U.S. Cybersecurity Policy: Problems and Principles

by Steven Titch

Introduction

Cybercrime and cyberattacks are genuine threats. Reports of data breaches, hacks, or thefts have become daily news:

- In January 2013, data servers at The New York Times and The Wall Street Journal were infiltrated in an attempt to identify the newspapers’ sources for their coverage of political and economic news in the People’s Republic of China. Although The Wall Street Journal never officially confirmed it was breached, the Times did and accused the Chinese government of being behind the hack.¹

- In February, the loose-knit hacker group Anonymous claimed credit for a series of hacks of the Federal Reserve Bank, Bank of America, and American Express, targeting documents about salaries and corporate financial policies in an effort to embarrass the institutions.²

- In May an organized ring of thieves based in the Dominican Republic fabricated counterfeit automated teller machine (ATM) prepaid “gift” cards, then deployed accomplices in cities in

---


© 2013 The Heartland Institute. Nothing in this report should be construed as supporting or opposing any proposed or pending legislation, or as necessarily reflecting the views of The Heartland Institute.
26 countries who used them to withdraw $45 million.  

- Also in May, a Pentagon report disclosed that Chinese hackers had stolen designs for more than two dozen major weapons systems deemed critical to U.S. missile defenses and combat aircraft and ships.  

These events add to the incident reports that have been gaining greater prominence each year. Sites such as eBay and Amazon deal with fraud attempts daily. Government agencies such as the Social Security Administration and Veterans Administration have lost sensitive data about taxpayers. Banks and mortgage lenders have had their Web sites come under direct denial of service (DDoS) attacks from individuals and groups who blame the institutions for the 2008 recession. The Defense Department, along with power companies and other major private-sector companies involved in critical infrastructure support, say their firewalls, malware protection tools, and other network safeguards are routinely being tested for vulnerabilities by hackers they believe are working for or with foreign governments such as China and Iran.

Organizations such as the National Research Council have been beating the drum for action. A November 2012 NRC report speculated that a cyberattack on the U.S. power system could knock out power to large regions of the nation for several months.  

---


Fueled by media hype of hacks and breaches, as well as popular entertainment that posits provocative yet highly speculative accounts of cyberattacks, cyberterrorism, and cyberwar, lawmakers feel compelled to demonstrate they are “doing something” about the problem.

Congress and the White House have pressed for action on cybersecurity. Despite their failure in 2012, two major bills were reintroduced in Congress this year. The first, the Cyber Intelligence Sharing and Protection Act (CISPA), passed the House of Representatives in April but failed in the Senate. The second, the Cybersecurity Act, a Senate bill cosponsored by Sens. Joe Lieberman (D-CT) and Susan Collins (R-ME), is pending.

Separately, President Barack Obama announced in his 2013 State of the Union Address that he had earlier that day signed an executive order on cybersecurity, although it was more of a framework for action than a set of rules.

**Government’s Role Still Needs Definition**

Few would say government has no role in cybersecurity. The U.S. Constitution identifies the common defense as a task of a federated government. Nonetheless, the same Constitution established limits on government power, primarily for the protection of individual liberty and respect for personal boundaries. For example, Congress may raise an army, but it can’t quarter soldiers in private homes.

Likewise, the principal tension in cybersecurity, which by definition involves computers, networks, and data, is between the need to protect citizens, property, and infrastructure while respecting the privacy and integrity of the data and systems being protected.

The government, along with contractors that might benefit from creation of a “cybersecurity industrial complex,” has stoked this tension further by wildly overestimating the cost of cybercrime to American industry. In 2009, computer-security firm McAfee claimed cybercrime was costing the U.S. $1 trillion a year, a figure used later by both President Barack Obama and Gen. Keith Alexander, head of U.S. Cyber Command, in calls for greater government control of the Internet. In July 2013, McAfee, in a joint study by the nonprofit Center for Strategic and International Studies, revised its estimate down to $100 billion – one-tenth of the 2009 figure. Although sizable, the $100 billion figure is comparable to other types of losses U.S. businesses confront. For example, auto accidents result in annual losses between $99 billion and $168 billion.

