measured government leadership, which exists in other spheres where broader U.S. well-being is at risk. With assistance from industry groups and U.S. government agencies, the companies that manage America's critical infrastructure have begun to address their vulnerability to cyber attacks. But these efforts remain insufficient and progress varies widely across sectors and the companies within them. According to reports, companies struggle to make the business case for cyber security because threats are difficult to monitor and the return on investment is ambiguous.[218] Should companies fail to defend successfully against cyber attacks, which are now frequent, the consequences would hurt Americans and the U.S. economy.

When helping to protect critical infrastructure, the U.S. government should not be heavy-handed or excessively regulatory. It should favor market solutions wherever possible. The overarching goal should be to enable more sophisticated critical infrastructure providers to become even more secure against a wider array of threats, while enabling less sophisticated providers to reach higher levels of security. To achieve this goal, the U.S. government should take the following actions.

- **Congress** should amend the Homeland Security Act of 2002 to provide DHS with more explicit authorities to coordinate the protection of U.S. critical infrastructure in cyberspace. This should include the authority to issue regulations mandating that critical infrastructure providers comply with a certain baseline for security practices. Although the president has articulated this authority through directives, it should be codified in statute to strengthen accountability.
- **Congress** should pass cyber security legislation that provides guidance on tailored regulatory strategies that comport with the needs and purposes of specific sectors. U.S. critical infrastructure is not a monolith and the regulations for telecommunications, where privacy and anonymity are core U.S. values, should differ from regulations for the electric grid, where privacy is not a concern.
- **Congress** should strengthen the authority and capacity of the Federal Energy Regulatory Commission (FERC) to enforce cyber security standards among utility companies, which currently protect their security unevenly. While DHS should remain responsible for top tier providers in the energy sector, as it is with other critical infrastructure sectors, FERC should gain expanded authority to enforce cyber security standards for other providers. Rather than developing in-house expertise, which would take a long period of time, FERC should develop standards based on National Institute of Standards and Technology guidelines and through consultation with DHS and sector-specific regulatory agencies.
- **The Department of Homeland Security** should approach regulation cautiously and focus on making the market work better. It should offer incentives such as liability protection to encourage greater security as long as doing so does not create moral hazards. One approach would be for the leading critical infrastructure providers to develop protection plans, which should include supply chain security practices, for DHS to review. This process already occurs in the nuclear power and chemical sectors, and could be expanded to cover other sectors.[219] The Department of Homeland Security should be "technology neutral" but not "performance neutral" toward the protection of critical infrastructure, meaning that it should allow critical infrastructure operators to select the technological solution they think will best meet required standards of performance.
- **Congress** should continue to promote and fund DOD, the Department of Energy and other agencies in their efforts to use military bases as test beds for cyber security innovation related to the smart grid, a plan for greater use of digital technology in the electric grid. The national labs and DOD collaborate frequently to address cyber challenges, and given their investments in smart grid technology, they have high stakes in maximizing cyber security. Congress also should

hold a hearing or require a report to gauge the progress made to date on cyber security innovation related to the smart grid, and to determine appropriate next steps.

- **Congress** should request an inventory of all smart grid investments that various stakeholders have made in DOD facilities to determine whether cyber security standards have been appropriate and consistent. **The Department of Defense** should likewise ensure that all its contracts for and acquisitions of smart grid technology meet the most stringent cyber security standards.

Harness the Private Sector's Innovative Power for Cyber Security

Since the innovative vibrancy of the U.S. technology sector is likely to continue unabated, the U.S. government must improve its ability to harness the private sector's innovative power for cyber security. Though the term "public-private partnership" often produces eye rolling, especially from private companies, the need for constant, committed and coherent engagement with the private sector remains as important as ever to both corporations and the federal government.[220] The U.S. government should recognize the differences within the private sector and not treat industry as a monolith. Instead, the U.S. government should craft policies tailored to get the best out of different companies, which include everything from large enterprises with scores of personnel trained in government contracting to tiny Internet startups.[221] (For more information, see Daniel Geer's chapter in Volume II.)

Throughout the course of this study, one theme emerged repeatedly from the private sector: a desire for the U.S. government to lead by example. Private sector representatives acknowledged their own need to address cyber security threats. They also noted, however, that the U.S. government has not gotten its own house in order. Companies are eager to collaborate with the U.S. government, but they want the U.S. government to invest in securing its own systems and realize that information sharing is a two-way street.

Empowering the private sector to promote cyber security is essential to U.S. national security. To increase its effectiveness as a strategic partner, the U.S. government should implement the following policies.

- **The White House** should direct each major agency that deals with cyber security to conduct a detailed review of its classification guides in order to identify unnecessary layers of secrecy that prevent information sharing among federal agencies and non-governmental stakeholders.[222] It also should increase the capacity of the Interagency Security Classification Appeals Panel, administered by the Information Security Oversight Office, so that it can manage its recently increased workload and continue to resolve interagency disputes over-classification.[223] The U.S. government needs to embrace more fully the collaborative "need to share" model for information sharing and abandon the less communicative "need to know" approach that prevailed during the Cold War and continues today.[224] As Jeff Brown, vice president and chief information security officer at Raytheon, told us, "Over-classification is one of the biggest problems in cyber security today, on both the government and industry sides."[225] Michael Hayden, former head of both the NSA and CIA, wrote recently, "Let me be clear: this stuff is overprotected…we need a broader flow of information to corporations and individuals to educate them on the threat. To do that we need to recalibrate what is truly secret."[226] Nearly half of the classification guides used during fiscal year 2009, the most recent year for which data is available, were not updated within the past five years as required.[227] Agencies are relying on classification guides that may be outdated, particularly on an issue like cyber security that evolves so rapidly. While the U.S. government must move cautiously so as not to reveal state secrets, improved information sharing can have real national security benefits.

