



An American Strategy for Cyberspace

Advancing Freedom, Security, and Prosperity

JEFFREY A. EISENACH • CLAUDE BARFIELD

JAMES K. GLASSMAN • MARIO LOYOLA • SHANE TEWS

JUNE 2016

WITH A FOREWORD BY MIKE DANIELS

A M E R I C A N E N T E R P R I S E I N S T I T U T E

An American Strategy for Cyberspace

ADVANCING FREEDOM, SECURITY, AND PROSPERITY

**JEFFREY A. EISENACH • CLAUDE BARFIELD
JAMES K. GLASSMAN • MARIO LOYOLA • SHANE TEWS**

WITH A FOREWORD BY MIKE DANIELS

JUNE 2016

A M E R I C A N E N T E R P R I S E I N S T I T U T E

© 2016 by the American Enterprise Institute. All rights reserved.

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed here are those of the author(s).

Table of Contents

FOREWORD	v
ABOUT THE GLOBAL INTERNET STRATEGY PROJECT	vi
GLOBAL INTERNET STRATEGY PROJECT NATIONAL ADVISORY BOARD	ix
EXECUTIVE SUMMARY	1
CHAPTER I. INTRODUCTION	5
CHAPTER II. CREATING A STRATEGIC FRAMEWORK FOR US CYBER POLICY	9
The Nature of the Challenge.....	9
Elements of a Strategic Framework.....	10
CHAPTER III. INTERNET FREEDOM AND HUMAN RIGHTS	13
Opportunities and Challenges.....	13
The Internet as an Engine of Freedom and Prosperity.....	13
The Authoritarian Challenge to Internet Freedom and the US Response.....	14
Internet Governance and Online Freedom.....	18
The Private Sector’s Role.....	20
Principles and Policies.....	22
CHAPTER IV. INTERNATIONAL TRADE AND DIGITAL COMMERCE	28
Opportunities and Challenges.....	30
The Challenge of China	30
Issues Affecting the EU.....	33
Barriers to Data Flows	35
Encryption	36
Developing a Comprehensive Digital Trade Strategy	37
Principles and Policies.....	39

CHAPTER V. CYBERCRIME AND LAW ENFORCEMENT 46

- Opportunities and Challenges46
- New Threats, New Defenses: The Internet Arms Race46
- Getting the Incentives Right: The Role of Cybersecurity Insurance.....49
- Empowering Global Internet Law Enforcement49
- CISA and the Need for Information Sharing..... 51
- Principles and Policies.....52

CHAPTER VI. CRITICAL INFRASTRUCTURE AND CYBER DEFENSE 57

- Opportunities and Challenges57
- Cyber Threats to National Security57
- Developing New Doctrines59
- Developing Norms of Conduct: The International Law of Cyberwar..... 60
- Defending Critical Infrastructure and Civilian Federal Agencies..... 61
- Principles and Policies.....63

CHAPTER VII. CONCLUSION AND SUMMARY OF FINDINGS 70

ABOUT THE AUTHORS..... 71

Foreword

By **Mike Daniels**, Chairman, National Advisory Board, AEI Global Internet Strategy Project

AEI's Global Internet Strategy (GIS) Project was conceived in 2014 with the goal of developing a comprehensive US strategy for the global Internet. The project is premised on the belief that the US must advance American ideals of personal freedom and human flourishing, protect our national security, promote global trade and commerce, and achieve the digital revolution's potential to improve human welfare on a global scale.

Why do we believe this? We know, first, that the Internet has brought and can continue to bring with it benefits almost beyond imagining. But we also know that the theft of intellectual property from US commercial firms is costing hundreds of billions of dollars per year; that theft of vital national security information and civilian records from the US government has reached crisis levels; that nation-states, criminal elements, and technology-savvy organizations have cyber operations targeting our nation around the clock; and that authoritarian governments are turning the promise of the Internet on its head by using it as a tool of censorship and oppression. We see no end in sight to these challenges as we move further into the global digital age. Without a coherent and comprehensive US strategy to address them, our nation is being picked apart piece by piece in the new digital world.

What have we learned? We have learned that experts, ordinary citizens, and those on the frontlines of the battle day and night are frustrated, are deeply concerned, and believe that what we are doing now is not working. We have learned that we need a different approach and we need it now.

To address these challenges, we have brought together experts, scholars, public officials, technologists, and business leaders to assess current policies, future challenges, and potential new strategies. Our ultimate

objective is to devise specific recommendations that together constitute a comprehensive, implementable strategy for current and future government leaders. This initial report represents the culmination of more than two years of that effort. A second report, refining the analysis and expanding on the recommendations, will be released in the months ahead.

We hope that this report and the rest of our work to follow will serve as a call to national action. The issues addressed in this project are at the heart of the sea change in our new and challenging digital world. The sooner we engage in a serious national debate about this range of issues, the better for all of us.

As the chairman of the GIS Project's National Advisory Board, I want to thank all the National Advisory Board members for their time and expertise. They are an extraordinary group. I want to give a special thanks to the report's authors—Jeff Eisenach (lead author), Claude Barfield, Jim Glassman, Mario Loyola, and Shane Tews—and to the staff of AEI's Center for Internet, Communications, and Technology Policy—Guro Ekrann, Matt Au, Evelyn Smith, and Tina Chao—for their hard work throughout this effort. I also want to express our gratitude to AEI's Sarah Crain and Claude Aubert, our editor and graphic designer, respectively, who went beyond the call of duty to help us finalize the report under tight deadlines. Without the fine work of these dedicated individuals, this report would not have seen the light of day. Finally, I want to acknowledge the contributions of the hundreds of experts who have been willing to share their thoughts, expertise, and time with us. We thank you!

June 14, 2016

About the Global Internet Strategy Project

The GIS project was launched two years ago with an inaugural conference, “After Snowden: The Road Ahead for Cybersecurity,” which was held at AEI on June 12, 2014.¹ Between that event and the end of 2014, we hosted two additional public events: “Who Governs the Internet? A Conversation on Securing the Multistakeholder Process” and “Government Surveillance: How Legal Intercept’s Tangled Web Impacts Trade, Economic Growth, and Civil Liberties.”² In January 2015, we held a conference titled “Tech Policy 2015: The Year Ahead,” which featured a keynote address from Senator John Thune (R-SD) and examined a variety of technology policy issues, including Internet governance and its effect on international trade, free speech, and property rights.³

In this timeframe, we also published two GIS-related papers: *US Government Surveillance Regulations for IT Company Networks: Toward a Global Framework* in December 2014 and *Internet Freedom in Vladimir Putin’s Russia: The Noose Tightens* in January 2015.⁴ In addition to holding public conferences, conducting research, and working on our publications, we began recruiting members of the advisory board.

From January to October 2015, we held a series of private working breakfasts and meetings as we began to identify the successes and shortcomings of current policies, looking for potential remedies and solutions. Some meetings were opportunities for AEI scholars to ask questions and gather feedback on policy proposals from thought leaders and members of the business and policy communities.

Several of these events featured members of our National Advisory Board. Other speakers and participants included Steve DelBianco (NetChoice), Andrea Glorioso (European Commission), Lani Kass (CACI), John Kneuer (National Telecommunications and

Information Administration), Christopher Painter (US Department of State), Ari Schwartz (Venable), and Christopher Walker (National Endowment for Democracy). We are grateful for their participation but emphasize that it does not imply an endorsement of the report or its recommendations.

In April 2015, we published a paper by Georgetown’s Theodore Moran titled *Cyber Surveillance Regulations: Is the United States Asking China to Accept a Double Standard?*⁵ That was followed by a pair of conferences on topics relevant to the GIS project: “The DOTCOM Act: A Roadmap for Congressional Oversight of the Internet Assigned Numbers Authority (IANA) Transition,” featuring a keynote from Rep. John Shimkus (R-IL), and “Domestic Surveillance on Foreign Shores: The Case of Microsoft’s Servers in Ireland.”⁶

In late October 2015, we held an invitation-only event, “America’s Strategy for Cyberspace: Is It Working?,” featuring a keynote address from Gen. Michael Hayden and panels moderated by AEI scholars.⁷ Our invited experts highlighted the ways that current policies were failing and offered ideas on what a future administration should do differently. In October, we also published a working paper from Claude Barfield titled “When Trade and Tech Collide,” in which Barfield conducted a detailed background analysis and made policy recommendations on issues in digital-trade policy.⁸

We opened 2016 with a half-day conference at AEI titled “Cyberspace Policy at Home and Abroad: The Agenda for 2016 and Beyond.”⁹ The conference featured a keynote address from Senator Ron Johnson (R-WI) and looked at issues in Internet policy that would be relevant in the year ahead, especially in cybersecurity, online freedom, Internet governance, and intellectual property.

We continued our working breakfast series in 2016 and have held dozens of meetings with more than 150 members of Congress, senior congressional staff, business leaders, government officials, and technology executives to seek input and discuss the project's findings and recommendations. We have held meetings with experts from the National War College, US Department of State Office of the Coordinator for Cyber Issues, Senate Republican Policy Committee, Senate Foreign Relations Committee, Senate Homeland Security and Governmental Affairs Committee, Senate Armed Services Committee, Senate Commerce, Science, and Transportation Committee, Senate Judiciary Committee, House Energy and Commerce Committee, House Homeland Security Committee, and various senior

personal staff members of leaders on cyber and Internet policy in Congress. Meetings with industry stakeholders have included briefings for the Edison Electric Institute and the Financial Services Roundtable.

In March 2016, AEI held a private dinner discussion on radical Islam and technological warfare, which was hosted by former US House Speaker Newt Gingrich and featured a presentation by the House Homeland Security Committee on the Apple/FBI controversy over encryption. That month, we also published another paper by Theodore Moran, *Surveillance Versus Privacy, with International Companies Caught in Between*.¹⁰ Most recently, we released a working paper by Ariel Rabkin and Jeremy Rabkin, "Enhancing Network Security: A Cyber Strategy for the Next Administration."¹¹

Notes

1. American Enterprise Institute, “After Snowden: The Road Ahead for Cybersecurity,” June 12, 2014, <https://www.aei.org/events/after-snowden-the-road-ahead-for-cybersecurity/>.
2. American Enterprise Institute, “Who Governs the Internet? A Conversation on Securing the Multistakeholder Process,” July 22, 2014, <http://www.aei.org/events/who-governs-the-internet-a-conversation-on-securing-the-multistakeholder-process/>; and American Enterprise Institute, “Government Surveillance: How Legal Intercept’s Tangled Web Impacts Trade, Economic Growth, and Civil Liberties,” December 10, 2014, <http://www.aei.org/events/government-surveillance-legal-intercepts-tangled-web-impacts-trade-economic-growth-civil-liberties/>.
3. American Enterprise Institute, “Tech Policy 2015: The Year Ahead,” January 28, 2015, <https://www.aei.org/events/tech-policy-2015-year-ahead/>.
4. Theodore H. Moran, *US Government Surveillance Regulations for IT Company Networks: Toward a Global Framework*, American Enterprise Institute, December 2014, <http://www.aei.org/publication/us-government-surveillance-regulations-for-it-company-networks-toward-a-global-framework/>; and Natalie Duffy, *Internet Freedom in Vladimir Putin’s Russia: The Noose Tightens*, American Enterprise Institute, January 2015, <http://www.aei.org/publication/internet-freedom-vladimir-putins-russia-noose-tightens/>.
5. Theodore H. Moran, *Cyber Surveillance Regulations: Is the United States Asking China to Accept a Double Standard?*, American Enterprise Institute, April 2015, <http://www.aei.org/publication/cyber-surveillance-regulations-is-the-united-states-asking-china-to-accept-a-double-standard/>.
6. American Enterprise Institute, “The DOTCOM Act: A Roadmap for Congressional Oversight of the Internet Assigned Numbers Authority (IANA) Transition,” July 29, 2015, <http://www.aei.org/events/the-dotcom-act-a-roadmap-for-congressional-oversight-of-the-internet-assigned-numbers-authority-iana-transition/>; and American Enterprise Institute, “Domestic Surveillance on Foreign Shores: The Case of Microsoft’s Servers in Ireland,” October 6, 2015, <http://www.aei.org/events/domestic-surveillance-on-foreign-shores-the-case-of-microsofts-servers-in-ireland/>.
7. American Enterprise Institute, “America’s Strategy for Cyberspace: Is It Working?,” October 27, 2015, <http://www.aei.org/events/americas-strategy-for-cyberspace-is-it-working/>.
8. Claude Barfield, “When Trade and Tech Collide” (working paper, American Enterprise Institute, October 2015), <https://www.aei.org/wp-content/uploads/2015/10/When-trade-and-tech-collide-Barfield-FINAL-not-embargoed.pdf>.
9. American Enterprise Institute, “Cyberspace Policy at Home and Abroad: The Agenda for 2016 and Beyond,” January 28, 2016, <https://www.aei.org/events/cyberspace-policy-at-home-and-abroad-the-agenda-for-2016-and-beyond/>.
10. Theodore H. Moran, *Surveillance Versus Privacy, with International Companies Caught in Between*, American Enterprise Institute, March 2016, <http://www.aei.org/wp-content/uploads/2016/03/Surveillance-versus-privacy.pdf>.
11. Ariel Rabkin and Jeremy Rabkin, “Enhancing Network Security: A Cyber Strategy for the Next Administration” (working paper, American Enterprise Institute, May 2016), <http://www.aei.org/wp-content/uploads/2016/05/Enhancing-network-security.pdf>.

Global Internet Strategy Project National Advisory Board

Mike Daniels, Chairman (Chairman, Logistics Management Institute)

Richard Andres (Professor of National Security Strategy, National War College)

Rebecca Arbogast (Senior Vice President for Global Public Policy, Comcast Corporation)

Richard Bejtlich (Chief Security Strategist, FireEye)

Teresa Carlson (Vice President, Worldwide Public Sector, Amazon Web Services)

Scott Carpenter (Managing Director, Jigsaw)

John Chen (CEO, Blackberry)

Robert Dix (Vice President, Government Affairs and Critical Infrastructure Protection, Juniper Networks)

Karen Evans (National Director, US Cyber Challenge)

Anup Ghosh (Founder and CEO, Invincea)

David Gross (Partner, Wiley Rein LLP)

Michael Hayden (Principal, The Chertoff Group)

Rhett Hernandez (President, CyberLens LLC)

Tom Kuhn (President, Edison Electric Institute)

Dominique Lazanski (Public Policy Director, GSM Association)

Jack London (Executive Chairman and Chairman of the Board, CACI International)

Kevin Martin (Vice President, Mobile and Global Access Policy, Facebook)

Matthew McCabe (Senior Vice President, Marsh FINPRO)

Bryan Palma (Senior Vice President, Cisco Systems)

Jeremy Rabkin (Professor, George Mason University School of Law)

Gary Shapiro (President and CEO, Consumer Technology Association)

Craig Silliman (Executive Vice President, Public Policy and General Counsel, Verizon Communications)

Jody Westby (CEO, Global Cyber Risk LLC)

Note: Members of the National Advisory Board participate in this project in their individual capacities. The views expressed in the project's reports and activities are those of the authors. They do not necessarily represent the views of the advisory board members, the institutions with which they are affiliated, the American Enterprise Institute, or any of its affiliates. AEI is a non-partisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues.

Executive Summary

Success in cyberspace is essential to advancing America's national interests. Digital technologies determine how many of the processes that define modern societies operate, from communications to finance, electricity to transportation, espionage to national defense. The ability to control how these technologies are used in the present—and to influence the course of their development in the future—is a vital element of national power. This report puts forward a comprehensive strategy for ensuring that the Internet continues to promote America's national interests by advancing its ideals—freedom, security, and prosperity.

The report begins from a recognition that, while the US invented and pioneered the Internet, today's cyberspace is truly global. Fewer than 1 out of 10 of the world's three billion Internet users live in the US, while nearly a quarter live in China. The global nature of cyberspace means that America cannot isolate itself from the global Internet nor expect to dictate unilaterally the policies and practices that govern its use and future development. However, it can and must use its influence and power to ensure the Internet remains a force for good in the world. To be successful, it needs a comprehensive strategy.

The task of devising such a strategy is complicated by the all-encompassing nature of cyberspace, which permeates every element of modern societies. This report deals with this challenge by focusing on four broad sets of policy objectives: (1) Internet freedom and human rights, (2) international trade and digital commerce, (3) cybercrime and law enforcement, and (4) critical infrastructure and cyber defense.

We begin by assessing the state of affairs in each area, and our findings are not encouraging. For example:

- Online freedom, as measured by Freedom House, has declined for five years running. More than half of the world's online population now lives in countries that significantly constrain online freedom;

more than a third live in authoritarian states such as China, Iran, and Russia, where Internet technologies increasingly are used as a tool of oppression and control.

- Digital commerce is threatened by the failure to agree on and enforce international norms for intellectual property, digital trade, and international data flows. Chinese digital mercantilism—including the theft of intellectual property and aggressive discrimination against US firms—seems aimed at creating a separate, and very large, Internet ecosystem.
- Cybercrime and malicious conduct continues to rise as cyber criminals devise new technologies and techniques (e.g., “ransomware”); the overall costs are projected to reach \$2 trillion by 2019. Efforts to reduce cybercrime are hampered by the global nature of cyberspace and the absence of adequate mechanisms and institutions for global cooperation by law enforcement.
- America's critical infrastructure is currently vulnerable to potentially devastating attacks by both nation-state and nonstate actors. Indeed, cyberattacks have already been used to severely harm major companies, such as Aramco and Sony, and critical infrastructure and communications in Estonia, Ukraine, and elsewhere. The US agencies charged with defending critical infrastructure do not have sufficient capacity to do so, and the agencies that have the capacity do not have the authority.

To address these challenges, the report puts forward a strategic plan grounded in the realities of cyberspace itself, including the rapid pace of change; the importance of economies of scale and scope; the extent to

which it is integrated into modern economies, cultures, and political structures; and its inherently global nature. Like our analysis, our recommendations are organized into four areas:

Internet Freedom and Human Rights. Acknowledge the real and immediate threat that authoritarian states' use of cyber technologies poses to human freedom. Take strong and effective actions to promote the values of liberal democracy in cyberspace.

- Use all elements of US diplomatic and economic policy to discourage autocratic states from censorship and oppression.
- Significantly expand US social media and other digital communication efforts to effectively communicate and promote fundamental online freedoms.
- Formalize, expand, and strengthen the Freedom Online Coalition.
- Promote increased Internet access through market-oriented policies.
- Strengthen civil society groups' role in studying and promoting online freedom.
- Expand, intensify, and support both public and private participation in international forums where Internet policies are set.
- Vigorously promote and defend the multistakeholder model of Internet governance.

International Trade and Digital Commerce. Recognize that America's commercial success in the Internet ecosystem has been a source of tremendous strategic advantage and that preserving a level playing field for digital trade—one that fosters competition—is a vital American national interest.

- Develop and execute a comprehensive, “full-court press” strategy designed to change China's conduct regarding digital trade and IP theft.

- Take effective concrete actions against cyber theft.
- Make clear that the US would retaliate against overly aggressive implementation of the Chinese National Security Law.
- Prosecute Chinese censorship through the WTO.
- Aggressively seek to negotiate a multilateral agreement (i.e., the TTIP) with the European Union that embodies the principles of the TPP and resolves current sources of friction, including data shield and the right to be forgotten.
- Incorporate protections against state participation in cyber theft in multilateral agreements.
- Promote reduced regulation of Internet firms and of the Internet.
- Continue developing and aggressively promoting a digital-trade policy.
- Do not require US firms to create backdoors in encrypted software and communications.
- Strengthen digital-trade priorities in multilateral trade agreements.
- Ensure that export controls under US law and under the multilateral Wassenaar Arrangement do not unnecessarily place US companies at a competitive disadvantage.

Cybercrime and Law Enforcement. Create the private incentives and public capabilities needed to effectively fight cybercrime and commercial hacking, including the capacity to engage in enforcement actions throughout cyberspace—that is, globally.

- Ensure that the private sector has the right incentives to protect itself.
- Empower the private sector to more effectively defend itself.

- More actively use government capabilities to defend the private sector.
- Strengthen international law enforcement cooperation against cybercrime.
- Create an enduring framework for public-private partnership.

Critical Infrastructure and Cyber Defense. Embrace the concept of cyber as a new domain for the projection of power and put in place the doctrines, capabilities, and resources necessary to protect our military, governmental, and critical civilian infrastructure assets.

- Develop and implement a coherent doctrine on the use of military force to deter, preempt, prevent, and retaliate against malicious activity by sovereign and non-sovereign actors.
- Deploy existing US cyber-defense capabilities to proactively defend civilian government agencies and critical infrastructure. Consider creating a Federal Cybersecurity Service to engage in real-time defensive operations.

- Increase the capacity and give greater priority to US intelligence agencies' efforts to gather actionable tactical and strategic intelligence on cyber threats to government and crucial private assets.
- Strengthen existing institutions and norms—and, where necessary, develop new institutions—to empower law-abiding governments to act against cyber threats.
- Prioritize maintaining the preeminent position of American and Western companies in the Internet ecosystem.

While we believe the challenges facing America in cyberspace are significant and demand a far more proactive and strategic response than is embodied in current policies, we are also optimistic about the future of digital technologies and their potential to improve the human condition. The challenge is to ensure that the digital revolution continues to develop in a way that respects and promotes American—and universal—ideals of individual liberty and human rights.

I. Introduction

The digital technologies we colloquially refer to as “the Internet” are deeply embedded in virtually every aspect of modern society. They define how we make things; how we trade goods and store wealth; how we organize our institutions and our lives; how we learn, communicate, and interact; and increasingly, how we fight wars. The space (or “domain”) in which digital information processing and communications take place has earned a name: “cyberspace”—or sometimes just “cyber.”

Because many of the technologies that make up the Internet were initially invented and exploited by the United States and other advanced, mostly Western countries, we—especially Americans—tend to think of cyber as primarily an American domain, enabled mainly by Western companies (for example, Amazon, Apple, Facebook, Google, and Microsoft) and defined mainly by democratic values. Indeed, the Internet’s rise has advanced America’s national interests by promoting freedom, democracy, and entrepreneurial capitalism, thus improving the human condition on a global scale.¹ It has also, as the White House put it in a recent report, “provided a strategic advantage to the United States, its citizens, and its allies.”²

The potential for continued Internet-driven progress is virtually unlimited—but it is also increasingly clear that the shape of the digital revolution is changing, and the change brings with it both challenges and opportunities.

First, thanks in part to the explosive growth of the mobile Internet in the developing world, the Internet has become a truly global phenomenon. As illustrated in Figure 1, more than three billion people are now connected, of whom fewer than 10 percent are Americans and nearly a quarter are Chinese.

Similarly, while American companies play a leading role in the economics of the global digital ecosystem—and ensuring that they continue to do so should be among the US government’s highest strategic

priorities—we should not assume that their current level of preeminence will persist indefinitely.

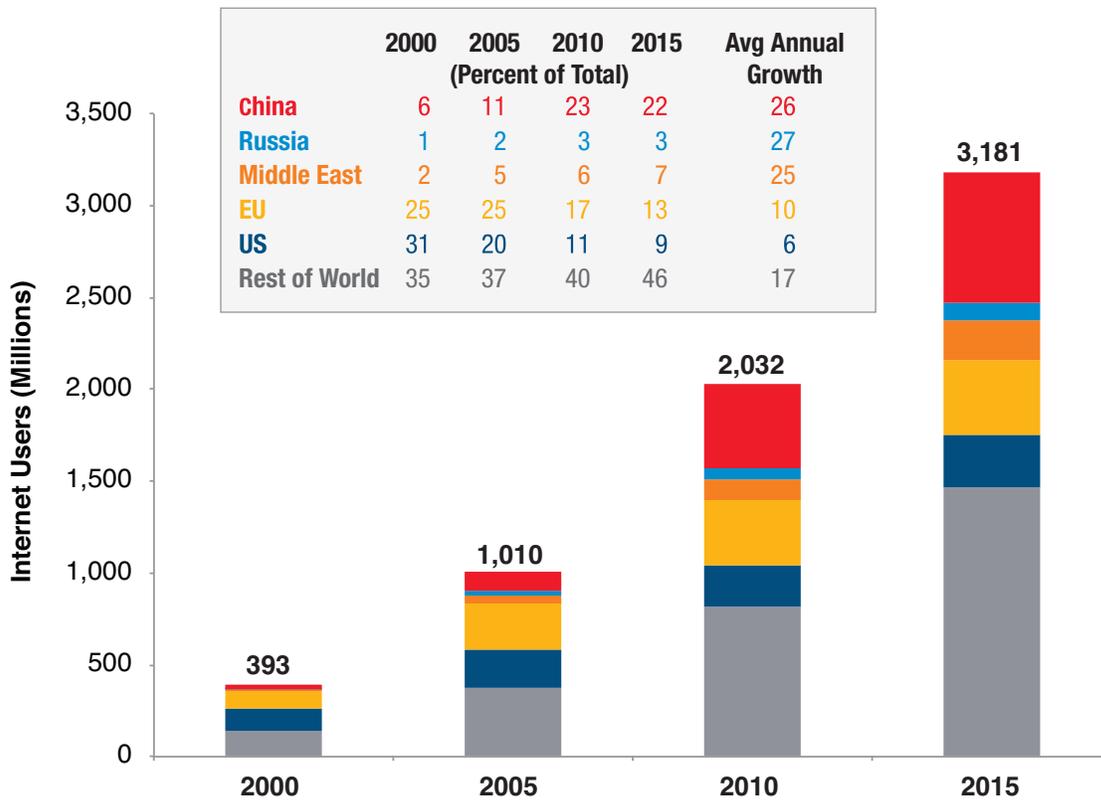
It has also become increasingly clear in recent years that digital technologies have costs as well as benefits. Among the most significant challenges are that authoritarian states have learned to use the Internet to repress political freedoms, that criminals (and sometimes nation-states) have learned to use it to steal property and commit extortion, and that America’s adversaries and potential adversaries have developed the ability to use malicious code and cyber warfare to threaten our economic and national security interests. America and its allies are still searching for effective responses to these developments.³

In this context, this report puts forward a comprehensive strategy for ensuring that the Internet continues to serve America’s national interests by promoting freedom, prosperity, and security on a global scale. It is premised on the belief that America cannot isolate itself from the global Internet nor expect to dictate unilaterally the policies and practices that govern its use and future development, but that it can and must effectively utilize its influence and power to ensure the Internet remains a force for good in the world. This report is also premised on the belief that, while our present policies are well intended, they have not been sufficiently effective in achieving our key national objectives; that much has been lost as a result; and that more can and must be done.

The report puts forward both an overall strategic framework and a specific set of policy proposals designed to be implemented starting in 2017. The proposals include significant changes in US international policies and doctrines, recommendations to strengthen or create new international agreements and institutions, and changes in the organization of the US government itself.

One challenge to such an effort is the scope of issues involved: cyber is everywhere in our lives and permeates every element of our societies. This report deals with

Figure 1. Global Distribution of Internet Users, 2000–15



Source: Internet Live Stats, “Internet Users by Country (2016),” accessed June 2, 2016, <http://www.internetlivestats.com/internet-users-by-country/>.

this challenge by focusing on four broad sets of policy objectives:

- **Internet Freedom and Human Rights.** Protecting and promoting the rights to freedom of expression and access to information, and working to ensure that governance of the Internet itself remains free of control by authoritarian governments.
- **International Trade and Digital Commerce.** Reducing barriers to electronic commerce, while protecting property rights and the ability to make and enforce contracts in the digital economy.
- **Cybercrime and Law Enforcement.** Protecting and promoting trust in the commercial Internet through effective data security policies, and putting in place effective incentives and enforcement mechanisms to reduce the effects of malware and deter criminal activity.
- **Critical Infrastructure and Cyber Defense.** Protecting America’s vital national interests, including enhancing our ability to protect vital assets, such as critical infrastructure and civilian government agencies, from cyberattacks from both state and nonstate actors.

Of course, the overlap among these four areas is extensive. When authoritarian nations prevent Western companies such as Facebook or Google from operating inside their borders, the effect is to diminish Internet freedom and—at least potentially—violate international trade agreements. When foreign gangsters acquire the capacity to hack into financial institutions, the immediate consequences may be limited to manageable financial losses, but the ultimate effects is to increase the threat of more serious attacks with devastating consequences.