---


Although the proposed government solutions vary in scope, they all have one element in common: They would broaden the power of the U.S. government to collect and examine the information private-sector companies use in their routine online relationships with consumers and businesses. These include not only telecommunications and Internet service providers (ISPs) such as Verizon, AT&T, and Comcast, but any company that relies on the Internet for a significant amount of operations – banks, retailers, social networks, airlines, application developers – whether they use their information technology to connect directly with customers or have internal IT mechanisms to process customer data for their proprietary use.

The Cybersecurity Act goes further, proposing a set of government-imposed, top-down regulations to combat cybersecurity threats. What these proposals overlook is the wide range of procedures and protocols that have been developed bottom-up over the past several decades – procedures that have been tested by real-world experience and subject to regular and ongoing review, revision, and updating.

Similarly, Obama’s executive order calls for information-sharing and mandated protocols, but it fails to provide specifics. Lack of specificity, in fact, is the principal drawback of all these cybersecurity actions and proposals. Politicians and policymakers coin terms such as cyberattack, cyberwar, cyberterrorism, and cybercrime without definition and construe them broadly. There has been little attempt to identify the goals of each bill or the scope of the activity it is aimed at preventing or proscribing.

In the rush to write additional laws, there has been little review of whether their provisions conflict with existing laws that safeguard privacy, such as the Electronic Communications Privacy Act (ECPA). An aspect of the current cybersecurity legislation that critics find particularly troubling is that their vagueness would give prosecutors too much discretion and the laws would end up being applied too broadly and incorrectly. This concern is more than hypothetical. The most notorious recent example is the prosecution of Aaron Swartz.

Federal prosecutors charged Aaron Swartz with 11 violations of the Computer Fraud and Abuse Act and other crimes carrying a cumulative maximum penalty of $1 million in fines plus 35 years in prison.

Swartz, an entrepreneur and Internet activist, was influential in the creation of the social news site Reddit and the development of RSS – the service that allows users to consolidate and track their favorite blog sites – and was a key participant in the development of Creative Commons, a structure for content creators to share their work voluntarily on the Web.

Swartz had a reputation for flouting Internet law and convention regarding content-sharing. In January 2011 Swartz was arrested by Massachusetts Institute of Technology police on charges of breaking and entering after he used unauthorized access to get inside an MIT building and open a server closet. There he connected a laptop computer to the MIT network and downloaded a high volume of content from Journal Storage (JSTOR), an MIT-maintained digital library and index of thousands of academic articles published by some 8,000 universities worldwide.

With cybercrime gaining political mindshare at the time and Swartz poised as a high-profile
defendant, federal prosecutors got involved, charging him with 11 violations of the Computer Fraud and Abuse Act (CFAA) and other crimes carrying a cumulative maximum penalty of $1 million in fines plus 35 years in prison, asset forfeiture, restitution, and supervised release. Although CFAA dates back to 1984, there has been a flurry of add-on amendments since 9/11, largely ad hoc reactions to cybersecurity concerns.

Even as they conceded there were ethical questions regarding Swartz’s action, mainstream advocates for Internet freedom, from organizations such as the Electronic Freedom Foundation to influential Internet figures such as Tim Berners-Lee and Lawrence Lessig, argued prosecutors were overreaching. Swartz did not compromise any private information or damage any computer equipment or service. Although access to JSTOR is fee-based, those fees are nominal and are used to support the service, not to compensate authors. Most Internet freedom advocates agreed that if Swartz did anything wrong aside from physical trespass on the MIT campus, he violated the terms of JSTOR’s service—a civil matter, not a criminal one. More telling was that MIT, the only party that could claim loss, dropped its own charges against Swartz and then changed JSTOR’s terms of service to provide more open access to its storehouse of articles, the precise goal of Swartz’s action.

