The Heritage Foundation
LEADERSHIP FOR AMERICA

BACKGROUNDER

No. 2785 | MARCH 28, 2013

A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace

Steven P. Bucci, PhD, Paul Rosenzweig, and David Inserra

Abstract
Cybersecurity is one of the most critical issues the U.S. faces today. The threats are real and the need is pressing. Despite the best intentions of those involved with previous cyber legislative efforts, a regulatory basis simply will not work: It will not improve security and may actually lower it by providing a false level of comfort and tying the private sector down with outdated regulations. Cyberspace's dynamic nature must be acknowledged and addressed by policies that are equally dynamic. Heritage Foundation national security analysts detail seven measures that the U.S. should implement to protect its assets and interests in the cyber domain.

The U.S. faces significant cybersecurity threats that jeopardize America's critical infrastructure, the freedoms that Americans exercise online, and the economic viability of U.S. businesses. The cybersecurity status quo is unstable, especially when considering the enormous and growing scope of these threats. To mitigate these threats, this paper provides a framework for congressional action that harnesses the power of U.S. industry and ingenuity, while safeguarding the freedoms and privacy of individual citizens. Through dynamic and cost-effective solutions, Congress can make cyberspace a safer and more productive place for U.S. citizens to pursue the American dream.

Failure to take responsible action, however, leaves the U.S. vulnerable to a variety of threats. Nation-states such as Russia, China, and Iran are more than willing to steal or destroy U.S. digital

Key Points

- The U.S. faces—and is largely unprepared for—significant cybersecurity threats that jeopardize America's critical infrastructure, the freedoms that Americans exercise online, and the economic viability of U.S. business.
- Russia, China, and Iran are trying to steal or destroy U.S. digital property to further their power or prestige. Hamas, Hezbollah, and criminal organizations from around the world have also employed cyber methods. Cyber espionage is rampant, with U.S. companies losing an estimated $250 billion every year in intellectual property.
- Despite the best intentions of those who supported previous cyber legislation, a regulatory basis simply will not work: It does not improve security and may even lower it by providing a false level of comfort and burdening the private sector with outdated regulations.
- Cyberspace's dynamic nature must be acknowledged and addressed by policies that are equally dynamic. And, any legislation must provide robust protection for privacy and individual freedoms.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2785**
Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies
The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

property to further their power or prestige. Nonstate actors such as Hamas and Hezbollah have also shown the capability to employ cyber methodologies and criminal organizations from around the world, and have acted as hired guns as well as on their own, using cyber tools as their weapon of choice.[1] Cyber espionage is rampant, with U.S. companies estimated to be losing a staggering $250 billion every year in intellectual property.[2]

The latent nature of this threat leads many people to forgo investment in security because it has not yet harmed their organization or because they mistakenly believe that they have nothing a cyber adversary would want. More important, they misunderstand that their own cyber insecurity has collateral effects on others—effects for which they are responsible. There is, therefore, a role for the federal government to encourage actions that will improve the overall cybersecurity posture of the U.S. That role, however, is not to set mandatory regulations. As the U.S. Government Accountability Office (GAO) has found, such an approach would be more like an anchor holding back U.S. entities while not providing additional security.[3]

Congress should reject a regulatory approach and adopt legislation that will actually improve the nation's cybersecurity. Such legislation must be able to adjust to the continuously developing challenge that is today's cyber environment. Additionally, any legislation must provide robust protection for privacy and individual freedoms. There are seven key components that need to be included in truly effective cyber legislation:

1. Enabling information sharing instead of mandating it;

2. Encouraging the development of a viable cybersecurity liability and insurance system;

3. Creating a private-sector structure that fosters cyber-supply-chain security ratings;

4. Defining limited cyber self-defense standards for industry;

5. Advocating for more private-sector efforts to promote general awareness, education, and training across America;

6. Reforming science, technology, engineering, and mathematics (STEM) education to create a strong cyber workforce within industry and government; and

7. Leading responsible international cyber engagement.

Past Efforts Have Failed for Good Reason

The 112th Congress tried, and failed, to pass comprehensive cybersecurity legislation. Several bills were considered in both chambers, and one bill, the Cyber Intelligence and Sharing Protection Act (CISPA), passed the House of Representatives. Yet, no law was ultimately produced.

President Barack Obama recently issued an executive order that mirrors the proposed Senate Cybersecurity Act (CSA) of 2012, the so-called Lieberman–Collins bill.[4] The CSA failed to pass, specifically, due to reasonable differences among Members of Congress regarding how the nation should approach the growing challenge of cybersecurity. These differing camps are not at opposite ends of the political spectrum, but are spread throughout the American ideological landscape.

The staffs of Senators Joe Lieberman (I–CT, now retired) and Susan Collins (R–ME) who wrote the bill did a very good job reaching out to a wide array of actors from the public and private sectors to try to bridge the gap between the different camps. As the vote neared, the staff members tried to soften several areas that opponents found objectionable. While they deserve commendation for their efforts, the revisions were not satisfactory: The key revision to the CSA made cybersecurity standards voluntary. Individual regulatory agencies, however, could have

[1] The variety of threats are detailed in Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Denver: Praeger, 2013).

[2] Rich Dandliker, "Putting a Face on Intellectual Property Theft," Symantec, July 11, 2012, http://www.symantec.com/connect/blogs/putting-face-intellectual-property-theft (accessed March 19, 2013).

[3] U.S. Government Accountability Office, *Cybersecurity: Challenges in Securing the Electricity Grid*, GAO-12-926T, July 17, 2012, http://www.gao.gov/assets/600/592508.pdf (accessed March 19, 2013).

promulgated regulations that would have made these voluntary standards mandatory in specific sectors. Ultimately, a significant number of relevant players believed—and still do—that regulation is the wrong way to foster cybersecurity. Such concerns prevented the Cybersecurity Act of 2012 from becoming law.

Proponents of a regulatory approach believe that this framework will improve the nation's general cybersecurity posture. The problem is that heavy-handed government regulation is a 19th-century solution for a 21st-century problem. It simply will not help. Such proponents claim that "doing anything" is better than "doing nothing." In fact, the regulatory approach can make matters worse than doing nothing. A network of regulations will force a slow and static compliance culture on the most dynamic technology the world has ever known. It will set a standard that will do nothing more than offer an invitation to America's adversaries in cyberspace. They will know that regardless of what that standard is, they only need to exceed it by the slightest bit to do severe damage to U.S. interests. This clearly will not suffice if the goal is to improve the national cybersecurity posture instead of "just doing something" so that politicians and the American public can feel better.