- **Congress** should pass legislation to extend liability protection to private sector providers of innovative cyber security products and services. The legislation should explicitly support mechanisms for private companies such as Internet service providers to share cyber security information among themselves and with U.S. government agencies without risking violations of laws such as the Electronic Communications Privacy Act, antitrust investigations or lawsuits. If companies believe they are in legal jeopardy, or think their brands will be damaged by sharing information, they are less likely to participate even if doing so is in the public interest. U.S. government agencies such as the FCC already operate under the principle of presumed confidentiality, but strengthening liability protection will improve information sharing and foster technological innovation, two advances that are critical to U.S. national security in the digital age.[228]
- **Congress** should pass legislation that requires federal agencies to prioritize security when writing requirements and awarding contracts for software and other information technology products.[229] The White House has emphasized how important it is "to integrate cybersecurity into all new systems rather than bolting it on as an afterthought."[230] By prioritizing security at the outset, the U.S. government will save money in the long run by avoiding costly upgrades and security breaches.
- **The Department of Commerce** should request funding for new research by technologists and economists to measure cyber security's costs, benefits, return on investment and business models. Private companies struggle to justify cyber security investments, price insurance and adapt business models.[231] New research would therefore provide a wide public benefit and ultimately help the U.S. economy.
- **The State Department** should task its foreign service officers stationed at U.S. embassies around the world to assume a greater role in helping U.S. companies partner with responsible cyber security stakeholders in the host country. Long global supply chains present more opportunities for malicious actors to insert harmful code and/or steal intellectual property. But foreign service officers can play a critical role in steering American businesses toward host nation partners that are known to be secure and reliable. Moreover, they can provide useful guidance regarding license requirements and contracting procedures in the host nation in order to help American firms protect their intellectual property. Larger embassies should create "cyber teams" comprised of foreign service officers who possess expertise on cyber security, while smaller embassies should rely on one or two knowledgeable individuals to provide this service.
- **The Department of Justice, DHS, the NSA, Department of Commerce and other executive branch agencies** should make clear what the private sector can – and cannot – expect from the U.S. government with respect to cyber security. Private companies value the threat information shared with them by the federal government, but agencies often ask them to share information without returning the favor. Companies report that that it is difficult to know whom to contact in the U.S. government with questions or concerns about cyber security.

VII. CONCLUSION

Just as perfect security eludes us in the physical world, there is not and never will be perfect security in cyberspace. America's goal, therefore, should be to minimize risks at an acceptable cost and enable the continued advances that the information age has heralded thus far.

This is no easy endeavor. Every day, more users exchange more data on more devices, creating ever more reliance on the Internet. American companies depend on the Internet for growth and the U.S. military depends on networked communication for its most important operations.

Yet as Daniel Geer, a contributor to Volume II, has noted, "A technology that can give you everything you want is a technology that can take away everything that you have."[232] America's very dependence has created new vulnerabilities. These vulnerabilities are being exploited as fast as or faster than the nation can respond. This is a race and America's future is on the line.

Current cyber threats, especially their economic toll, are cause for serious concern. Yet the greatest threats lie ahead. Investing only in efforts to thwart today's threats will leave America ill prepared for tomorrow. Ignoring future threats will expose the United States in ways that endanger the nation's enduring security interests. The challenge is to prepare for cyber threats with insight, diligence and rigor, while avoiding what the 9/11 Commission report termed failures of imagination. The nation's security and prosperity are at stake. There is no time to waste.

ENDNOTES

1. Pew Research Center's Internet & American Life Project, "Trend Data – Online Activities, Total" (as of 26 April 2011), http://www.pewinternet.org/Trend-Data/Online-Activites-Total.aspx.

2. The White House, National Economic Council, *A Strategy for American Innovation: Driving Towards Sustainable Growth and Quality Jobs* (September 2009).

3. International Telecommunication Union (ITU), *The World in 2010* (October 2010).

4. President Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure" (29 May 2009).

5. The White House, *National Security Strategy* (May 2010): 27; Department of Defense, *Quadrennial Defense Review Report* (February 2010): 37; Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (February 2011): 3-4; Department of State, *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review* (December 2010): 12; and Department of Homeland Security, *Quadrennial Homeland Security Review Report* (February 2010): 29-30.

6. This trend also exists in the theoretical literature. See Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27:3 (July 2006): 221-244.

7. The authors are indebted to Monitor 360's Jesse Goldhammer for sharing this insightful point. For a related argument, see Robert Dallek, "The Tyranny of Metaphor," *Foreign Policy* (November 2010).

8. See the chapter in Volume II by Gary McGraw and Nathaniel Fick. For analysis of existing case studies, see Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010); and Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," Working Paper No. 10-77, Mercatus Center, George Mason University (January 2011).

9. As Michael Hayden, former director of both the NSA and CIA, wrote recently about cyber security, "Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon." See Michael Hayden, "The Future of Things 'Cyber'," *Strategic Studies Quarterly* (Spring 2011): 3.

10. The White House, *National Security Strategy* (May 2010): 7.

11. Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom" (21 January 2010).