As support for Swartz grew from influential circles, prosecutors offered him a plea deal of six months in jail but insisted that a permanent designation of “convicted felon” remain on his record. Swartz, who had a history of depression, committed suicide before his case could be adjudicated. Although prosecutors to the end maintained Swartz’s guilt, after his suicide they dropped all charges, effectively exonerating Swartz posthumously. Federal legislators then introduced bills to amend CFAA specifically to prevent its use in cases of terms-of-service violations. This amendment, known colloquially as “Aaron’s Law,” has failed to gain traction thus far.

Reasonable people may debate the seriousness of Swartz’s crime. Nonetheless, the same reasonable people should question a legal framework in which the U.S. government elected to bring down the full weight of cybercrime laws on a respected, contributing member of the Internet establishment.

Defining the Threat

The Swartz case argues that instead of rushing to write vague, poorly defined laws against computer crime, lawmakers must first understand the nature and scope of the cybersecurity threat, the countermeasures that work, and how people and property can be protected within the bounds of the Constitution and Bill of Rights.
Sound cybersecurity policy begins with accurate definitions and a thorough understanding of the threat. Cybersecurity can be defined as the protection of the computer and networking assets and information technology functions of an organization, including the electronic data that are either proprietary to the organization or with which the organization has been entrusted. Specifically, these data could include (but not be limited to):

- documents and records,
- customer/employee data,
- intellectual property, and
- data and software processes critical to operations.

There are different types of cybersecurity threats, each of which targets different parts of an organization’s information technology infrastructure and each with its own goal. Broadly, they can be divided into three categories: theft and fraud, espionage, and disruption or destruction. (See Table 1.)

**Theft and Fraud**
The motive behind cybertheft and cyberfraud is profit, and the targets can be individuals or institutions. Examples include the global ATM hack in May 2013 and identity theft through illegal use of Social Security numbers, credit card accounts, or other private information. These activities are generally the work of organized crime rings supported by a decentralized infrastructure. Individuals working on their own might illegally acquire private information and then sell that data to other criminals.

**Espionage and Threat of Exposure**
The motive of cyberespionage is to acquire information. In the business sector, this can include theft of blueprints, formulas, strategic planning documents, or other proprietary information that could yield a competitive advantage. In the government sphere it can involve military intelligence, classified data, or simply embarrassing documents. Even nonprofit organizations can be targets: The Heartland Institute, publisher of this *Policy Brief*, was the target of such an attack in February 2012, when disgraced water scientist Peter Gleick, president of the Pacific Institute, stole confidential documents and circulated a forged document in an effort, successful in some respects, to embarrass Heartland and its donors.\(^8\) Espionage also includes state-sponsored cyberattacks; hacking becomes just another tool in the spy’s kitbag.

---

**Disruption or Destruction**

The motive of disruption or destruction attacks is to cause harm or losses through an assault designed to slow, disable, or destroy systems and operations. Examples are many and varied, ranging from DDoS attacks for which groups such as Anonymous are noted, up through state-sponsored cyberterrorism, where the goal might be significant disruption of a nation’s critical infrastructure, utilities, transportation, financial services, or other systems in order to create social or economic havoc for the short or long term. The most damaging cyberattack against U.S. interests disclosed to date was against Saudi Arabia-based ARAMCO, the world’s largest oil company: A large-scale hack of some 30,000 ARAMCO personal computers in August 2012 erased all data on their hard drives. A militant Islamic group called the Sword of Justice took credit, although U.S. Defense Department analysts believe the government of Iran provided support.\(^9\)