Regulation, particularly federal regulation, is slow, cumbersome, and static. Once in place, regulations are very difficult to remove or even change. This is exactly the wrong approach for dealing with the fast-moving and incredibly dynamic field of cybersecurity. The processing power of computers has historically doubled every 18 to 24 months—the time it takes to write and implement a major regulation is at least 24 to 36 months.[5] As a result, cybersecurity regulations will already be outdated on the day they are issued—and quick updates will not be possible. Faced with a slow, static standard, hackers, whether working independently or for another government, will easily circumvent the standard, just as the Germans circumvented France's Maginot Line in World War II. Furthermore, government control and regulations are already incapable of protecting networks. The federal government has had at least 65 cybersecurity breaches and failures, with at least 13 of those occurring recently.[6] Given that it cannot protect its own networks, it should not be responsible for determining standards for the private sector.

Federal regulation is exactly the wrong approach for dealing with the fast-moving and incredibly dynamic field of cybersecurity.

President Obama's executive order indicates that he favors a regulatory approach to cybersecurity. In cybersecurity, however, such actions go against the wisdom of the majority of major technology businesses and government auditors such as the GAO, who feel that cyber regulations will foster a "culture… focusing on compliance with cybersecurity requirements, rather than a culture focused on achieving comprehensive and effective cybersecurity."[7] It is clear that together with other concerns over innovation and costs, the dynamic nature of cyber is not amenable to the strait jacket of regulation.

The Need Is Real

While there is disagreement over the correct role of the federal government in cybersecurity, there is little disagreement that something must be done to improve the U.S.'s cybersecurity. The threats that the U.S faces from adversaries in the cyber realm are real and daunting. Indeed there are three tiers of cyber threats to consider. First, cyber crime hits

[4] News release, "Executive Order—Improving Critical Infrastructure Cybersecurity," The White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed March 19, 2013).

[5] "Moore's Law Inspires Intel Innovation," Intel.com, http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html (accessed March 20, 2013).

[6] Paul Rosenzweig, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government," Heritage Foundation *Backgrounder* No. 2695, May 24, 2012, http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government, and Paul Rosenzweig, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government Continues," Heritage Foundation *Issue Brief* No. 3772, November 13, 2012, http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue.

[7] U.S. Government Accountability Office, "Cybersecurity: Challenges in Securing the Electricity Grid," GAO-12-926T, July 17, 2012, http://www.gao.gov/assets/600/592508.pdf (accessed March 20, 2013).

many Americans in the form of identity theft, phishing, or cyber vandalism. In 2006, the GAO estimated that cyber identity theft cost U.S. citizens and companies almost $50 billion, and this cyber threat has only grown since then.[8] These crimes are usually committed by individual criminals, so-called hacktivists, or criminal organizations, and represent the most common form of cyber threat.

Next is the threat of cyber espionage. Espionage pursues large, important targets, such as military blueprints or proprietary business plans, and is often state-sponsored. China, for instance, is a known bad actor in cyberspace. The Chinese not only allow and sponsor hackers, but have entire military and government units dedicated to stealing data from governments and private companies, as the recent Mandiant report makes clear.[9] China has been engaged in a prolonged campaign of stealing U.S. intellectual property and military secrets, as exemplified by the Titan Rain/Byzantine Hades hackers of the mid-2000s, which may have stolen portions of the F-35 designs.[10] Together with other hackers and cyber operations, China has stolen billions, if not trillions of dollars in U.S. intellectual property, not to mention compromising U.S. national security secrets.

Finally, while cyber crime and espionage are serious problems, the U.S. also faces a threat from cyberwarfare. The ability to impair the functioning of critical systems, as a stand-alone attack or in connection with a kinetic attack, is a worrisome proposition. Taking down communications, transportation, or other systems would severely impair the U.S. response to a physical attack, increasing the damage sustained.[11] While such an event is “unlikely” according to Director of National Intelligence James Clapper, the U.S. must prepare for these threats since terrorists or isolated states are *likely* to use such attacks as they gain the capabilities to do so.[12]

Nearly everyone understands that, for such serious problems, the federal government has a role to play. Cyber legislation should contain the following seven major components if it is to actually lower risk to American businesses and be sufficiently flexible to avoid a static culture of compliance.

1. Information Sharing

The first element of any legislation must be to enable and foster information sharing between the public and private sectors, and among private-sector entities themselves.

Effective information sharing is a critical and fundamental part of today’s cybersecurity measures. Various organizations and government agencies collect and analyze information regarding cyber threats and vulnerabilities. Examples of the types of shared information include analysis of a completely new cyber attack that penetrated an entity’s system, or the discovery of a hole in the coding of a piece of software. This information is helpful to all cybersecurity actors as it allows them to prepare for these threats and patch or disable offending software.

Unfortunately, critical data on threats and vulnerabilities often remains locked within each company or organization due to different concerns and fears. These include fear of liability if shared information turns out to be wrong or causes unintended damage; concerns that sharing information could put proprietary information within the reach of Freedom of Information Act (FOIA) requests by competitors; and worries that shared information might be used against a company by regulators. As a result, cybersecurity information sharing is currently limited to a select few sharing programs, such as the DOD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE), or

[8] U.S. Government Accountability Office, “Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats,” GAO-07-705, June 2007.

[9] Mandiant Report, “APT 1: Exposing One of China’s Cyber Espionage Units,” http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed March 20, 2013).

[10] Rosenzweig, *Cyber Warfare*, p. 38.

[11] Indeed, the 2008 conflict between Georgia and Russia may be the first example of cyberwarfare. Russian “patriotic hackers,” with the support of Russian organized crime syndicates and the blessing of Russian intelligence agencies, attacked numerous targets in Georgia at the same time as the Russian military invasion. These hackers disabled certain Georgian communication systems, hampering Georgia’s ability to communicate with the world and with its own people. Ibid., pp. 32–33.

[12] James R. Clapper, “Worldwide Threat Assessment of the U.S. Intelligence Community,” testimony before the Select Committee on Intelligence, U.S. Senate, March 12, 2013.

between small networks of companies that trust each other.[13] Instead of limited and fragmented information sharing, an ideal cybersecurity approach would foster trusted and widespread sharing.

The government has its own rules, concerns, and processes that inhibit information sharing on its part. While these processes must be respected, they should not be considered sacrosanct. For example, the government is reluctant to share intelligence for fear of revealing classified "sources and methods." This reluctance should be overcome by more appropriate classification of information and providing more clearances to appropriate personnel in the private sector. By opening up the process, industry's confidence, trust, and ability to work with the government will improve, increasing opportunities for private and public collaboration. Additionally, information should not be stovepiped within the government, but should be available to other agencies for legitimate purposes. Specifically, sharing should not be restricted as long as one significant purpose of the information sharing was for cybersecurity or national security, with appropriate oversight by existing government privacy officers to ensure its correct usage.