12. Of course, cyber capabilities are not a panacea for military challenges. On the limitations of information warfare and related concepts, see David J. Betz, "The More You Know, the Less You Understand: The Problem with Information Warfare," *The Journal of Strategic Studies* 29:3 (June 2006): 505-533; and Matt Carr, "Slouching Towards Dystopia: The New Military Futurism," *Race & Class* 51:3 (January 2010): 13-32.

13. P.W. Singer, *Battlefields of the Future* (Washington: Brookings Institution, 4 February 2011); and Principal Deputy Under Secretary of Defense for Policy James Miller, submitted testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011): 1.

14. Damien McElroy, "Military Balance Report: Countries Creating New Cyber Warfare Organisations," *The Telegraph* (9 March 2011).

15. Fred B. Schneider, submitted testimony before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities (19 February 2010): 2.

16. Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academies Press, 2010): 79.

17. GEN Keith Alexander, testimony before the House Armed Services Committee (23 September 2010).

18. Deputy Secretary of Defense William Lynn, "Introducing U.S. Cyber Command," *The Wall Street Journal* (3 June 2010).

19. Jack Goldsmith, "The New Vulnerability," *The New Republic* (7 June 2010).

20. Siobhan Gorman, Yochi Dreazen and August Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal* (17 December 2009).

21. Joby Warrick, "Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack," *The Washington Post* (16 February 2011).

22. Robert D. Atkinson, Stephen J. Ezell, Scott M. Andes, Daniel D. Castro and Richard Bennett, *The Internet Economy 25 Years After .Com: Transforming Commerce & Life* (Washington: The Information Technology and Innovation Foundation, March 2010): 43.

23. Ibid.: 42-51.

24. Organisation for Economic Co-operation and Development, "Broadband and the Economy," Ministerial Background Report No. DSTI/ICCP/IE(2007)3/FINAL (May 2007): 5.

25. Authors' private communication with technology advisor Peter Bloom (14 April 2011).

26. Ellen Nakashima, "U.S. Agencies Respond to Cyberattack on Information Security Firm," *The Washington Post* (23 March 2011).

27. Riva Richmond, "An Attack Sheds Light on Internet Security Holes," *The New York Times* (6 April 2011).

28. Ken Dilanian, "Virtual War a Real Threat," *Los Angeles Times* (28 March 2011).

29. Jon Oltsik, *Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure* (Milford, MA: Enterprise Strategy Group, November 2010): 8.

30. Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom" (21 January 2010).

31. Secretary of State Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World" (15 February 2011).

32. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011).

33. Kristin M. Lord, *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace* (Albany, NY: SUNY Press, 2007).

34. For a dissenting argument about how the Internet actually may reinforce like-minded opinions that can foster and enflame hate groups, see Cass Sunstein, *Republic.com* (Princeton, NJ: Princeton University Press, 2001).

35. On the growing complexity of international networks, see Anne-Marie Slaughter, "America's Edge," *Foreign Affairs* (January/February 2009): 113; and National Intelligence Council, *Global Trends 2025: A Transformed World* (November 2008): 84-85.

36. For a similar philosophy, see Deputy Under Secretary of the Department of Homeland Security National Protection and Program Directorate Philip Reitinger, submitted testimony before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies (16 March 2011): 2.

37. Center for a New American Security Cyber Security Strategy Workshop (18 November 2010).

38. For background on the legal definition and existing law, see Scott Eltringham, ed., *Prosecuting Computer Crimes* (Washington: Department of Justice, February 2007). The broader definition used here is consistent with Benjamin S. Buckland, Fred Schreier and Theodor H. Winkler, "Democratic Governance Challenges of Cyber Security," DCAF Horizon 2015 Working Paper No. 1 (2010): 15; and GEN Keith Alexander, submitted testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011): 7.

39. Authors' interview with Deputy Assistant Director of the FBI Cyber Division Steven Chabinsky (22 March 2011). In addition to the estimates listed in the text, see Andy Greenberg, "Putting a Price on Cyberspying," *Forbes* (29 January 2009); Symantec, *State of Enterprise Security 2010* (February 2010); Deb Shinder, "Calculating the True Cost of Cybercrime," *Tech Republic* (14 September 2010); Thomas Claburn, "Data Loss Costing Companies $6.6 Million Per Breach," *Information Week* (3 February 2009); and Detica and the Office of Cyber Security and Information Assurance in the U.K. Cabinet Office, *The Cost of Cyber Crime* (February 2011).

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

41. McAfee, *Web 2.0: A Complex Balancing Act* (September 2010).

42. See Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0* (April 2010): i; and FBI Director Robert Mueller, testimony before the Senate Select Committee on Intelligence (16 February 2011).

43. Demetri Sevastopulo, "Cyber Attacks on McCain and Obama Teams 'Came From China'," *Financial Times* (7 November 2008).

44. See Siobhan Gorman, August Cole and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal* (21 April 2009); and Siobhan Gorman, "U.S. Backs Talks on Cyber Warfare," *The Wall Street Journal* (4 June 2010).

45. Deputy Secretary of Defense William Lynn, "Defending a New Domain," *Foreign Affairs* (September/October 2010): 97.

46. Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network* (29 March 2009).

47. Center for a New American Security Cyber Security Strategy Workshop (18 November 2010).

48. Derived in part from Benjamin S. Buckland, Fred Schreier and Theodor H. Winkler, "Democratic Governance Challenges of Cyber Security," DCAF Horizon 2015 Working Paper No. 1 (2010).

49. Charles Arthur, "Inside 'Anonymous': Tales from Within the Group Taking Aim at Amazon and Mastercard," *Guardian Technology Blog* (13 December 2010).