<table>
<thead>
<tr>
<th>Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary of Threat Types and Responses</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Theft/Fraud</strong></td>
</tr>
<tr>
<td>Motive: Profit</td>
</tr>
<tr>
<td>Targets: Individuals, corporations, institutions</td>
</tr>
<tr>
<td>Perpetrators: Domestic and international organized crime rings</td>
</tr>
<tr>
<td>Response: Isolate and identify the perpetrator; arrest and prosecute if possible. Tools and procedures include the collection of forensic data, analysis of the means of attack, and development of policies and countermeasures.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Espionage/Exposure</strong></td>
</tr>
<tr>
<td>Motive: Information acquisition</td>
</tr>
<tr>
<td>Targets: Corporations, universities, defense contractors, government agencies, nonprofit organizations</td>
</tr>
<tr>
<td>Perpetrators: Rival corporations, private investigators, foreign governments, hacker groups, ideological activists</td>
</tr>
<tr>
<td>Response: Pre-emptive protection and prevention. Institutional awareness of potential threats, as well as policies and countermeasures.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Disruption/Destruction</strong></td>
</tr>
<tr>
<td>Motive: Disruption of online operations to outright destruction of systems</td>
</tr>
<tr>
<td>Targets: Large institutions that manage significant economic, government, or public infrastructure</td>
</tr>
<tr>
<td>Perpetrators: Political activists, terrorists, nation-states</td>
</tr>
<tr>
<td>Response: Rapid response that can isolate and neutralize an attack within minutes or seconds. Information-sharing mechanisms that can be used to identify source of the attack.</td>
</tr>
</tbody>
</table>

Tailoring the Response

Just as the categories of cybercrime represent different objectives and motivations for attack, they require solutions engineered to address the specific threat in order to combat it effectively. That’s why the current one-size-fits-all approach to cybersecurity, exemplified by CISPA, the Cybersecurity Act, and CFAA, cannot help but fail.

It’s important to understand there is a limit to what government can do to prevent cybercrime or cyberattacks. For the most part, physical security is understood to entail personal responsibility. We lock our homes and garages, purchase alarm systems and similar services, and don’t leave valuables in plain sight. Businesses contract with private security companies to safeguard employees and property. Government law enforcement can be effective after the fact – investigating the crime and arresting and prosecuting the perpetrators – but police are not routinely deployed to protect private assets.

Similarly, it should not be the government’s job to protect private information assets. As with physical property, that responsibility falls to the property owner.

Businesses consider best practices to be the first line of cybersecurity defense, and they are in fact doubtful about the effectiveness of government regulations.

Indeed, the private sector understands effective cybersecurity begins with effective physical security. The “genius hacker” – the brilliant individual who can use his talents to overcome firewalls and subvert network protection software – is a myth. Most hackers compromise cybersecurity by first compromising physical security. They use the tools of the thief or confidence artist – stealing laptops and employee directories, lying to or emotionally manipulating a target to extract desired information, or simply infecting a networked computer with a virus or malware introduced via email or a thumb drive surreptitiously plugged into a USB port. Sometimes a cybercriminal can induce the target to do this himself. Among IT security auditors, it is a standard test to scatter thumb drives around the parking lot of a corporate campus and then see how many employees pick them up and use them.

Individuals who work in businesses that rely on secure data have even more protocols to follow. Don’t take laptops home. Verify a customer’s identity before discussing, accessing, or sharing information from that customer’s file. Don’t allow individuals to “tailgate” through doors – if a badge or access card is required to get in, make sure they use it.

Businesses consider best practices to be the first line of cybersecurity defense, and they are in fact doubtful about the effectiveness of government regulations. In a 2011 survey, 1,861 IT professionals across a wide range of industries, including government, were asked what factors have the biggest impact on improving cybersecurity. Of those surveyed, 58 percent said implementing best practices and better security policies. Another 20 percent said employee
awareness. Only 15 percent said cybersecurity can be improved through better technology, and just 7 percent said government regulation and law enforcement were the answer.\(^\text{10}\)

**Current Government Policy and Proposals**

Despite these realities, regulation remains the cornerstone of the government’s cybersecurity policy. Key elements are centralized information collection and top-down mandates, all of which involve privacy invasion while promising little effectiveness in countering cyberthreats. Let’s look at some examples.

*Cyber Intelligence Sharing and Protection Act (CISPA)*

Much of CISPA sets out requirements about how the private sector would share private information in the event of a cyberattack. A key component of the bill is its abrogation of any liability on the part of corporations that share personal information with the government. Typically, as part of user agreements, companies such as Facebook, Google, Amazon, and other commercial Web sites pledge not to provide third parties with data that can be used to identify a user personally.