The report acknowledges the most important of these overlaps explicitly, but the reader should keep in mind that it is meant to be read holistically—that is, with the recognition that everything is in some sense related to everything else. The reader should also recognize that the report focuses on issues the authors believe are most central to devising and executing a successful strategy and is not presented as a comprehensive survey of the entire cyber-policy landscape.⁴

The remainder of this report is organized as follows. Chapter II presents a set of broad strategic principles for thinking about, designing, and executing a successful American cyberspace policy. One central conclusion is that the issues that comprise global Internet policy will have a profound effect not just on America's success but on the principles, ideals, and institutions that govern the future of human civilization. Another

important conclusion is that America's greatest asset in the global digital ecosystem is its entrepreneurial and innovative private sector—and the relatively market-oriented policies that have supported it—and accordingly that the private sector, not the government, must lead.

Chapters III–VI deal, respectively, with Internet freedom, digital trade, cybercrime and law enforcement, and critical infrastructure and cyber defense. A complete summary of the analysis, findings, and recommendations in each chapter would be out of place in this introduction, but broadly speaking, the report finds that America's national interests in each area are not well served by current institutions and policies; that Internet freedom is waning with the spread of adaptive authoritarianism; that barriers to trade in digital goods and services are limiting the Internet's ability to raise standards of living and improve lives; that the costs and consequences of malicious and criminal conduct on the commercial Internet are increasing; and that America is currently vulnerable to potentially devastating cyberattacks from a variety of state and nonstate actors. The report also finds that these circumstances are susceptible to remediation through the adoption of sound policies, and each chapter puts forward specific policy recommendations. Chapter VII briefly summarizes the report's findings and recommendations.

Notes

1. One seminal work on the impact of information technology on political change is Ithiel de Sola Pool, *Technologies of Freedom* (Belknap Press, 1983).
2. White House, “Fact Sheet: Cybersecurity National Action Plan,” press release, February 9, 2016, <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.
3. See, for example, Christopher Walker, “The West’s Failure of Imagination,” *Wall Street Journal*, August 3, 2015.
4. It is worth noting three specific areas that lie outside the report’s main focus. First, because the effort here is to put forward a global strategy, the report focuses on issues whose effects extend beyond the sovereign borders of nation-states. This is not to say that national policies cannot affect global outcomes—they obviously can and do—but rather that the focus here is on the policies that do have such effects, not on those with mainly or exclusively domestic implications. Second, while the report addresses issues of national security and cyber defense from the perspectives of strategy, diplomacy, and institutional design, it does not delve into the tactical and technological issues of how to fight and win a cyber war. The US military appears to be making substantial strides in developing the doctrines and capacities necessary to fight and win in cyberspace. See US Department of Defense, *The Department of Defense Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. Third, this report does not discuss in any detail strategies for countering the use of social networks and other online communication tools by terrorist networks such as ISIS.

II. Creating a Strategic Framework for US Cyber Policy

The ultimate goal of US cyberspace policy is to ensure that the Internet continues to serve America's national interests by promoting freedom, prosperity, and security on a global scale, including and especially for the US and its citizens.¹

The Nature of the Challenge

Achieving our strategic objectives requires understanding cyberspace's role in the modern world, and that is no small task. The Internet permeates every aspect of modern life, shaping culture, communications, economies, and politics on a global scale. Like the natural world we take for granted, its properties define what is possible and what is not; they determine *how things work*. Internet-enabled technologies run power plants and aircraft carriers, conduct financial transactions, perform medical procedures, monitor nurseries (both kinds), and fly drones. Soon they will be driving cars. To control the technology is to control these activities, for better or worse.

The Internet has also become the dominant medium through which we communicate ideas, both individually and socially. A fundamental premise of liberal democracy is that the freedom to communicate is essential to liberty; conversely, the power to control communication carries with it the ability to affect what people believe and how society is organized. The upshot is that the future shape of cyberspace will profoundly affect political systems everywhere—and authoritarian states such as China and Russia know it.

While cyberspace is like the natural world in some respects, there are profound differences. First, because of its interoperable design and nearly ubiquitous presence, the Internet enables both communication *and effect* across territorial borders. By weakening the

relationship between geography and cause and effect, it creates a new form of global interdependence.

Second, far more than the physical world, the Internet is elastic, constantly shifting and evolving—malleable. Cyberspace is what humans make it. We are making and remaking it at a dizzying pace, and because no nation monopolizes the ability to write computer code or (increasingly) manufacture Internet-connected devices, the process of creation is also global.

These characteristics of cyberspace—its borderless nature and its dynamism—work together to complicate the strategic challenge. Because of the Internet's dynamism, it is not sufficient to comprehend our objectives in the current environment and devise ways of achieving them. An effective strategy must also seek to shape what cyberspace is *becoming*. And what it is becoming will be determined globally—whether we like it or not—in an environment where our adversaries also get a vote.

Three further characteristics of cyberspace are central to understanding the strategic challenge. First, cyberspace is primarily a creature of the private sector—and its future development depends on it remaining so. Governments have contributed to the Internet's development—most obviously through early US funding through the Defense Advanced Research Projects Agency (DARPA)—but the pace of the entrepreneurship and innovation that have characterized its growth are beyond most government organizations' capacity. For the US, with its entrepreneurial culture and market-oriented economy—and a substantial first-mover advantage that makes America home to the world's most successful Internet companies—the Internet's private-sector-centric nature is a strategic advantage.

Second, the Internet's future will be determined largely by its underlying economic characteristics,

including strong economies of scale and scope, network effects, and what economists refer to as “modularity.”² These characteristics imply that larger ecosystems tend to prevail over smaller ones, not only in their ability to win participants and earn revenues, but also in influencing the course of innovation and standards development. The ability to interconnect—to reach the largest possible audience—is crucial to success on the Internet.³

For most of the Internet’s brief history, these economic characteristics have worked in America’s favor. As more of the world comes online—Americans today account for less than 10 percent of the online population—the balance is shifting. If the American-led Internet ecosystem that defines cyberspace today were to become smaller than some alternative model, America could find itself a victim of what economists refer to as tipping: the sudden shift from one dominant standard to another.⁴ Like Betamax versus VHS or Blackberry versus iPhone, America could find itself on the losing end of a standards war.⁵

A third characteristic—somewhat paradoxically—is that the Internet empowers individuals and small groups: anyone with a PC or a smartphone can participate as a user, and anyone capable of writing a few lines of code can affect how it functions. This characteristic has unleashed a torrent of innovation and entrepreneurship, creating new products and services that have enriched human lives worldwide. It has also enabled cyber criminals and empowered malicious actors. At the extreme, cyberspace creates the potential for the most radical form of asymmetric warfare yet: the ability to disrupt or shut down an electric grid, a financial system, or an aircraft carrier with nothing more than a laptop computer, an Internet connection, and a few lines of computer code.

Elements of a Strategic Framework

Seven key elements of a US global Internet strategy emerge from the goals and characteristics we have described.⁶

First, it is appropriate, as US military doctrine has lately accepted, to recognize that cyber has emerged as a new domain, comparable in significance to land, sea, air, and space. While the analogies have important

limitations, as a simple matter of priorities, America’s future success clearly is as dependent on its ability to prosper and prevail in cyberspace as on, say, freedom of navigation or air superiority.

Second, just as the US pursues its objectives in other domains using all elements of national influence and power—gathering intelligence, negotiating treaties, imposing sanctions, exercising soft power, engaging in persuasion and communication, and preparing to use force and where necessary doing so—a successful strategy will employ all the tools at our disposal.

Third, prevailing in the cyber domain will often require that the private sector, not the government, takes the lead. If entrepreneurs and innovators continue to define the future of the Internet, American interests and ideals will be well served. In doctrinal terms, that means government must frequently embrace a supporting rather than a leading role. In practical terms, it translates into curbing domestic impediments—regulatory and otherwise—to private-sector innovation and also bringing diplomacy and power to bear when US firms are discriminated against in foreign markets. In time it could also mean giving the private sector more freedom to act in its own defense.

Fourth, government has an essential role to play in protecting and promoting US interests in cyberspace. Much has been written about the desirability of establishing norms of international conduct, and some progress has been made in this regard. But for norms to be taken seriously, they need to be backed by the threat of enforcement. The Department of Defense (DOD) indicated in 2015 that America would respond to acts that threaten “loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States.”⁷ The North Korean attack on Sony North America suggests the kind of circumstances in which American cyber combat power might be used to deter, disarm, or retaliate against a renegade state or other cyber actor in the future.

Fifth, the Internet’s borderless nature and capacity for empowering cybercrime and enabling threats to critical infrastructure by both nation-states and non-state actors challenge traditional law enforcement mechanisms and national security doctrines. In particular, while deterrence will continue to be an important

element of cyber-defense strategy, particularly against traditional state actors, the asymmetric nature of cyber-crime and cyber warfare requires that we be able to identify and disrupt imminent threats before they can cause significant harm.⁸

Sixth, an American strategy for cyberspace must reflect and serve our ideals. In our zeal to secure the Internet, we must be careful not to destroy that which we are trying to preserve: an open, accessible, ubiquitous, egalitarian, and free World Wide Web. Our adversaries view these attributes of cyberspace not as virtues but as threats—the threat of the free movement of ideas. We must take care in our efforts to prevent cyber-enabled crime and terrorism that we do not legitimize our adversaries' efforts to censor and control. While strong encryption, for example, makes life more

difficult for the legitimate surveillance needs of law enforcement and intelligence agencies, it also serves the public—including dissidents in oppressive states—by protecting personal and business information from being exploited.

Seventh, in a democracy, the ability to successfully pursue and execute any long-run strategy requires a consensus on basic principles, and that must be the product of a meaningful national discussion. In previous eras, our political leaders have led discussions and created consensus around how US responses to strategic challenges, whether from Soviet communism or radical Islamic terrorism. A central challenge for the next administration is to lead a national discussion about how America can best serve its ideals and advance its interests in cyberspace.

Notes

1. This is not a controversial objective. See, for example, White House, *An International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, May 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. For a relatively early effort to define America's national interests regarding cyberspace, see Graham Allison and Robert Blackwill, *America's National Interests*, Commission on America's National Interests, July 2000, 48–50, <http://belfercenter.ksg.harvard.edu/files/amernatinter.pdf>.
2. See Jeffrey A. Eisenach, *Broadband Competition in the Internet Ecosystem*, American Enterprise Institute, October 18, 2012, <https://www.aei.org/publication/broadband-competition-in-the-internet-ecosystem/>.
3. The potential for private actors to deny interconnection for anticompetitive purposes has been the source of much study and controversy, including the Microsoft antitrust trials of the 1990s and early 2000s and the two-decades-old net neutrality regulatory debate. At the level of global strategy, government conduct—such as China excluding US Internet platforms such as Facebook and Google—is of far greater concern.
4. See Jeffrey H. Rohlfs, *Bandwagon Effects in High-Technology Industries* (Cambridge, Massachusetts: MIT Press, 2003).
5. One sign of this: Huawei is now the world's third-largest manufacturer of smartphones, with a market share of more than 8 percent, trailing only Apple and Samsung. In the first quarter of 2016, its smartphone sales rose by 50 percent from the prior year, while Samsung sales were flat and Apple's actually declined. See Wade Shepard, "China's Huawei 'Growing Up' to Become the World's No. 1 Smartphone Brand," *Forbes*, May 25, 2016, <http://www.forbes.com/sites/wadeshepard/2016/05/25/chinas-huawei-growing-up-to-become-the-worlds-number-one-smartphone-brand/#26of637e589a>.
6. Portions of this section are drawn from Michael Hayden, "An American Strategy for the Internet and Cybersecurity," *Real Clear Defense*, October 26, 2016, www.realcleardefense.com/articles/2015/10/26/an_american_strategy_for_the_internet_and_cybersecurity_108615.html.
7. US Department of Defense, *The Department of Defense Cyber Strategy*, 5.
8. In this report, the phrase "imminent threat" is used broadly to describe cyber threats that have the potential to cause significant economic disruption or loss of life or to otherwise harm vital US interests. Because of the nature of cyberspace, cyber threats are often inherently more immediate, or "imminent," than kinetic ones.

III. Internet Freedom and Human Rights

Just 20 years ago, the Internet was available to a small fraction of the world's population. Today, more than three billion people have Internet access, and more than five billion people have mobile phones.¹ The digital revolution has brought opportunity and connectivity to virtually every corner of the world.

Despite—or perhaps because of—this success, Internet freedom globally is under assault. Authoritarian governments have come to see the Internet as a tool of political control and the Internet ecosystem as something that government must shape to promote “social norms” that subordinate the individual to the state. Operating under the banner of cyber sovereignty, they have sought to legitimize their repressive practices in international forums such as the United Nations.² Online freedom is waning.

Western governments have been slow to respond to these trends. While diplomatic efforts have yielded repeated affirmations of central principles of free expression and access to information, such declarations have not, by and large, been matched by effective actions. And in the battle over Internet governance, the US has found itself playing defense against authoritarian states' efforts to subject the Internet to political control under the auspices of the United Nations.

Opportunities and Challenges

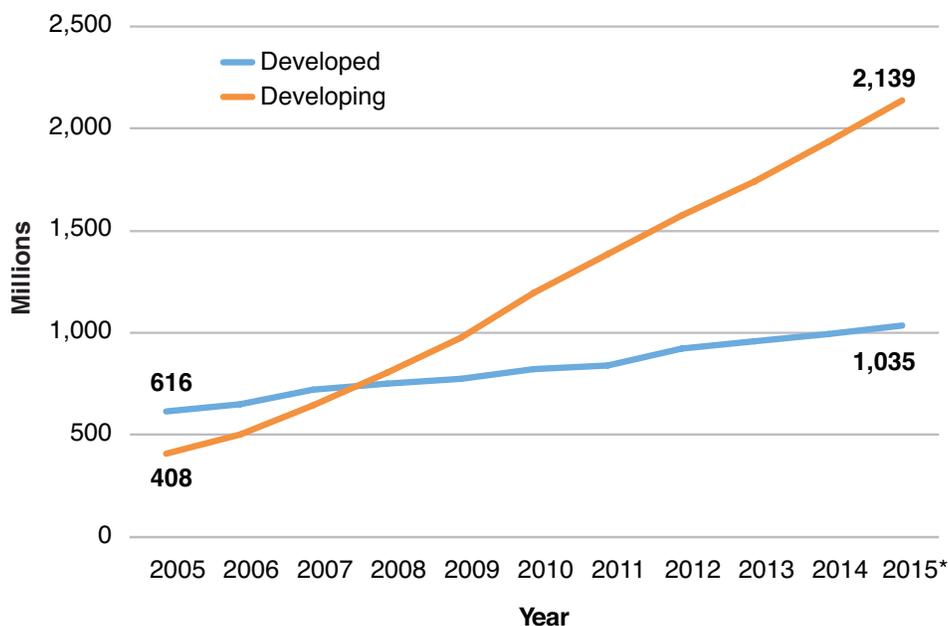
The opportunities inherent in the spread of the Internet—access to information, freedom of discourse and communication, the ability to participate effectively in civic affairs and to engage politically, and of course, the tremendous opportunities for improving the human condition through entrepreneurship and innovation—are only beginning to be realized. Especially in

the developing world, the potential for improving governance and increasing the standard of living is just beginning to be exploited. In the following discussion, we highlight some key challenges to realizing these benefits, including authoritarian governments' use of cyber as a tool of repression, the effort to replace the multistakeholder model of Internet governance with a government-centric model, and the difficulties private companies encounter when faced with demands to collaborate with repressive practices.

The Internet as an Engine of Freedom and Prosperity. While Internet adoption began in the US and initially spread to other developed countries, the number of users in developing countries surpassed that of the developed world in 2008, and two-thirds of today's three billion Internet users now reside in the developing world. (See Figure 2.) The spread of the Internet to the developing world has helped spur both economic development and desires for political liberalization.

The economic benefits of widespread Internet access have been profound.³ In Africa, McKinsey Global Institute estimates that the Internet will account for as much as 10 percent of the continent's gross domestic product (GDP) by 2025, generating \$318 billion in productivity gains.⁴ Sub-Saharan Africa has become a hotbed of Internet innovation, highlighted by the well-publicized success of the M-Pesa mobile money app and the lesser-known success of Ushahidi, a widely used crowdsourcing app developed in Kenya and based in Nairobi.⁵ Venture capital funding for high-tech startups increased tenfold between 2012 and 2014, to more than \$400 million.⁶

Sub-Saharan communities now have access to mobile financial services that enable economic growth, mobile literacy and job-training programs, and mobile medical

Figure 2. Internet Users in Developed Versus Developing Countries, 2005–15

Source: International Telecommunications Union, “ICT Facts and Figures—The World in 2015,” 2015, <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>.

Note: The * denotes an estimate.

services that help identify counterfeit medicines and disseminate health information.⁷ Similarly, in rural regions in South India, Internet access has empowered farmers with information to better guard crops against disease and track market values in real time, leading to higher and more stable incomes.⁸

The Internet’s contribution to fostering democratic yearnings and enabling dissent against repressive regimes is well documented, although not uncontroversial.⁹ While the ultimate effects of Internet-assisted uprisings against authoritarian regimes have been mixed or even tragic, the ability to communicate online has unquestionably fostered political dissent. One recent Pew poll found that majorities in most countries now expect to be able to access the Internet free of government censorship.¹⁰ Polling data also show a high correlation between expanded Internet access and the popular desire for Internet freedom.¹¹

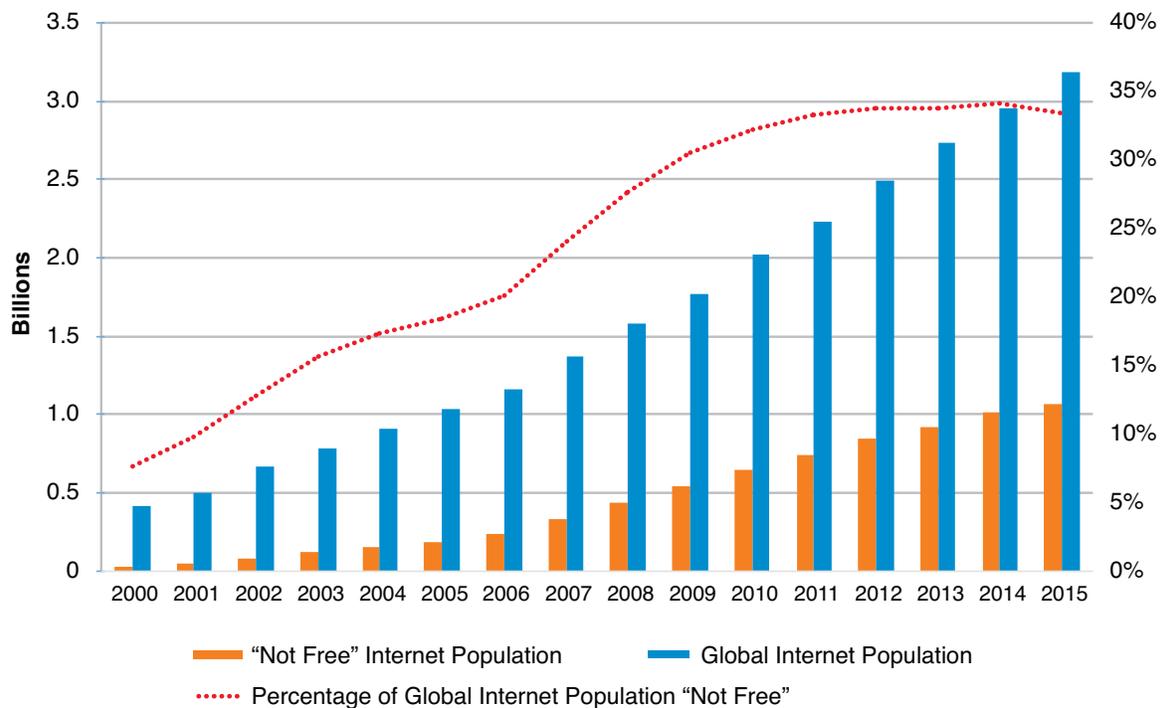
The explosive growth of Internet penetration is far from over: as smartphone penetration grows, mobile Internet adoption is projected to reach 71 percent in

2019, implying an online population of more than five billion people.¹²

The Authoritarian Challenge to Internet Freedom and the US Response. Fifteen years ago, nearly all those with Internet access lived in free, democratic countries. Since then, access has spread to countries with more authoritarian regimes—and authoritarian regimes have become more effective in repressing online freedom.

Freedom House has been tracking specific indicators of online freedom for a large group of countries since 2011. Its latest report, *Freedom on the Net 2015*, finds that overall Internet freedom declined for a fifth consecutive year and that more than a third of all Internet users now reside in “not free” countries—those with the most extreme forms of online repression, such as China, Iran, and Russia (Figure 3).

Indeed, Freedom House finds that *most* people with Internet access now live in countries where online freedom is at least partially suppressed.¹³ Specifically:

Figure 3. Internet Users Living Under Selected Authoritarian Regimes, 2000–15

Sources: Freedom House, "Freedom on the Net 2015," 2015, <https://freedomhouse.org/report/freedom-net/freedom-net-2015>; and Internet Live Stats, "Internet Users by Country," <http://www.internetlivestats.com/internet-users-by-country/>.

Note: "'Not Free' Internet population" based on 19 countries classified by Freedom House as "not free" in 2015; online populations for 2000–15 are from Internet Live Stats.

- About 60 percent of Internet users live in countries where criticism of the government, military, or ruling family is subject to censorship; more than half live in countries that heavily censor, filter, and monitor the Internet; and about half live in countries where people have been attacked or killed for their online activities, or where Internet users have been imprisoned for political, social, or religious commentary.
- Authorities in 42 of the 65 countries analyzed in 2015 required private companies or Internet users to restrict or delete web content dealing with political, religious, or social issues during 2015, up from 37 countries in 2014.¹⁴
- Surveillance laws and technologies have multiplied. Governments in 14 of the 65 countries examined by Freedom House passed new laws to increase surveillance, and many more have upgraded their surveillance capabilities. Authorities in 40 countries have imprisoned people for sharing information concerning politics, religion, or society through digital networks.¹⁵

Distinguishing between the methods of censorship and surveillance and the kinds of speech that have been censored is important. Many governments censor speech of a political, social, or religious nature in line with cultural norms. For example, most countries ban online gambling and consider child pornography on the Internet to be a criminal offense. In South Korea,

criticism of government policy is permitted and widely practiced, but insulting public officials is subject to prosecution. The most serious threats to political freedom result from censorship of political opposition, satire, or social commentary—that is, of civic discourse. As Freedom House concludes, “Fearing the power of the new technologies, authoritarian states have devised subtle and not-so-subtle ways to filter, monitor, and otherwise obstruct or manipulate the openness of the Internet.”¹⁶

Internet service providers (ISPs) and other online service providers are often called on to facilitate censorship. Faced with the choice between blocking whole websites and ISPs and giving up control altogether, repressive regimes have opted instead to target the middleman. They have passed laws restricting content, often imposing liability on intermediaries to force them to censor themselves or face onerous penalties.¹⁷

China and other countries have increasingly restricted foreign companies’ ability to provide Internet services inside their borders, ensuring that they can exercise full control over providers. Google, Facebook, Twitter, and YouTube are completely blocked in China. Other American companies, such as Yahoo, do business there under severe restrictions. For instance, in February 2015, China required users of blogs, microblogs, instant messaging services, discussion forums, news comment sections, and related services to register with their real names.¹⁸ New rules also prohibit foreign companies from publishing online content without government permission.¹⁹ In April 2016, Chinese regulators forced Apple to completely suspend offering its iBooks and iTunes movie services.²⁰

Russia has enacted a flurry of laws designed to expand government control and surveillance of the Internet, while restricting its use and limiting online privacy.²¹ Its so-called “Blacklist Law,” enacted in July 2012, has been used to block thousands of websites the Russian government considers offensive, with virtually no due process.²²

Censorship techniques have also begun to evolve rapidly, becoming better designed and more precisely targeted, using techniques scholars have aptly labeled “adaptive authoritarianism.” As the *Economist* explained, “The Internet requires the party centre to be more efficient at being authoritarian. This is the online blueprint

for what scholars call ‘adaptive authoritarianism’, and there is an international market for it.”²³ It means that governments have moved from rudimentary blocking techniques, such as keyword-list blocking, domain-name poisoning, IP blocking, and bandwidth throttling, to more sophisticated blocking techniques, such as traffic classification and deep packet inspection.²⁴ China has selectively applied its censorship laws to messages that get more than 500 reposts or 5,000 views.²⁵

These sophisticated techniques allow repressive governments to permit broad access to online information for many citizens, relying on surveillance to detect, detain, and punish dissidents. Repressive regimes have targeted individuals, threatening their civil liberties and economic interests for publishing offensive content. As Ron Diebert explains:

Second generation controls include finer-grained registration and identification requirements that tie people to specific accounts or devices, or even require citizens to obtain government permission before using the Internet. Pakistan has outlawed the sale of prepaid SIM cards and demands that all citizens register their SIM cards using biometric identification technology. . . . China has imposed real-time name registration on Internet and social media accounts, and companies have dutifully deleted tens of thousands of accounts that could not be authenticated. Chinese users must also commit to respect the seven “baselines,” including “laws and regulations, the Socialist system, the national interest, citizens’ lawful rights and public order, morals, and the veracity of information.”²⁶

Because encryption provides a powerful way to avoid government surveillance and control, many governments have sought to limit encryption, in part by stigmatizing it as a tool for terrorists. In Egypt, for example, journalists who use encryption have been arrested on terrorism charges.

Regimes such as China and Russia also use the Internet as a powerful propaganda tool. Russia’s multimedia propaganda apparatus has been extremely successful in influencing public opinion in a pro-government direction.²⁷ In China, the government has enlisted a “50-cent

army” of up to two million people paid to censor online content and post comments critical of the West and supportive of the Chinese Communist Party.²⁸ A recent study found that of the estimated 448 million yearly social media posts attributable to this propaganda army, the vast majority are “cheerleading” for China and the Communist Party, apparently to flood social media with positive, distracting content.²⁹

The American response to the authoritarian assault on Internet freedom has been led by the State Department and the Broadcasting Board of Governors (BBG).³⁰ The Obama administration’s 2011 *International Strategy for Cyberspace* makes Internet freedom a core objective of US cyber policy.³¹ In it, the administration pledged to support efforts to achieve safe platforms for commercial privacy; freedoms of expression and association, including protecting ISPs from intermediary liability; and “end-to-end interoperability of an Internet accessible to all.”³²

The NetFreedom Task Force is the State Department’s policy-coordinating body for Internet freedom. It has helped people in dozens of countries circumvent political censorship through tools and training and has provided more than \$100 million in support for civil-society organizations to promote Internet freedom abroad.³³ Its annual *Country Reports on Human Rights Practices* includes discussions of online freedom designed to call attention to repressive practices.

The US also has sought to advance Internet freedom through bilateral diplomacy and multilateral organizations, including the UN, the Organisation for Economic Co-operation and Development (OECD), the G7-G8, and the Organization for Security and Co-operation in Europe. These efforts have resulted in a surprising degree of at least nominal agreement on principles of online freedom. Some recent examples include:

- A 2012 resolution of the UN Human Rights Council affirmed that “the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice,” thereby formally applying article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights to the Internet.³⁴
- The 2011 Deauville Declaration of the G8 (essentially the G7 plus Russia) affirmed that “the openness, transparency and freedom of the Internet have been key to its development and success. These principles, together with those of non-discrimination and fair competition, must continue to be an essential force behind its development.”³⁵ However, the declaration also stressed that the implementation of those principles must be part of a “broader framework” that includes “rule of law . . . security, [and] transparency,” buzzwords often used in the context of Internet governance by governments seeking to ensure that the state’s power will always trump Internet freedom.
- A 2011 OECD communiqué on Internet policy endorsed a commitment to promote the global free flow of information and the open, distributed, and interconnected Internet.³⁶

The US has also helped support and promote the Freedom Online Coalition (FOC), which currently has 30 members among developed and developing nations and was created to coordinate diplomatic efforts and engage with civil society and the private sector to support Internet freedom globally. In the 2014 *Tallinn Recommendations for Freedom Online*, FOC member states pledged to “condemn—through diplomatic channels, public statements, and other means—violations and abuses of human rights and fundamental freedoms online as they occur in different countries throughout the world.”³⁷

The BBG advances Internet freedom abroad specifically through its Internet Anti-Censorship (IAC) division, which supports development of techniques to circumvent censorship.³⁸ Together with Radio Free Asia’s Open Technology Fund, the budget for the BBG’s IAC effort was \$17.5 million in 2015, including Voice of America’s Persian and Chinese services.