50. On influence in cyberspace, see Amy Zalman, "Narrative as an Influence Factor in Information Operations," *IO Journal* 2:3 (August 2010): 4-10; and Franklin D. Kramer and Larry Wentz, "Cyber Influence and International Security," Defense Horizons No. 61, Center for Technology and National Security Policy, National Defense University (January 2008).

51. Glenn Kessler, "WikiLeaks Unveiling of Secret State Department Cables Exposes U.S. Diplomacy," *The Washington Post* (29 November 2010).

52. Gautham Nagesh, "U.S. Ambassador to Mexico Resigns Over WikiLeaks," *Hillicon Valley Blog* (21 March 2011).

53. See Joseph S. Nye, Jr.'s chapter in Volume II; and Martin Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* (Spring 2011): 138.

54. Rain Ottis, *From Pitchforks to Laptops: Volunteers in Cyber Conflicts* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010).

55. Drawn from Anna-Maria Talihärm, *Cyber Terrorism: in Theory or in Practice?* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010); Catherine A. Theohary and John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace* (Washington: Congressional Research Service, March 2011): 3; and James Lewis, *A Note on the Laws of War in*

Cyberspace (Washington: Center for Strategic and International Studies, April 2010): 3.

56. Catherine A. Theohary and John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace* (Washington: Congressional Research Service, March 2011): 5.

57. Deputy Assistant Director of the FBI Cyber Division Steven Chabinsky, submitted testimony before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security (17 November 2009): 2-3.

58. On the character of cyber war, see Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the 'First Battle' in 21st-Century War," Defense Horizons No. 68, Center for Technology and National Security Policy, National Defense University (September 2009). For more on the use of cyberspace in irregular warfare, see Department of Defense, *Foreign Internal Defense Joint Integrating Concept* (February 2010).

59. For analysis of related scenarios, see Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academies Press, 2010): 77-97.

60. GEN Keith Alexander has argued that cyber war constituting the entirety of a conflict is less likely to occur. "I believe [cyber war] would not exist in and of itself but as part of a larger military campaign," he remarked in 2010. See Alexander, testimony before the Senate Armed Services Committee (15 April 2010).

61. See Thomas Mahnken's chapter in Volume II.

62. For legal analysis of cyber war, see Tom Gjelten, "Extending the Law of War to Cyberspace," NPR (22 September 2010); Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review* 64 (2009): 139-171; James P. Farwell, "The Emerging Battlespace of Cyberwar: The Legal Framework and Policy Issues," *IO Journal* 1:4 (February 2010): 12-20; and David E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law & Policy* 4:1 (Winter 2010): 87-102.

63. Senator Susan Collins, "How to Make Internet More Secure?" *Politico* (7 March 2011).

64. Principal Deputy Under Secretary of Defense for Policy James Miller, submitted testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011): 2.

65. Director of National Intelligence James Clapper, testimony before the House Permanent Select Committee on Intelligence (10 February 2011).

66. Authors' interview with Deputy Assistant Director of the FBI Cyber Division Steven Chabinsky (22 March 2011).

67. For a brief history of the creation of the Internet, see Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff, *A Brief History of the Internet* (Reston, VA: Internet Society, undated).

68. See Robert Kahn's chapter in Volume II.

69. Ibid.

70. On the attribution challenge, see David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academies Press, 2010): 25-40.

71. Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information," *Science* 332:60 (April 2011): 60-65.

72. Intel, "Moore's Law" (2005).

73. On the possibility that solid-state electronics will fail to keep pace with Moore's Law, and the implications for the U.S. military, see Gerald M. Borsuk and Timothy Coffey, "Moore's Law: A Department of Defense Perspective," Defense Horizons No. 30, Center for Technology and National Security Policy, National Defense University (July 2003).

74. McAfee, *A Good Decade for Cybercrime* (January 2011): 4.

75. International Telecommunication Union, "Key Global Telecom Indicators for the World Telecommunication Service Sector" (updated 21 October 2010).

76. On increased processor speeds and improved algorithms, see the White House, President's Council of Advisors on Science and Technology, *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology* (December 2010): 56, 71.

77. Robert D. Atkinson, Stephen J. Ezell, Scott M. Andes, Daniel D. Castro and Richard Bennett, *The Internet Economy 25 Years After .Com: Transforming Commerce & Life* (Washington: The Information Technology and Innovation Foundation, March 2010): 43.

78. Discussed during Center for a New American Security Cyber Security Working Group (21 January 2011); and Jack Goldsmith and Melissa Hathaway, "The Cybersecurity Changes We Need," *The Washington Post* (29 May 2010).

79. McAfee, *McAfee Threats Report: Fourth Quarter 2010* (February 2011): 7.

80. Ibid.: 2.

81. Cited in McAfee, *A Good Decade for Cybercrime* (January 2011): 7.

82. Department of Homeland Security, *National Infrastructure Protection Plan* (February 2009): 122-123.

83. Shari Lawrence Pfleeger, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (11 February 2011).

84. See Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (September 2007): 5.

85. The Department of Homeland Security's so-called Aurora Generator Test reaffirmed that a cyber attack could inflict kinetic damage on U.S. critical

infrastructure. See Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," CNN (26 September 2007).

86. Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (September 2007): 14; and Kim Zetter, "Attack Code for SCADA Vulnerabilities Released Online," *Wired* (22 March 2011).

87. McAfee and the Center for Strategic and International Studies, *In the Dark: Crucial Industries Confront Cyberattacks* (April 2011): 6.

88. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *The Wall Street Journal* (8 April 2009).