In a scenario where a hostile country launches a cyberattack against Google or Facebook, the Department of Homeland Security can ask those companies to turn over users’ private information it believes will be helpful in tracking the source and nature of the threat. Under CISPA, companies would not be required to anonymize the data, as they would under any other circumstance. CISPA grants a company automatic immunity from any lawsuits that might result from unauthorized disclosure of personally identifiable information.\(^\text{11}\)

The threshold the government could use for information collection under CISPA is vague. Instead of specifically referring to investigation of malicious activity, such as the appearance of hacker-controlled “botnets,” new viruses, or malware, the bill would give the government authority to act on anything it designated as a “threat indicator.” As one CISPA critic wrote, this could mean giving government regulators access to “anything from users’ online habits to the contents of private e-mails – creating a broad loophole in all federal and state privacy laws and


even in private contracts and user agreements.”

The CISPA provision relieving corporations from the cost of scrubbing data was one reason the bill enjoyed support from most of the Internet industry. However, opposition from users and organizations lobbying on their behalf, as well as White House opposition, succeeded in killing the bill.

Cybersecurity Act

The White House opposition to CISPA did not stem from concerns over consumer privacy. Quite to the contrary, the administration argues CISPA did not go far enough. The Obama administration instead is backing the Lieberman-Collins Cybersecurity Act which, in addition to information-sharing, mandates protocols and procedures the private sector must use to counter cyberthreats.

The bill’s initial draft would have required U.S. companies to adopt cybersecurity standards set by the Department of Homeland Security. This was later amended to legislate voluntary adoption of these standards, but the provision came with a condition: Companies that chose not to adopt the “voluntary” standards would be cut out of any information-sharing in the event of a major cyberattack or hack. This struck one respected security consultant as counterproductive and petulant: “Denying [affected companies] the informational tools … because they don’t follow the government’s lead may be cutting off our nose to spite our own face.”

Presidential Executive Order

In his State of the Union Address on February 13, 2013, President Barack Obama announced he had earlier in the day signed an executive order calling for an information-sharing “framework” similar to what CISPA and Lieberman-Collins propose, but with even fewer specifics. For instance, terms such as “cyberthreat” and “cyberintrusions” were left undefined. The framework would allow intelligence to be gathered on cyberattacks and cyberthreats against privately owned critical national infrastructure – such as the private defense sector, utility networks, and the banking industry – so they can better protect the infrastructure itself as well as the general U.S. population, the economy, and other nations reliant on U.S. support. The order excluded


consumer information technology services such as those operated by Microsoft, Google, Facebook, and Twitter, appeasing some privacy advocates, including the American Civil Liberties Union.\textsuperscript{14}

\textit{Computer Fraud and Abuse Act}

Absent any new legislation, the Computer Fraud and Abuse Act remains the federal government’s primary weapon against computer crime and domestic cyberterrorism. It has all the flaws of reactionary legislation while offering little in terms of effectiveness or deterrent.

The vagueness of laws such as CFAA enables excessive prosecutorial discretion. Speaking on the use of CFAA in the Swartz case, James Grimmelman, a professor of law at New York Law School and a member of its Institute for Information Law & Policy, suggested the U.S. attorney in the case could not discern the difference between ordinary computer crime and what, to Grimmelman, was an act of civil disobedience. CFAA, Grimmelman said, “creates this huge zone for prosecutors to charge multiple overlapping crimes with enormous sentences which they then use to bargain down to lesser sentences and keep the plea bargain machine moving. This causes all kinds of perverse consequences.”\textsuperscript{15}

Its misapplication in the Aaron Swartz case is enough to justify a thorough review, if not repeal, of CFAA. The “Aaron’s Law” amendment removing violation of terms-of-service from CFAA’s purview was a step in the right direction but to date has gone nowhere. The law states anyone who “exceed[s] authorized access” can face felony charges. This means virtually any American could be targeted as a violator.