Any arrangement that forces a business to share information is, by definition, not cooperation but coercion. And, strong liability protection is critical to expanding information sharing.

There are four steps that can be taken to enable and encourage the needed cyber information sharing. First, Congress should remove barriers to voluntary private-sector sharing. Currently, legal ambiguities impede greater collaboration and sharing of information.[14] As a result, nearly every cybersecurity proposal in the last Congress contained provisions for clarifying these ambiguities to allow sharing. The 2011 Cyber Intelligence Sharing and Protection Act (CISPA), the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, and the Cyber Security Act (CSA) of 2012 all authorized sharing by stating that "[n]otwithstanding any other provision of law" a private-sector entity can "share" or "disclose" cybersecurity threat information with others in the private sector and with the government.[15] While sharing information is important, all of it should be voluntary, in order to encourage true cooperation. After all, any arrangement that forces a business to share information is, by definition, not cooperation but coercion. Voluntary sharing will also allow organizations with manifest privacy concerns to simply avoid sharing their information, while still receiving helpful information from the government and other organizations.

Second, those entities that share information about cyber threats, vulnerabilities, and breaches should have legal protection. The fact that they shared data about an attack, or even a complete breach, with the authorities should never open them up to legal action. This is one of the biggest hindrances to sharing today, as it seems easier and safer to withhold information than to share it, even if it will benefit others. The Information Technology Industry Council (ITIC) provides several examples of how liability concerns block effective information sharing. Under current law, "Company A [could] voluntarily report what may be a cybersecurity incident in an information-sharing environment, such as in an ISAC (Information Sharing and Analysis Centers), or directly to the government, such as to the FBI." The result of such sharing could be that

> government prosecutors, law enforcement agencies, or civil attorneys use this information as the basis for establishing a violation of civil or criminal law against Company A or a customer, partner,

[13] DOD Cyber Crime Center, http://www.dc3.mil/dcise/dciseAbout.php (accessed March 20, 2013).

[14] The ambiguities arise from the detailed provisions of the Wiretap Act and the Stored Communications Act, neither of which contemplated systematic sharing of threat and vulnerability information for cybersecurity purposes. For a detailed analysis, see Paul Rosenzweig, "Cybersecurity and Public Goods: The Public/Private 'Partnership,'" Hoover Institution, 2011, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf (accessed March 20, 2013).

[15] Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 3523, 113th Cong., 1st Sess., and SECURE IT Act, S. 2151, 112th Cong., 2nd Sess. None of these bills became law—principally for reasons unrelated to the information-sharing provisions.

> or unaffiliated entity harmed by the incident sues Company A for not informing them of the incident as soon as they were aware of it. Company A's disclosure can be seen as a "smoking gun" or "paper trail" of when Company A knew about a risk event though Company A did not yet have a legal duty to report the incident. Such allegation could lead to costly litigation or settlement regardless of its validity.[16]

With the threat of legal action, businesses have determined that they are better off not sharing information. Strong liability protection is critical to expanding information sharing.

Third, the information that is shared must be exempted from FOIA requests and use by regulators. Without such protection, a competitor can get its hands on potentially proprietary information through a FOIA action. Alternatively, if information is shared with a regulator, it will dampen voluntary sharing, since organizations will fear a backlash from regulators, who could use shared information to penalize a regulated party or tighten rules. Once again, the ITIC provides a valuable example. If a company shares information on a potential cybersecurity incident and "later finds that a database was compromised that included Individually Identifiable Health Information as defined under the Health Insurance Portability and Accountability Act (HIPAA)," then the Federal Trade Commission could use the shared information "as evidence in a case against [that company] for violating the security provisions of HIPAA."[17] If shared information is exempted from FOIA and regulatory use, a company can share important data without fear that its competitive advantages will be lost to other firms or used by regulators to impose more rules or costs.[18]

Lastly, the government must be compelled to share information and intelligence with the private sector much more quickly and completely than it currently does. If that is not done, the private sector will never build any confidence that it is truly a partner in the fight to maintain the security of American computer networks. The mechanism for disseminating information could take several forms, ranging from a sharing center in one organization, such as the National Cybersecurity and Communications Integration Center at the Department of Homeland Security (DHS), to multiple sharing centers. In this area, President Obama's executive order goes in the right direction—but not far enough.

Concerns over DHS or National Security Agency (NSA) control have been a major sticking point in the cybersecurity discussion, however. The CSA put DHS in charge, while SECURE IT, sponsored by Senator John McCain (R–AZ), largely put the NSA in the leadership role. Both agencies claim to be the most able or most appropriate for cybersecurity leadership.[19] Perhaps the wisest path to promote information sharing would be the creation of a public-private partnership. Such a partnership would include DHS, the NSA, and privacy and industry representatives to ensure effective sharing and to avoid turf battles. Such a system would be similar to the current organization of Internet governance, in which organizations like the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society operate as nonprofit organizations with boards and advisory groups that incorporate worldwide business, privacy, government,

[16] Information Technology Industry Council, "ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing," January 2012, http://www.itic.org/dotAsset/fae2feab-7b0e-45f4-9e74-64e4c9ece132.pdf (accessed March 520 2013).

[17] Ibid.

[18] While some might worry that the FOIA exemption is too broad, the application of FOIA in this context turns FOIA on its head. The purpose behind the FOIA is to ensure the transparency of government functions. Here, the FOIA exemption contemplated is in relation to private-sector information that is not otherwise in the government's possession. For voluntary agreement of the private-sector actors to provide the cyber threat information in the first instance, the information would not be in the government's possession and thus not subject to disclosure. See Paul Rosenzweig, "Cybersecurity Information Sharing and the Freedom of Information Act," testimony before the Committee on the Judiciary, U.S. Senate, March 13, 2012. Likewise, though some might fear that a corporation would "overshare" its dirty laundry to avoid regulation, that concern seems unfounded—the type of threat and vulnerability information subject to sharing will not typically contain corporate operational data. Regardless, nothing should prohibit the government from developing a regulatory response based on data obtained from other sources. In short, with respect to the government's unrelated regulatory agenda, cybersecurity information sharing will act neither to the government's advantage, nor to its disadvantage.