The technologies developed under the BBG’s auspices continue to promote political dissidents’ ability to access the Internet anonymously. For example, in the 1990s, the US Department of Defense launched a “dark web” project known as The Onion Router (Tor). Now maintained as an open-source resource by a non-profit, Tor has allowed users worldwide to circumvent

The Onion Router Network

The Onion Router network, commonly known as Tor, is a massive network of servers that provides a free way to connect anonymously to the Internet. The method was originally developed in the mid-1990s by the US Navy to protect intelligence communications, and in 2004 the Naval Research Laboratory published the source code under a free license.³⁹ The Tor network relies on “onion routing” to mask Internet activity: instead of making a conventional, direct connection to the destination website, Tor directs and encrypts traffic through a randomized selection of servers that function as routers.⁴⁰ Currently, more than 7,000 such routers are active on the Tor network.⁴¹

Some popular uses of Tor include circumventing government or institutional restrictions or surveillance; hiding hacking activity; and hiding personal information from advertisers, ISPs, and corporations. Tor also has the ability to host hidden websites that are accessible by only other Tor users, on what is known as the “dark web.” One infamous example was Silk Road, which served as a platform of trade in illegal drugs, forged IDs, child pornography, and various other illegal goods.

Internet censorship. As repressive regimes devised ways of blocking access to Tor, the Open Technology Fund helped develop the Cupcake Bridge, a browser extension that allows a user to transform a browser into a flash proxy—a temporary Tor bridge not listed in the main Tor directory—which allows censored users to get around the Tor block and access the free Internet.

Lastly, it is worth noting that recent trends in Western countries to limit freedom of speech—whether through the right to be forgotten in Europe or through codes prohibiting hate speech or microaggressions on US college campuses—are not conducive to US efforts to limit repression abroad. As the *Economist* recently put it:

The threat to free speech on Western campuses is very different from that faced by atheists in

Afghanistan or democrats in China. But when progressive thinkers agree that offensive words should be censored, it helps authoritarian regimes to justify their own much harsher restrictions and intolerant religious groups their violence. When human-rights campaigners object to what is happening under oppressive regimes, despots can point out that liberal democracies such as France and Spain also criminalise those who “glorify” or “defend” terrorism, and that many Western countries make it a crime to insult a religion or to incite racial hatred.⁴²

While the US government’s ability to effectively promote Western values and online freedom is limited, the long-run interests of the US and its democratic allies depend on preserving and expanding the ability of citizens everywhere to access information and engage freely in political speech. Our current efforts are not achieving that goal.

Internet Governance and Online Freedom. The freedom and prosperity made possible by the Internet depend on its free, open, and decentralized architecture. That architecture in turn depends on letting the technology of the Internet continue to evolve with minimum government interference. As the Internet has spread and grown in significance, authoritarian governments have recognized the nexus between online freedom and Internet governance. The future of Internet freedom will be decided in part by the clash between proponents of the government-centric model and adherents of the multi-stakeholder model—the decentralized, civil-society arrangements that have governed the Internet through decades of exponential growth.

The multistakeholder model arose organically from the Internet’s early success in demonstrating the power of an open, decentralized architecture. Open architecture allows an endless number of different networks and devices to connect and communicate, facilitating a limitless flow of information among a practically infinite number of access points. It creates the ideal conditions for innovation anywhere to spread rapidly everywhere. More than anything else, it is what has made possible the explosive innovation and expansion of the Internet, and it is the indispensable condition of its future potential.

The idea of open-architecture networking was introduced by Robert E. Kahn shortly after his arrival at DARPA in 1972. Kahn's conception depended on four crucial ground rules, of which the most important was that there would be "no global control at the operations level."⁴³ Shielded from government interference, the private sector quickly proved that innovation could produce not just the best technology but also the best organization and regulation. That is why President Bill Clinton, in announcing the administration's 1997 *Framework for Global Electronic Commerce*, declared that the Internet should be "global free-trade zone" where "government makes every effort first . . . to do no harm." He explained his vision this way:

We want to encourage the private sector to regulate itself as much as possible. We want to encourage all nations to refrain from imposing discriminatory taxes, tariffs, unnecessary regulations, cumbersome bureaucracies on electronic commerce. Where government involvement is necessary, its aim should be to support a predictable, consistent, legal environment for trade and commerce to flourish on fair and understandable terms.⁴⁴

The principles President Clinton articulated became part of the bedrock of Internet governance. The term "Internet governance," as the World Summit on the Information Society (WSIS) defined it in 2015, refers to the "shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."⁴⁵ Thus the Clinton administration answered the crucial question of who would devise the necessary principles and procedures by establishing what came to be called the multistakeholder model. Responsibility for Internet governance soon devolved to a global community of its users, "a cooperative, consensus-based, decision-making process involving a wide variety of individuals."⁴⁶

Repressive regimes soon realized the danger that the free and open Internet posed to their rule. They began to adapt. In the words of Christopher Walker of the National Endowment for Democracy, those regimes were soon bent not just on "defending authoritarianism

at home, but reshaping the international norms that stigmatize such governance."⁴⁷

To accomplish these goals, repressive governments—along with increasing numbers of democratic governments—are pushing for an international, multilateral system of Internet governance in which governments have the primary role. They want a "reasonable allocation of Internet resources" in terms of the functions of the Internet Corporation for Assigned Names and Numbers (ICANN), IANA, and other international bodies, including the management of the Domain Name System. They also seek to limit extraterritorial surveillance while shielding their own "sovereign" right to conduct surveillance over their own citizens.

As WSIS had affirmed in 2005, "Policy authority for Internet related public policy issues is the sovereign right of States." When WSIS celebrated its 10th anniversary with a review of Internet governance at the United Nations General Assembly in December 2015, authoritarian governments came prepared. Many filed recommendations for the content of an "outcome document" that sought to steer the Internet in a more authoritarian direction.⁴⁸

China specifically advocated a multilateral (multistate) approach. While acknowledging the multistakeholder model, it emphasized:

Any tendency to place sole emphasis on the role of businesses and non-governmental organizations while marginalizing governments should be avoided. . . . It is necessary to ensure that the United Nations plays a facilitating role in setting up international public policies pertaining to the Internet.⁵⁰

Russia was even more direct:

*We consider it necessary to consecutively increase the role of governments in the Internet governance, with strengthening the activity of the International Telecommunication Union (ITU) in this field, as well as with support of the UNESCO activity in the development of ethical aspects of the Internet use and ICTs as a whole.*⁵¹

Fortunately, these positions were broadly rejected by the UN General Assembly: in a diplomatic victory for the US, the final resolution continued to embrace the multistakeholder model.⁵²

Importantly, the resolution also included language renewing the mandate for the Internet Governance Forum (IGF) for another 10 years. Created as an outgrowth of the original 2003–05 WSIS meetings, IGF is a voluntary organization that brings together representatives from all over the world from civil society, the private sector, government, the technical and academic community, intergovernmental organizations, and the media. While its recommendations are nonbinding, it has served an important function by facilitating an open dialogue on issues such as online freedom and Internet governance.

In March 2014, an important new phase in the evolution of Internet governance was set in motion with the US Department of Commerce’s announcement that it planned to cede control of the IANA function to an international body. The National Telecommunications and Information Administration (NTIA) stated that it would not accept any transition proposal that would replace the NTIA role with a government-led or an intergovernmental-organization solution. In addition, the NTIA told ICANN that the transition proposal must have broad community support and adhere to four principles:

1. Support and enhance the multistakeholder model;
2. Maintain the security, stability, and resilience of the Internet DNS;
3. Meet the needs and expectation of the global customers and partners of the IANA services; and
4. Maintain the openness of the Internet.

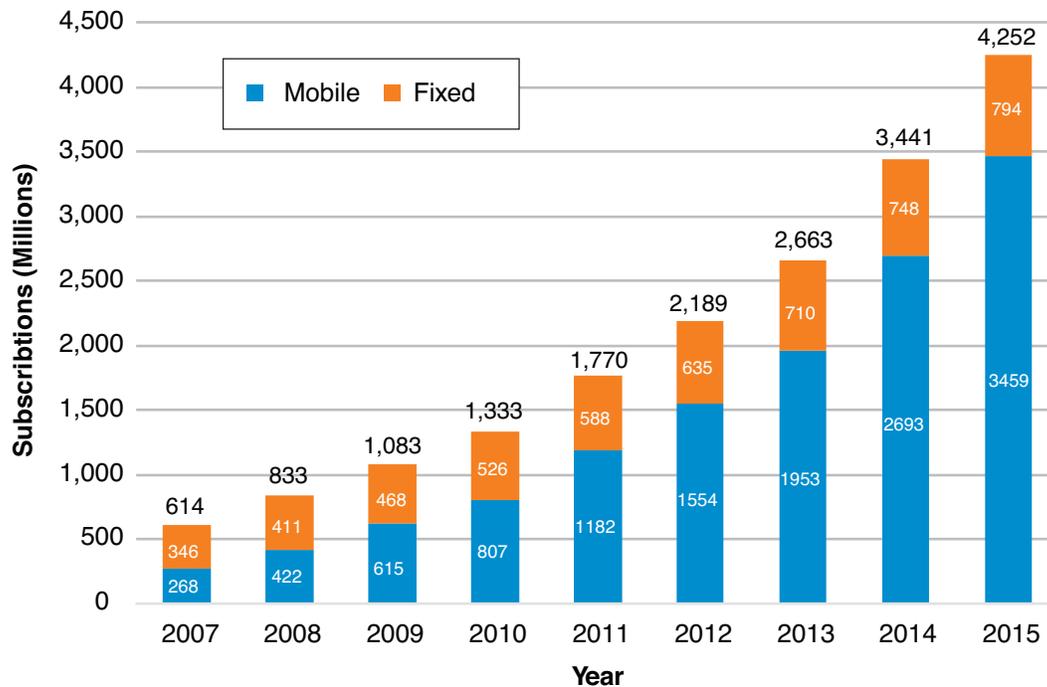
The shape of the IANA transition was significantly clarified at the March 2016 ICANN meeting in Marrakesh. The organizations that make up the Cross-Communication Working Group approved an “enhanced accountability” proposal for ICANN governance. A separate proposal related specifically to IANA stewardship had already been approved by the IANA Stewardship Transition Coordination Group, although it left important questions unresolved. Both proposals were approved by the ICANN board on March 10, 2016.

In the ICANN enhanced accountability proposal, the US and like-minded stakeholders were able to fend off an attempt by China, Russia, and other governments to give governments substantially greater control over ICANN through the Governmental Advisory Committee (GAC). Those governments hoped to weaken the voting threshold required for GAC “advice” to the ICANN board from the current requirement of full consensus to a simple majority. Had they succeeded, the US and its allies could have lost their ability to prevent the GAC from seeking to impose policies on the ICANN board—and even changes to ICANN bylaws—that could be highly damaging to the multistakeholder model. Fortunately, the proposal was not adopted: moving forward, the GAC will be unable to give advice to the ICANN board unless it has full consensus, with no country lodging a formal objection.

While this outcome represents a victory for the US position, it leaves an important set of issues unresolved: the means by which ICANN or some other body will oversee the IANA function itself. The administrator of the new post-transitional IANA, as an affiliate of ICANN, should not be expected to decide policy questions, such as whether “.ram” is an appropriate domain name. Neither should the ICANN community, which sets policy, be given the power to enforce that policy. Enforcement should be done by a separate body that is structured to ensure impartiality and that is as insulated as possible from political influence.

The promise of the Internet inheres in its open architecture, its user-driven standards, and the freedom to innovate technologically. That promise is at risk when governments insist on establishing controls over those spontaneous processes. Internet technology must be allowed to progress unhindered. Proper Internet governance is crucial for both human rights and the promise of prosperity.

The Private Sector’s Role. As President Clinton foresaw, technological innovation holds tremendous promise for prosperity and freedom around the world. One key to realizing that promise lies in the Internet’s open architecture, which in turn requires keeping the crucial role of organizations such as the Internet Engineering Task Force (IETF) free of government regulation.

Figure 4. Growth of the Mobile Internet, 2007–15

Source: International Telecommunication Union, “Statistics,” <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.

The IETF is the organization that sets the standards, or “protocols,” that the networks, routers, computers, and other devices that make up the Internet use to “talk” to each other and transmit information seamlessly. The US and like-minded stakeholders, including the IETF itself, have so far succeeded in preserving the IETF’s independence. But the IETF’s independent role—and that of an unfettered private sector more broadly—needs to be more fully enshrined in domestic and international laws and institutions.

The private sector is also the key to enhancing freedom in countries with repressive regimes. Private firms, many of them entrepreneurial startups, have been almost exclusively responsible for connecting billions of people to the Internet—primarily, as noted earlier, through the explosive growth of mobile wireless broadband. (See Figure 4.)

The private sector has also led the way in developing technologies that have facilitated online freedom even in the face of political repression. For example,

private-sector innovation led to the development of Virtual Private Networks (VPNs), which have proved effective in evading the most common censorship tools available to repressive governments. VPNs have become increasingly difficult to block, and Cloud technologies have now opened the possibility of Cloud-based VPNs to become universally distributed from virtually any IP address. Jigsaw (previously Google Ideas), Google’s think tank and technology incubator, has created a source tool called uProxy, which allows Internet users to circumvent government firewalls.⁵³ The combination of privacy, encryption, and Cloud computing holds enormous promise for Internet freedom, and the US government should do what it can to promote it.

Because the Internet is dominated by private firms, the private sector is inevitably caught up in government efforts to control how it is used, sometimes placing companies in direct conflict with nation-states. In such situations, the private sector has an obligation to self-regulate—to be transparent about the requests it

receives for content removal, data localization, and similar impositions, especially in repressive countries. To the extent that private companies facilitate strategies of repression, they become part of the problem. They have an obligation to resist unlawful demands—and to oppose the enactment of legal regimes that may require private-sector participation in strategies of repression and control as a condition of doing business.

At the same time, the US and other Western governments must recognize that private firms are limited in their ability to resist sovereign states' persistent efforts to enforce censorship or demand production of information for surveillance and law enforcement purposes. To date, there is little evidence of US engagement—beyond talk—to support US companies' efforts to resist authoritarian demands. One avenue to be explored, discussed further in Chapter IV, is to more actively enforce trade agreements that limit such practices.

In this context, the private sector has been correct to resist US officials' proposals to mandate backdoors into encryption software. If the US prohibits the development of unbreakable encryption, the effect will simply be to drive encryption and privacy services overseas, putting at risk one of America's most powerful and valuable competitive advantages in the world economy. While the US government has a strong and legitimate interest in the ability to investigate and prosecute terrorism, cybercrime, and other activities involving digital communications, it must meet those responsibilities by exploiting the full array of intelligence-gathering capabilities at its disposal, not by weakening the overall security of the Internet.

Principles and Policies

There is broad agreement that advancing Internet freedom throughout the world is in America's national interests. As President Clinton's top Internet adviser said in 1999, "The Internet is a medium that has tremendous potential for promoting individual freedom and individual empowerment. . . . We should maximize the opportunity for human freedom."⁵⁴ In its May 2011 *International Strategy for Cyberspace*, the Obama administration reaffirmed that commitment:

The United States will be a tireless advocate of fundamental freedoms of speech and association through cyberspace; will work to empower civil society actors, human rights advocates, and journalists in their use of digital media; and will work to encourage governments to address real cyberspace threats, rather than impose upon companies responsibilities of inappropriately limiting either freedom of expression or the free flow of information.⁵⁵

There is also a broad consensus about what online freedom means in practice. As discussed earlier, the right to access information and express one's political views is recognized in a variety of treaties and agreements. It hardly seems likely that further refinements in the concepts embodied in international agreements or the words in which those concepts are expressed is necessary.

What is needed is action. The recent success of authoritarian regimes detailed earlier shows that our efforts, and those of our allies, to promote Internet freedom have not been sufficient. If freedom is to advance, we must accompany our words and intentions with greater resources and more assertive policies. In short, the US must be willing to take risks and bear costs in the cause of online freedom.

Government's first role is to support civil society and the private sector. The digital economy is in many respects a medium of communication—from email and text messages to social media, mobile apps, and electronic games, Internet commerce consists of facilitating interpersonal communications. Thus, it is no coincidence that cutting off access to social media and other online communication tools has become a top priority of repressive governments, especially when under stress.

The US government can assist in such situations through both technological and diplomatic means, including the exercise of soft power and the threat or actual imposition of sanctions. What it cannot do is stand by while foreign governments violate their human rights and international trade obligations.

In addition to supporting the private sector, the US government must work more effectively with like-minded

states to advocate and act on behalf of online freedom, and together they must seek to expand the universe of countries that recognize and respect those rights. Thanks to the globalization of communication and culture brought about by the Internet, liberal democracy is engaged in the cultural equivalent of a standards war—a battle of ecosystems, one closed and repressive, the other open and free. As in every standards war, scale matters. The US cannot win by going at it alone.

The US has a strong national interest in preserving and enhancing the Internet’s role in furthering fundamental values of individual liberty, self-determination, and the rule of law. These values are under attack by sophisticated state actors who are actively working to advance authoritarian ideologies through political repression and are increasingly and effectively utilizing digital technologies to achieve their ends.

The US must develop and implement effective strategies to counter and defeat these efforts, by asserting and *actively promoting* global rights of online freedom of expression, association, and access to online information. To do so, it should be prepared to act unilaterally, through bilateral engagements with other nation-states and through multilateral institutions. Specifically, the US should do the following.

Use all elements of US diplomatic and economic policy to discourage autocratic states from censorship and oppression. The US should seek to raise the costs to autocratic governments of censorship, surveillance, or suppression of political, social, cultural, and scientific speech using all appropriate tools. These tools include raising public awareness of violations of Internet freedoms and being prepared to take tangible actions, up to and including imposing sanctions, on a multilateral basis wherever possible, against repressive governments that persistently violate individual rights.

To increase global focus on the importance of online freedom, the Department of State should publish an annual report that brings together the relevant sections of the existing country reports into a single document—and publicize its findings aggressively. As discussed in detail in Chapter IV, the US should also

consider filing actions in the World Trade Organization (WTO) against repressive governments, such as China, whose censorship of global information services appears to violate the General Agreement on Trade in Services.

Significantly expand US social media and other digital communication efforts to effectively communicate and promote fundamental online freedoms. While the private sector must lead in promoting US values, the US government can and should ensure that its positions, and the values behind them, are communicated globally, including in countries where repressive governments seek to censor political information and punish political expression and where dissidents are actively resisting oppression. Toward this end, the US should expand funding for the BBG and the NetFreedom Task Force.

Formalize, expand, and strengthen the Freedom Online Coalition. The US should more actively engage with the FOC to organize diplomatic activity at the ministerial and head-of-government level and to harmonize principles of domestic Internet policy and norms of global Internet governance. Working with the FOC, the US government should lead a multilateral Freedom Online Initiative that would bring to bear the financial, technological, diplomatic, and communications capabilities of the civilized world to advocate freedom of speech and free access to information in the digital ecosystem and to promote international agreement around issues such as transnational surveillance and data access.⁵⁶

Promote increased access to the Internet through market-oriented policies. Polling data show a high correlation between expanded Internet access and popular desire for Internet freedom.⁵⁷ Private investment and market-oriented policies have dramatically increased online access. The US should continue to promote such policies through its bilateral relationships and international forums, such as the International Telecommunications Union and the World Bank, and actively oppose policies that discourage investment, such as excessive regulation.

Strengthen civil-society groups' role in studying and promoting online freedom. Specifically, the US should provide additional funding to the National Endowment for Democracy to promote Internet freedom through grants, studies, and global collaboration with civil-society organizations.

Expand, intensify, and support both public and private participation in international forums where Internet policies are set. Countries such as Russia and China are increasingly engaged in the technical-standard-setting activities that take place in international forums such as the IGF, ITU, IETF, ETSI, IEEE, W3C, and 3GPP. The US should cooperate with and support the efforts of the private sector, civil society, and like-minded governments to promote standards and policies consistent with Internet freedom. One good example would be to support the IETF's Internet Engineering Steering Group's proposed "HTTP Status Code to Report Legal Obstacles," which would tell users when access to websites is being

blocked for legal reasons, allowing users eventually to know *why* and *by what authority* their Internet access has been blocked.⁵⁸

Vigorously promote and defend the multistakeholder model of Internet governance. The ICANN board is structured by the multistakeholder community to facilitate Internet governance. Some of the more authoritarian governments have tried to establish state leverage over the ICANN board deliberations by requiring the board to obey the Government Advisory Committee's "advice." In March 2016, the ICANN board approved accountability proposals that successfully blocked this bid, requiring consensus of all governments in the GAC before they can intervene decisively in Internet governance decisions. That gives the US a veto over GAC actions, and it is vital that the US not give up or in any way weaken its veto in GAC or similar intergovernmental bodies. The US should also insist that the IANA function be supervised by an independent entity shielded from the politics of ICANN and "the community."

Notes

1. World Bank, *World Development Report 2016: Digital Dividends*, 2016, <http://www.worldbank.org/en/publication/wdr2016>.
2. See, for example, BBC News, “China Internet: Xi Jinping Calls for ‘Cyber Sovereignty,’” December 15, 2015, <http://www.bbc.com/news/world-asia-china-35109453>.
3. The economic impact of the Internet is discussed further in Chapter IV.
4. James Manyika et al., “Lions Go Digital: The Internet’s Transformative Potential in Africa,” McKinsey Global Institute, November 2013, <http://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa>.
5. See generally GSM Association, *The Mobile Economy: Sub-Saharan Africa 2015*, 24, <https://www.gsmainelligence.com/research/?file=721eb3d4b80a36451202d0473b3c4a63&download>. M-Pesa was recently featured on *60 Minutes*. See Lesley Stahl, “The Future of Money,” *60 Minutes*, aired November 22, 2015, <http://www.cbsnews.com/news/future-of-money-kenya-m-pesa-60-minutes/>. For information on Ushahidi, see Ushahidi, “About Ushahidi,” <https://www.ushahidi.com/about>.
6. See GSM Association, *The Mobile Economy*, 24.
7. Jeffrey Eisenach and Evelyn Smith, “Some Good News About Africa: The Amazing Mobile Internet,” TechPolicyDaily.com, May 15, 2015, <http://www.techpolicydaily.com/communications/africa-amazing-mobile-internet/>.
8. Stanford University, “The Impact of the Internet on Developing Countries,” Winter 2001, <http://cs.stanford.edu/people/eroberts/cs201/projects/third-world/india-cases.html>.
9. For example, a 2012 study by the Pew Research Center found that Internet users in Arab countries were the most likely to use social networks to express political opinions online. See Pew Research Center, “Social Networking Popular Across Globe,” December 12, 2012, <http://www.pewglobal.org/2012/12/12/social-networking-popular-across-globe/>.
10. Richard Wike and Katie Simmons, “Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech,” Pew Research Center, November 18, 2015, <http://www.pewglobal.org/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/>.
11. Richard Wike, “Broad Support for Internet Freedom Around the World,” Pew Research Center, February 23, 2016, <http://www.pewresearch.org/fact-tank/2016/02/23/broad-support-for-internet-freedom-around-the-world/>.
12. See Internet Society, *Internet Society Global Internet Report 2015: Mobile Evolution and Development of the Internet*, 44, http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf.
13. *Freedom on the Net 2015* divides countries into “free,” “partially free,” and “not free.” Freedom House, *Freedom on the Net 2015*, October 2015, 16–17, <https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf>.
14. *Ibid.*, 6.
15. *Ibid.*, 10.
16. Freedom House, “Internet Freedom,” <https://freedomhouse.org/issues/internet-freedom>.
17. Freedom House, *Freedom on the Net 2015*, 7.
18. Josh Chin, “China Is Requiring People to Register Real Names for Some Internet Services,” *Wall Street Journal*, February 4, 2015, <http://www.wsj.com/articles/china-to-enforce-real-name-registration-for-internet-users-1423033973>.
19. David Barboza and Paul Mozur, “New Chinese Rules on Foreign Films’ Online Content,” *New York Times*, February 19, 2016, <http://www.nytimes.com/2016/02/20/business/media/new-chinese-rules-on-foreign-firms-online-content.html>.
20. Paul Mozur and Jane Perlez, “Apple Services Shut Down in China in Startling About-Face,” *New York Times*, April 21, 2016, <http://www.nytimes.com/2016/04/22/technology/apple-no-longer-immune-to-chinas-scrutiny-of-us-tech-firms.html>.
21. Duffy, *Internet Freedom in Vladimir Putin’s Russia*.
22. *Ibid.*
23. *Economist*, “A Giant Cage,” April 6, 2013, <http://www.economist.com/news/special-report/21574628-Internet-was-expected-help-democratise-china-instead-it-has-enabled>.
24. See Patricia Moloney Figliola, *Promoting Global Internet Freedom*, Congressional Research Service, October 22, 2013, Appendix B, <https://www.fas.org/sgp/crs/row/R41837.pdf>.

25. Vauhini Vara, “The World Cracks Down on the Internet,” *New Yorker*, December 4, 2014, <http://www.newyorker.com/tech/elements/world-cracks-Internet>.
26. See Ron Diebert, “Cyberspace Under Siege,” in *Authoritarianism Goes Global: The Challenge to Democracy*, ed. Larry Diamond, Marc F. Plattner, and Christopher Walker (Baltimore, MD: Johns Hopkins University Press, 2016), 198–213. Authoritarian governments are now deploying “third-generation” controls, which “involve surveillance, targeted espionage, and other types of cover disruptions in cyberspace.”
27. Vladimir Ryzhkov, “The Absurd World of Russian Public Opinion,” *Moscow Times*, February 25, 2015, <http://www.themoscowtimes.com/opinion/article/the-absurd-world-of-russian-public-opinion/516531.html>.
28. Christina Sterbenz, “China Banned the Term ‘50 Cents’ to Stop Discussion of an Orwellian Propaganda Program,” *Business Insider*, October 17, 2014, <http://www.businessinsider.com/chinas-50-cent-party-2014-10>.
29. Gary King, Jennifer Pan, and Margaret E. Roberts, “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument” (working paper, June 1, 2016), <http://j.mp/1Txxizi>; and Gary King, Jennifer Pan, and Margaret E. Roberts, “How Censorship in China Allows Government Criticism but Silences Collective Expression,” *American Political Science Review* 107, no. 2 (2013): 1–18, <http://j.mp/LdVXqN>.
30. Figliola, *Promoting Global Internet Freedom*.
31. White House, *International Strategy for Cyberspace*.
32. *Ibid.*, 8.
33. US Department of State, “Internet Freedom,” <http://www.state.gov/e/eb/cip/netfreedom/index.htm>.
34. US Mission Geneva, “HRC Affirms That Human Rights Must Also Be Protected on the Internet (Resolution Text),” <https://geneva.usmission.gov/2012/07/05/internet-resolution/>; and United Nations, “The Universal Declaration of Human Rights,” December 10, 1948, <http://www.un.org/en/universal-declaration-human-rights/>.
35. G8 Summit, “Deauville G8 Declaration: Renewed Commitment for Freedom and Democracy,” May 26–27, 2011, https://www.whitehouse.gov/sites/default/files/uploads/deauville_declaration_final_-_eng_8h.pdf.
36. OECD High Level Meeting on the Internet Economy, “Communiqué on Principles for Internet Policy-Making,” June 28–29, 2011, <https://www.oecd.org/Internet/innovation/48289796.pdf>.
37. Freedom Online Coalition, “Recommendations for Freedom Online,” April 28, 2014, <https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf>.
38. Broadcasting Board of Governors, “Internet Anti-Censorship,” <http://www.bbg.gov/wp-content/media/2015/04/Anti-Censorship-Fact-Sheet-10182015.pdf>.
39. ExpressVPN, “The Unlikely History of Tor,” <https://www.expressvpn.com/internet-privacy/tor/history/>.
40. Onion Routing, “Onion Routing Executive Summary,” 2005, <http://www.onion-router.net/Summary.html>.
41. Blutmagie.de, “Tor Network Status,” <https://torstatus.blutmagie.de/>.
42. *Economist*, “Under Attack,” June 4, 2016, <http://www.economist.com/news/leaders/21699909-curbs-free-speech-are-growing-tighter-it-time-speak-out-under-attack>.
43. Barry M. Leiner et al., *Brief History of the Internet*, Internet Society, October 15, 2012, <http://www.Internetsociety.org/Internet/what-Internet/history-Internet/brief-history-Internet#REK72>.
44. White House, “Remarks by the President in Announcement of Electronic Commerce Initiative,” July 1, 1997, <http://clinton4.nara.gov/WH/New/Commerce/remarks.html>.
45. World Summit on the Information Society, “Tunis Agenda for the Information Society,” November 18, 2005, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>; and Jovan Kurbalija, *An Introduction to Internet Governance*, 6th ed. (Msida, Malta: DiploFoundation, 2011), 5.
46. Kurbalija, *An Introduction to Internet Governance*, 5. For a detailed treatment of the privatization of Internet governance under the Clinton administration, see J. Robert Beyster and Michael A. Daniels, *Names, Numbers, and Network Solutions: The Monetization of the Internet* (La Jolla, California: CreateSpace Independent Publishing Platform, 2013).
47. Christopher Walker, “The New Containment: Undermining Democracy,” *World Affairs*, May/June 2015, <http://www>.

worldaffairsjournal.org/article/new-containment-undermining-democracy.