For example, although the Facebook terms of service require all users to be 13 or older, many parents allow younger children to have accounts, usually because they turn 13 later in the school year relative to their grade-level peers.\textsuperscript{16} Parents who do this technically are in violation of CFAA and have committed a felony.

Similarly, the terms of service for the \textit{New York Times} Web site restrict visitors to ten free articles a month, after which they are obliged to purchase a subscription. However,


\textsuperscript{15} James Grimmelman made these comments on the podcast \textit{Surprisingly Free}, produced by the Mercatus Center of George Mason University, January 29, 2013, http://mercatus.org/podcast. This quote can be found at the 42:50 mark.

knowledgeable users know the Times’ quota does not include articles accessed via Google. Find yourself stymied by the Times’ site’s quota? Simply type the headline of the article into a Google search field and you’ll be able to read it. However, at any time the FBI can interpret that access as “unauthorized” under CFAA and charge you.

The notion that centralized government control is the only thing that lies between cyberattack and civil disorder should be met with extreme skepticism.

It’s not hypothetical or far-fetched. The government has a broad definition of “unauthorized access.” In July 2009, federal prosecutors in Las Vegas arrested a video poker player on CFAA charges after the player exploited a software glitch that altered the payout on a particular type of machine. According to reports, the player discovered the glitch by accident; the game paid out incorrectly if a series of buttons on the machine was pressed in a certain order. Prosecutors allege the player, John Kane, used this knowledge to rig $500,000 in payouts from machines in several states.

Although Kane may have violated state and local laws regarding cheating, and the casinos affected may have a legal argument for getting their money back, the federal prosecutor’s claim that “unauthorized access” extends to the player’s pressing of buttons in a specific sequence is a stretch. The player did not attempt to access or alter the software running the machine or otherwise hack into it, and the machine itself was freely available in the casino for public use. The rules of the game allowed a player to press buttons in any order. The software flaw was either the manufacturer’s or casino’s responsibility to detect and correct. In 2012, a federal magistrate agreed with the defendant and recommended the CFAA hacking charges be dismissed, and in May 2013 the Department of Justice dropped the CFAA charges outright.¹⁷

Is Cyberterrorism Overhyped?

Finally, there is the worry about U.S. vulnerability to a cyberterrorist attack that would create a large-scale economic or humanitarian disaster. While one should not discount such a threat, it needs to be viewed rationally. Frankly, the notion that centralized government control of the nation’s Internet and data networking assets is the only thing that lies between cyberattack and civil disorder should be met with extreme skepticism.

As a word, cyberterrorism has a dramatic ring. And certainly movies and TV have upped the ante in the popular zeitgeist. Last fall saw the premiere of the TV series Revolution, which imagines a complete civil breakdown after a technological cataclysm renders all electric and electronic items inoperable.

But if we step back and think rationally, we can assess potential outcomes and strategize about an appropriate level of prevention and response.

For starters, while a cyberattack may be disruptive, it cannot carry the cost or the visceral weight of a physical attack. The Boston Marathon bombers did more physical and psychological damage with their relatively contained attack than a hacker can do with malware. The bombing and the manhunt that followed were front-page news for days. The cyberattack on ARAMCO barely registered a blip in our 24/7 news cycle.

But can a cyberattack cause death and destruction on a massive scale? There have been a number of suppositions. Could power plants across the U.S. be shut down? Could the rail system be hacked so freight trains carrying dangerous or toxic cargo, such as chlorine gas, derail or crash? Could hackers take over air traffic control and cause horrifying mid-air collisions?

Theoretically, yes. However, as a number of analysts have noted, the sheer scope of logistics, communication, and coordination needed to carry off attacks of this magnitude with any degree of success makes a direct physical bombing or assault easier and much more effective. The popular notion is that a massive cyberattack can be carried out by a lone individual or at worst, a small terrorist cell with a laptop and an Internet connection. That’s not feasible.

Let’s take the “nightmare scenario” of an air traffic control (ATC) breach. First, there are hundreds of ATC centers throughout the U.S. If an attacker disabled ATC operations at O’Hare International Airport in Chicago, ATC towers at nearby airports such as Midway, DuPage County, Gary, Indiana, and possibly Milwaukee and St. Louis would be able to pick up aircraft communications and control.