[19] Josh Smith, "Turf War: As Agencies Duke It Out Over Who Keeps Cyberspace Secure, Everyone Is Vying for a Piece of the Action," *National Journal*, April 25, 2012, http://www.nationaljournal.com/columns/wired-in-washington/turf-war-20120424 (accessed March 20, 2013).

and other stakeholders.[20] Such an approach has served Internet governance well, and should serve as a model for a cybersecurity information-sharing organization.

> When a cyber criminal exploits a vulnerability in a piece of software to hack into a consumer's computer and steal financial data, the loss is borne by the consumer, not by the code manufacturer.

2. Cyber Insurance

Private-sector actors with responsibility for cybersecurity include those who write the computer codes, who build the hardware on which the code operates, who provide information transmission services, who build and maintain intrusion detection and prevention systems, and many others. Most, if not all, of these actors deny any liability for injuries to third parties who are affected by cybersecurity breaches as a result of the acts or omissions of the original actors. The result is a classic market externality—the full costs of any breach are not incorporated in the manufacturing costs of the product that is causally tied to the breach. Instead, the costs are borne by others—most commonly those who purchase products in the marketplace and suffer a loss. Put simply, when a cyber criminal exploits a vulnerability in a piece of software, such as Adobe Acrobat, to hack into a consumer's computer and steal valuable financial data, the loss is borne by the consumer, not by the code manufacturer. This is so even if the code writers were objectively negligent or, worse, reckless, and did not even try to find or eliminate the vulnerability.[21]

This state of affairs is, in the long run, unsound. Congress needs to reverse the system of incentives so that costs are borne by those who impose them, not by innocent consumers. To achieve this, the U.S. must arrange the development of a liability system that would require providers of goods and services to pay for any harm caused by their failure to take reasonable protective actions. This would force software manufacturers and Internet service providers to internalize many of the negative costs they now externalize.

Theoretically, such a structure has several benefits. Liability for tortious wrongs is a comparatively efficient method of modifying private-sector behavior, and does not require the government to set a constantly changing standard of conduct. Instead, the law would simply require that a provider take "reasonable" precautions. It leaves the determination of what constitutes a reasonable precaution to the development of the common law.[22]

More important, the creation of a liability system often naturally leads to the development of an insurance system against liability. The insurance function allows a further spreading of risk in a way that fosters broad private-sector responsiveness. With enough data, insurance companies routinely and efficiently price the comparative costs and benefits of preventative actions and require cost-effective protective measures as a condition of insurance. Indeed, in maturing markets, insurance companies often take the lead in setting reasonable standards of care—much as they did with the development of building and fire codes in the late 19th century. Cybersecurity insurance companies and policies are already emerging, such as CyberSecurity™ by the Chubb Group of Insurance Companies. CyberSecurity™, merely one of more than 50 estimated cyber-insurance carriers,[23] "combines third party (cyber liability) and first-party (cyber crime expense) coverage" in one

[20] Internet Corporation for Assigned Names and Numbers, http://www.icann.org/en/groups (accessed March 20, 2013), and Internet Society, http://www.internetsociety.org/ (accessed March 20, 2013).

[21] This section is derived from Rosenzweig, "Cybersecurity and Public Goods."

[22] We (the authors of this *Backgrounder*) acknowledge that the "reasonable man" standard is a flexible one that some skeptics of the tort system may see as an invitation to litigation abuse. We share those concerns. In the end, we have opted for a tort system of liability as the preferred method of standard setting because it is the least-bad option. As we have elaborated already, doing nothing is untenable in light of the significant threat, and a regulatory leviathan response from the government would freeze innovation, cost too much, and do more harm than good.

[23] U.S. Department of Homeland Security, "Cybersecurity Insurance Workshop Readout Report," November 2012, http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf (accessed March 20, 2013), p. 8.

policy that can be connected to a business's normal insurance policy.[24] Such policies and insurance companies demonstrate that cybersecurity insurance is viable and in demand.[25]

But it may be exceedingly difficult for this system to fully mature. Insurance pricing is not feasible without standards against which to measure conduct, as well as liability that arises from failure to meet those standards. In the cyber domain, neither is currently available. There are no generally accepted cybersecurity standards, and there is no generally applicable liability system in place to account for failures to meet those standards. Despite the growth of some private-sector standard-setting initiatives like ICASI, private-sector actors are likely to be highly resistant to voluntarily creating standards that lead to liability where none currently exists.

As a result, the only sure way to create liability would be for the government to take some initial action in creating a liability system. This does not mean putting the government in charge of a system of determining which standards businesses must meet. Instead, the role of the government is merely to create a law that allows the imposition of liability on firms that are recklessly or negligently responsible for cybersecurity losses incurred by others. The law should specifically leave the development of liability standards to the common law and private-sector organizations like ICASI.

There are no generally accepted cybersecurity standards, and there is no generally applicable liability system to account for failing to meet those standards.

Likewise, it may be difficult to gather sufficient data to accurately price insurance. In the physical world, insurance companies have plenty of data about the frequency of events, such as car accidents, that allow them to accurately price their products. The U.S., and the rest of the world for that matter, still has a long way to go in collecting data on cyber intrusions. But that lack of data can be fixed—companies such as Lockheed Martin are building extensive databases that assess the costs of cyber intrusions and, no doubt, at some point in the near future a commercial product for cyber risk assessment will be available. Additionally, the public-private partnership for information sharing described in the previous section could easily provide data to insurance companies to alleviate the lack of up-to-date information on threats and risks. With more data on cyber risks and threats, insurance companies will be able to better price insurance products, likely resulting in lower prices due to fewer unknowns.

3. Cyber-Supply-Chain Security

One of the biggest holes in the U.S. cyber system is in the area of supply chain security, especially hardware and key infrastructure components. Software vulnerabilities, while still capable of causing substantial loss, can be fixed relatively easily by updating the code or, if need be, replacing the software entirely. For example, if a company were to buy a piece of software with a vulnerability that gave hackers access to certain files, that company could mitigate that vulnerability by updating the software so that the vulnerability was removed. If the company was concerned that vulnerabilities might be widespread throughout the product, it could delete the software and install a different product.

With hardware security problems, however, instead of a simple software patch or even the modestly cumbersome process of replacing software, often the only answer is replacing each piece of offending hardware. According to a report by the Brookings Institution,

> Once malicious hardware has been built into a chip, a hardware attack can be initiated and act in a wide variety of ways. An attack can be internally triggered, based, for example on the arrival of a particular calendar day. Alternatively, an external trigger could be hidden within data sent by

[24] Chubb Group of Insurance Companies, "CyberSecurity by Chubb," http://www.chubb.com/businesses/csi/chubb822.html (accessed March 20, 2013).