89. Center for a New American Security Cyber Security Strategy Workshop (18 November 2010).

90. For discussion of the advantages and disadvantages of the "Internet of things," see "It's a Smart World," *The Economist* (4 November 2010).

91. Nicolas Falliere, Liam O. Murchu and Eric Chien, *W32.Stuxnet Dossier Version 1.4* (Cupertino, CA: Symantec, February 2011): 5-7.

92. John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New York Times* (1 August 2009).

93. Deputy Assistant Director of the FBI Cyber Division Steven Chabinsky, submitted testimony before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security (17 November 2009): 2-3.

94. With the advent of nuclear weapons, the time required to inflict massive damage also shrunk, though to a lesser extent. For a comparison of crisis pressure in the nuclear and cyber contexts, see Stephen J. Cimbala, "Nuclear Crisis Management and 'Cyberwar': Phishing for Trouble?" *Strategic Studies Quarterly* (Spring 2011).

95. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *The Wall Street Journal* (8 April 2009).

96. See "Cyber Banking Fraud – Global Partnerships Lead to Major Arrests," FBI (1 October 2010); and "More Than 100 Arrests, as FBI Uncovers Cyber Crime Ring," BBC (1 October 2010).

97. David Pett, "High-Frequency Swaps, Dark Pools Under Scrutiny," *National Post's Financial Post & FP Investing* (8 May 2010).

98. Kara Scannell and Tom Lauricella, "Flash Crash Is Pinned On One Trade," *The Wall Street Journal* (2 October 2010).

99. Joseph Menn, "US Probes Anonymous Plans for Attack on Marines," *Financial Times* (8 March 2011).

100. Ibid.

101. CACI International and the U.S. Naval Institute, *Cyber Threats to National Security* (July 2010): 7-8. For an opposing viewpoint on how barriers to entry may not be lower in cyberspace, see Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal* 1:1 (April 2009).

102. William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times* (15 January 2011).

103. Gary McGraw, "Software [In]security: How To P0wn a Control System with Stuxnet," *InformIT* (23 September 2010).

104. Center for a New American Security Cyber Security Policy Workshop in San Francisco (10 February 2011).

105. Colin Gray, "Information and Security: A Rejoinder," *Orbis* 50:1 (Spring 1996): 276.

106. Rain Ottis, *From Pitchforks to Laptops: Volunteers in Cyber Conflicts* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010).

107. Authors' private communication with Gary McGraw (26 April 2011).

108. On the profitability of black market hacking, see Peter T. Leeson and Christopher J. Coyne, "The Economics of Computer Hacking," *The Journal of Law, Economics and Policy* 1:2 (2005).

109. Charlie Miller, *The Legitimate Vulnerability Market: Inside the Secretive World of 0-Day Exploit Sales* (Baltimore: Independent Security Evaluators, May 2007): 3-4.

110. Authors' interview with Deputy Assistant Director of the FBI Cyber Division Steven Chabinsky (22 March 2011).

111. Deputy Secretary of Defense William Lynn, "Remarks on Cyber at the RSA Conference" (15 February 2011).

112. See Project Grey Goose, Phase I Report, *Russia/Georgia Cyber War – Findings and Analysis* (17 October 2008); and U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008* (August 2009): 3.

113. On the challenges of creating arms control treaties for cyberspace, see Jason Barkham, "Information Warfare and International Law on the Use of Force," *New York University Journal of International Law and Politics* 34:1 (2001): 96-111; and James Bret Michael, Eneken Tikk, Peter Wahlgren and Thomas C. Wingfield, "From Chaos to Collective Defense," *Computer* (August 2010). For an argument in favor of a cyber arms treaty, see Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco, 2010): 268-271.

114. National Security Agency Information Assurance Director Debora Plunkett, remarks at *The Atlantic*'s and *Government Executive*'s First Annual Cybersecurity Forum (16 December 2010).

115. Seymour E. Goodman and Herbert S. Lin, eds., *Toward a Safer and More Secure Cyberspace* (Washington: The National Academies Press, 2007): 151.

116. Center for a New American Security Cyber Security Working Group (25 October 2010).

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

118. GEN Keith Alexander, testimony before the Senate Armed Services Committee (15 April 2010).

119. Glenn Chapman, "Two Years and 100 M Dollars Buys Winning Cyber Army," *Agence France-Presse* (1 August 2010).

120. Defense Advanced Research Projects Agency Director Regina E. Dugan, submitted testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (1 March 2011): 16-17.

121. Mark Clayton, "Cyberattacks Represent a New Arms Race Era," *Homeland1.com* (8 March 2011).

122. Authors' interview with former Assistant Secretary of Defense for Global Strategic Affairs Michael Nacht (24 February 2011).

123. Gregory Rattray, Chris Evans and Jason Healey, "American Security in the Cyber Commons," in *Contested Commons: The Future of American Power in a Multipolar World*, Abraham Denmark and James Mulvenon, eds. (Washington: Center for a New American Security, January 2010): 170.

124. Michael A. Vatis, "Cyber Attacks During the War on Terrorism: A Predictive Analysis," Institute for Security Technology Studies at Dartmouth College (September 2001). The challenge of legal authorities in such a scenario was discussed by GEN Keith Alexander, testimony before the Senate Armed Services Committee (15 April 2010).

125. Center for a New American Security Cyber Security Working Group (25 October 2010).

126. GEN Keith Alexander, testimony before the House Armed Services Committee (23 September 2010).

127. See Mike McConnell's chapter in Volume II.

128. See Brian M. Mazanec, "The Art of (Cyber) War," *Journal of International Security Affairs* 16 (Spring 2009); Northrop Grumman, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (October 2009); and Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," submitted testimony before the House Foreign Affairs Committee (10 March 2010).