48. UN General Assembly, Resolution 70/125, “Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society,” December 16, 2015, <http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf>.

49. See Permanent Mission of the People’s Republic of China to the United Nations, “Position Paper of China on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society (WSIS),” August 12, 2015, <http://www.china-un.org/eng/gdxw/t1288450.htm>. “We should establish a *multilateral*, democratic, and transparent international Internet governance system that ensures equal participation of all, reasonable allocation of Internet resources, and joint management of key Internet infrastructure.” (emphasis added).

50. *Ibid.*

51. Permanent Mission of the Russian Federation to the United Nations, “Written Submission of the Russian Federation to the Draft Final Document of the UN General Assembly High-level Meeting on the Implementation of WSIS Outcomes,” November 2016, <http://workspace.unpan.org/sites/internet/Documents/UNPAN95313.pdf>. (Emphasis in original.)

52. UN General Assembly, Resolution 70/125.

53. Hadas Gold, “Vice Teams with Alphabet Incubator Jigsaw on Doc Series ‘Blackout,’” *Politico*, May 13, 2016, <http://www.politico.com/blogs/on-media/2016/05/vice-google-jigsaw-blackout-documentary-223164>.

54. Ira C. Magaziner, “Creating a Framework for Global Electronic Commerce,” Progress & Freedom Foundation, July 1999, <http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html>.

55. White House, *International Strategy for Cyberspace*, 24.

56. See, for example, Brad Smith, “Time for an International Convention on Government Access to Data,” Microsoft on the Issues, January 20, 2014, <http://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/>.

57. Wike and Simmons, “Global Support for Principle of Free Expression.”

58. T. Bray, “An HTTP Status Code to Report Legal Obstacles,” Internet Engineering Task Force, February 2016, <https://tools.ietf.org/pdf/rfc7725.pdf>; and Diebert, “Cyberspace Under Siege,” 212–13.

IV. International Trade and Digital Commerce

The digital economy encompasses virtually every aspect of global commerce. It has enhanced productivity, enabled entrepreneurship, accelerated innovation, made supply chains vastly more efficient, and opened up access to distant markets for even the most modest startups.¹ It has spawned a tidal wave of new business models and many of the world's most innovative and powerful companies. Of the world's 10 largest companies by stock market capitalization, half are giants of the digital ecosystem.²

Cross-border data flows are indispensable to this success. The Internet continues to reach even more people with even faster connection speeds. In 2015, 3.2 billion people had Internet access, accounting for 43 percent of the world's population.³ Internet industries alone accounted for \$966.2 billion of US GDP in 2014, about 6 percent of the overall economy.⁴

The Internet has become integral to virtually every sector of industry and is contributing to global growth on a systemic basis. According to the McKinsey Global Institute, from 2004 to 2009 the Internet was responsible for 11 percent of GDP growth in the 13 countries surveyed and for 21 percent of growth in the nine most developed economies.⁵ A more recent report from the McKinsey Global Institute estimates that the volume of data flows multiplied 45 times between 2005 and 2014, contributing an estimated \$2.8 trillion to global GDP—a larger impact than the trade of physical goods.⁶

As shown in Figure 5, from an economic perspective, the phrase “information age” is more than a slogan: intangible assets (i.e., intellectual property) now account for more than 80 percent of the value of the S&P 500, up from less than 20 percent in 1975.

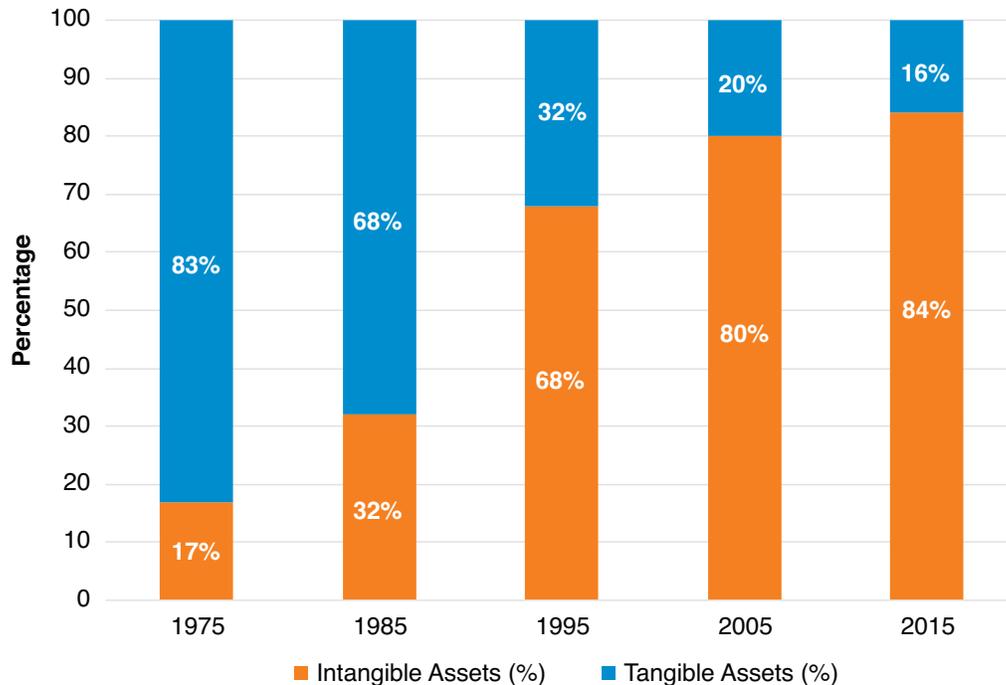
The Internet's chief effect on overall global economic growth comes from the increased productivity

that results from increased data flows. The Internet allows tighter management of the production chain and increases its efficiency.⁷ It allows production chains to be more dispersed by reducing the effective “distance” between points of comparative advantage. Cloud computing puts companies in constant contact with suppliers and customers, reducing delay, risk, and other transaction costs.

While the disruptions associated with the digital economy are not without costs, the net impact is positive. McKinsey, for example, found that 2.6 jobs were created for every one destroyed in the digital economy.⁸ The United States International Trade Commission (USITC) concluded that digital trade has raised US GDP by between 3.4 to 4.8 percent and in the aggregate has created as many as 2.4 million jobs.⁹

The Internet has dramatically leveled the playing field for small- and medium-sized businesses (SMEs), including in developing countries where SMEs are the largest contributors to job creation.¹⁰ The Internet gives SMEs access to a global market without the need to be physically present anywhere. It has led to the creation of micro-multinationals: small companies that can compete globally, almost from startup.¹¹

For similar reasons, Internet connectivity has also become crucial for economic prospects in the developing world. Internet penetration has an even more positive impact for low- and middle-income countries' economic growth than for high-income countries (Figure 6). Where agriculture remains a large part of the local economy, the Internet could increase farmers' income by more than 20 percent, for example by making accurate information about weather and pricing more readily available, thereby increasing productivity and reducing risks and other costs.¹²

Figure 5. Value of Tangible and Intangible Assets as a Proportion of S&P 500 Market Value

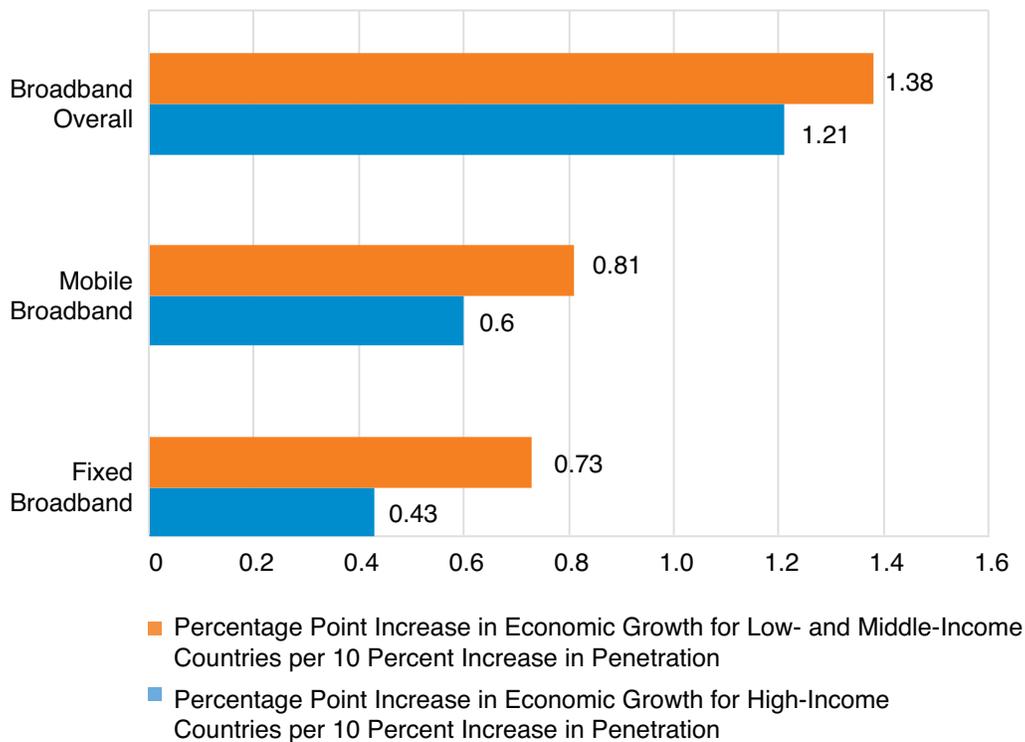
Source: Kristi Stathis, "Ocean Tomo Releases 2015 Annual Study of Intangible Asset Market Value," Ocean Tomo Insights Blog, March 5, 2015, <http://www.oceantomo.com/blog/2015/03-05-ocean-tomo-2015-intangible-asset-market-value/>.

The dramatic expansion in global data flows has led to the proliferation of multinational supply chains of ever-increasing complexity and, in turn, to disruptive business models that are revolutionizing the world economy. The USITC has estimated that the Internet can reduce trade costs by an average of 26 percent.¹³

The iPhone remains a great example. Apple creates the overall design and its most complicated parts, but many components are designed and manufactured around the world, crossing borders several times, until much of the final product is assembled in China and then shipped, distributed, and sold globally, often with some form of financing. This complex supply chain, which would be impossible without the Internet, is what allows Apple and its competitors to provide astonishingly powerful devices to the public in miniature packages, at prices most people can afford.

Maintaining free trade in electronic commerce is also in America's national interest from a strategic perspective. As discussed earlier, the benefits of the digital ecosystem depend mightily on economies of scale and scope. The ability of US Internet companies to prosper thus depends on having access to the global market. Conversely, if the US Internet sector were to be limited or excluded from serving such massive and rapidly growing markets as China and India, it would find itself at a severe comparative advantage. The stakes are therefore high for trade agreements such as the recently completed Trans-Pacific Partnership Agreement (TPP) and those on the horizon: the US-EU Trade and Investment Partnership Agreement (TTIP), Trade in Services Agreement (TISA) negotiations in the WTO, and negotiations on digital issues in a future WTO trade round.

Figure 6. Effects on Economic Growth of Technology Penetration



Source: World Bank, “Information and Communications for Development 2009: Extending Reach and Increasing Impact,” 2009.

Opportunities and Challenges

The rising standards of living and increased connectivity among societies and cultures that have been enabled by digital commerce are good for the world and for America. But the emergence of the global digital economy has also created policy challenges that the US must address. This section focuses first on China, whose mercantilist policies significantly threaten digital trade’s integrity and vitality. Next we focus on issues specific to trade relations with the European Union. Lastly we discuss the need to develop and successfully execute a comprehensive digital-trade strategy.

The Challenge of China. China’s increasingly aggressive strategy of economic cyber espionage, combined with its protectionist digital-trade policy, poses a major challenge for US policy.

IP Theft. General Keith Alexander, former director of National Security Agency (NSA), has called China’s economic espionage and cyber theft of US intellectual property “the greatest transfer of wealth in history.”¹⁴ On the legal side, China is erecting costly barriers to ICT commerce in the form of counterterrorism, national security, business regulation, and censorship, typically in the guise of regulation for “public morals.” These activities, among other things, give Chinese companies an unfair and—under WTO and other international agreements—often illegal competitive advantage over US companies.

The total losses to the US economy from theft of IP and trade secrets have been estimated at more than \$300 billion annually, and the vast majority of those attacks originate from China.¹⁵ Regrettably, the US government’s response has been ineffective. A much more energetic and strategic approach is urgently needed.

In devising a strategy for combating Chinese cyber theft, it is important to distinguish between traditional espionage, including economic espionage, and commercial theft—that is, between espionage for national security and other state purposes and the theft of intellectual property for the commercial benefit of individual corporations.

The distinction is acknowledged in the Obama administration’s Executive Order 13694 (April 1, 2015), which provides for sanctions against persons engaged in significant cyberattacks. The order seeks to punish “significant malicious cyber-enabled activities,” defined as cyberattacks originating outside the US that could result in “a significant threat to the national security, foreign policy, or economic health or financial stability of the United States,” through harm to critical infrastructure, computers or computer networks, or “significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information *for commercial or competitive advantage or private financial gain.*”¹⁶

In September 2015, Chinese President Xi Jinping and President Obama issued a joint statement during a state visit in Washington that “China and the United States agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”¹⁷

During a subsequent meeting with President Xi, in March 2016, President Obama said, “We have deep concerns about our ability to protect the intellectual property of our companies.”¹⁸ The administration has indicated that it would consider sanctions if there is no progress on cyber theft, but it has not been clear on whether and to what extent there has been improvement.¹⁹

Indeed, US officials have continued to express doubts that China has been compliant with the terms of the Obama-Xi agreement. In a recent Senate Foreign Relations Committee hearing, Senator Ben Cardin (D-MD) stated that China “might not be living up to its terms” to stop conducting or supporting cyber-enabled theft of intellectual property.²⁰ These comments echo the doubts of other officials, such as those made by Adm.

Mike Rogers, commander of US Cyber Command, and Director of National Intelligence James Clapper in congressional hearings in early 2016.²¹

While condemning IP theft, neither the executive order nor the Obama-Xi agreement express disapproval of traditional economic espionage. The challenges of maintaining and enforcing such distinctions are evident in the 2014 US indictment of five members of the Chinese People’s Liberation Army. The US alleged that the soldiers, members of the secretive Unit 61398, had hacked into several American companies and a steelworkers’ union to steal trade secrets for state-owned Chinese firms to help give them a competitive edge. As Attorney General Eric Holder explained:

The alleged hacking appears to have been conducted for no reason other than to advantage state-owned companies and other interests in China, at the expense of businesses here in the United States. This is a tactic that the US government categorically denounces. As President Obama has said on numerous occasions, we do not collect intelligence to provide a competitive advantage to US companies, or US commercial sectors.²²

A closer look at the indictment demonstrates the challenge for US policy. The indictment charges that the Chinese hackers stole corporate data that related to an antidumping case against a Chinese company. Although labeled “trade secrets” in the indictment, the information taken—mostly pricing data and other information relevant to the legal case—is arguably not qualitatively different from the sorts of information targeted by US intelligence agencies for many years. Indeed, one 1996 report noted: “According to the National Security Agency (NSA), the economic benefits of SIGINT contributions to US industry taken as a whole have totaled tens of billions of dollars over the last several years.”²³

The US has indeed conducted espionage of a strategic economic nature, including hacking into private companies in several countries. The US has also conducted surveillance on the EU antitrust commissioner for information regarding potential actions against Google, Intel, and Microsoft; on Japanese officials

during auto trade negotiations in the 1990s; on French officials for insight into their allegedly protectionist trade positions; and on Chinese companies, including telecom-equipment maker Huawei.²⁴

For US policy to effectively prevent and deter cyber theft by China and other potential offenders, it is important to clarify the distinction between illegitimate cyber theft and strategic economic espionage and, having done so, to forge international consensus on the boundaries for legitimate state conduct. While WTO rules do not yet include comprehensive cyberspace rules, they do cover IP and trade secrets. The US should vigorously use the WTO to enforce proper international rules of the road for the Internet ecosystem. In addition, the US should continue to refine its domestic legal framework for IP and trade secrets as the foundation for dealing with international cyber threats of an economic nature.

Trade Policy and Mercantilism. China's trade policy has also been trending in a worrisome direction. After a period of growing liberalization on the road to WTO membership in 2001 and for several years afterward, China has pursued an increasingly protectionist trade strategy. American companies have been harassed with specious business practice and antitrust complaints,²⁵ foreign direct investment is often subject to onerous conditions, and national security and public-morals censorship laws have been used to gain a competitive advantage for Chinese companies at the expense of US and other foreign entities seeking to do business in China. In addition, Chinese leaders have embraced a strategy of "indigenous innovation," identifying key technologies, subsidizing Chinese companies to compete against foreign companies, and closing off strategic sectors to foreign control. China reportedly hopes to purge most outside technology from its banks, military, state-owned enterprises, and key government agencies by 2020.²⁶

Late in 2014, in the wake of the Snowden revelations, Beijing announced plans for new national security, cybersecurity, and antiterrorism laws. A new National Security Law was passed by parliament in the summer of 2015.²⁷ Effective January 1, 2016, ICT companies operating in China are required to provide law enforcement with technical assistance, including decryption of sensitive user data in connection with terrorism investigations.

While the final version of the law dropped explicit provisions to which the White House had objected, including data localization and backdoors, it is worded in terms sweeping enough that such requirements could still be imposed administratively.

The law, in combination with counterterrorism and cybersecurity laws, leaves foreign companies trying to do business in China exposed to considerable risk in the form of regulatory uncertainty and arbitrary regulatory action. Repeated reference in the law to the requirement that data and technology be "secure and controllable"²⁸ is widely interpreted as providing authority for the Chinese government to require foreign technology companies to build backdoors into their systems or hand over source code or encryption keys.²⁹ Such requirements could be imposed through a series of national security reviews that will focus on investment in key materials and technologies, including Internet and information technologies.

Censorship as Cyber Protectionism. China's increasingly sophisticated use of censorship also has increasingly serious implications for trade. As the US Trade Representative (USTR) noted in its latest *National Trade Estimate Report*, "China's filtering of cross-border Internet traffic has posed a significant burden to foreign suppliers."³⁰ Although it gives no indication that the US government is moving toward an effective response, the USTR reports that 8 of the 25 most trafficked worldwide websites are currently blocked by the Chinese government, including Google, Facebook, Twitter, and YouTube.³¹ The *New York Times* has been banned since 2012.

Some websites are banned permanently, others only temporarily, but the protectionist effect is increasingly clear. For example, the now-giant Chinese firm Baidu received a huge boost when Google was forced to withdraw from the Chinese market—Baidu stock shot up 16 percent the day it was announced—and similar instances abound.³²

When challenged to defend its "purge" of foreign Internet firms, China invokes WTO escape clauses that allow governments to intervene to protect "public morals" or "public order." But there are several challenges to the misuse of those exceptions that the US could and should raise on the basis of WTO rules.

When China achieved WTO membership, it assumed substantial obligations under the WTO's General Agreement on Trade in Services (GATS). GATS imposes several across-the-board mandates relating to transparency, impartiality, nondiscrimination in government actions, and opportunity for independent judicial review of administrative decisions. The Chinese government has routinely ignored these due process obligations in taking regulatory action against foreign companies, providing one route for a WTO challenge.

In addition, WTO members undertake sector-specific commitments that apply, for example, to web-based and telecommunications services. There is at least some support in WTO case law for challenging censorship as a violation of those commitments.³³ In cases involving China, the WTO Appellate Body has clarified that the public-morals exception could be invoked for only narrow, individual circumstances and was not a license for unrestricted censorship.³⁴ Technology that permits selective filtering also provides a basis for arguing that arbitrary blockages and permanent bans on websites should be considered disproportionate.³⁵

The US should vigorously use WTO mechanisms to challenge China's actions in this domain. It should also insist, as a matter of priority in bilateral relations, that China clarify in regulation how the new laws are to be implemented. The US should make it clear that it will retaliate if Beijing uses the new laws as a pretext to exclude competition from US and other foreign firms in the Chinese market.

While punitive reciprocal measures are best avoided in trade, the US has strong leverage because China wants Chinese companies to be able to invest in the US, and restricting access to such investment opportunities is not nearly as costly to the practitioner as other measures. Since 2013, China has invested more in the US than in any other country and is expected to invest \$30 billion in 2016, twice the 2015 figure.³⁶

The US economy greatly benefits from Chinese investment, and tit-for-tat reciprocity does not generally constitute good trade policy. But the aggressive Chinese cyber strategy is tilting the playing field in ways that hurt strategic US interests and individual US companies. An appropriately forceful strategy is warranted in response. The US should communicate the intention to retaliate

and demonstrate, through carefully chosen actions, that China is well-advised to take the threat seriously.

On the other hand, part of the TPP's strategy was to establish a framework for cooperative international relations on a free and open basis with China's neighbors. Henry Kissinger has argued that the best hope for a future of peaceful and fruitful relations with China lies in creating opportunities for cooperation while limiting the possibilities for conflict, perhaps through a "Pacific Community" based on security cooperation and free trade as in Europe. Hence the importance of the TPP in US-China relations. The US government should think of TPP as a framework for cooperative relations that China may one day be willing to join. That strategy enhances the chances that, in the long-run, issues of concern in the digital domain will be resolved more in the spirit of cooperation than confrontation.

Issues Affecting the EU. The US also faces digital-trade challenges with the European Union, although they are not nearly as severe as those with China. EU countries are more committed to free and open trade, particularly in the digital arena. The main challenge in Europe arises not from a desire to protect and advantage domestic companies at the expense of foreign ones, but rather from a particularly strong desire to protect privacy, sometimes at the expense of free speech and free commerce.³⁷

The two main problem areas here arise from the emerging right to be forgotten and the EU's data-protection policies, which create a need for the US to negotiate "safe harbor" agreements for American companies to be able to operate relatively freely. These and related issues of free data flows should be folded into the main trade negotiations, namely the TTIP and TISA. The issues have taken on added urgency with France's decision to fine Google more than \$110,000 for refusing its demand to implement the right to be forgotten by removing material on websites accessible outside of France.³⁸

In 1995, the European Union adopted the Data Protection Directive, which provides several special protections for personal information, including the right to notice and consent to the collection and public disclosure of personal data and guaranteed security for any

Timeline: The Right to Be Forgotten

The right to be forgotten arose out of an obscure Spanish court case, but it has become a major obstacle to EU-US digital commerce.

1998: Spanish citizen Mario Costeja Gonzalez puts his home up for auction to address his financial troubles. The auction details are covered in a Spanish newspaper and later published online.

2010: Mr. Gonzalez lodges a complaint with the Spanish Data Protection Agency (AEPD) against the newspaper, Google, and Google's Spanish subsidiary. He argues that the search results related to the auction of his home are irrelevant and damaging to his reputation and that Google should delist all search results related to the repossession. The case is referred to the ECJ.

May 13, 2014: The ECJ rules in favor of Mr. Gonzalez. In this ruling, the ECJ establishes EU citizens' right to request personal information be delisted from search results, subject to case-by-case analysis and balanced against competing rights such as freedom of expression and the public interest.⁴³

September 21, 2015: CNIL, France's privacy regulator, rejects Google's attempt to limit the application of the right to be forgotten to EU domains, effectively calling for a global application of the rules.⁴⁴

January 2016: The EU releases the General Data Protection Regulation (GDPR)—a massive overhaul of European privacy law—which includes a provision on the right to be forgotten. The provision establishes a system under which platforms have a strong disincentive to dispute takedown requests, threatening free expression and access to information on the Internet.⁴⁵

May 2016: Google announces it is appealing France's fine for failing to accept extraterritorial application of right to be forgotten.⁴⁶

To date: As of May 19, 2016, Google has received 381,495 requests, evaluated 1,344,859 URLs for removal, and delisted 485,627 links.⁴⁷

data collected, with certain exceptions.³⁹ The US, on the other hand, provides certain protections for private information (e.g., the Fair Credit Reporting Act), but the First Amendment broadly protects the right to publish information about people.

After the EU directive was passed, the US and the EU negotiated a so-called Safe Harbor agreement, under which US companies could certify that they met privacy obligations prescribed in the 1995 directive. These obligations include notice to individuals that data are being collected, an option for the individual to opt out of data collection, certification that data are transferred only to third parties that also abide by the Safe Harbor rules, adequate data security, allowing individuals to see and correct data if necessary, and proof of effective enforcement of the rules.⁴⁰

The Snowden leaks helped make the Safe Harbor agreement highly controversial in Europe, as information emerged about the access that NSA has gained to private European information through US companies.⁴¹ On October 8, 2015, the European Court of Justice (ECJ) ruled that the Safe Harbor agreement was invalid. The court ruled that EU citizens were not adequately protected and that individual EU member states could investigate and rule on privacy complaints from their citizens.⁴²

With thousands of companies reliant on the Safe Harbor agreement to do business in Europe suddenly facing enormous potential legal liability, US and EU negotiators scrambled to negotiate a new framework. On February 2, 2016, they released the US-EU Privacy Shield, which appears to have effectively covered American companies, although it is also expected to be challenged in court.⁴⁸

On April 14, 2016, the EU Parliament formally approved the General Data Protection Regulation (GDPR), which will go into effect in 2018. It will strengthen the individual's control over their personal data by new rights that will be bestowed on EU citizens, such as the right to data portability and the right to be forgotten.⁴⁹ This timeline raises the pressure on negotiators to conclude TTIP.

In 2014, the ECJ ruled that individuals had the right to demand that links on the Internet with information about themselves be removed from search engines, even if the information was accurate, the so-called "right to be forgotten."⁵⁰ This ruling forced on Google, which has 80 percent of the search-engine market in Europe, the responsibility for implementing EU privacy regulations. By the end of 2014, Google had complied with 41 percent of the requests to remove links (208,000 of 503,000 links) under the right to be forgotten.⁵¹

In July 2015, the situation took a dramatic turn for the worse when CNIL, France's data-protection authority, demanded that Google remove the prohibited links from all its search engines worldwide. In effect, the French government, extrapolating from the ECJ decision, is mandating that a US-based multinational company follow the extraterritorial dictates of a national regulator on a worldwide basis.⁵² As noted earlier, in March 2016, France fined Google more than \$110,000 for not scrubbing web search results widely enough.⁵³ In May 2016, Google announced it was appealing the decision.⁵⁴

The US and EU are currently negotiating the TTIP agreement, which will include modernize provisions for data flows and Internet regulation. Europe's right to be forgotten directly flouts principles of free trade in data, as well as in other goods and services. US negotiators should introduce this issue into the ongoing talks, with the stipulation that, at a minimum, Europe's attempt to force a worldwide delisting of information would not be allowed. In addition, since the TTIP negotiations are likely to stretch out over some years, the Obama administration should immediately initiate bilateral negotiations on this issue.

Barriers to Data Flows. Cross-border data flows, which are essential to the new economy, have been made possible by the Internet's free and open architecture.