[25] Indeed, the market for third-party liability continues to grow, an important indication that businesses realize the importance of insurance against losses their customers or business partners may incur as a result of a breach or cyber attack. U.S. Department of Homeland Security, "Cybersecurity Insurance Workshop Readout Report."

an attacker. More complex hybrid triggers could also be used. For example, a malicious circuit hidden within a GPS chip could be configured to attack only when the chip is located in a specific geographical area after a certain date.

There are multiple forms of potential attacks. In an overt attack, the malicious hardware could cause the device containing the corrupted chip to either cease functioning altogether or to continue to operate but in an obviously impaired manner. The existence of a problem would be clear, though its cause would not. In a personal electronics device such as a mobile phone such an attack could be nothing more than an inconvenience. If conducted on a large scale on thousands of chips within a critical portion of the national infrastructure, this form of attack could be devastating.[26]

Covert or mixed attacks could also allow information theft or impair critical operations. Of course, such hardware vulnerabilities are more easily hidden due to their imbedded nature. In addition to serious cyber crime and espionage concerns, such imbedded vulnerabilities are clearly a serious national security threat as well.

Indeed, there are no shortages of warnings. A GAO report published in March 2012 examined the supply-chain-surety procedures of the Departments of Energy, Homeland Security, Defense, and Justice.[27] The report found that except for the Defense Department, the departments all failed to implement supply chain protection measures, even though all acknowledged the threat. Cybersecurity supply concerns abounded in the October 2012 House Permanent Select Committee on Intelligence report on Chinese telecommunications giants Huawei and ZTE.[28] These companies are understood to be under the direct control of the Chinese Communist Party, as telecommunications is considered an area of absolute state control in China. In the event of a conflict with China, these companies would give the Chinese access to immitigable vulnerabilities that U.S. defenses would not even know about. Such vulnerabilities in U.S. critical infrastructure, such as the electrical grid or financial sector, would pose a serious risk to the U.S and thus the committee's recommendation to avoid Huawei and ZTE as a source of telecommunications infrastructure and services.

Under a grading system, market forces would push companies toward better security in order to have a competitive advantage, while allowing the consumer to make more informed choices.

This risk must be mitigated without impairing the highly effective global system that keeps cutting-edge technology affordable and accessible to most people. The Open Group consortium, an organization focused on improving businesses through IT standards, has developed the most viable model to deal with the supply chain, and it should be adapted by Congress. An effective cyber policy should establish a nonprofit organization that will evaluate and accredit technology companies' supply chain security, even to the point of giving them grades.[29] This approach would be similar to the well-known Underwriters Limited, which certifies the safety of electronic appliances.

[26] John D. Villasenor, "Ensuring Hardware Cybersecurity," *Issues in Technology Innovation*, No. 9 (May 2011), http://www.brookings.edu/~/media/research/files/papers/2011/5/hardware%20cybersecurity/05_hardware_cybersecurity.pdf (accessed March 20, 2013).

[27] U.S. Government Accountability Office, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," GAO-12-361, March 2012, http://www.gao.gov/assets/590/589568.pdf (accessed March 20, 2013).

[28] Mike Rogers and C. A. Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," Permanent Select Committee on Intelligence, U.S. House of Representatives, October 8, 2012, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf (accessed March 20, 2013).

[29] The Open Group Trusted Technology Forum, "Open Trusted Technology Provider Framework: Industry Best Practices for Manufacturing Technology Products that Facilitate Customer Technology Acquisition Risk Management Practices and Options for Promoting Industry Adoption," February 2011, pp. 20–21.

For example, if a company has outstanding supply chain security across its entire global process, it would receive a high grade. Another firm might have a less comprehensive system and only receive a middling grade. Those companies with the highest grades would be able to charge higher prices for their technical equipment and software than companies with lower grades.[30] This has the benefit of giving the consumer a way to "vote" on the level of security he or she feels is adequate and make better risk-based decisions on the acquisition of technical equipment. If an organization needed multiple systems for a certain budgeted amount, it might have to buy from a company with a lower grade. Again, market forces would push companies to have better security in order to have a competitive advantage, while allowing the consumer to make more informed choices.

4. Cyber Self-Defense

Presently, there are no well-defined rules to tell businesses what they can and cannot do to establish self-defense mechanisms in the cyber domain. The Department of Justice is trying to increase its capacity for prosecuting cyber attackers. The National Security Division of the Justice Department is creating new positions across the country in its National Security Cyber Specialist (NSCS) network for people who can competently prosecute cyber cases. Implicit in this program is the burgeoning willingness to pursue these cases. As the ability to attribute involvement to specific players expands, law enforcement can prosecute not just those who steal the data, but those who use it as well.

The NSCS program is in its embryonic stage, however, and the collection capabilities in many cases are even less developed. The Justice Department must enlist the help of the companies who have become targets of cyber attacks. If these entities have the realistic capabilities to collect data on intrusions, they should do so in the interests of self-defense. However, defense cannot stop at passively collecting information on attacks that have or are trying to breach a network. Current law prohibits businesses from doing anything more than attempting to defend their networks with firewalls and other security software, and collecting information on attacks.

In this area, the U.S. should take a tip from the government of Georgia.[31] In 2012, the Georgian government suspected that one of its critical computer systems had been hacked and that the intruder was searching for data to steal. Georgian government officials planted a file marked "Georgian-NATO Agreement," and waited. In short order, the file was copied and exfiltrated from the Georgian system to an unauthorized computer. The hacker did not realize that the file had been booby trapped. As soon as he opened the file, the Georgian malware took control of his web camera, capturing his face, and immediately seized his files. These contained e-mails from a Russian FSB (intelligence agency) "handler" to the hacker, instructing him to find and steal certain types of data. It was a huge coup to find and identify the culprit.

U.S. companies should be able to execute similar operations, either in cooperation with law enforcement, or alone, with the intent of providing the evidence to law enforcement after the fact.[32] Such tactics are not the cyber equivalent of a "trap gun" that shoots any intruder who comes in a front door. It is

[30] "It is difficult to overstate the importance of the security of the firm's suppliers, and suppliers throughout the supply chain, including those upstream from the tier-one supplier. This comes as a result of the increasing interdependencies among supply chain parties, particularly as firms outsource more activities to third parties, inherently bringing in greater risk of security breach. End-to-end supply chain security is therefore of fundamental importance to overall supply chain security." By providing ratings to suppliers, companies have more information with which to navigate the complex international market of IT infrastructure and make better risk-based decisions about the security of their purchases. See James B. Rice Jr. and Philip W. Spayd, "Investing in Supply Chain Security: Collateral Benefits," IBM Center for the Business of Government, May 2005, http://web.mit.edu/scresponse/repository/Rice_Spayd_IBM_Investing_in_SC_Security_Collateral_Benefits.pdf (accessed March 20, 2013).