129. Department of Defense, *Military Power of the People's Republic of China 2008* (March 2008): 21.

130. Martin Libicki, "Chinese Use of Cyberwar as an Anti-Access Strategy," submitted testimony before the U.S.-China Economic and Security Review Commission (27 January 2011).

131. Authors' interview with former U.S. government official (February 2011).

132. David E. Sanger, John Markoff and Thom Shanker, "U.S. Steps Up Effort on Digital Defenses," *The New York Times* (28 April 2009).

133. Quoted in Seymour M. Hersh, "The Online Threat," *The New Yorker* (1 November 2010).

134. Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (December 2006): 9-10. Emphasis included in the original.

135. Authors' interview with senior U.S. military official (April 2011).

136. For the White House's assessment of the risks and rewards of cloud computing, see U.S. Chief Information Officer Vivek Kundra, *Federal Cloud Computing Strategy* (8 February 2011).

137. Aliya Sternstein, "NSA Testing Smartphones, Tablets on Safe Mobile Architecture," *NextGov* (25 March 2011).

138. Symantec, *Internet Security Threat Report: Trends for 2010*, 16 (April 2011): 6.

139. In 2008, the United States accounted for only 40 percent of global spending on information technology, according to Catherine M. Mann, testimony before the Senate Finance Committee, Subcommittee on International Trade, Customs and Global Competitiveness (18 November 2010).

140. President Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure" (29 May 2009).

141. Secretary of Commerce Gary Locke, "Remarks at Cybersecurity Event with White House Cybersecurity Coordinator Howard Schmidt, Stanford, California" (7 January 2011).

142. The White House, *National Strategy for Trusted Identities in Cyberspace* (April 2011): 1.

143. Authors' interview with senior U.S. government official (April 2011).

144. Government Accountability Office, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed* (October 2010).

145. See Dana Priest and William M. Arkin, "A Hidden World, Growing Beyond Control," *The Washington Post* (19 July 2010); Government Accountability Office, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance* (July 2010): 32; Ellen Nakashima, "U.S. Cyber-Security Strategy Yet To Solidify," *The Washington Post* (17 September 2010); and John M. Gilligan, submitted testimony before the House Oversight and Government Reform Committee, Subcommittee on Government Management, Organization and Procurement (24 March 2010).

146. Deputy Secretary of Defense William Lynn, "Remarks on Cyber at the RSA Conference" (15 February 2011).

147. GEN Keith Alexander, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011).

148. Department of Homeland Security, "Joint Statement by Secretary of Defense Robert Gates and Secretary of Homeland Security Janet Napolitano on Enhancing Coordination to Secure America's Cyber Networks" (13 October 2010).

149. U.S. Air Force, “24th Air Force Fact Sheet” (1 April 2010).

150. U.S. Air Force, *Cyberspace Operations: Air Force Doctrine Document 3-12* (15 July 2010).

151. Fleet Cyber Command/10th Fleet Public Affairs, “Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet” (29 January 2010).

152. See Alan J. McCombs, “Marines Launch into Cyberspace with New Command,” *Fort Meade News* (28 January 2010); and LtGen George Flynn, testimony before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities (24 September 2010).

153. Amanda Palleschi, “Marines Conducting Capabilities-Based Assessment for Cyberwarfare,” *Inside the Pentagon* (3 March 2011).

154. U.S. Army, *Cyberspace Operations Concept Capability Plan 2016-2028* (22 February 2010).

155. John Van Winkle, “Cadets, NSA Engage in Cyber Wargames,” *U.S. Air Force Academy Public Affairs* (29 April 2010).

156. Amanda Palleschi, “DOD to Lay Out Cyberspace Vision for 2020s in New Joint Concept,” *Inside the Pentagon* (14 October 2010).

157. Deputy Secretary of Defense William Lynn, “Remarks on Cyber at the RSA Conference” (15 February 2011).

158. Principal Deputy Under Secretary of Defense for Policy James Miller, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011). Readers should note that Miller was a founding member of the Center for a New American Security.

159. Philip J. Bond, submitted testimony before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities (25 February 2010): 6. Readers should note that the Department of Defense’s total information technology budget increased by approximately 50 percent during the same period.

160. William Matthews, “Debate Continues Over Cyber Protection, NSA Role,” *Defense News* (17 November 2009).

161. For discussion of these different authorities, see GEN Keith Alexander, testimony before the House Armed Services Committee (23 September 2010).

162. Senate Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2011, Report 111-201* (4 June 2010): 181.

163. Department of Homeland Security, *Quadrennial Homeland Security Review Report* (February 2010): x.

164 Deputy Under Secretary of the Department of Homeland Security National Protection and Program Directorate Philip Reitinger, submitted testimony before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies (16 March 2011): 2.

165. Representative James R. Langevin, Representative Michael T. McCaul, Scott Charney, Harry Raduege and James Lewis, *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters* (Washington: Center for Strategic and International Studies, July 2010): 6.

166. Sarah Laskow, *Is Congress Failing on Homeland Security Oversight?* (Washington: Center for Public Integrity, July 2009).

167. Authors’ interview with senior Department of Homeland Security official (March 2011).

168. Authors’ analysis of Office of Management and Budget’s *Analytical Perspectives* volumes for FY 2002-2011.

169. All the data in this paragraph comes fromthe Office of Management and Budget, *Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002* (3 February 2011): 23-27.