So it would not be enough to strike at O’Hare ATC; the attacker would have to take down ATC operations at all regional airports nearby. While ATC systems are connected to the Internet, each system nonetheless operates independently and has its own security protocols. To hack into six airport systems, the attacker would need access to all six systems, not just one. He would have to suborn or manipulate insiders at all these places to gain system passwords as well as mundane but crucial information on shift times and staffing. The attacker would have to manage this intrusion simultaneously at all locations without detection. The attacker also would have to figure out a way to jam radar and radio communications between aircraft and ground over a huge area. Pilots are also trained for loss-of-communication scenarios and are fully capable of flying their planes using onboard controls.

As you follow this line of reasoning, what emerges is an operation that requires substantial resources yet relies on a huge number of variables the cyberattacker can’t control. If terror and

---

massive loss of life are the objective, a bomb smuggled aboard a plane in a shoe or piece of clothing, or a missile from a shoulder-mounted launcher from the ground, has a far better chance at success.

If terror and massive loss of life are the objective, a bomb smuggled aboard a plane or a missile from a shoulder-mounted launcher has a far better chance at success.

The railroad example posits that a cyberattacker can hack into the rail traffic control system and cause two trains carrying hazardous cargo to collide by placing them on the same track. The hacker first would have to go through the time and effort of acquiring highly secure data on freight schedules and hazardous cargo. Again, that would mean hacking several systems over a period of time while avoiding detection. He then would have to gamble on the accuracy of the manifests and how close the trains were operating to their timetables. He can’t afford to hack in and spend too much time waiting for trains to get in position. Every extra moment he spends in the system increases the chance of his hack being discovered. He also would have to hope that internal alarms designed to alert operators and prevent such collisions go unnoticed.

By contrast, by simple observation on public highways, an attacker can note grade-level rail crossings in populated areas where trains carrying tons of poisonous chemicals regularly pass. All he needs now is a suicide bomber and a pick-up truck full of explosives.

With respect to power plants, analysts believe an effective means of attack would be to hack into a turbine control system and power up the turbines to such a high speed that they burn out. Again, scale presents obstacles. The U.S. power grid is not a single network. Each power plant would have to be attacked individually, which like the ATC example means involving a large number of people, unwittingly or not, in the conspiracy. Even if the first few hacks are successful, within minutes the pattern would be discernible and other plants would disconnect from the larger Internet.

To be sure, power would be out, business and commerce would be affected, travelers would be delayed, and there likely would be some hardship. But the effect would be localized. There would not be the mass civilian casualties and devastating property damage that come from a true act of war. It would be nothing most people have not experienced at least once in their lives. There would not be the massive property damage or humanitarian problems that accompany natural disasters. People would be able to go back their homes. There would be no need for large-scale evacuations or temporary sheltering centers.

Consider recent examples, such as Tropical Storm Sandy, the tornadoes in Moore, Oklahoma, and Hurricane Katrina. Civilization did not break down. Emergency services were able to get through. Rebuilding was able to commence. Essential services had backup power.

Seen in this perspective, the terms “Cyber Pearl Harbor” and “Cyber 9/11” are seen as the hyperbole they are.
If the New York Stock Exchange were shut down by a virus, trading would stop, just like it does at 4 p.m. every day. The stock market might remain closed for several days while the problem was sorted out, but the New York markets were closed for a week after 9/11 and the world kept turning. New York, moreover, isn’t the world’s only financial trading center. Stock exchanges would be open in London, Hong Kong, Tokyo, and elsewhere.

Regarding cyberterror dangers to personal financial records, note that information is stored redundantly in fixed media. It can’t all be erased at one time. You have bank statements at home, on your PC. Your money can be stolen, but it can’t be erased.