[31] Jeremy Kirk, "Georgia Outs Russia-Based Hacker—with Photos," *PC World*, October 30, 2012, http://www.pcworld.com/article/2013289/georgia-outs-russia-based-hacker-with-photos.html (accessed March 18, 2013).

[32] We have not, in this *Backgrounder*, specified a particular method by which private companies might be authorized to conduct active defensive operations. One model might be a licensure system akin to that used for private detectives. Another, more militarized, model might be to revive the constitutional practice of Letters of Marque and Reprisal. See Jeremy A. Rabkin and Ariel Rabkin, "To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict," Hoover Institution, May 21, 2012, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf (accessed March 20, 2013).

more akin to a cyber "dye bomb" on bank money bags that marks the thief. This sort of operation should be encouraged by the Justice Department, not prohibited, albeit with clear guidelines. Sending out destructive malware would have unintended consequences and should probably remain illegal, but the Georgian style of self-defense should be permitted.

The U.S. law enforcement, military, and intelligence communities are not capable of addressing all cyber breaches and attacks that occur across the growing network of the U.S. cyber realm. At the same time, many companies have internal capabilities to fight back against those who threaten to pillage their intellectual property or corrupt their critical data. This is not to advocate making the Internet more of a Wild West environment than it already is—quite the contrary. It is an attempt to codify rules within which cyber self-defense can take place. These would need to be realistic and have provisions to inform and foster cooperation with law enforcement. They would also have to allow actions beyond simple static defensive measures. This would clearly be a controversial component, but nonetheless an important one.

5. Awareness, Education, and Training

The American people recognize that there is a problem with securing the cyber domain. They hear about it regularly on the news, and know, abstractly, that it is there. The difficulty is that they receive mixed messages. What the public lacks is consistent, accurate, and up-to-date information. The federal government has tried to play a role here but has failed. That is no surprise. Initiatives like the Department of Homeland Security's Cyber Security Month send exactly the wrong message because it does little to change how the citizens see cybersecurity. More must be done by the private sector and local organizations to bring this issue to the attention of the American public—a once-a-year public relations stunt is not enough. All Americans, not just Washington, have agency in cyberspace. The nation, not Washington, must take ownership and responsibility for the cyber commons. Top-down directives are not the answer. Private entities, nongovernmental organizations, along with universities and other research institutions, ought to play a much more active and prominent role in supporting personal cybersecurity safety and community-centric programs.

There must also be a viable program of professional base-level training that is encouraged for the general non-IT workforce. Nearly every job now involves the use of digital devices in some aspect of work. The general workforce must receive continuing education that goes beyond the present system, which is comprised of FISMA-compliant classes that accomplish little beyond checking off a box. These cyber "survival skills" should employ a dynamic curriculum, developed by the private sector, which keeps the workforce current and prevents it from being easily victimized. Any legislation should acknowledge this and encourage meaningful but dynamic training from nongovernmental sources.

6. Cyber Workforce

While the above provision is aimed at the population in general, this one is aimed at the development of a workforce to serve the technology industry and the key government organizations that use cyber means for higher-order activities, such as cyberwarfare, defense of specific technical industry intellectual property, and critical infrastructure defense. The GAO surveyed 11 chief information officers (CIOs) of federal agencies and 12 outside cybersecurity experts and found that four of the CIOs and five of the outside experts "cited weaknesses in education, awareness, and workforce planning as a root cause hindering progress in improving the nation's cybersecurity posture."[33] The development of an adequate cyber workforce will begin with improvements in STEM education. These improvements need to span from kindergarten through high school, and into university and graduate school.

For this to happen, the process of acquiring and keeping good teachers needs to change. This can be done by eliminating the last-in-first-out policy that is currently applied to teachers, and moving toward merit-based compensation systems. Instead of evaluating teachers based on how long they have held their positions, their pay should directly reflect how well they teach their students.[34] As Heritage

[33] U.S. Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," GAO-13-187, February 2013, p. 68, http://www.gao.gov/assets/660/652170.pdf (accessed March 20, 2013).

Foundation economic and education policy expert Jason Richwine notes:

> Under a market-driven pay-for-performance system, teacher compensation will begin to move toward levels matching those of similarly skilled private-sector employees. Whether fundamental reforms of this kind can be implemented within the public-school system is questionable, which makes flexible school models—such as expanded charter school options or vouchers—attractive options that policymakers should consider. Any reform that allows schools to operate with a less onerous regulatory burden could potentially improve the teacher-compensation system.[35]

Another way to encourage greater STEM education is by encouraging the use of online educational options.[36] Online learning can provide students with access to highly qualified teachers no matter where they live. More STEM graduates will help to round out the United States workforce. Along these lines, the U.S. government should modify its visa system so that foreign STEM graduates are no longer forced to leave the U.S. as soon as they complete their U.S. education.[37]

The U.S. can also improve its cyber workforce by capitalizing on attributes the country already has in place. The U.S. should:

- **Increase the number of IT professionals with security certifications.** Information-security certifications like the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM) represent the minimum level of training that a cybersecurity professional needs. For those who want to go beyond, intensive college and university programs are the next step. Some institutions streamline the degree process by granting credit to certificate holders for the education they have already completed.

- **Develop more IT leaders with cybersecurity expertise.** After 9/11, many pointed out the need for more cybersecurity professionals. Since then, the National Security Agency and the Department of Homeland Security have laid out stringent criteria for cybersecurity education programs—and recognized institutions that met these criteria as National Centers of Academic Excellence in Information Assurance Education (CAEIAE). Many of these centers are now following the National Initiative for Cybersecurity Education (NICE) framework, guaranteeing even more alignment with the security standards needed by government and industry. Graduates of these Centers are working to help the NSA and DHS, as well as many corporations, with the cybersecurity issues they face today. But more graduates are needed.

- **Draw on current military personnel.** With proven leadership abilities and valuable security clearances, military service members are in a unique position to support U.S. cybersecurity. By gaining high-level cybersecurity knowledge, these experienced professionals can provide valuable insights to a variety of government agencies. For these professionals in particular, online institutions are an excellent fit because they offer flexibility, including the ability to complete courses from

[34] Jason Richwine, "A Better Way to Pay: Five Rules for Reforming Teacher Compensation," Heritage Foundation *Backgrounder* No. 2681, April 24, 2012, http://www.heritage.org/research/reports/2012/04/a-better-way-to-pay-five-rules-for-reforming, and Ethel Machi, "Improving U.S. Competitiveness with K–12 STEM Education and Training," Heritage Foundation *Special Report* No. 57, June 16, 2009, http://www.heritage.org/research/reports/2009/06/improving-us-competitiveness-with-k-12-stem-education-and-training.