170. The Department of Defense did not provide cyber security cost information in the form of an Exhibit 53B as required by OMB Circular A-11; thus, its spending could not be included in this calculation. See ibid.: 22.

171. Assistant to the President for Science and Technology and Director of the White House Office of Science and Technology Policy John P. Holdren, *The 2012 Budget: Winning the Future Through Investments in Innovation, Education, and Infrastructure* (14 February 2011).

172. Department of Homeland Security, National Protection and Programs Directorate, Infrastructure Protection and Information Security, *Fiscal Year 2012 Congressional Justification* (February 2011): 9.

173. Due to the uncertainty surrounding the Department of Defense’s cyber security budget estimates, a comparison to FY 2010 enacted appropriations – consistent with the analysis throughout this section – is not possible. See Aliya Sternstein, “Pentagon Seeks $3.2 Billion for Revised Cyber Budget,” *NextGov* (24 March 2011).

174. Deputy Secretary of Defense William Lynn, “Remarks on Cyber at the RSA Conference” (15 February 2011).

175. See Aliya Sternstein, “Pentagon Seeks $3.2 Billion for Revised Cyber Budget,” *NextGov* (24 March 2011); and Aliya Sternstein, “Defense Funding for Cybersecurity Is Hard to Pin Down,” *NextGov* (29 March 2011).

176. Adam Rawnsley, “Go Inside the $56 Billion ‘Black’ Budget,” *Danger Room* (18 February 2011).

177. Authors’ interview with senior Senate staffer (March 2011); and authors’ interview with senior House staffers (March 2011).

178. National Security Agency, *Best Practices for Keeping Your Home Network Secure* (April 2011).

179. This recommendation draws on Seymour E. Goodman and Herbert S. Lin, eds., *Toward a Safer and More Secure Cyberspace* (Washington: The National Academies Press, 2007).

180. For related analysis, see Anil Somayaji, "Immunology, Diversity, and Homeostasis: The Past and Future of Biologically Inspired Computer Defenses," *Information Security Technical Report* 12:4 (October 2007); Department of Homeland Security, *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action* (23 March 2011); and Scott Charney, *Collective Defense: Applying Public Health Models to the Internet* (Redmond, WA: Microsoft Corporation, October 2010).

181. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008): 2-4.

182. Authors' interview with senior U.S. government official (March 2011).

183. Gigi Schumm, "Outdated FISMA Threatens Cybersecurity," *Federal Times* (6 March 2011).

184. These programs provide undergraduate and graduate scholarships in exchange for a commitment to enter the U.S. government's information technology workforce after graduation. They also provide capacity building grants to academic institutions so they can strengthen their cyber security education and workforce development programs. For analysis of these scholarship programs, see Partnership for Public Service and Booz Allen Hamilton, *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce* (July 2009): 4-6; Lance J. Hoffman, "Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development," Report No. GW-CSPRI-2010-3, Cyber Security Policy and Research Institute, The George Washington University (15 December 2010); and Diana L. Burley, "Recruiting, Educating and Retaining Cyber Security Professionals in the Federal Workforce: Lessons Learned but not yet Applied," Report No. GW-CSPRI-2011-1, Cyber Security Policy and Research Institute, The George Washington University (2 February 2011).

185. For discussion of the challenges of an international agenda, see Jeffrey Hunker, "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away," *Journal of National Security Law & Policy* 4:1 (Winter 2010): 197-216.

186. See the chapter in Volume II by David Gross, Nova Daly, Ethan Lucarelli and Roger Miksad.

187. Aliya Sternstein, "International Cybersecurity Treaty Might Not Be Achievable, Report Says," *NextGov* (11 January 2011).

188. Robert Knake, "Internet Governance in an Age of Cyber Insecurity," Special Report No. 56, Council on Foreign Relations (September 2010): 19.

189. Such an effort was recommended by the National Broadband Plan (Recommendation 14.12) and is being developed by the National Telecommunications and Information Administration in the Department of Commerce. See Federal Communications Commission, *National Broadband Plan* (March 2010): 288-289; and Department of Commerce, National Telecommunications and Information Administration, *FY 2012 Budget as Presented to Congress* (February 2011): 42.

190. U.S. officials have publicly expressed their belief that the Law of Armed Conflict should apply in cyberspace. For example, see GEN Keith Alexander, submitted testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011): 14.

191. See the chapter in Volume II by Richard Fontaine and Will Rogers.

192. See Martha Finnemore's chapter in Volume II.

193. Stephen J. Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academies Press, 2010): 113.

194. See Michael Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academies Press, 2010): 155-156; James Lewis, *A Note on the Laws of War in Cyberspace* (Washington: Center for Strategic and International Studies, April 2010); Jason Barkham, "Information Warfare and International Law on the Use of Force," *New York University Journal of International Law and Politics* 34:1 (2001): 85-95; Charles J. Dunlap, Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* (Spring 2011): 85-86; and Duncan B. Hollis, "New Tools, New Rules: International Law and Information Operations," in *Ideas as Weapons: Influence and Perception in Modern Warfare,* G. David and T. McKeldin, eds. (Herndon, VA: Potomac Books, 2009).

195. Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco, 2010): 277.

196. Council of Europe, *Convention on Cybercrime* (Budapest: 23 November 2001).

197. The Associated Press, "US Lacks People, Authorities to Face Cyber Attack" (16 March 2011).

198. Sandra Erwin, "Cyber Command Wrestling With Unresolved Technology and Policy Issues," *National Defense* (2 March 2011).