The Microsoft-Ireland Case

France is not the only country asserting extraterritorial jurisdiction over digital information. In what is commonly known as the Microsoft-Ireland case, the US Department of Justice (DOJ) is asserting the right to force Microsoft to produce data stored on the company's servers in Dublin, Ireland.

The case began on December 14, 2013, when the DOJ was granted a warrant ordering Microsoft to produce the contents of emails connected to a drug-trafficking case. The emails themselves were stored in a data center owned and operated by Microsoft but located in Dublin. Microsoft challenged the warrant, which was upheld in April 2014, and a series of rulings and appeals have now landed the case in the Second Circuit Court of Appeals.⁵⁵

The fundamental legal questions at stake in this case are whether the DOJ's search would technically be taking place in the US or Ireland and whether Microsoft's data center or Microsoft itself is subject to the warrant. A favorable ruling for Microsoft could make it difficult for US law enforcement to pursue and indict criminal behavior, while a favorable ruling for the DOJ would establish what some characterize as a dangerous legal precedent, by which nations such as China, Iran, and Russia could compel the disclosure of data stored in the US. A massive amount of Cloud-enabled commerce hangs in the balance, with some of Microsoft's allies alleging that a decision in DOJ's favor "could cost U.S. businesses billions of dollars in lost revenue."⁵⁶

Alas, even as data flows increase along with access and connection speeds—and the emergence of Cloud-based storage and data-processing services—governments around the world are racing to erect barriers. Barriers to data flows come in many forms, but their impact is almost uniformly negative for foreign companies, domestic companies, and the Internet itself.⁵⁷

Barriers to market access affect data flows by generally affecting flows of goods, financing, and services. Data-localization measures require companies to store data or conduct other digital activities within a country's borders. Local content requirements mandate that a certain percentage of a good or service be produced locally or discriminate against foreign providers in other ways. Digital examples include requiring Internet searches to be performed by local data centers. Forced transfers of intellectual property as a condition of doing business in a country are particularly pernicious, with China being the preeminent example.⁵⁸

Like all forms of protectionism, barriers to data flows obviously hurt foreign companies hoping to enter a country's domestic market. But they are just as hurtful to the home country's economy. Behind such barriers, businesses and business practices tend to fall further and further behind the longer they are shielded from competition and, often, from access to the latest technology. The effects are felt throughout the local economy as local firms are deprived of the distributed, hyper-efficient supply chains made possible by a free and open global Internet.

The effects also diminish world economic growth by diminishing the network effect, which increases an Internet platform's productivity and value in proportion to the number of users on the system. Barriers to data flows are particularly devastating for the developing world. A recent Deloitte study concludes that expanding Internet access to the four billion people who do not currently have it in developing countries to the levels of developed countries would increase productivity by 25 percent, add \$2.2 trillion to their collective GDP, and increase GDP growth by more than 70 percent.⁵⁹

The US government should make digital-trade issues its highest priority in its trade strategy and should seek to eliminate barriers to data flows through diplomatic and commercial forums and in the WTO. Of course the US should be sensitive to legitimate government interests in safeguarding privacy or preventing access to morally offensive content.

Export controls on computer software constitute another form of barriers to international data flows. Such controls exist under US law⁶⁰ and through international agreements, primarily the Wassenaar Arrangement—a

multilateral export-control regime for sensitive dual-use technologies, which replaced the Cold War-era Coordinating Committee for Multilateral Export Controls (CoCom).⁶¹ Based on concerns that authoritarian regimes were using certain software technologies to censor and repress dissent, the 41 nations that participated in the scheme agreed in 2013 to subject intrusion software to the Wassenaar export-control regime.⁶² However, in the implementing regulations proposed by the Obama administration, the definition of intrusion software was so broad that it would have prohibited US companies from exporting legitimate security software used to prevent hacking, thereby weakening network security and putting US companies at a competitive disadvantage.⁶³

In February 2016, the Department of State bowed to pressure from Congress and the business community and announced it was giving up efforts to implement the software-intrusion provisions and withdrawing US agreement to the new provisions.⁶⁴ However, export controls' impact on the competitiveness of US information technology companies, especially on Cloud computing, remains a source of concern.⁶⁵

Encryption. The debate over encryption and law enforcement presents policymakers with painful dilemmas in many areas.⁶⁶ It is a major source of tension in trade policy, affecting the privacy of American consumers, the global competitiveness of US tech companies, and barriers to data flows abroad. Careful consideration of these ramifications compels the conclusion that the US government should reject a policy of weakening encryption for the benefit of law enforcement.

The battle between encryption and law enforcement burst into the headlines with the FBI's investigation into the San Bernardino terrorist attacks. On February 16, 2016, a federal judge ordered Apple to help the FBI access an iPhone 5C belonging to dead terror suspect Syed Farook. The FBI needed to circumvent a security feature that wipes all data on the iPhone after 10 failed attempts to enter the password. Apple CEO Tim Cook vowed to fight the FBI's demand, arguing that it was asking the company to build a backdoor to the iPhone that would weaken its security generally. The controversy was resolved when the FBI contracted with a third party to

bypass the iPhone's security feature by exploiting a previously unknown ("zero-day") vulnerability; on March 28, 2016, the FBI withdrew its petition for the court order.

Apple, Google, and makers of apps such as WhatsApp (owned by Facebook) and Signal have announced that they are adopting sophisticated end-to-end encryption that will soon be virtually unbreakable.⁶⁷ FBI Director James Comey has accused the tech companies of "marketing something expressly to allow people to place themselves beyond the law."⁶⁸ Senator Tom Cotton (R-AR) has warned that encryption could make Apple, Facebook, and Google "the preferred messaging services of child pornographers, drug traffickers, and terrorists alike" and has called for legislation to mandate a backdoor.⁶⁹ Senators Richard Burr (R-NC) and Dianne Feinstein (D-CA) have circulated a proposed Compliance with Court Orders Act of 2016, which would require encryption providers to be able to decrypt data subject to a court order, essentially requiring a backdoor.⁷⁰

The idea of requiring that encryption be breakable has several major drawbacks. First, there is no technical way to comply with such demands without introducing weaknesses into the encryption that other governments and cyber criminals might be able to exploit, making American companies and citizens alike more vulnerable to massive economic espionage and cybercrime. Second, mandating that American companies weaken their encryption will give a competitive advantage to foreign companies in jurisdictions that do not impose similar legal constraints, so the demand for encryption would merely be exported abroad. And finally, other governments will demand the same access of American companies abroad and may do so to conduct surveillance on political dissenters or for other nefarious purposes.

As three former US national security officials wrote, "China will insist on the same. There will be no principled basis to resist that legal demand. The result will be to expose business, political and personal communications to a wide spectrum of governmental access regimes with varying degrees of due process."⁷¹ As Claude Barfield writes, "The encryption debate forces a careful balancing of privacy and security. As matters now stand, the balance tilts in favor of the proponents of end-to-end encryption."⁷²

Developing a Comprehensive Digital Trade Strategy. The best approach for addressing cyber-trade issues is through multilateral trade agreements. The US can exert its influence in crafting free-market, competitive rules for the Internet in several potential trade negotiations. These include the TPP, the TTIP, the WTO TISA negotiations, and a future WTO trade round.

The final text of the TPP was released on January 26, 2016, and is awaiting enactment in the various capitals, including Washington, DC.⁷³ The TPP includes comprehensive rules for digital trade that would be legally binding and part of an overall dispute-settlement mechanism, including mandates on free data flows, on nondiscrimination of digital goods and services, and against local data storage and processing. Specifically, the e-commerce chapter of the TPP includes the following rules:

- **Cross-Border Data Transfer.** The TPP requires member states to allow the free flow of cross-border transfers of information, including personal information, for the conduct of business. The only exception to this obligation is in the pursuit of a "legitimate public policy objective."⁷⁴ The exception, however, cannot be undertaken in a manner that constitutes arbitrary or unjustifiable discrimination or a disguised restraint of trade.
- **Forced Localization.** No TPP member may require a business to locate computing facilities—including servers and storage devices—within its territory, with the same public-interest exception described earlier.
- **Transfer of Source Code.** The TPP prohibits a requirement to transfer software source codes as a condition of conducting business or investing in a TPP country. There is an exclusion from this rule for "critical infrastructure," which is undefined in the agreement.⁷⁵
- **Customs Duties on Internet Traffic.** The TPP prohibits the imposition of customs duties on cross-electronic transmission. This prohibition does not preclude TPP countries from imposing

internal taxes or fees on content transmitted electronically.

- **Privacy and Consumer Protection.** Other sections of the e-commerce chapter contain consumer-protection requirements and mandates to provide consumers with full information concerning their privacy rights.
- **Dispute Settlement.** Finally, the entire e-commerce chapter comes under the full scope of the TPP dispute-settlement system.

Why is TPP important? The 12 nations party to the agreement already constitute more than a quarter of total world trade and about 40 percent of world GDP. Several other trans-Pacific nations (Colombia, Indonesia, Korea, and Thailand) have expressed strong interest in joining this megaregional pact. Thus, if successful, the TPP will exert a powerful precedent-setting role in international trade rules governing the Internet.

Washington's long-range goal should be to incorporate the TPP template into the WTO whenever WTO member states agree to a new trade round. The sooner TPP passes, the better because of the crucial precedent it will set. Its principles should provide the baseline for all future US digital-trade negotiations.

Specifically, the principles that have defined US negotiating goals in TPP were set forth by Deputy US Trade Representative Robert Holleyman in May 2015.⁷⁶ Among the most important are:

- Agreeing unanimously to the principle of a free and open Internet;
- Completely prohibiting customs duties on Internet products;
- Guaranteeing nondiscrimination between domestic and foreign competitors;
- Opposing requiring technology transfers as a condition of doing business;
- Minimizing barriers to cross-border data flows;

- Preventing trading nations from forcing companies to localize data services;
- Safeguarding network competition;
- Ensuring technologically neutral electronic signatures and authentication; and
- Fostering innovative and effective encryption products.

These principles will hopefully guide US negotiators on future trade negotiations, starting with the TTIP. As TTIP negotiations progress, settling looming questions and potential conflicts regarding the Internet will be important. These would include several major issues described earlier, including the right to be forgotten and negotiations for a new Safe Harbor agreement. For both issues, the goal should be a binding legal settlement as a part of the final TTIP agreement.⁷⁷

The WTO Uruguay Round, which concluded in 1995, created a separate discipline for trade in services that is now binding for all WTO members: GATS. GATS introduced two sets of obligations on member states. The first simply adds the existing most-favored-nation (MFN) principle to the services sector. The second includes the national treatment principle and a set of market-access rules to ensure fair competition across and within borders. Examples would include a prohibition on limiting the number of service providers in a given sector.

These rules, however, apply only to sectors in which a member state has specifically committed to such liberalization. Among the sectors that have the highest WTO member commitments are professional, financial, and telecommunications services.⁷⁸ Importantly, these sectors are central to Internet services.

After the Uruguay Round, separate negotiations were mounted for financial services and basic telecommunications services. In addition, as noted earlier, individual bilateral and regional free-trade agreements (FTAs) have advanced services liberalization in general and have updated rules that include the Internet.

In 2000, WTO members agreed to launch a new overall round specifically for services negotiations. Participation is voluntary, but at this point some 24

WTO members have joined the negotiations. (This counts the 28 EU nations as one body: counting them separately would bring the total to more than 50.) They encompass more than 70 percent of the world's total services trade.⁷⁹

If successful, the negotiations would multilateralize many of the goals and provisions in existing FTAs, as well as those under negotiation. It is also assumed that more of the 161 current WTO members would gradually sign onto the updated services disciplines. As to substance, there is a good deal of overlap in the specific proposals being considered in the TPP and TTIP. From leaked documents, it is clear that the negotiators are tackling most of the priority issues, including restrictions on data flows, particularly regarding financial data, balanced privacy protections, consumer protections, prohibitions on mandated technology transfers, intellectual property rights protection for digital products and services, protection of source code, nondiscriminatory authentication and signature rules, and prohibition of customs duties.⁸⁰

Down the road, rules for digital trade should become a central element of the next WTO round of negotiations. The United States will certainly not achieve all its goals for digital-trade rules. But among the top priorities should be the extension of time-honored rules of the General Agreement on Tariffs and Trade (GATT) and WTO rules regarding nondiscrimination and national treatment. In digital-trade terms, this will mean lowering data flow barriers on an MFN basis, ensuring technological neutrality so that goods and services supplied electronically receive the same treatment as traditional modes of delivery, holding domestic and foreign service providers and Internet-related businesses to the same rules, adopting rules to avoid data-localization requirements, and adhering to a prohibition of mandated technology transfers as a condition of doing business in a country.

Principles and Policies

The ability of US and other Western information technology companies to operate freely in the global digital marketplace is a vital American national interest. With that freedom, the entrepreneurship and innovation

spawned by democratic capitalism will continue to give the US and its allies a strategic advantage in defining the future of cyberspace while ensuring that the continued march of technology contributes to the preservation and spread of our shared values. America's national interest is served by creating the largest, most open digital ecosystem possible.

To achieve these objectives, the US should take the following specific steps.

Develop and execute a comprehensive, “full-court press” strategy designed to change China’s conduct regarding digital trade and IP theft. An effective strategy will bring to bear all appropriate elements of US power and persuasion, including collaborating with our allies and trading partners, taking action through multilateral organizations such as the WTO, and if necessary, imposing bilateral sanctions, to persuade China to change its behavior regarding IP theft, mercantilism, and censorship.

Take effective concrete actions against cyber theft. The jury is still out on whether China is fulfilling its commitment under the Obama-Xi agreement. Some private Internet security companies report that cyber theft is continuing while others indicate it has declined significantly. If it is ultimately demonstrated that significant IP theft is continuing, the US should act with dispatch to bring cases and impose sanctions against both individuals and organizations. Having laid down a strong gauntlet before the August agreement, the US should not falter in its resolve—and show the world that it again cannot act on its own “red lines.”

Make clear that the US would retaliate against overly aggressive implementation of the Chinese National Security Law. Should the Chinese government act to force backdoors or demand source keys of de-encryption as a condition of doing business in China, the US government should move immediately to retaliate. Although generally tit-for-tat reciprocity is not a good policy because it harms both sides, given the high stakes involved in the future of US technological superiority, the US government should invoke the powerful pull of the US economy and act to curtail or

halt the activities of Chinese companies in the US market. China is desperate to promote outward investment for its growing manufacturing and technology companies, and the US should not cavil at using the huge market power of the US economy as a trade weapon if necessary.

Prosecute Chinese censorship through the WTO.

The US and its allies should make vigorous use of WTO mechanisms to challenge Chinese laws and regulations that violate its due process and obligations under GATS and other trade agreements.

Aggressively seek to negotiate a multilateral agreement (i.e., the TTIP) with the European Union that embodies the principles of the TPP and resolves current sources of friction, including data shield and the right to be forgotten.

Shift the focus of EU-US discussions to larger issues with larger long-run consequences, such as the need to act jointly to combat Internet balkanization and censorship, promote digital free markets, fight intellectual property theft, and defeat the efforts of authoritarian states to transfer Internet governance to international organizations.

Incorporate protections against state participation in cyber theft in multilateral agreements.

Extend the agreement between President Obama and President Xi Jinping that the two nations will refrain from knowingly participating in operations that result in the theft of trade secrets or other intellectual property, such as patents, copyrights, and trademarks. That pledge has been extended to the G20 nations.

While important, such pledges lack the full force of international law. With that in mind, the US should add this commitment to the TTIP negotiations with the EU and at least attempt the same tactic in the TISA negotiations. Again, the long-range goal would be to incorporate IP and trade secret electronic theft into the WTO Trade Related Aspects of Intellectual Property (TRIPS) agreement.

Promote reduced regulation of Internet firms and of the Internet. Work with G7, OECD, and other like-minded countries to develop a consensus on

minimizing economic regulation and taxation of the Internet, including discouraging the use of competition policy and antitrust regulation to discriminate against US Internet firms.

Continue developing and aggressively promoting a digital-trade policy. Strengthen the US digital-trade agenda to promote international data flows, while opposing data localization and nationalization. Embrace GATT/WTO rules of nondiscrimination. In digital-trade terms, this will mean lowering data flow barriers on an MFN basis, ensuring technological neutrality so that goods and services supplied electronically receive the same treatment as traditional modes of delivery, holding domestic and foreign service providers and Internet-related businesses to the same rules, adopting rules to avoid data-localization requirements, and adhering to a prohibition of mandated technology transfers as a condition of doing business in a country.

Do not require US firms to create backdoors in encrypted software and communications. Going forward, there will be two types of software and communications products: those that are as secure against hacking and malicious conduct as technologically possible, and those that are less secure because of government regulation. In a cyber version of Gresham's Law ("the bad currency drives out the good"), products with strong encryption will drive those with weaker encryption from the marketplace. If American firms are to continue being successful in the global marketplace, they must be able to offer the strongest possible encryption. Indeed, a credible commitment by the US government on this score could give US firms an important competitive advantage—and hence advance the strategic objective of ensuring that the US private sector continues to lead in creating the future of the Internet.

Strengthen digital-trade priorities in multilateral trade agreements. Embrace and build upon the TPP. In addition to reaching a comprehensive accord with the EU creating a digital free-trade zone as part of the TTIP, work to incorporate principles of digital free trade as part of the 50-participant TISA.

Ensure that export controls under US law and under the multilateral Wassenaar Arrangement do not unnecessarily place US companies at

a competitive disadvantage. Seek to reform existing rules to reduce compliance costs and regulatory risks.

Notes

1. Barfield, “When Trade and Tech Collide.”
2. Those companies are: Apple, Alphabet (the parent company of Google), Microsoft, Facebook, and Amazon. Dogs of the Dow, “Largest Companies by Market Cap Today,” <http://www.dogsofthedow.com/largest-companies-by-market-cap.htm>.
3. International Telecommunications Union, “ITU Releases 2015 ICT Figures,” http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx.
4. Stephen E. Siwek, *Measuring the US Internet Sector*, Internet Association, <http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf>.
5. McKinsey Global Institute, “Internet Matters: The Net’s Sweeping Impact on Growth, Jobs, and Prosperity,” May 2011, 16, <http://www.mckinsey.com/industries/high-tech/our-insights/internet-matters>.
6. James Manyika et al., *Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect the World Economy*, McKinsey Global Institute, April 2014, <http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age>.
7. Barfield, “When Trade and Tech Collide.”
8. McKinsey Global Institute, “Internet Matters,” 16.
9. United States International Trade Commission, “Digital Trade in the US and Global Economies, Part 2,” 2014, www.usitc.gov/publications/332/pub4485.pdf.
10. Meghana Ayyagari, Asli Demircuc-Kunt, and Vojislav Maksimovic, “Small vs. Young Firms Across the World—Contribution to Employment, Job Creation, and Growth,” World Bank, 2011, 26–27, http://www-wds.worldbank.org/servlet/WDSContentServer/WDS/IB/2012/11/06/000158349_20121106091157/Rendered/PDF/WPS5631.pdf.
11. Penny Pritzker and Devin Wenig, “The Rise of the Micro-Multinational, and Why it Matters to the US Economy,” *San Jose Mercury News*, May 14, 2015, http://www.mercurynews.com/opinion/ci_28115417/penny-pritzker-and-devin-wenig-rise-micro-multinational.
12. Naomi J. Halewood and Priya Surya, “Mobilizing the Agricultural Value Chain,” World Bank, 2012, 34, <http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Chapter-2.pdf>.
13. United States International Trade Commission, “Digital Trade in the US and Global Economies, Part 2,” 65.
14. Josh Rogin, “NSA Chief: Cybercrime Constitutes the Greatest Transfer of Wealth in History,” *Foreign Policy*, July 9, 2012, www.foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history.
15. The Commission on the Theft of American Intellectual Property, *The IP Commission Report*, May 2013, www.ipcommission.org/report/ip_commission_report_052213.pdf.
16. Exec. Order No. 13,694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities” (April 1, 2015), <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>. (Emphasis added.) Sanctioned persons would be denied access to the US financial system.
17. White House, “Fact Sheet: President Xi Jinping’s State Visit to the United States,” September 25, 2015, <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>. See also Jack Goldsmith, “Correction/Update: China Did Accept the American Formulation in the Cyber Deal,” *Lawfare*, September 27, 2015, <https://www.lawfareblog.com/correctionupdate-china-did-accept-american-formulation-cyber-deal>.
18. Cory Bennett, “Obama Talks Cyber with Chinese President Xi Jinping,” *Hill*, March 31, 2016, <http://thehill.com/policy/cybersecurity/274845-obama-talks-cyber-with-chinese-president-xi-jinping>.
19. Tom Risen, “Obama Pressures China’s Xi Jinping on Cybersecurity,” *US News & World Report*, November 30, 2015, <http://www.usnews.com/news/articles/2015/11/30/obama-pressure-chinas-xi-jinping-on-cybersecurity>.
20. Tim Starks, “Cardin Worried China Not Living Up to Cyber Theft Deal,” *Politico Pro Cybersecurity Whiteboard*, May 25, 2016, <https://www.politicopro.com/cybersecurity/whiteboard/2016/05/cardin-worried-china-not-living-up-to-cyber-theft-deal-072480>.
21. Bill Gertz, “DNI: China Continues Cyber Espionage,” *Washington Free Beacon*, February 9, 2016, <http://freebeacon.com>

/national-security/dni-china-continues-cyber-espionage/.

22. David E. Sanger, “With Spy Charges, US Draws a Line That Few Others Recognize,” *New York Times*, May 19, 2014, www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html.

23. Kenneth W. Dam and Herbert S. Lin, eds., *Cryptography’s Role in Securing the Information Society* (Washington, DC: National Academy Press, 1996), <http://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society>.

24. James Glanz and Andrew W. Lehren, “N.S.A. Spied on Allies, Aid Groups and Businesses,” *New York Times*, December 20, 2013, www.nytimes.com/2013/12/21/world/nsa-drag-net-included-allies-aid-groups-and-business-elite.html; Carla Anne Robbins and Helene Cooper, “Why Is the U.S. Spying on Its Allies?” *Wall Street Journal*, March 11, 1997, www.wsj.com/articles/SB858035232512801500; and Claude Barfield, “NSA Hacks Huawei: Man Bites Dog Story? Not Really,” *TechPolicyDaily.com*, March 25, 2014, www.techpolicydaily.com/technology/nsa-hacks-huawei-man-bites-dog-story-really/.

25. One US company was fined \$975 million for an “antitrust violation” that most experts consider spurious. See William Pesek, “China Will Pay Most for Qualcomm Fine,” *Bloomberg View*, February 10, 2015, <http://www.bloombergvie.com/articles/2015-02-11/china-will-pay-for-huge-qualcomm-fine>.

26. Joshua Eisenman, “Evaluating China’s Foreign Investment Reforms,” testimony before the US-China Economic and Security Review Commission, January 28, 2015, http://www.uscc.gov/sites/default/files/Joshua%20Eisenman_Testimony.pdf.

27. Edward Wong, “China Approves Sweeping Security Law, Bolstering Communist Rule,” *New York Times*, July 1, 2015, www.nytimes.com/2015/07/02/world/asia/china-approves-sweeping-security-law-bolstering-communistrule.html.

28. Paul Mozur, “China Tries to Extract Pledge of Compliance from US Tech Firms,” *New York Times*, September 16, 2015, www.nytimes.com/2015/09/17/technology/china-tries-to-extract-pledge-of-compliance-from-us-techfirms.html.

29. Timothy P. Stratford and Yan Luo, “China’s New National Security Law,” *National Law Review*, July 7, 2015, www.natlawreview.com/article/china-s-new-national-security-law; Frank Ching, “China Overreaches with New Security Law,” *Globe and Mail*, July 8, 2015, www.theglobeandmail.com/globe-debate/china-reaches-wide-and-deep-with-new-security-law/article25343592; and Michael Martina, “China Adopts New Security Law to Make Networks, Systems ‘Controllable,’” *Reuters*, July 1, 2015, www.reuters.com/article/2015/07/01/us-china-security/idUSKCN0PB39H20150701.

30. Michael B. G. Froman, 2016 *National Trade Estimate Report on Foreign Trade Barriers*, Office of the United States Trade Representative, <https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf>.

31. Lincoln Davidson, “Banging Your Head Against a Wall: China Shrugs at US Criticism of Censorship,” *Council on Foreign Relations Net Politics*, April 13, 2016, <http://blogs.cfr.org/cyber/2016/04/13/banging-your-head-against-a-wall-china-shrugs-at-u-s-criticism-of-censorship/>.

32. Claude Barfield, “China’s Internet Censorship: A WTO Challenge Is Long Overdue,” *TechPolicyDaily.com*, April 29, 2016, <http://www.aei.org/publication/chinas-internet-censorship-a-wto-challenge-is-long-overdue/>.

33. World Trade Organization, “Dispute Settlement: Dispute DS285: United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services,” January 28, 2013, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

34. *Ibid.*

35. Fredrik Erixson, Brian Hindley, and Hosuk Lee-Makiyama, “Protectionism Online: Internet Censorship and International Trade Law” (working paper, ECIPE, no. 12/2009), <http://ecipe.org/app/uploads/2014/12/protectionism-online-internet-censorship-and-international-trade-law.pdf>.

36. *Economist*, “China Going Global Investment Index,” http://www.eiu.com/public/topical_report.aspx?campaignid=ChinaODI2015.

37. Nevertheless, some observers regard recent antitrust actions against Google—and threats of actions against other US Internet firms—as being motivated at least partly by protectionist sentiments. Michael Martina, “U.S. Businesses Lobby Obama on China Tech Protectionism Concerns,” *Reuters*, August 12, 2015, <http://www.reuters.com/article/us-usa-china-tech-idUSKCN0QH1DM20150812>.

38. Julia Fioretti, “France Fines Google over ‘Right to Be Forgotten,’” *Reuters*, March 24, 2016, <http://www.reuters.com/article/us-google-france-privacy/idUSKCN0WQ1WX>.

39. Data Protection Commissioner of Ireland, “EU Directive 95/46/EC—The Data Protection Directive,” www.dataprotection.ie/docs/EU-Directive-95-46-EC/89.htm.

40. Barfield, “When Trade and Tech Collide.”
41. Claude Barfield, “Backlash: Commercial and Diplomatic Spillovers from the NSA Revelations,” TechPolicyDaily.com, November 22, 2013, www.techpolicydaily.com/technology/backlash-commercial-diplomaticspillovers-nsa-revelations/.
42. Natalia Drozdiak and Sam Schechner, “EU Court Says Data-Transfer Pact with US Violates Privacy,” *Wall Street Journal*, October 6, 2015, www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-datatransfer-pact-1444121361.
43. European Commission, “Factsheet on the ‘Right to be Forgotten,’” 2014, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.
44. Mark Scott, “France Rejects Google’s Efforts to Limit Application of Privacy Ruling,” *New York Times*, September 21, 2015, <http://bits.blogs.nytimes.com/2015/09/21/france-rejects-googles-efforts-to-limit-application-of-privacy-ruling/>.
45. Daphne Keller, “The New, Worse ‘Right to Be Forgotten,’” *Politico*, January 27, 2016, <http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/>.
46. Julia Fioretti and Mathieu Rosemain, “Google Appeals French Order for Global ‘Right to Be Forgotten,’” Reuters, May 19, 2016, <http://www.reuters.com/article/us-google-france-privacy-idUSKCN0YA1D8>.
47. Google, “European Privacy Requests for Search Removals,” May 29, 2016, <http://www.google.com/transparencyreport/removals/europeprivacy/>.
48. European Commission, “EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU–US Privacy Shield,” press release, February 2, 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm.
49. Todd Ruback, “EU Data Laws: An Update on GDPR and Privacy Shield,” Econsultancy, April 27, 2016, <https://econsultancy.com/blog/67784-eu-data-laws-an-update-on-gdpr-privacy-shield/>.
50. Alan Travis and Charles Arthur, “EU Court Backs ‘Right to Be Forgotten’: Google Must Amend Results on Request,” *Guardian*, May 13, 2014, www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eucourt-google-search-results.
51. Claude Barfield, “The Misbegotten ‘Right to Be Forgotten,’” *US News & World Report*, December 5, 2014, www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-misbegotten-right-to-beforgotten.
52. Samuel Gibbs, “French Data Regulator Rejects Google’s Right-to-Be-Forgotten Appeal,” *Guardian*, September 21, 2015, www.theguardian.com/technology/2015/sep/21/french-google-right-to-be-forgotten-appeal.
53. Fioretti, “France Fines Google over ‘Right to Be Forgotten.’”
54. *Ibid.*
55. Digital Constitution, “Milestones and Documents,” <http://digitalconstitution.com/about-the-case/>.
56. Chairman Michael McCaul (R-TX) of the Homeland Security Committee and Senator Mark Warner (D-VA) of the Senate Intelligence Committee have introduced legislation (HR 4651) that would create a Digital Security Commission to develop recommendations for maintaining privacy and digital security while ensuring that law enforcement and national security agencies have adequate authorities. Homeland Security Committee, “McCaul-Warner Commission on Digital Security,” <https://homeland.house.gov/mccaul-warner-commission-2/>. See also Matt A. Mayer, *National Commission on Terrorists’ Use of Technology Is Needed*, American Enterprise Institute, January 2016, <https://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf>.
57. One way of describing limitations on international data flows is in terms of “Internet fragmentation,” although this phrase is used to describe several distinct issues. For a useful discussion, see William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, *Fragmentation of the Internet: An Overview*, World Economic Forum, January 2016, http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.
58. Office of the United States Representative, “Remarks by Ambassador Michael Froman to AmCham China and the US Chamber of Commerce,” April 27, 2015, <http://ustr.gov/about-us/policy-offices/pressoffice/speechestranscripts/2015/april/remarks-ambassador-michael>.
59. Chris Williams and Davide Strusani, “Value of Connectivity: Economic and Social Benefits of Expanding Internet Access,” Deloitte, February 2014, www.deloitte.com/view/en_GB/uk/industries/tmt/extending-internet-access/index.htm.
60. See John F. McKenzie, *United States Export Controls on Internet Software Transactions*, Baker & McKenzie, August 2010, <http://>

www.bakermckenzie.com/files/Uploads/Documents/United%20States%20Export%20Controls%20on%20Internet%20Software%20Transactions.pdf.