[35] Jason Richwine and Andrew Biggs, "Assessing the Compensation of Public-School Teachers," Heritage Foundation *Center for Data Analysis Report* No. 11-03, November 1, 2011, http://www.heritage.org/research/reports/2011/10/assessing-the-compensation-of-public-school-teachers.

[36] Lindsey M. Burke and Jena Baker McNeill, "'Educate to Innovate': How the Obama Plan for STEM Education Falls Short," Heritage Foundation *Backgrounder* No. 2504, January 5, 2011, http://www.heritage.org/research/reports/2011/01/educate-to-innovate-how-the-obama-plan-for-stem-education-falls-short.

[37] Jessica Zuckerman and Landon Zinda, "STEM Jobs Act: Next Step for High-Skilled Immigration Reform," Heritage Foundation *Issue Brief* No. 3792, December 4, 2012, http://www.heritage.org/research/reports/2012/12/stem-jobs-act-next-step-for-high-skilled-immigration-reform.

far-flung locations, and quality, as some online schools have earned CAEIAE designations.[38]

The U.S. needs more qualified personnel in the general STEM fields, and specifically in the advanced cyber skill sets, such as code writing, defensive procedures, deep-packet inspection, and big data analysis techniques. A major effort must be made to find the sort of people who can flourish in this field, and give them the opportunity to pursue the higher STEM education they require. Additionally, Congress should change or remove barriers to pursuing these careers, such as outdated security clearance procedures and do more to retain these experts and keep them current. If this effort is not adequately enabled, the U.S. will slowly fall further behind its competitors. Every effort must be made to encourage the adjustment of hiring practices in order to allow the hiring of individuals who have proven cyber skills, even if they do not have the standard educational credentials. This would also mean that security clearance restrictions might need to be adjusted on a case-by-case basis. To lose the services of a willing former hacker in the struggle against cyber foes due to bureaucratic regulations would be foolish.

7. Cybersecurity Beyond the Borders

Cybersecurity is not now, and never will be, an issue that one country can solve alone. The solution will require a concerted—and ongoing—collaboration between the U.S. and like-minded free nations. Treaties and global governance do not contain bad actors, and should thus not be the focus of U.S. or international cybersecurity efforts. Instead, the U.S. must work with other friendly nations to alter bad cyber behavior by raising the costs of such behavior.

The first step to effectively conducting a fruitful international strategy is to determine a U.S. *domestic* policy on cybersecurity. It would be foolish to jump into international negotiations until the U.S. has the kind of national conversation that sorts out definitional and policy positions such as those policies described above. However, it would be just as foolish to ignore the need to make international connections and establish cooperative relationships in this field. Both should be done as soon as is practical. The federal government must lead efforts dealing with other nations and international organizations.

The U.S. must respond to aggressive actions by bad cyber actors, such as China, to make it clear that cyber espionage is unacceptable. In light of the recent report published by Mandiant, it has become clear that China regards hacking as a low-cost method of extracting valuable secrets and intellectual property from companies and governments, especially those in the U.S.[39]

So far, the Obama Administration has pursued a multilateral approach to international cyber issues. The White House's recently released "International Strategy for Cyberspace" points toward the creation of an "open, interoperable, secure, and reliable" communications and information architecture through building and sustaining norms of international behavior.[40] The strategy also articulates the norms it seeks to foster, such as freedom, privacy, respect for property, protection from crime, and the right to self-defense. Though desirable, these norms are articulated at too high a level of generality and are unlikely to find great acceptance in many nations that value neither privacy nor freedom.

The limits of this sort of strategy are best exemplified by how the strategy addresses the problem of cyber crime. Currently, one of the most widely touted multilateral approaches to cybersecurity is the Budapest Cybercrime Convention. Indeed, it "is the only binding international instrument on this issue."[41] Yet, despite its prominence, it is widely agreed that the Budapest Cybercrime Convention has been ineffective. More than 10 years after its adoption, only 39 nations (of more than 190 countries worldwide and only 49 convention signatories) have ratified the convention. Furthermore, of those countries that have ratified it, some, such as Ukraine, remain havens for hackers, showing how little force

[38] Sue Talley, "Cyber Warfare, Education is Our Most Powerful Weapon," *The Huffington Post*, December 12, 2012, http://www.huffingtonpost.com/sue-talley-edd/in-cyber-warfare-education_b_2244950.html (accessed March 20, 2013).

[39] Mandiant Report, "APT 1: Exposing One of China's Cyber Espionage Units."

[40] The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed March 20, 2013).

[41] Council of Europe, "Action Against Economic Crime," http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (accessed March 20, 2013).

the convention actually has. And yet, the principal goal of the new Obama Administration strategy for addressing cyber crime is to harmonize criminal cyber laws internationally by expanding accession to the convention. If there were a realistic prospect that criminal havens, like Russia, Ukraine, and China, would both join the convention and implement it aggressively, this policy could be effective. However, in the absence of that prospect, the promise of a multilateral policy is an empty one.

Instead, large-scale, state sponsored cyber espionage must be deterred by making the cost to bad actors unacceptably large or frustrating. The U.S. could pursue several different solutions depending on how aggressive another nation is in its attempts to steal U.S. information.[42]

Official naming and shaming of bad cyber actors is precisely the type of international policy the U.S. needs in cyberspace.

First, congressional action should be aimed at enabling the executive branch to identify countries that serve as havens for criminal activity and use the levers of influence and power to prompt changes in their behavior. The Gillibrand–Hatch proposal from the 112th Congress is a good model.[43] Under the proposed legislation, the Administration would be authorized to highlight the practices of governments that disregard outreach efforts and demonstrate a sustained pattern of ignoring criminals who use the Internet to hide as they exploit victims with impunity around the world. This form of naming and shaming is precisely the type of international policy the U.S. needs in cyberspace.

Second, the U.S. should cease cooperating with bad cyber actors on issues of cyber and national security. The U.S. has conducted at least two cyber war games with China in the last year, even as China's cyber aggression has become more evident worldwide. Such a policy provides the Chinese a perfect opportunity to learn what the U.S. cyber capabilities are, and only emboldens them to continue their aggression as the U.S. stumbles to confront them.[44] The U.S. should not engage in such war games and military exchanges with nations that use such cooperation to further their attacks against the U.S.