199. Shari Lawrence Pfleeger, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (11 February 2011).

200. Indeed, a 2009 National Academy of Sciences report found that "Today's policy and legal framework for guiding and regulating the U.S. use of cyber attack is ill-formed, undeveloped, and highly uncertain." See William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: The National Academies Press, 2009): 4.

201. See Steven Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line,*" Journal of National Security Law & Policy* 4:1 (Winter 2010): 27-39; and James Lewis, *Cross-Domain Deterrence and Credible Threats* (Washington: Center for Strategic and International Studies, July 2010).

202. Authors' interview with former U.S. government official (February 2011).

203. U.S. Joint Forces Command, *The Joint Operating Environment 2010* (March 2010): 63.

204. Lynn M. Scott, Raymond E. Conley, Richard Mesic, Edward O'Connell and Darren D. Medlin, *Human Capital Management for the USAF Cyber Force* (Santa Monica, CA: RAND Corporation, 2010): 35.

205. Kristin F. Lynch, John G. Drew, Sally Sleeper, William A. Williams, James M. Masters, Louis Luangkesorn, Robert S. Tripp, Dahlia S. Lichter and Charles Robert Roll, Jr., *Supporting the Future Total Force* (Santa Monica, CA: RAND Corporation, 2007): xxiii-xxiv.

206. Principal Deputy Under Secretary of Defense for Policy James Miller, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011).

207. Jim Fenton, "The National Strategy for Trusted Identities in Cyberspace," *Cisco Blog* (13 July 2010).

208. TechAmerica, Business Software Alliance and Information Technology Industry Council, letter to Gary Locke, Howard Schmidt and Patrick Gallagher (3 March 2011).

209. For exploratory analysis of privacy protection, see Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (December 2010).

210. William Jackson, "ID Management's Weakness: 'There Is No Demand'," *Government Computer News* (3 February 2011).

211. Authors' interview with SAIC's Jeffrey Cooper (22 November 2010).

212. Authors' interview with senior Pentagon official (January 2011).

213. Authors' interview with senior Senate staffer (March 2011).

214. Center for a New American Security Cyber Security Strategy Workshop (18 November 2010).

215. U.S. Air Force, *Cyberspace Operations: Air Force Doctrine Document 3-12* (15 July 2010): 9.

216. GEN Keith Alexander, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (16 March 2011).

217. For related analysis, see Joseph H. Scherrer and William C. Grund, "A Cyberspace Command and Control Model," Maxwell Paper No. 47, Air War College (August 2009); and Robert D. Critchlow, *Nuclear Command and Control: Current Programs and Issues* (Washington: Congressional Research Service, May 2006).

218. See Daniel E. Geer, Jr.'s chapter in Volume II.

219. See David Perera, "Lewis: CFATS Could Be Model for Public-Private Cybersecurity Model," *Fierce Government IT* (17 March 2011); and Shari Lawrence Pfleeger, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities (11 February 2011).

220. For an excellent recent study of this issue, see Business Software Alliance, Center for Democracy and Technology, Internet Security Alliance, TechAmerica and U.S. Chamber of Commerce, *Improving Our Nation's Cybersecurity through the Public-Private Partnership* (8 March 2011).

221. Authors' interview with the Professional Services Council (14 October 2010).

222. For a detailed rationale for such a move, see Steven Aftergood, "Reducing Government Secrecy: Finding What Works," *Yale Law & Policy Review* 27:2 (Spring 2009): 411.

223. Information Security Oversight Office, *Report to the President, 2009* (31 March 2010): 21.

224. Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy* (22 February 2008): 3

225. Authors' meeting with Raytheon Vice President and Chief Information Security Officer Jeff Brown (22 March 2011).

226. Michael Hayden, "The Future of Things 'Cyber'," *Strategic Studies Quarterly* (Spring 2011): 5.

227. Information Security Oversight Office, *Report to the President, 2009* (31 March 2010): 1. On the cost of classification activities, see Information Security Oversight Office, *2009 Cost Report* (25 June 2010).

228. Center for a New American Security Cyber Security Working Group (17 November 2010); authors' interview with senior Federal Communications Commission official (December 2010); and David Z. Bodenheimer, submitted testimony before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities (10 February 2010): 13.

229. Steve Towns, "Security Expert: Fight Cyber-Crime Through Procurement," *Government Technology* (30 January 2009).

230. The White House, "Presidential Memorandum – Accountable Government Initiative" (14 September 2010).

231. For analysis of corporate decision making and risk assessment on cyber security, see Shari Lawrence Pfleeger, Martin Libicki and Michael Webber, "I'll Buy That! Cybersecurity in the Internet Marketplace," *IEEE Security and Privacy* 5:3 (May 2007); Ginger Davis, Alfredo Garcia and Weide Zhang, "Empirical Analysis of the Effects of Cyber Security Incidents," *Risk Analysis* 29:9 (September 2009); Shari Lawrence Pfleeger and Rachel Rue, "Cybersecurity Economic Issues: Clearing the Path to Good Practice," *IEEE Software* (January/February 2008): 35-42; and Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk* (2010).

232. Daniel E. Geer, Jr., "Cybersecurity and National Policy," *Harvard National Security* Journal 1 (7 April 2010): 215.

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.

♻ PRINTED WITH SOY INK™

Center for a
New American
Security

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 978-1-935087-48-9
50999>
9 781935 087489

PRINTED WITH SOY INK

Printed on Post-Consumer Recycled paper with Soy Inks