61. See Wassenaar Arrangement, “About Us,” <http://www.wassenaar.org/>.

62. Federal Register, “Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items,” May 20, 2015, <https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>.

63. See Nate Cardozo and Eva Galperin, “House Grills State Department over Wassenaar Arrangement,” Electronic Frontier Foundation, January 12, 2016, <https://www.eff.org/deeplinks/2016/01/house-grills-state-department-over-wassenaar-arrangement>.

64. Katie Bo Williams, “Obama Administration to Renegotiate Rules for ‘Intrusion Software,’” *Hill*, February 29, 2016, <http://thehill.com/policy/cybersecurity/271204-obama-administration-to-renegotiate-international-anti-hacking-regs>.

65. See, for example, Ryan M. Murphy, “U.S. Export Controls over Cloud Computing: The Forecast Calls for Change,” *Syracuse Journal of Science & Technology Law* 28 (Spring 2013): 65, <http://jost.syr.edu/wp-content/uploads/Murphy-Final.pdf>.

66. Chairman Michael McCaul (R-TX) of the Homeland Security Committee and Senator Mark Warner (D-VA) of the Senate Intelligence Committee will be leading a Digital Security Commission to develop recommendations for maintaining privacy and digital security while ensuring that law enforcement and national security agencies have adequate authorities. Homeland Security Committee, “McCaul-Warner Commission on Digital Security.” See also, Mayer, *National Commission on Terrorists’ Use of Technology Is Needed*.

67. Jordan Robertson and Sarah Frier, “WhatsApp Encrypts User Messages Following Google, Apple,” Bloomberg Business, November 18, 2014, www.bloomberg.com/news/articles/2014-11-18/whatsapp-encrypts-user-messages-following-google-apple.

68. BBC News, “FBI Boss ‘Concerned’ by Smartphone Encryption Plans,” September 26, 2014, www.bbc.com/news/technology-29378172.

69. Office of Tom Cotton, “Cotton Responds to Apple CEO Tim Cook’s Comments on 60 Minutes,” press release, December 21, 2015, http://www.cotton.senate.gov/?p=press_release&id=283.

70. Office of Dianne Feinstein, “Intelligence Committee Leaders Release Discussion Draft of Encryption Bill,” press release, April 13, 2016, <http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649>.

71. Mike McConnell, Michael Chertoff, and William Lynn, “Why the Fear over Ubiquitous Data Encryption Is Overblown,” *Washington Post*, July 28, 2015, www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

72. Claude Barfield, “When Trade and Tech Collide.” As discussed elsewhere in this report, the US can and should respond to the encryption problem by enhancing its human and signals intelligence capabilities.

73. Office of the United States Trade Representative, “TPP Full Text,” November 4, 2015, <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text>.

74. *Ibid.*, Article 14.11(3).

75. *Ibid.*, Article 14.17(2).

76. Robert Holleyman, “Digital Economy and Trade: A 21st Century Leadership Imperative” (speech, New Democrat Network, Washington DC, May 1, 2015), <https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2015/may/remarks-deputy-us-trade>.

77. Julia Fioretti, “Court Adviser Deals Major Blow to EU-US Data Share Deal,” Reuters, September 23, 2015, www.reuters.com/article/2015/09/23/ireland-eu-privacy-idUSL5N11T11L20150923.

78. Joshua P. Meltzer, *A New Digital Trade Agenda*, International Centre for Trade and Sustainable Development and World Economic Forum, August 2015, <http://e15initiative.org/wp-content/uploads/2015/07/E15-Digital-Economy-Meltzer-Overview-FINAL.pdf>.

79. European Commission, “Trade in Services Agreement (TiSA),” May 26, 2016, <http://ec.europa.eu/trade/policy/in-focus/tisa/>.

80. WikiLeaks, “Trade in Services Agreement: Annex on Electronic Commerce,” June 3, 2015, www.wikileaks.org/tisa/ecommerce/05-2015/page-1.html.

V. Cybercrime and Law Enforcement

The Internet is a series of interactions based on trust. Unfortunately, each trust relationship entails a degree of vulnerability, and the number of trust relationships involved in opening up a computer and navigating to a website—or performing any online activity—has increased exponentially with the number of devices connected to the Internet. The resulting vulnerabilities are exploited in a variety of ways by a variety of perpetrators, ranging from economically motivated cybercrime (e.g., “ransomware”) to sabotage of critical-infrastructure systems such as electricity grids or financial networks.

This chapter focuses on strategies for addressing cybercrime—commercially motivated criminal behavior whose consequences, while large and rising, are primarily economic. Threats to national security associated with critical infrastructure are addressed in Chapter VI.

While precise estimates are difficult, one study estimates that the costs of cybercrime will reach \$2 trillion by 2019.¹ Another finds that the average cost of data breaches is rising and could exceed \$150 million per breach by 2020. Small businesses are particularly vulnerable, with an estimated 60 percent going out of business within six months of an attack.²

The largest companies are not immune, nor are the millions of people who depend on them. In November 2014, for example, malware installed in Target’s security and payments systems stole information from more than 40 million credit cards swiped at the company’s 1,797 stores nationwide. The company reportedly spent \$162 million in response to the breach, but some analysts estimate the total costs to be much higher.³ The Target breach was one of the largest recorded data breaches in history and was a major factor behind the company’s fourth-quarter profit decrease of 46 percent compared to the previous year.⁴

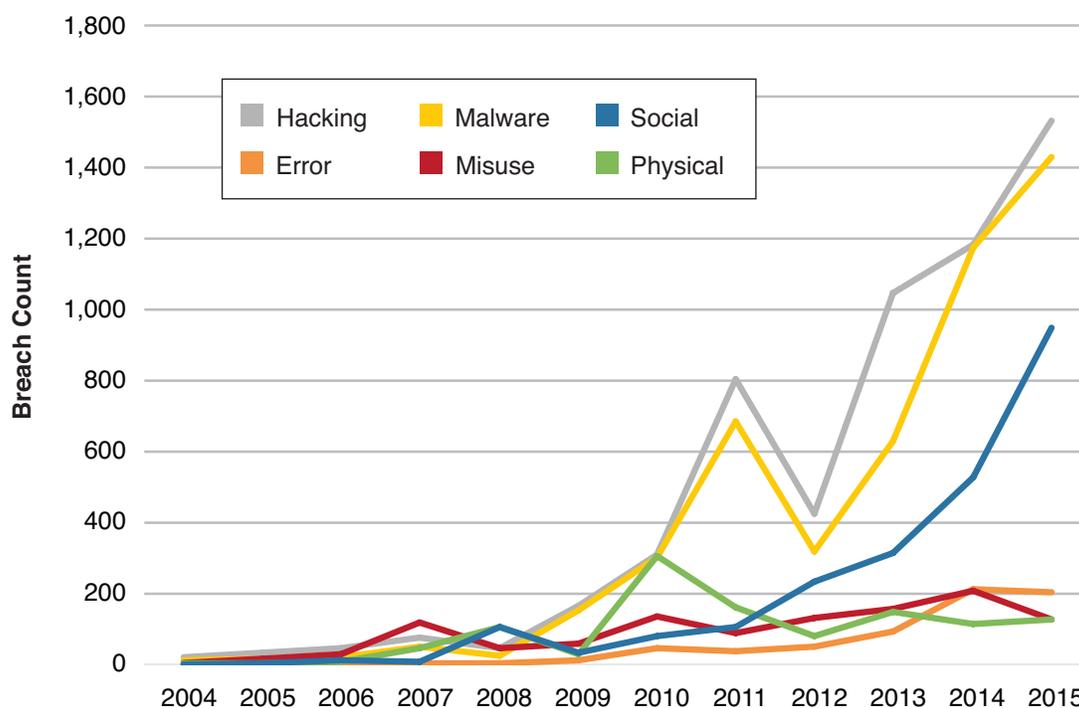
The almost daily occurrence of such incidents threatens to erode trust in the reliability and security of information, financial and otherwise, on the global Internet, perhaps significantly limiting its economic and other benefits. The World Economic Forum’s 2016 Global Risks Report found that “cyberattacks and related incidents have been entering the global risks landscape as among the most likely and most potentially impactful risks for the past two to three years — in North America, cyberattacks ranks as the most likely risk by far.”⁵

Maintaining the trustworthiness of the Internet against malicious actors and cybercriminals will require increased effort by both the private sector—whose networks and activities are the primary target of cybercrime—and governments, especially when it comes to addressing the transnational nature of cybercrime and the resulting challenges for law enforcement. In the “real world” of crime fighting, the criminal, crime, and victim are generally located in the same jurisdiction. With cybercrime, this is rarely the case: multiple national jurisdictions are the rule rather than the exception.⁶

Opportunities and Challenges

This section highlights the evolving nature of the “Internet arms race” and calls attention to three immediate policy challenges: enhancing incentives for effective self-defense, improving global collaboration among law enforcement agencies, and promoting and enabling information sharing among private actors and between the private sector and government.

New Threats, New Defenses: The Internet Arms Race. The economic consequences of cybercrime are large and growing. One study estimates that security

Figure 7. Cyber Breaches by Type, 2004–15

Source: Verizon, *2016 Data Breach Investigations Report*, 2016, 8, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>.

breaches will cost the global economy \$445 billion in 2016, more than the market capitalization of ExxonMobil, Facebook, or Microsoft.⁷ Another study projects the annual cost of cybercrime to businesses will top \$2 trillion by 2019.⁸ One important component of the cost is the resources devoted to prevention: recent forecasts put global cybersecurity spending at more than \$75 billion in 2015,⁹ growing to more than \$170 billion by 2020.¹⁰ Cloud security will account for more than half of this growth, as more and more businesses and consumers move their data to the Cloud.¹¹

The extent of the problem is staggering and getting worse. Nearly every corporate and civilian government network routinely suffers security breaches of one sort or another. The security firm FireEye reported in 2015 that of the 1,600 private networks it monitored, 96 percent had been breached at least once in the previous 12 months.¹² Verizon's latest report on data-breach investigations shows that the number of reported hacking

and malware attacks has tripled in the last five years (Figure 7).

The Internet ecosystem faces two broad categories of threats—those that are random, attacking wherever possible, and those that are highly targeted. Random attacks are cheap to produce, and the Internet is an ocean full of such threats. They are costly to individual devices on the network, but they rarely affect the overall system. That is because the scale-free structure of the Internet, in which only a relatively small number of nodes are highly connected and critical to the connectivity of the overall system, minimizes the repercussion of random failure at any given point.¹³ And because the expected return on any given random attack is low, expected returns do not justify more than minimal investment on the attacker's part, which is why most such attacks are automated.

More targeted attacks, however, have a higher expected return and can justify greater investment from the attacker. The difference is illustrated by the

difference between phishing and spear phishing. A phishing attack is when someone purporting to be, for example, an African heiress writes you an email addressed “My dear,” with a sob story meant to gain your confidence—and money. Such emails are randomly generated spam sent indiscriminately to every possible email address and are easy for spam filters to detect and segregate into a spam folder.

But some phishing attacks are more carefully packaged and targeted, as with a spear phishing attack, in which a cyber attacker seeks to gain the confidence of a particular person or group by imitating someone known to the target, such as the company CEO or a friend. The FBI recently warned about a “dramatic” increase in “CEO fraud,” in which the attacker spoofs a message by the boss and tricks an employee into wiring funds, saying that such attacks have cost businesses \$2.3 billion in the past several years.¹⁴

The private sector has responded aggressively to growing cybercrime. Strategies include stronger authentication (e.g., stronger passwords and the growing use of two-factor authentication) and increased reliance on encryption to protect data both at rest and in transit. More sensitive data can be compartmented, and key systems can be “air gapped,” creating physical space between the protected network and the rest of the Internet. And because—as the Iranians discovered with the Stuxnet virus—human error can defeat any of these defenses, the private sector has also devised ways to reduce human error through education and better e-hygiene. Networks are also becoming more resilient, with systems designed to continue operating even after penetration.¹⁵

Another avenue that has received growing attention is active defense—sometimes referred to as “hacking back.” In general, active defense involves some form of cyber activity by the targeted entity that reaches beyond the entity’s own network—that is, to disrupt the digital pathways through which the attack is occurring or to degrade or disrupt the attacker’s own network.

Active defense can take many forms. A relatively mild form involves detecting incoming traffic while in progress and turning it aside, as in a distributed denial-of-service attack. In one documented case, a company rerouted a flood of incoming messages back to the

sender—so an attack designed to temporarily shut down a website ended by shutting down the attacker’s computer system.¹⁶ In other cases, companies have sought to “retrieve” stolen data from the computer systems of the data thieves—that is, to make the stolen data unreadable by outsiders.¹⁷

Such countermeasures are not always effective, as they often depend on the attacker’s carelessness or technical limitations. Their effectiveness arguably is also limited because they impose only temporary costs on the attacker and thus have little long-term effect either as a deterrent or on the attacker’s capability.¹⁸

Private actors also can engage in counterattacks against the systems of attackers, either as a means of stopping ongoing intrusions or of imposing a cost designed to deter future ones. There are good reasons not to permit such activity by private companies, including that the attackers in question are sometimes foreign governments or enabled by foreign governments and that the ability to precisely target the effects of cyberattacks is inversely related to their effectiveness: to counterattack effectively likely involves a risk of collateral damage. At least for the time being, giving the private sector permission to conduct destructive cyber operations against the sources of cyber intrusions involves risks that exceed the likely benefits.¹⁹

One area where the private sector can contribute is in solving the difficult challenge of attribution. In September 2015, for example, two Internet security companies used social media and other online sources to expose the identities of a secretive hacking unit of the Chinese military.²⁰ Private firms should be encouraged to identify and report the sources of malicious attacks.

The US government has substantial capabilities to attribute the source of attacks, both through monitoring the Internet itself and through its broader signals (SIGINT) and human intelligence (HUMINT) gathering activities. Thus, attribution—as in other areas of national security—is based on the totality of the available information, and the absence of complete certainty about the identity of an attacker or potential attacker is not an insurmountable barrier to taking action.²¹

As discussed further in Chapter VI, the US also possesses substantial offensive cyber capabilities, although these capabilities are seldom used to target foreign

attackers, and such activities are almost never reported publicly.²² If other options—such as enhanced law enforcement activities, described later—are not effective in significantly reducing the costs of cybercrime to the US economy, the US government should consider announcing publicly that it is prepared to engage in offensive cyber operations against persistent foreign attackers.²³

Getting the Incentives Right: The Role of Cybersecurity Insurance. The private sector typically moves much faster than the government in developing and deploying advanced computer technologies. As a result, the first choice for improving cybersecurity is to give industry the right incentives and reduce regulatory barriers to adopting best practices.

Online-payment processing is a relatively bright spot in the cybersecurity story and should be treated as a model. Consumers in America are well insulated from the costs of computer crime. Due to a combination of regulation and commercial pressures, the costs of fraud are usually borne by banks and card issuers, not consumers. Thanks to sophisticated fraud-detection systems—and despite the best efforts of cyber criminals—it appears that these have thus far been kept in check. In a survey by the Federal Reserve Bank of Dallas of financial institutions and merchants, 90 percent of respondents reported 2013 losses from financial fraud were less than 0.5 percent of revenue.²⁴

The basic principle here should be extended more widely. The government does not tell merchants, payment-card processors, or banks what technologies to use or how to detect fraud; it tells them they are liable for the costs and leaves them to work out the best arrangements. Similarly, with other forms of cybercrime, the government should manage liability and other incentives but should not dictate specific technical solutions. One specific opportunity for improvement is data-breach notification. Currently, requirements vary from state to state. Having a uniform national standard would reduce compliance costs and lower uncertainty about how different courts would interpret terms such as “unreasonable delay.” President Obama has proposed a national data-breach law with a preemption clause. Similar bills have been introduced in both chambers of Congress.

In this context, the growing market for cyber insurance

not only offers a valuable safeguard from the financial damage that a data breach can impose on a company, but also incentivizes firms to take steps that reduce the risk of incursion and lower the costs when incursions occur.

The general liability coverage that most businesses maintain does not cover many or most of the potential losses from cybersecurity breaches, such as reputational damage, stock-price impacts, identity theft, and lawsuits from affected customers or employees. To cover those risks, insurers are developing specialized cyber insurance policies. These efforts have been somewhat hampered by the lack of actuarial data, which makes cyber risk difficult for underwriters to quantify, resulting in a substantial premium above what competitive insurance would be in a world of perfect information. Spotty information sharing on cyberattacks contributes significantly to this lack of data.

Another area of uncertainty for underwriters—and correspondingly a source of higher premiums—is the currently fluid and rapidly evolving security measures that firms take to protect themselves, which are difficult to standardize. These factors force insurance policies to be individually tailored.²⁵ One way to encourage the development of the cybersecurity market might be to adopt a model for liability protection similar to that of the SAFETY Act, which provides incentives for developing and deploying antiterrorism technologies by creating a system of risk management and limiting liability in cases in which qualified technologies and practices have been deployed.²⁶

Cyber insurance can play an important role in creating incentives for companies to enhance resilience in the face of cyberattacks by using, for example, disaster-recovery testing.²⁷ Another effective strategy is to reduce the amount of data that can be stolen in a breach. If the only access to sensitive data is via paper files, or via a separate offline computer system, hackers are much less able to get at that data. The government and private companies would improve their security by keeping data offline when it does not need to be readily or continuously accessed—and making sure that sensitive data that is kept online is strictly compartmented.

Empowering Global Internet Law Enforcement. In the “real world,” criminal investigations tend to begin

with substantial clarity about who the victims are, what the criminal act was, and where it occurred. Even when the perpetrator's identity is not immediately known, the motive is often clear. In cybercrime, all those crucial puzzle pieces can be shrouded in mystery.²⁸

In cybercrime, where the criminal act took place, much less who did it, is often unclear, making it difficult to determine which law enforcement agency—or country—has jurisdiction. Moreover, the same malicious act—for example, cyber theft of intellectual property—can be espionage, cyber theft, hacktivism, terrorism, or an act of war, depending on the perpetrator's motivation. Motive often remains a mystery even if law enforcement is able to discern the territorial location and the perpetrator's identity.

Determining the right agency and appropriate response to criminal cyber intrusion can also depend on the perpetrator's motives and identity. The DOD typically has the lead with nation-states and terrorists; the Department of Homeland Security (DHS) or the DOJ can take the lead with cybercrime; and both of those, along with the NSA and other elements of the intelligence community, can take the lead with cyber espionage.²⁹

The jurisdictional problem is further complicated by the fact that in a large proportion of cybercrimes, the perpetrator, criminal act, and victim are not located in the same national jurisdiction.³⁰ Indeed, many complex hacking schemes involve criminal organizations in which the perpetrators are themselves in multiple national jurisdictions. The Butterfly Botnet perpetrators, for example, were located in at least seven different countries. The near-simultaneous arrest of 10 suspects in Bosnia, Croatia, Herzegovina, Macedonia, New Zealand, Peru, the UK, and the US was a herculean effort in international coordination—and a risky one, given that cyber criminals often operate with the tolerance, if not connivance, of local law enforcement.³¹

International law enforcement capabilities have not kept pace with the jurisdictional challenges presented by cybercrime. Rather, the investigation and prosecution of cybercrime continue to rely on methods developed for traditional—and relatively rare—cross-border criminal activity. The problems start with extradition: even when the US has an extradition treaty, it may be that the crime in question is not a crime in the country where

the alleged perpetrator is located. For example, half the world's countries have no laws criminalizing child pornography.³² Even in countries that criminalize cybercrime, legal regimes can vary considerably.

The US government has responded to the challenge by relying more on information sharing and joint operations, both domestically and internationally. FBI agents are embedded in countries such as Estonia, the Netherlands, Romania, and Ukraine, but these activities typically focus on only the most high-profile investigations.³³

These challenges point to a need to reduce complexity; enhance law enforcement through more streamlined coordination and more effective imposition of costs, particularly with transnational cybercrime; and ensure the right incentives for market participants.

The Council of Europe Convention on Cybercrime was a valuable first step toward harmonizing national cybercrime laws. The G8 has created a cybercrime subgroup under its group of experts on transnational organized crime. The United Nations Convention Against Transnational Organized Crime, which the US ratified in 2005, provides for greater law enforcement cooperation and requires signatories to criminalize cybercrimes and certain related organized-crime offenses. However, a global legal environment that adequately facilitates international cooperation among law enforcement agencies still does not exist. Law enforcement agencies need to be able to interact with their peers in other countries on a fast track for investigative purposes—including, for example, ensuring that evidence of cybercrime is captured and preserved—and a more deliberate track for complex legal details, such as jurisdiction.³⁴

There are several reasons for the lack of adequate progress. First, the resources available to law enforcement vary around the world in quality and quantity. Of the more than 250 countries and territories connected to the Internet, few have law enforcement agencies with the training and capability to conduct investigation or law enforcement operations in cybercrime cases, including digital search and seizure, particularly on a real-time basis.³⁵ Second, more progress needs to be made to homogenize cybercrime laws and legal doctrines. Third, the processes embedded in Mutual Legal Assistance Treaties (MLATs) need to be updated and enhanced to address cybercrime's specific challenges.

Currently, law enforcement organizations often pursue cybercrime investigations more on the basis of informal relationships than established procedures, with predictably mixed results.

Recent conflicts between law enforcement and technology companies have also exacerbated the challenges to creating an effective global legal environment, and the battles over law enforcement access to data have called into question the viability of public-private cooperation. Data must be preserved in a timely fashion for law enforcement purposes. However, in an age in which data privacy is highly valued by consumers and concerns about government surveillance abound, preserving the data necessary to fight crime can be difficult, particularly when minimizing personally identifiable information is an industry priority and may be required by regulation.

On the diplomatic front, the US should be more vocal and effective in holding countries accountable for investigating and prosecuting cybercrime within their borders, cooperating in investigations, and helping create a global code of conduct for responding to cyberattacks.³⁶

CISA and the Need for Information Sharing. One crucial element of any effective cybersecurity strategy is information sharing on cyber threats across the public and private sectors. From a regulatory point of view, there are broad categories of information sharing: first, information that the federal government shares among agencies or with the private sector; second, information that private-sector entities share with each other; and finally, information that private-sector entities share with the government. As the Congressional Research Service observed in March 2015, “Despite widespread agreement about the need for enhanced cyber-information sharing, there is similar agreement among cyber-experts that current public and private sector information sharing efforts are simply inadequate.”³⁷

Information has been hampered by two obstacles: lack of legal clarity, particularly regarding potential criminal or civil legal liability, and collective-action problems. These problems affect the private sector sharing information in its possession more than the federal government’s ability to share information. The DHS’s legal authority to serve as repository and distributor of

cyber intelligence for the federal government is ample, although overlapping authorities across various agencies can lead to coordination problems, and there are limits to federal flexibility arising under various sources of law. Private-sector entities, on the other hand, have been particularly reluctant to share information with each other or the federal government because of both the fear of incurring legal liability for violation of privacy, anti-trust, or other laws and the collective-action problem mentioned earlier (i.e., free riders).

Regarding legal liability, President Barack Obama signed into law the Cybersecurity Information Sharing Act of 2015 (CISA) in December 2015 as part of the umbrella Cybersecurity Act of 2015 in the 2016 omnibus spending bill, which includes several other important cyber-related bills from the 114th Congress.³⁸ CISA authorizes the federal government to share among federal agencies, and with the private sector, unclassified “cyber threat indicators” and “defense measures”—that is, information on how networks have been or might be attacked and on how attacks have been or might be detected, prevented, or mitigated.

For classified cyber-threat information, CISA allows sharing with only private-sector entities that hold the relevant security clearances, which unfortunately is only a tiny fraction of those that could benefit from that information. CISA requires that the federal government protect personally identifiable information contained within information to be shared.

For information private entities may share with each other or with the federal government, CISA authorizes businesses to monitor their information systems and all information stored on, processed by, or transiting through the information system, as long as the monitoring is to protect the information or information systems. It grants to businesses full immunity from government and private lawsuits and other claims that may arise out of activities authorized by the law.

CISA enables businesses to share cyber-threat information with certain federal agencies, provides immunity from any resulting lawsuit, and further ensures that sharing does not constitute a waiver of IP protections. It requires businesses to minimize any personal information included in any cyber-threat indicators they share with the federal government that is not directly related

to a cybersecurity threat and to develop the necessary technical capability to do so.

CISA requires the federal government to develop and release periodic cybersecurity best practices tailored to the particular challenges faced by small businesses. It also requires the US attorney general and secretary of homeland security to publish guidelines to assist businesses in identifying information that would qualify as a cyber-threat indicator and eliminating personal information from shared cyber-threat information. These guidelines will seek to identify (1) cyber-threat indicators that contain personal information and are unlikely to directly relate to a cybersecurity threat, and (2) types of information that are protected under privacy laws and are unlikely to directly relate to a cybersecurity threat.

It is as yet too early to tell whether CISA will succeed in providing a sound legal framework for needed information sharing, and much depends on the manner in which it is implemented.

Meanwhile, beyond the legal question, CISA does not appear to have affected the underlying economic incentives at play in the information-sharing question, so the collective-action problems will remain. Given the enormous losses American companies suffer from cybercrime every year, companies could collectively increase their cybersecurity at relatively little cost by sharing information about cyberattacks. But, apart from fears of legal liability, cyber-threat information sharing has typically been bedeviled by a collective-action problem. Companies can “free ride” on their competitors’ disclosures, without incurring the risks of sharing any information themselves, which include perceived potential losses from giving away security lessons learned at great cost, loss of reputation and possible stock-price decline, and other benefits to competitors.

Moving forward, transparency, accountability, and trust are requirements for any cybersecurity information-sharing environment to function effectively. Clear guidelines that determine what and how information will be shared are necessary so that companies are comfortable disclosing real-time threat information with one another and with the government. Because corporate legal advisers have concerns about litigation liability, customer privacy, and potential government regulatory actions as a consequence of information they

share, companies will not contribute to any such system unless their concerns and exposure to risk are mitigated. In this way, these corporations’ incentives are more aligned with consumer interests than some privacy advocates would admit.