Third, the U.S. should place travel and commercial restrictions on individuals and organizations tied to hacking. Visiting the United States for business or leisure is a privilege that should be withheld from individuals and organizations that seek to harm the U.S. Organizations that steal American secrets should not be permitted free access to U.S. markets as they are clearly untrustworthy trading partners. Similarly, companies and nations dealing in stolen intellectual property should be subject to criminal charges with assets liable to seizure. Beyond the legal consequences, such actions will also have reputational and financial implications as these organizations find it increasingly difficult to sell products in certain countries or to be listed on many stock exchanges.[45]

Fourth, the U.S. should also be willing to link the level of hacking in which another nation engages to its efforts to break down foreign Internet controls. In other words, particularly malicious nations should have their control of the Internet challenged by the U.S. in proportion to the level of their aggression. Nations that are truly bad cyber actors are often nations that are also active in censoring their own Internet in order to rein in their own populace and keep the public under surveillance. As a result, U.S. efforts to weaken or break these Internet

[42] The actions we advocate here are far more substantive and muscular than the recently announced Administration policy: The White House, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013, http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (accessed March 20, 2013).

[43] The International Cybercrime Reporting and Cooperation Act, S. 1469, 112th Cong., 1st Sess., August 2011.

[44] Nick Hopkins, "US and China Engage in Cyber War Games," *The Guardian*, April 16, 2012, http://www.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games (accessed March 20, 2013), and "China and US to Co-operate to Avoid Cyber Cold War," BBC, May 8, 2012, http://www.bbc.co.uk/news/technology-17989560 (accessed March 20, 2013).

[45] Dean Cheng, "Chinese Cyber Attacks: Robust Response Needed," Heritage Foundation *Issue Brief* No. 3861, February 23, 2013, http://www.heritage.org/research/reports/2013/02/chinese-cyber-attacks-robust-response-needed.

control mechanisms could impose greater domestic costs on these nations. U.S. support for democratic movements within these countries would similarly raise the cost of domestic control.

Fifth, the U.S. should lead a coalition of nations in these efforts to raise the costs of cyber crime to bad cyber actors. Nations that support Internet freedom and want to crack down on cyber crime can and should join together in reprimanding China, Russia, and other malicious cyber states for their direct or indirect roles in cyber crime. The U.S. should continue to lead this coalition in defending Internet freedom at various international bodies, such the International Telecommunications Union. Through constant and forceful condemnations, travel and commercial restrictions, less cooperation, and weakening bad actors' control over the Internet, the U.S. can lead the world in a practical and principled approach to dealing with international cyber threats.

A Cybersecurity Policy that Works

Congress should pursue a cybersecurity policy that avoids a cumbersome and expensive regulatory approach and includes the seven key elements detailed there that will produce truly dynamic cybersecurity defenses. Such an approach should:

- **Enable cyber information sharing by removing ambiguities, providing strong protections to sharers, and establishing a public-private partnership to facilitate sharing.** Entities that share cybersecurity information need certain protections. These protections include exempting all shared information from FOIA requests and regulatory use, and providing information sharers with strong liability protection. Effective information sharing requires the government to share fully and in a timely manner with the private sector through a public-private partnership established for this purpose.

- **Promote the development of a viable cybersecurity liability and insurance system.** Liability for irresponsible cybersecurity actions should be established through common law development. This process may need some initial incentives from the government, but, ultimately, such a system returns cybersecurity liability to those who are largely responsible for cybersecurity losses. The natural establishment of a cyber insurance community will then assist in the administration of risk assessments and foster improved security methodologies.

- **Encourage the creation of cyber-supply-chain security ratings.** Such ratings should be granted by a nonprofit organization that will assess the surety of an organization's supply chain, similar to how Underwriters Limited assesses the safety of various commercial products. By promoting such ratings, consumers will be able to make risk-based decisions and support better security by tying it to their profit motive.

- **Clarify boundaries and standards for cyber self-defense.** The terms of an entity's right to self-defense must be set within reasonable limits. Such terms would allow entities with the correct capabilities to take active measures to protect themselves without usurping the responsibility or authority of the federal government.

- **Advocate more private-sector awareness, education, and training for the general population.** Such an effort will ensure that the American public becomes an asset, not a liability, in the struggle. Making the public more aware, without hype or feel-good security measures, is a start. Ongoing cyber education for the general workforce must also be promoted through standardized yet dynamic education programs, most likely originating in the private sector. This must be a major priority, not a minor ancillary effort.

- **Alter technical education and clearance practices to encourage the development of a cyber workforce.** A well-trained cyber workforce is critical to the task facing America. The U.S. should promote STEM education and adjust visa, security clearance, and certification practices to attract, train, and retain the very best personnel for America's key public-sector and private-sector entities. This requires issuing more security clearances as appropriate and emphasizing cyber certification and credentialing programs. Achieving the workforce needed requires the U.S. to more effectively leverage its cybersecurity personnel, whether that is integrating military personnel into cyber efforts, or tapping highly skilled hackers who would normally not be eligible to work for businesses or government agencies.

- **Lead international cyber engagement.** The U.S. should lead international efforts to "name and shame" nations that use the cyber realm for malicious purposes, either against other nations or their own people. Additionally, the U.S. must respond to aggressive cyber campaigns by other nations by causing those nations to feel diplomatic and economic pain to deter cyber aggression. The U.S. response should include ceasing naive cooperation, curtailing visas for guilty parties, and subjecting those with stolen information and intellectual property to criminal charges and other legal action. Furthermore, many bad cyber actors also maintain some form of control over the Internet in their country. The U.S. should explore ways to weaken these nations' grip on the Internet in order to weaken their control of the populace. All of these efforts should be tied to the completion of a coherent national conversation concerning the entire array of cyberspace issues.

Cybersecurity is one of the most critical issues the U.S. faces today. The threats are real and the need is pressing. Despite the best intentions of those involved with previous cyber legislative efforts, a regulatory basis simply will not work. It will not improve security and may actually lower it by providing a false level of comfort and tying the private sector down with outdated regulations. Cyberspace's dynamic nature must be acknowledged and addressed by policies that are equally dynamic.

*—**Steven P. Bucci, PhD,** is Director of the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies; **Paul Rosenzweig** is a Visiting Fellow in the Center for Legal and Judicial Studies and the Allison Center for Foreign Policy Studies; and **David Inserra** is a Research Assistant in the Allison Center for Foreign Policy Studies, at The Heritage Foundation.*