Protecting personal information must be a fundamental part of the agreement among all parties that share information. The Cybersecurity Act of 2015 is a promising start down this path. Enabling fast information sharing that exposes stakeholders to minimal risk will support a stronger cyber defense, help networks endure attacks, and keep future attack attempts outside the digital wall.³⁹

It is also important to educate the public that the information relevant for cybersecurity does not generally consist of relevant personal identifiable information. The fundamental purpose of information-sharing legislation is to reduce liability risks, encourage beneficial conduct, safeguard the networks American companies and consumers use, and ultimately strengthen America’s cyber readiness. With the focus on the speed of sharing and expanded liability protections, the point must still be made that cyber-threat information consists of things such as IP addresses, lines of malicious code, and network traffic data—not the personally identifiable information of a company’s customers. There needs to be a clear understanding that information sharing is used to stop computer-based crime, not invading an individual’s personal life.⁴⁰

Principles and Policies

An American strategy for addressing cybercrime involves three main elements: (1) incentivizing the private sector to lead the battle against cybercrime by adopting prevention and mitigation practices that reduce the incidence and costs of cybercrime; (2) collaborating with the international community to create an effective international legal framework and put in place the resources—abroad and at home—needed to apprehend and prosecute cyber criminals; and (3) being prepared to raise the costs of cybercrime to attackers and, ultimately, nation-states that refuse to cooperate in bringing them to justice. Specifically, the US should do the following.

Ensure that the private sector has the right incentives to protect itself. The right legal framework will incentivize private firms to build more secure products and practice more effective cybersecurity while reducing regulatory burdens.

The private sector typically moves much faster than the government in developing and deploying advanced computer technologies. Service companies, software and hardware vendors, and critical-infrastructure operators have different needs, and different incentive schemes will be appropriate for different sectors. The government should hold companies accountable for security breaches and require data-breach notification through a federal law that preempts state law to avoid redundant and unnecessarily burdensome requirements. The US should avoid any steps that could interfere with developing an efficient market for cyber insurance and should consider adopting a model for liability protection similar to that of the SAFETY Act.

Empower the private sector to more effectively defend itself. The private sector should be encouraged to explore the feasibility of a wide range of responses, including “turning aside” incoming attacks, retrieving stolen information, degrading a known attacker’s own cyber capabilities, and sharing attribution and other information with the US government and others. While recognizing that authorizing private actors to “hack back” could have undesirable consequences, the US should consider reforming the Computer Fraud and Abuse Act to clarify and perhaps in limited ways expand private companies’ ability to engage in active defense.

More actively use government capabilities to defend the private sector. While recognizing the need to maintain secrecy about sources, methods, and capabilities, the US should be more aggressive in using its full range of capabilities to detect and degrade the effectiveness of known, persistent foreign threats against public and private US systems and those of our allies. Given the sensitivity of classified information about capabilities and vulnerabilities and other operational considerations, it may sometimes be appropriate for the US government to assume the role of guardian angel without informing the private sector.

Strengthen international law enforcement cooperation against cybercrime. Develop an effective global legal framework for law enforcement agencies to cooperate internationally. Such a framework should also harmonize and streamline procedures for determining jurisdiction and for seamless cooperation in time-sensitive investigations and “hot pursuit” law enforcement operations. The differing cybercrime legal regimes and legal priorities of different countries need to be harmonized. Processes surrounding MLATs also need to be improved so law enforcement officials do not have to rely on informal relationships and other ad hoc arrangements.

Create an enduring framework for public-private partnership. First steps include (1) implementing CISA to encourage cooperation and trust between the law enforcement and intelligence communities and the private sector; and (2) making information sharing more of a two-way street—for example, by reducing the lag between the identification of new cyber threats by government and notification of private-sector targets.

Notes

1. Juniper Research, “Cybercrime Will Cost Businesses over \$2 Trillion by 2019,” press release, May 12, 2015, <http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>.
2. Robert Stromayer, “Hackers Put a Bull’s-Eye on Small Business,” PCWorld, August 12, 2013, <http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html>.
3. Ingrid Lunden, “Target Says Credit Card Data Breach Cost It \$162M in 2013-14,” TechCrunch, February 25, 2015, <http://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/>; Michael Riley et al., “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It,” Bloomberg, March 13, 2014, <http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>; and Brian Krebs, “The Target Breach, By the Numbers,” Krebs on Security, May 2014, <http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/>.
4. Riley et al., “Missed Alarms and 40 Million Stolen Credit Card Numbers.”
5. World Economic Forum, *The Global Risks Report 2016, 11th Edition*, 17, <http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf>.
6. Kristin M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, Congressional Research Service, January 17, 2013, 7, <https://www.fas.org/sgp/crs/misc/R41927.pdf>.
7. World Economic Forum, *The Global Risks Report 2016, 11th Edition*.
8. Juniper Research, “Cybercrime Will Cost Businesses over \$2 Trillion by 2019.”
9. Gartner, “Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach \$75.4 Billion in 2015,” press release, September 23, 2015, <http://www.gartner.com/newsroom/id/3135617>.
10. Markets and Markets, “Cyber Security Market by Solution (IAM, Encryption, DLP, Risk and Compliance Management, IDS/IPS, UTM, Firewall, Antivirus/Antimalware, SIEM, Disaster Recovery, DDOS Mitigation, Web Filtering, and Security Services)—Global Forecast to 2020,” June 2015, <http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html>. It may be tempting to see the growth of the cybersecurity market as a silver lining, but as an economic matter, the dedication of scarce resources to ameliorating cybercrime are a cost, not a benefit. See Gordon Tullock, “The Welfare Costs of Tariffs, Monopolies and Theft,” *Western Economic Journal* (1967): 224–32.
11. Steve Morgan, “Worldwide Cybersecurity Spending Increasing to \$170 Billion by 2020,” *Forbes*, March 9, 2016, <http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/>.
12. FireEye, *Maginot Revisited: More Real-World Results from Real-World Tests*, January 2015, <https://www2.fireeye.com/rs/fireeye/images/rpt-maginot-revisited.pdf>.
13. William D. O’Neil, “Cyberspace and Infrastructure,” in *Cyberpower and National Security*, ed. Franklin D. Karmar, Stuart H. Stahl, and Larry Wentz (Washington, DC: National Defense University Press, 2009), 3–4.
14. FBI Phoenix Division, “FBI Warns of Dramatic Increase in Business E-Mail Scams,” April 4, 2016, <https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams>.
15. See, for example, P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York, Oxford University Press: 2014), 36. “Resilience is what allows a system to endure security threats instead of critically failing. A key to resilience is accepting the inevitability of threats and even limited failures in your defenses.”
16. Deborah Radcliff, “Should You Strike Back?,” *Computerworld*, November 13, 2000.
17. Michael Riley and Jordan Robertson, “FBI Probes If Banks Hacked Back as Firms Mull Offensives,” Bloomberg News, December 30, 2014, <http://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives>.
18. Rabkin and Rabkin, “Enhancing Network Security.”
19. This does not mean such measures should not be considered in the future. See Commission on the Theft of American Intellectual Property, *The IP Commission Report*, National Bureau of Asian Research, May 2013, 83, www.ipcommission.org/report/ip_commission_report_052213.pdf. Possible steps include making clear that the CFAA should not be read extraterritorially to prohibit foreign companies from undertaking countermeasures against other foreign targets on behalf of US companies and considering the cir-

cumstances in which the US government might—as provided for under CFAA—authorize private actors to take countermeasures.

20. Richard Bejtlich, “Outside Perspectives on the Department of Defense Cyber Strategy,” testimony before US House of Representatives Committee on Armed Services, September 29, 2015, <http://docs.house.gov/meetings/AS/AS00/20150929/103985/HHRG-114-AS00-Wstate-BejtlichR-20150929.pdf>.

21. Thomas Rid and Ben Buchanan argue that “actual attribution of cyber events is already more nuanced, more common, and more political than the literature has acknowledged so far” and that “attribution is what states make of it.” They go on to explain: “Matching an offender to an offence is an exercise in minimising uncertainty on several levels. On a technical level, attribution is an art as much as a science. There is no one recipe for correct attribution, no one methodology or flow-chart or check-list. Finding the right clues requires a disciplined focus on a set of detailed questions—but also the intuition of technically experienced operators. It requires coup d’œil, to use a well-established military term of art. On an operational level, attribution is a nuanced process, not a simple problem. That process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades. As a result, it is also a team sport—successful attribution requires more skills and resources than any single mind can offer. Optimising outcomes requires careful management and organisational process. On a strategic level, attribution is a function of what is at stake politically. The political stakes are determined by a range of factors, most importantly by the incurred damage. That damage can be financial, physical, or reputational. Viewed from the top, attribution is part resourcing and guiding the internal process; part participating in final assessments and decisions; and part communicating the outcome to third parties and the public.” Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, nos. 1–2 (2014): 4–37.

22. An exception is the US government’s recent, publicly reported cyber offensive against ISIS. Cory Bennett, “Pentagon Hits ISIS with ‘Cyber Bombs’ in Full-Scale Online Campaign,” *Hill*, April 25, 2016, <http://thehill.com/policy/cybersecurity/277493-pentagon-targets-isis-with-first-full-scale-cyber-campaign>.

23. See, for example, Richard Bejtlich, “Outside Perspectives on the Department of Defense Cyber Strategy,” testimony before US House Committee on Armed Services, September 2015, <http://docs.house.gov/meetings/AS/AS00/20150929/103985/HHRG-114-AS00-Wstate-BejtlichR-20150929.pdf>. “US offensive digital capabilities should . . . directly target the foreign teams that are attacking private US entities.”

24. Federal Reserve Bank of Dallas, *2014 Payments Fraud Survey Summary of Results*, November 5, 2014, 12, <https://www.dallasfed.org/assets/documents/banking/firm/14survey.pdf>.

25. National Association of Insurance Commissioners and the Center for Insurance Policy and Research, “Cybersecurity,” January 25, 2016, http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

26. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), Section 861.

27. For example, Netflix has a tool called ChaosMonkey, which randomly turns off various computer systems, during business hours, to ensure that operations continue uninterrupted. Similar techniques are used at Amazon and other leading technology companies. Cory Bennett and Ariel Tseitlin, “Chaos Monkey Released into the Wild,” Netflix Tech Blog, July 30, 2012, <http://techblog.netflix.com/2012/07/chaos-monkey-released-into-wild.html>.

28. See, for example, Kristin Finklea and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, Congressional Research Service, January 15, 2015, <https://www.fas.org/sgp/crs/misc/R42547.pdf>.

29. Kristin M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, Congressional Research Service, January 17, 2013, 7, <https://www.fas.org/sgp/crs/misc/R41927.pdf>.

30. Internet Crime Complaint Center, *2014 Internet Crime Report*, Federal Bureau of Investigation, <https://pdf.ic3.gov/2014-IC3Report.pdf>.

31. Federal Bureau of Investigation, “FBI, International Law Enforcement Disrupt International Organized Cyber Crime Ring Related to Butterfly Botnet,” press release, December 11, 2012, <https://www.fbi.gov/news/pressrel/press-releases/fbi-international-law-enforcement-disrupt-international-organized-cyber-crime-ring-related-to-butterfly-botnet>.

32. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction*, 11.

33. Robert S. Mueller III, “RSA Cyber Security Conference” (speech, San Francisco, California, March 1, 2012), <https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>.

34. See generally, Jody R. Westby, *International Guide to Combating Cybercrime* (Chicago: American Bar Association Publishing, 2003).

35. Jody Westby, “Congress Needs to Go Back to School on Cyber Legislation,” *Forbes*, August 13, 2012, <http://www.forbes.com/sites/jodywestby/2012/08/13/congress-needs-to-go-back-to-school-on-cyber-legislation/3/#238d91821d98>.

36. Jody Westby, “Cyber Attacks on Press Reveal Gap in US Diplomacy,” *Forbes*, February 1, 2013, <http://www.forbes.com/sites/jodywestby/2013/02/01/cyber-attacks-on-press-reveal-gap-in-us-diplomacy/#474657c339ea>.

37. Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, Congressional Research Service, March 16, 2015, <https://www.fas.org/sgp/crs/intel/R43941.pdf>. The failure to adequately address information sharing is long-standing, dating to at least the late 1990s. See Jeffrey A. Eisenach, “Cybersecurity: Still Failing After All These Years,” *TechPolicyDaily.com*, September 21, 2015, <http://www.techpolicydaily.com/technology/cybersecurity-failing-after-years/>.

38. Consolidated Appropriations Act, Pub. L. No. 114-113 (2015). The Cybersecurity Act of 2015 is Division N of Pub. L. No. 114-113 and includes the Cybersecurity Information Sharing Act of 2015 at Title I, Secs. 101 et seq.

39. Shane Tews, “Information Sharing: A Necessary Tool for Securing America’s Networks,” *TechPolicyDaily.com*, April 2, 2015, <http://www.techpolicydaily.com/technology/information-sharing-a-necessary-tool-for-securing-americas-networks/>.

40. Shane Tews, “Congress Can Help American Companies Better Protect Themselves Against Cyber Attacks,” *TechPolicyDaily.com*, April 20, 2015, <http://www.techpolicydaily.com/technology/congress-can-help-american-companies-better-protect-themselves-against-cyberattacks/>.

VI. Critical Infrastructure and Cyber Defense

While the private sector can and must play a leading role in advancing freedom, security, and prosperity in cyberspace, responsibility for preventing and defending against threats to national security rests squarely with the federal government and ultimately the military—the Department of Defense and the forces it commands. However, the nature of cyberspace is such that the boundaries between military and civilian are blurred: both civilian (nonstate) and military (state) attackers are capable of inflicting great damage, and the targets of cyberattacks are at least as likely to be civilian as military. The unique characteristics of cyber threats—for example, difficulties in attributing the source of attacks—create further complications. This chapter focuses on the resulting challenges for US strategy and policy.¹

One challenge lies in defining clearly the responsibility for defending critical infrastructure, specifically the 16 critical-infrastructure sectors identified by President Obama in 2013 in Presidential Policy Directive (PPD)-21.² Thus far, that goal remains elusive: in important respects, responsibilities are not clearly defined, either within the federal government or between the government and private sector. As a result, America’s critical infrastructure is more vulnerable to a potentially devastating cyberattack than necessary.

A second challenge is to overcome the conceptual difficulties of characterizing and categorizing the new realm of cyber threats and to adjust US policies and strategies accordingly. Currently, there is little clarity regarding what sorts of attacks and attackers the US views as sufficiently serious to warrant use of military force, either for prevention or retaliation, and there has not been sufficient progress in developing doctrines for responding to threats from nonstate or rogue-state actors, against which traditional models of deterrence

are likely to be less effective than they are against established adversaries. These challenges are further complicated by technological impediments to quickly and accurately identifying the sources, or even understanding fully the effects, of cyberattacks.

A third challenge lies in establishing international norms and institutions for conduct in cyberspace, including creating mechanisms to reduce the likelihood of “accidental” wars resulting from misunderstandings such as incorrectly attributing the source of attacks.

The central objective is to prevent cyberattacks that could cause substantial loss of life or economic disruption.³ The prospect of such an attack—potentially disabling our financial systems or leaving millions without electricity and water for an extended period—seriously threatens our national security.

Opportunities and Challenges

The threat of serious cyberattacks is not prospective. As the first section of this chapter discusses, both the US and its adversaries currently have the capacity to use cyber weapons to significantly damage civilian and military interests, and such attacks are taking place with increasing regularity and severity. The following two sections describe the need for new strategies and doctrines to respond to the unique aspects of the cybersecurity challenge and for improved international norms and institutions to avoid and mitigate potential cyberwars. The last section discusses the need for reform of the current US approach to defending civilian government agencies and critical infrastructure.

Cyber Threats to National Security. The ability to use cyber power to disrupt and disable critical systems

Sources of Cyberattacks

Cyber threats may originate from several different types of actors, each of which poses different challenges. Cyber terrorists use cyberattacks to disrupt and potentially kill in pursuit of their objectives, most likely against public or private critical infrastructure. Cyber criminals are those who commit crimes in cyberspace or using the Internet; cyber thieves do so for profit. Cyber spies steal secret or confidential information from governments and private entities for a wide variety of purposes, usually in the service of governments. Cyber warriors make war in cyberspace on behalf of states. Cyber activists, hacktivists, and cyber vandals wreak havoc on the Internet for specific causes, or sometimes just to show they can.

These categories have no clear delineation: attacks may be carried out by multiple entities for multiple purposes. Each category of attack and attacker can implicate a different US government agency, policy, or legal regime, depending on the location, affiliation, and motive of the attacker, and the categories often overlap.¹²

and infrastructures, as well as to conduct cyber espionage, has been demonstrated repeatedly.

The first cyberattack for a military purpose that received wide public notice was the 2009 Stuxnet attack by the US and Israel against an Iranian nuclear facility in Natanz.⁴ The attack destroyed approximately one-fifth of Iran's uranium centrifuges by infecting their Siemens control systems; it subsequently spread to other Siemens control systems worldwide, eventually leading to its discovery.⁵ The effect was to significantly delay Iran's nuclear enrichment program by two years or more.

In August 2012, in an attack most observers attribute to Iran, Saudi Aramco suffered what has been called "the biggest hack in history."⁶ A virus delivered via a phishing email devastated the company's oil and energy divisions, wiping or destroying 35,000 computers in a matter of hours. The attack crippled operations, forcing the

company to rely on paper, typewriters, and snail mail. Saudi Aramco was forced to temporarily stop oil sales to domestic gas tank trunks, relenting after 17 days and giving oil away for free within the country. It was finally able to come back online after five months.

Iran was also behind attacks in 2011–13 on the US banking system and on a small dam in Rye, New York. While neither had catastrophic effects, they demonstrated further the ability of a rogue state such as Iran to employ cyber power. The DOJ subsequently indicted seven hackers alleged to be working for front companies of the Iranian Revolutionary Guard Corps.⁷

Another rogue state, North Korea, was behind the most widely publicized cyberattack to date, the 2014 attack on Sony Pictures' global network, which erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers. Stolen data later dumped publicly online included draft movie scripts, sensitive emails, salary lists, more than 47,000 Social Security numbers, and four unreleased films. The company has estimated that the direct costs of the attack were \$41 million, excluding litigation.⁸

As the Stuxnet case suggests, major powers are also actively engaged in using cyber power for national security. In the case of China's well-publicized 2014 intrusion into the Office of Personnel Management systems, the objective was espionage, and the theft unquestionably caused significant damage to US national security.⁹ In December 2015, a highly sophisticated attack on the Ukrainian power grid blacked out about 230,000 residents for several hours, sabotaging servers with malware and disabling remote operator management.¹⁰ That attack—the first confirmed successful attack on a national power grid—is generally attributed to some combination of Russian cyber criminals and the Russian government.¹¹

US officials have repeatedly warned of the threat of cyberattacks on the US. In April 2015, for example, Secretary of Defense Ashton Carter—announcing a new DOD cyber strategy—said:

The cyber threat against US interests is increasing in severity and sophistication. While the North Korean cyberattack on Sony was the most destructive on a US entity so far, this threat affects us all.

Just as Russia and China have advanced cyber capabilities and strategies ranging from stealthy network penetration to intellectual property theft, criminal and terrorist networks are also increasing their cyber operations. Low-cost and global proliferation of malware have lowered barriers to entry and made it easier for smaller malicious actors to strike in cyberspace.¹³

NSA Director Admiral Mike Rogers put it more succinctly: “I think it’s only a matter of time until we see destructive offensive actions taken against critical US infrastructure.”¹⁴ As CIA Director John Brennan explained on *60 Minutes* in February 2016:

Having the capability but then also having the intent are two different things. I think fortunately right now those who may have the capability do not have the intent. Those who may have the intent right now I believe do not have the capability. Because if they had the capability they would deploy and employ those tools.¹⁵

In January 2016, Director of National Intelligence James Clapper, testifying before Congress on the intelligence community’s official Worldwide Threat Assessment, placed cyber at the top of the list of US security threats.¹⁶

Developing New Doctrines. Despite the threat’s severity, the US continues to struggle to formulate and coalesce around a coherent doctrine for defending against cyberattacks. Initially, as Dr. Richard Andres of the National War College has explained, the US relied primarily on “the same formula that protects the United States from noncyber attacks.” He continues:

The federal government accepts responsibility for defending the nation against large-scale cyber attacks from nation-states and significant non-state actors on critical infrastructure but relies almost exclusively on the premise that it can deter major attacks by the same means it uses to deter conventional attacks.¹⁷

Effective deterrence is playing an important role in cyber defense, but a proper strategy must take account of its limits in the cyber context.¹⁸ During the Cold War, deterrence strategy focused on nuclear deterrence. The doctrine that came to be known as “mutual assured destruction” was hardly comforting, as Albert Wohlstetter noted in his seminal 1958 article, “The Delicate Balance of Terror.”¹⁹ But the Cold War’s deterrence construct had several important characteristics that contributed to its effectiveness and stability, including a known adversary (the Soviet Union, joined later by the People’s Republic of China), a single modality of attack (nuclear weapons), reasonably predictable potential consequences, a well-defined array of potential retaliatory options (also with reasonably predictable consequences), and the ability to identify (attribute) the source and estimate the damage from an attack quickly and with a high degree of certainty.²⁰

None of these characteristics are present with conflict in cyberspace. The possible sources of a cyberattack are virtually infinite; the attack vectors and methods numerous and poorly understood; the potential consequences unpredictable, even to the attacker; the options for response equally diverse and differentiated; and the ability to attribute the source of the attack and even to accurately assess the damage limited. As the Obama administration’s controversial characterization of the Sony attack as “cyber vandalism” highlights, even *characterizing* an attack may prove problematic. These characteristics necessarily limit the effectiveness of a doctrine that depends largely on the ability to credibly threaten potential adversaries with consequences contingent on the nature and effects of their hostile acts.²¹

To be sure, both cyber intelligence and more traditional intelligence-gathering techniques often afford ways of attributing cyberattacks to their sources, and there is no reason to think that the threat of retaliation cannot continue to be effective against established nation-states. But even in those cases, the ability to utilize proxies and other techniques may be sufficient to provide attackers with plausible deniability, thus making retaliation problematic.²² For example, cyberattacks against the US during the Kosovo action in 1999, and against Georgia and Estonia more recently, were never formally attributed to their most likely ultimate source,

the Russian government.²³ As one prominent study puts it, “Attribution is what states make of it.”²⁴

The Department of Defense Cyber Strategy for 2015 acknowledges the challenges cyber poses to a traditional deterrence approach to cyberattacks:

Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors’ behavior. . . . DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.²⁵

While deterrence must play a significant role in US cyber-defense strategy—just as it continues to play a role in our strategies against terrorism²⁶—deterrence by itself most likely cannot provide sufficient assurance against a serious cyberattack on the US.

Developing Norms of Conduct: The International Law of Cyberwar. As the attacks of September 11, 2001, showed, distinguishing between crimes and acts of war can sometimes be very difficult. The technologies of modern society allowed the criminal conspiracy of a few terrorists to result in mass destruction and civilian deaths such as no foreign enemy had ever inflicted on United States territory.

In the context of cyberspace, no less than with terrorism, old categories are difficult to apply, hampering the US government’s effort to devise a strategy to deal with a rapidly evolving security environment. NATO has sponsored the development and publication of *The Tallinn Manual on the Law Applicable to Cyber Warfare*, of which an expanded second edition is forthcoming.²⁷ The 2015 Department of Defense *Law of War Manual* has an entire chapter devoted to cyber operations.²⁸ But no international, legally binding instruments have

yet been drafted to explicitly regulate interstate relations in cyberspace.

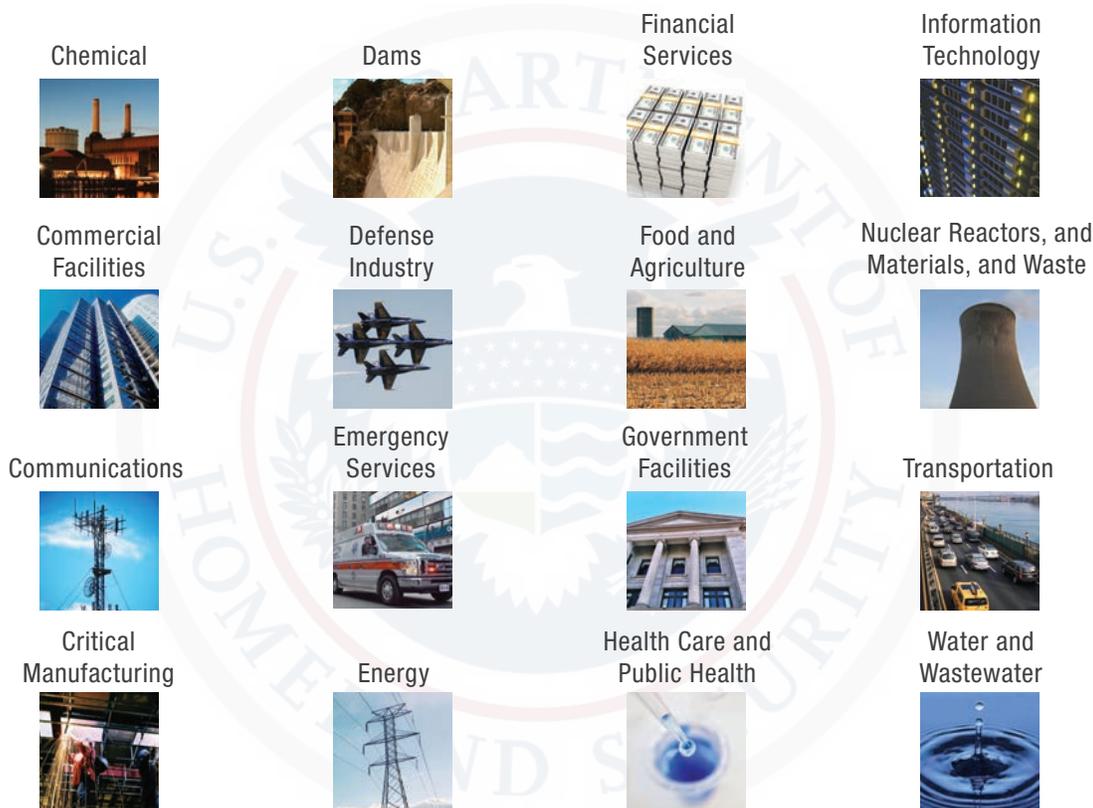
As noted earlier, the Obama administration has begun to lay out criteria that will trigger a national and potentially military response—basically when a cyber-attack significantly damages the US, its foreign policy, or its economy.²⁹ But there are no clear criteria yet for determining whether a cyberattack is criminal, hacktivism, terrorism, or an act of war.

In September 2012, the State Department took a public position on whether cyber activities could constitute a use of force under Article 2(4) of the UN Charter and customary international law. According to Harold Koh, the State Department’s legal adviser, “Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.”³⁰ Koh suggested that a meltdown at a nuclear plant, opening a dam and causing flood damage, and causing airplanes to crash by interfering with air traffic control would constitute examples.

By focusing on the ends achieved rather than the means with which they are carried out, this definition of cyberwar seems to fit within existing international legal frameworks. If an actor employs a cyber weapon to produce effects that might result from actual weapons, then using that cyber weapon rises to the level of the use of force. However, the United States recognizes that cyberattacks without such “kinetic effects” are also an element of armed conflict under certain circumstances.

Koh explained that cyberattacks on information networks in the course of an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyberattack with a proportional use of kinetic force. In addition, “computer network activities that amount to an armed attack or imminent threat thereof” may trigger a nation’s right to self-defense under Article 51 of the UN Charter.³¹

The White House’s *International Strategy for Cyberspace* of 2011 affirms that “when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.” It maintains that the US reserves the right to use all means necessary—

Figure 8. The 16 Critical Infrastructure Sectors

Source: Department of Homeland Security, “Critical Infrastructure Sectors,” <https://www.dhs.gov/critical-infrastructure-sectors>.

diplomatic, informational, military, and economic—as appropriate and consistent with applicable law.

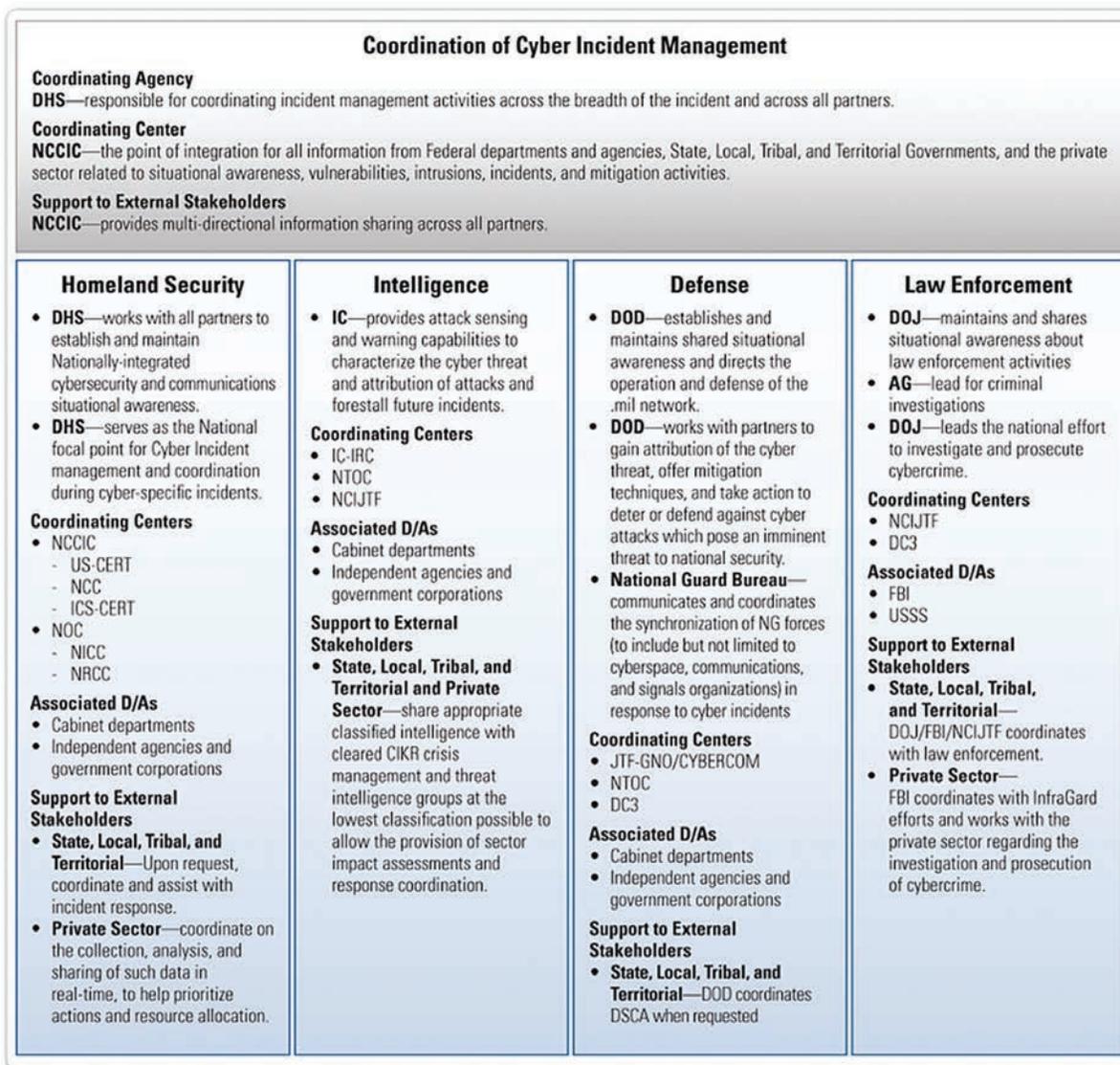
Such declarations are only a step in the direction of developing the necessary norms. The Internet ecosystem is one of intense national and economic competition. Where clear rules are lacking, the chances that competition will trigger conflict are heightened. This is particularly true when significant asymmetries exist between different adversaries’ cyber power, as between the US and rogue actors such as Iran and North Korea.

Defending Critical Infrastructure and Civilian Federal Agencies. Under current policy—specifically, PPD-21, issued by President Obama in 2013—responsibility for protecting critical infrastructure is dispersed across dozens of federal agencies and committees, with the private sector itself playing a lead role.³² The lack

of a centralized, general purpose “cybersecurity czar” is a strength, not a weakness. As shown in Figure 8, the PPD-21 defines 16 “critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”³³

The very diversity of these sectors, from banking to chemical manufacturing, communications to transportation, shows the folly of attempting to adopt a one-size-fits-all approach. And, as explained earlier, the pace of innovation in cyber technologies is far more rapid than any government regulatory process could hope to match. For critical infrastructure for the rest of the economy, the private sector must lead in designing

Figure 9. Coordination of Cyber Incident Management



Source: Department of Homeland Security, *National Cyber Incident Response Plan, Interim Version*, September 2010.

and operating networks in ways that make them resistant and resilient against cyberattacks.

Responsibility for defending civilian government networks and critical infrastructure—to the extent it resides in any single agency—resides primarily with the DHS.³⁴ The complexity of the challenge it faces is illustrated by the current scheme for coordinating cyber incident management. As shown in Figure 9, the DHS is tasked with coordinating “incident management activities across the

breadth of the incident and across all partners,”³⁵ with actual responsibility spread across literally dozens of agencies. While there are good reasons to be concerned about how effective this scheme would be, its complexity arguably is more an unavoidable consequence of the underlying problem’s complexity than of any obvious failure of planning or organization.

One area in which US capabilities and responsibilities are clearly mismatched is in the defense of civilian

government agencies and privately held critical infrastructure. It is widely agreed that neither the DHS itself nor the compendium of civilian agencies and committees now authorized to perform this mission has the operational capacity to actively engage in real-time defense of civilian agencies or critical infrastructure.³⁶ It is equally well understood that this capacity does reside within the US government, specifically within NSA's Information Assurance Directorate (IAD)³⁷ and DOD's Cyber Command. Indeed, network defense is IAD's primary function under National Security Directive 42 (NSD-42).³⁸ Active defense operations are also formally defined and authorized in PPD-20:

Defensive Cyber Effects Operations: Operations and related programs or activities—other than network defense or cyber collection—conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace.³⁹

While PPD-20 refers to actions to protect against “imminent” and ongoing threats, the reality is that the DOD currently does not have the authority to engage proactively in the defense of civilian agencies or critical infrastructure.

There have been several efforts to bridge the gap between the DHS's responsibilities and the DOD's capabilities. In 2010, the DOD and the DHS signed a Memorandum of Agreement (MOA) outlining procedures for bringing the DOD's cyber-warfare capabilities to bear in defending domestic civilian networks.⁴⁰ But the MOA does not give the DOD authority to proactively defend federal civilian networks or critical infrastructure on a day-to-day basis, relying instead on a cumbersome and time-consuming process requiring that the agencies negotiate terms of a “Request for Technical Assistance” before DOD can actively engage.

The Department of Defense Cyber Strategy of 2015 appears to expand the military's responsibilities. Whereas previous

strategies emphasized the DOD's role in protecting military networks from attack, the new DOD strategy also pledges to “defend the US homeland and vital interests from disruptive or destructive cyber attacks of *significant consequence*.”⁴¹ And PPD-20 specifically authorizes the DOD to undertake an “Emergency Cyber Action” if “such action is necessary, pursuant to the requirements of this directive, to mitigate an imminent threat or ongoing attack against U.S. national interests from inside or outside cyberspace and under circumstances that at the time do not permit obtaining prior without first obtaining the presidential approval that would otherwise be required.”⁴²

The problem with this status quo is that it is inherently reactive, effectively sidelining America's most capable cyber-defense assets until after a serious attack is either underway or at least known to be imminent. Not only does current doctrine leave unclear precisely what would constitute such an attack, or at what point the DOD would assume primary responsibility from the DHS; it also leaves US civilian agencies and critical-infrastructure industries effectively on their own to defend against the continuing daily barrage of cyber intrusions and attacks from private, state-enabled, and sovereign attackers—many with the potential for serious consequences.

A bill recently introduced in the House (H.R. 5390), which would redesignate the National Protection and Programs Directorate in DHS as an operational component to be called the “Cybersecurity and Infrastructure Protection Agency,”⁴¹ might represent an incremental improvement, but would not resolve the underlying problem: the persistent mismatch between DHS' capabilities and responsibilities.⁴³

Given the acknowledged—and demonstrated—vulnerability of US civilian agencies and critical-infrastructure operators, the US government's full capacity is needed to defend these critical networks. One means of doing so would be to grant authority to NSA's IAD to expand its field of operations beyond national security assets—as currently authorized under NSD-42—to civilian agencies and (more controversially) private-sector critical infrastructure, an idea suggested by then Deputy Secretary of Defense Bill Lynn in 2010.⁴⁴ Another alternative would be to move a portion of our cyber-defense capacity out of NSA into a

Figure 10. Unifying Capabilities and Responsibilities for Effective Cyber Defense



Source: Authors.

new agency—the Federal Cybersecurity Service—that is tasked with this mission and that operates under new statutory authority that would allow it to engage actively throughout the cyber domain. (See Figure 10.)

Principles and Policies

Because the 21st-century global economy depends on the Internet for electronic commerce, financial

settlements, and the coordination of trillions of dollars of economic activity, Internet security is a foreign policy and national security imperative, comparable to preserving maritime security and freedom of navigation. It is a vital national interest of the United States to maintain the Internet's integrity and ability to sustain an ever-growing digital ecosystem.

The same openness and dynamism that made the Internet's rapid expansion possible now provides

dangerous state and nonstate actors the means to undermine US interests. America's critical infrastructure and the federal government itself are vulnerable to devastating attacks that could severely disrupt our economy and throw millions into crisis.

Familiar concepts of deterrence and containment are of reduced utility, but no coherent strategic doctrine has replaced them. Moreover, the capabilities most urgently needed to protect the nation's critical infrastructure and federal civilian agencies are not unified. The US will have to develop new arrangements and strategies to use all the elements of national power—diplomatic, economic, technological, and military—to defend against the growing threat of serious cyberattacks. Specifically, the US should do the following.

Develop and implement a coherent doctrine on the use of military force to deter, preempt, prevent, and retaliate against malicious activity by sovereign and non-sovereign actors. The protection of US government agencies and privately owned and operated critical infrastructure against serious disruptions is a vital interest that the US must be prepared to achieve using all elements of national power. Similarly, threats to the long-run stability and functionality of the commercial Internet—while less dramatic in their immediate effects—can also cause serious harm over time.

Both types of threats present challenges to existing doctrines, which rely heavily on concepts of deterrence and retaliation that may not be applicable. Current approaches, which rely heavily on public attribution, criminal indictments of individuals, and the so far largely unexercised threat of economic sanctions, have not prevented the continuing increase in the incidence and effects of malicious conduct, nor have they ameliorated the threat of a debilitating or catastrophic attack. The US and its allies must engage more actively in identifying, interdicting, and preemptively degrading the capabilities of known, persistent threats against public and private US targets and those of our allies.

Create, empower, and resource a Federal Cybersecurity Service. There is an urgent need to bring the sophisticated network defense capabilities of the

US government, housed primarily within the NSA, to bear to protect civilian government agencies and critical infrastructure. One potential means of doing so would be to simply extend NSA's information assurance mission to these sectors, but for a variety of reasons—including concerns about allowing military operations within US borders—a more likely course would be to create a new Federal Cybersecurity Service (FCS) with the responsibility, authority, and operational capacity to engage in real-time defense of US civilian agencies and critical-infrastructure assets against cyberattacks. While the FCS's statutory authorities and responsibilities would be new, its operational capacity would come mainly from repurposing existing assets and capabilities now housed mainly within the IAD at the NSA. Conceptually, the task is to “clone” the IAD so as to quickly produce two highly capable operational forces, each with the resources necessary to perform its mission.

Creating such an entity would require confronting and resolving a variety of operational and policy issues, including how it would coordinate with agencies performing related functions (e.g., the DOD, DHS, and DOJ), how much authority it would have to operate within privately owned networks, how it would gather and share information inside and outside of government, and how much it would cost. One institutional model worthy of consideration is the US Coast Guard. While housed within the DHS, the Coast Guard has substantial institutional autonomy and dual reporting authority to the DOD.

As should be clear from the discussion throughout this report, it is not envisioned that the FCS would seek to manage, consolidate, or centralize all (or any) of the cybersecurity policy, coordination, or regulatory functions now performed by agencies throughout the federal government. To the contrary, its core mission would be limited to a simple task: identifying serious cyber threats and stopping them before they cause significant harm.

Increase the capacity and give greater priority to US intelligence agencies' efforts to gather actionable tactical and strategic intelligence on cyber threats to government and crucial private assets. The National Cyber Threat Intelligence Integration

Center, announced by the director of national intelligence in January 2016, should result in better coordination of existing intelligence.⁴⁵ Similarly, the CIA's new directorate of digital innovation promises to enhance the agency's ability to conduct cyber espionage. What remains to be done is to increase the capacity for, and priority accorded to, gathering the actionable intelligence needed for the US and its allies to neutralize and interdict the actions of foreign cyber attackers through traditional espionage (HUMINT and SIGINT) and cyber espionage.

Strengthen existing institutions and norms—and where necessary develop new institutions—to empower law-abiding governments to act against cyber threats. New doctrines of international law are needed to allow rapid action against known, persistent foreign threats across borders. Cyber threats present a major challenge to the Westphalian state system that must be addressed globally. In 2013, the UN's Group of Governmental Experts issued a report on cyber norms that states should follow, which included the norm of state responsibility for cyberattacks emanating from their territory.⁴⁶

Specific international institutions are needed to monitor and respond to cyberattacks, including institutions and agreements to facilitate communication with actual or potential adversaries in the event of a cyber-motivated crisis. The US should work to create an intergovernmental cyber analogue to Interpol and the IAEA.

Prioritize maintaining the preeminent position of American and Western companies in the Internet ecosystem. Promote the continued success of US private-sector companies in global Internet commerce. Forebear from actions (e.g., extraterritorial data collection, mandated encryption backdoors, and export controls) that harm US competitiveness, while advancing actions that allow US companies to operate successfully in key foreign markets, such as China, India, and the developing world. Maintaining the vitality of Internet innovation and entrepreneurship in the US is essential to advancing our long-run national interests. To do so, the US government must ensure that American-based companies have the freedom to compete in the global economy and the ability to exploit the global economies of scale and scope, which are essential to commercial success and economic progress.

Notes

1. As noted at the outset, it is beyond the scope of this report to assess specific military strategies, tactics, and capabilities.
2. White House, “Presidential Policy Directive 21—Critical Infrastructure Security and Resilience,” February 12, 2013, <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
3. President Obama defined the criteria under which the US would apply certain forms of financial sanctions to persons engaging in cyberattacks in an executive order. See Exec. Order No. 13,694 (April 1, 2015), <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>; and Barack Obama, “Presidential Policy Directive PPD-20, ‘U.S. Cyber Operations Policy,’” October 16, 2012, <https://archive.org/details/2012USPresidentialDirectiveForeignComputerNetworkTargets>.
4. Another candidate would be the distributed denial-of-service attacks aimed at Estonia in 2007. For a good summary of that incident and subsequent ones, see Dan Holden, “Estonia, Six Years Later,” Arbor Networks, May 16, 2013, <https://www.arbornetworks.com/blog/asert/estonia-six-years-later/>.
5. William J. Broad, John Markoff, and David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times*, January 15, 2011, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>.
6. Jose Pagliery, “The Inside Story of the Biggest Hack in History,” CNN, August 5, 2015, <http://money.cnn.com/2015/08/05/technology/aramco-hack/>.
7. See Ellen Nakashima and Matt Zapposky, “U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y. Dam,” *Washington Post*, March 24, 2016, https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html; and Sam Jones, “Cyber Warfare: Iran Opens a New Front,” *Financial Times*, April 26, 2016, <http://www.ft.com/cms/s/0/15e1acfo-0a47-11e6-b0f1-61f222853ff3.html>.
8. Peter Elkind, “Part 1: Who Was Manning the Ramparts at Sony Pictures?,” *Fortune*, July 1, 2015, <http://fortune.com/sony-hack-part-1/>; and Risk Based Security, “A Breakdown and Analysis of the December, 2014 Sony Hack,” December 5, 2014, <https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>; and Todd Smith, “Responding to the Hack of the Century,” Datapipe, October 11, 2015, <https://www.datapipe.com/blog/2015/10/11/responding-to-the-hack-of-the-century/>.
9. Bill Gertz, “Cybercom: OPM Hack Highlights China Big Data Spying,” *Washington Free Beacon*, January 25, 2016, <http://freebeacon.com/national-security/cybercom-opm-hack-highlights-china-big-data-spying/>.
10. Industrial Control Systems and Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
11. Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” *Wired*, March 3, 2016, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
12. Catherine A. Theohary and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief*, Congressional Research Service, March 27, 2015, <http://fas.org/sgp/crs/natsec/R43955.pdf>.
13. Beth Duff-Brown, “At Stanford, Secretary of Defense Ashton Carter Unveils Cyber Strategy, Calls for Renewed Partnership with Silicon Valley,” *Stanford News*, April 24, 2015, <https://news.stanford.edu/2015/04/24/ash-carter-talk-042415/>.
14. Phillip Swartz, “NSA Chief Says U.S. Cyber Infrastructure Lags Behind Adversaries, Expects Major Attack,” *Washington Times*, February 23, 2015, <http://www.washingtontimes.com/news/2015/feb/23/adm-mike-rodgers-nsa-director-says-us-infrastructure/>.
15. Scott Pelley, “CIA Director John Brennan on 60 Minutes,” *CBS News*, February 14, 2016, <http://www.cbsnews.com/news/cia-director-john-brennan-60-minutes-scott-pelley/>.
16. See James R. Clapper, “Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community,” testimony before US Senate, Select Committee on Intelligence, February 9, 2016, <http://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf>; and Alex R. McQuade, “2016 Worldwide Threat Assessment of the U.S. Intelligence Community,” *Lawfare*, February 12, 2016, <https://www.lawfareblog.com/2016-worldwide-threat-assessment-us-intelligence-community>.
17. Richard B. Andres, “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 91.

18. For a seminal discussion of cyberwarfare in general and the role of deterrence in particular, see William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs*, September/October 2010, <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.

19. Albert Wohlstetter, *The Delicate Balance of Terror*, RAND Corporation, November 6, 1958, <http://www.rand.org/about/history/wohlstetter/P1472/P1472.html>. President Reagan’s morally grounded concerns about MAD led him to develop the Strategic Defense Initiative. See Paul Lettow, “President Reagan’s Legacy and U.S. Nuclear Weapons Policy,” Heritage Foundation, February 6, 2006, <http://www.heritage.org/research/lecture/president-reagans-legacy-and-us-nuclear-weapons-policy>.

20. For a full discussion of strategic stability in the context of nuclear deterrence, see Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations* (Strategic Defense Institute and US Army War College, 2013), <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub1144.pdf>. The seminal document defining US Cold War strategy is NSC 68. “A Report to the National Security Council—NSC 68,” April 12, 1950, https://www.trumanlibrary.org/whistlestop/study_collections/coldwar/documents/pdf/10-1.pdf.

21. US Department of Defense, *The Department of Defense Cyber Strategy*, 11. “Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary’s attack will succeed.”

22. *Ibid.*, 9. “Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests.”

23. David E. McNabb, *Vladimir Putin and Russia’s Imperial Revival* (Boca Raton: CRC Press, 2015).

24. Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, nos. 1–2 (2015), <http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382>.

25. US Department of Defense, *The Department of Defense Cyber Strategy*, 10. This passage suggests an important distinction between deterrence by purely cyber means and deterrence using all elements of national power.

26. Matthew Kroenig and Barry Pavel, “How to Deter Terrorism,” *Washington Quarterly* 35, no. 2 (2012): 21–36, <https://www.ciaonet.org/attachments/20192/uploads>.

27. NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, <https://ccdcoe.org/research.html>.

28. US Department of Defense, *Law of War Manual*, June 2015, chap. 16, <http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf>.

29. Exec. Order 13,694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” April 1, 2015, <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.

30. Harold H. Koh, “International Law in Cyberspace,” remarks to USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012, <http://www.state.gov/s/l/releases/remarks/197924.htm>.

31. *Ibid.*

32. Responsibility for defending civilian government agencies is also dispersed across numerous agencies, although the OMB, under FISMA, is responsible for overall coordination. The GAO reports that federal agencies have “significant weaknesses in information security controls that continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support their operations, assets, and personnel.” See US Government Accountability Office, “Cybersecurity,” http://www.gao.gov/key_issues/cybersecurity/issue_summary.

33. US Department of Homeland Security, “Critical Infrastructure Sectors,” October 27, 2015, <https://www.dhs.gov/critical-infrastructure-sectors>.

34. US Department of Homeland Security, *National Cyber Incident Response Plan, Interim Version*, September 2010. According to a GAO report, “Department of Homeland Security officials told us that while the plan is identified as an ‘Interim Version,’ the officials have been told to treat this plan as if it was finalized.” US Government Accountability Office, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities During Cyber Incidents*, April 2016, <http://www.gao.gov/assets/680/676569.pdf>.

35. US Department of Homeland Security, *National Cyber Incident Response Plan, Interim Version*, September 2010.
36. See, e.g., US Government Accountability Office, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, January 2016, <http://www.gao.gov/assets/680/674829.pdf>.
37. National Security Agency, Information Assurance Directorate, “Message from the Director,” <https://www.iad.gov/iad/index.cfm>.
38. White House, “National Security Directive 42,” July 5, 1990, <https://www.cnss.gov/cnss/assets/authorities/NSD-42.pdf>.
39. Obama, “Presidential Policy Directive PPD-20,” 3.
40. US Department of Homeland Security and US Department of Defense, “Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity,” September 27, 2010, <https://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf>.
41. US Department of Defense, *The Department of Defense Cyber Strategy*. (Emphasis added.)
42. Obama, “Presidential Policy Directive PPD-20.”
43. See Aliya Sternstein, “US Homeland Security Could Get Its Own Cyber Defense Agency” *Defense One*, June 8, 2016, <http://www.defenseone.com/technology/2016/06/us-homeland-security-could-get-its-own-cyber-defense-agency/128940/>. She reports, “A bill introduced yesterday by the Homeland Security Committee—approved by a voice vote—would turn an existing DHS bureaucracy, the National Protection and Programs Directorate, or NPPD, into an ‘operational’ agency, like the Transportation Security Administration.” H.R. 5390 implements proposals made by DHS in a report to Congress on March 17, 2016. See US Department of Homeland Security, *Cyber and Infrastructure Protection Transition Way Ahead Fiscal Year 2016 Report to Congress*, March 17, 2016, <https://www.hsd.org/?view&did=791688>.
44. See Lynn, “Defending a New Domain.”
45. Office of the Director of National Intelligence, “DNI Clapper Announces Leadership of Cyber Threat Intelligence Integration Center,” press release, January 7, 2016, <https://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1299-dni-clapper-announces-leadership-of-cyber-threat-intelligence-integration-center>.
46. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174; and Adam Segal, “The UN’s Group of Governmental Experts on Cybersecurity,” Council on Foreign Relations, April 13, 2015, <http://blogs.cfr.org/cyber/2015/04/13/the-uns-group-of-governmental-experts-on-cybersecurity/>.

VII. Conclusion and Summary of Findings

Success in cyberspace is essential to the defense and promotion of America’s national interests. Digital technologies determine how many of the processes that define modern societies operate. The ability to control how these technologies are used in the present—and to influence the course of their development in the future—is a vital element of national power.

In the face of paradigmatic shifts, incumbents often get left behind. Three times in its history, the US has managed to avoid that fate, first by mastering modern sea power, then by understanding (just in time) the importance of air power, and then by leading the way into space. In all three cases, America succeeded both commercially and militarily. The rise of cyberspace arguably poses the most daunting challenge yet: its implications are more sweeping, its impact more complex, and its pace more rapid than anything that has come before.

This report puts forward the beginnings of a comprehensive strategy designed to ensure that the Internet revolution continues to serve America’s national interests by advancing freedom, security, and prosperity. In summary, these are the report’s key recommendations:

- Devise an overall strategic plan that is grounded in the realities of cyberspace itself, including the rapid pace of change; the importance of economies of scale and scope; the extent to which it is integrated into modern economies, cultures, and political structures; and its inherently global nature.

- Acknowledge the real and immediate threat to human freedom that is posed by authoritarian states’ use of cyber technologies. Take strong and effective actions to promote the values of liberal democracy in cyberspace.
- Recognize that America’s commercial success in the Internet ecosystem has been a source of tremendous strategic advantage and that preserving a level playing field for digital trade—one that fosters competition on the merits—is a vital American national interest.
- Create the private incentives and public capabilities needed to effectively fight cybercrime and commercial hacking, including the capacity to engage in enforcement actions throughout cyberspace—that is, globally.
- Embrace the concept of cyber as a new domain for the projection of power and put in place the doctrines, capabilities, and resources necessary to protect our military, governmental, and critical civilian infrastructure assets.
- Do all these things in the service of America’s central ideals of liberty and human rights.

Accomplishing these goals will take courage, imagination, and leadership, but America has risen to the challenge before. We hope these ideas will help it to do so again.

About the Authors

Jeffrey Eisenach is a visiting scholar at AEI and director of AEI's Center for Internet, Communications, and Technology Policy. He has served in senior positions at the Federal Trade Commission and the Office of Management and Budget. At AEI, he focuses on policies affecting the information technology sector, innovation, and entrepreneurship. Dr. Eisenach is also a senior vice president at NERA Economic Consulting and an adjunct professor at the George Mason University School of Law, where he teaches regulated industries. He writes on a wide range of issues, including industrial organization, communications policy and the Internet, government regulations, labor economics, and public finance. He has also taught at Harvard University's Kennedy School of Government and the Virginia Polytechnic Institute.

Claude Barfield is a resident scholar at AEI who researches international trade policy (including trade policy in China and East Asia), the World Trade Organization (WTO), intellectual property, and science and technology policy. He is a former consultant to the Office of the US Trade Representative. His many books include "Free Trade, Sovereignty, Democracy: The Future of the World Trade Organization" (AEI Press, 2001), in which he identifies challenges to the WTO and the future of trade liberalization.

James K. Glassman is a visiting fellow at AEI, where he works on Internet and communications policy in AEI's Center for Internet, Communications, and Technology Policy. He rejoined AEI in August 2014 after having served as undersecretary of state for public diplomacy and public affairs, during which time he led America's public diplomacy outreach and inaugurated the use of new Internet technology in these efforts, an approach he christened "public diplomacy 2.0." He was also chairman of the Broadcasting Board of Governors, the independent federal agency that oversees all US government

nonmilitary international broadcasting. Most recently, he was instrumental in the creation of the George W. Bush Institute, where he remains the founding executive director. Before his government service, Mr. Glassman was a senior fellow at AEI, where he specialized in economics and technology and founded the *American*, AEI's magazine. In addition to his government service, he was a former president of the *Atlantic*, publisher of the *New Republic*, executive vice president of *US News & World Report*, and editor-in-chief and co-owner of *Roll Call*.

Mario Loyola, a contributing editor at *National Review*, is the senior researcher and writer for AEI's Global Internet Strategy reports. He is director of the Center for Competitive Federalism at the Wisconsin Institute for Law and Liberty and a fellow of the Classical Liberal Institute of New York University School of Law. He is also an adjunct professor of law at George Mason University. He has served on Capitol Hill as counsel for foreign and defense affairs to the US Senate Republican Policy Committee and on the staff of Senator Ben Sasse (R-NE). He also served at the Department of Defense as assistant to the under secretary of defense for policy. His articles have appeared in the *Wall Street Journal*, *Atlantic Monthly*, *Weekly Standard*, *National Affairs*, *National Review*, *University of Chicago Law Review*, and elsewhere. He received a B.A. in European history from the University of Wisconsin-Madison and a J.D. from Washington University in St. Louis School of Law.

Shane Tews is a visiting fellow at AEI's Center for Internet, Communications, and Technology Policy, where she works primarily on cybersecurity and Internet governance issues. She is also an outside policy consultant at Vrge Strategies (formerly 463 Communications), a firm that advises high-tech organizations on Internet policies. Ms. Tews managed Internet security and domain issues as vice president of global policy

for Verisign Inc. She is currently vice chair of the board of directors of the Internet Education Foundation, a nonprofit organization whose mission is to promote a decentralized global Internet. She began her career in the George H. W. Bush White House, in the Office of Cabinet Affairs, and at the US Department of

Transportation, then moved to Capitol Hill as a legislative director for a member of Congress. Ms. Tews studied communications at Arizona State University and at American University, where she graduated with a bachelor's degree in general studies with an emphasis on communications and political science.