On the Web, information storage is becoming more virtualized every day. Your data are not all in one place. The Internet itself is decentralized, highly redundant, and remarkably robust. Cut one part of the global backbone and the network will reroute around the break. The principal vulnerabilities, ironically, are the bottlenecks governments intentionally set up. Repressive regimes such as Syria and Iran, for example, make sure all (non-satellite) traffic into and out of the country connects through a small number of regime-controlled gateway switches. Democratic governments, including the United States, consider creating the same vulnerabilities by proposing ideas such as an Internet “kill switch,” a single central control point for all domestic Internet traffic. Such a switch is unnecessary for security purposes: Most private networks can disconnect from the public Internet backbone easily if necessary. In addition, the public Internet is more secure the more decentralized it is.

In 2002, someone tried to bring down the entire Internet by orchestrating a massive DDoS attack on the 13 top-level domain name servers that manage worldwide information traffic. The attack disabled seven of the servers for about three hours before administrators resolved the problem. Although traffic slowed, the worldwide Internet never crashed.

Since cyberwarfare is only now emerging as an element of combat, there remain questions regarding what is an appropriate response.

Finally, since cyberwarfare is only now emerging as an element of combat, there remain questions regarding what is an appropriate response. Here matters diverge from domestic security and enter the area of military strategy. Cyberwarfare, like terrorism, changes the rules of engagement, which address questions of appropriate response to provocation or attack, especially when there has been no formal declaration of war. How should a nation be prepared to retaliate against a cyberattack? Is it appropriate for a nation’s military to respond with a physical military strike that might not only destroy an actual military target but also cause collateral damage and civilian casualties? What options are available if an attack is attempted but fails? Is it justifiable to respond with a successful and devastatingly effective hack?

Before Congress begins writing laws or the president starts declaring more “red lines,” the national government ought to articulate and legislate a rational cyberdefense policy through
Principles of Sound Cybersecurity Policy

The flaw in the federal government’s cybersecurity policymaking is that it sees cybersecurity as something separate and apart from conventional law-and-order and national defense issues. People have been committing theft, fraud, vandalism, and espionage throughout history, through whatever means were at hand. Similarly, an objective of warfare always has been to damage the enemy’s manufacturing, transportation, logistics, and communications. Exploitation of vulnerabilities in computer networking is simply a new method for achieving these objectives. That’s why effective cybersecurity builds on existing laws and law enforcement mechanisms. Effective cyberwarfare defense builds on international diplomacy, cross-border police cooperation, and rules of engagement. Congress, the White House, and the Pentagon need not reinvent the wheel.

To some degree, the National Research Council realized this when it tied together the physical and cyber vulnerabilities of the U.S. power grid in its November 2012 report. For example, a bomb can knock out an electric transformer as effectively as a computer virus can – perhaps more easily, the NRC notes, if physical security is not accorded the same attention as cybersecurity.

Any new laws or amendments should follow a discrete set of principles to prevent their abuse and address specific security objectives while remaining within Constitutional limits. Those principles are outlined in the rest of this section.

New laws should be a last resort.

If cybersecurity is understood in the context of general security, the first step in sound policymaking is to examine existing laws before rushing to create new ones. Existing law may indeed be effective. If not, laws can be passed or amended to address new dimensions cybersecurity creates. This reduces the promulgation of vague laws with vague objectives, as well as the risk of prosecutorial overreach.

---


20 Supra note 5.
Certainly cybersecurity might require sharing of data. Investigators need to know how the attack occurred, the nature of any malware or virus, and how it infiltrates systems and replicates. To some extent, however, government access to the targeted information or application should be a secondary concern. The government may need to know how malware stole $100,000 from Joe Smith’s bank account, but does it need to know Joe Smith’s transaction history for the past ten years? Does it need to know what other bank accounts he has? Does it need to know his creditors, debtors, and tax payments?

**Security efforts should target wrongdoers only.**

Cybersecurity law should be written to punish and deter acts that involve destruction and loss. The severity of the penalties must be consonant with the severity of the act. Because civil disobedience can be an element of cybercrime, the law must account for it.

The law must come down hard on deliberate theft, destruction, or other clear criminal intent. At the same time, there must be accounting for severity. A DDoS attack may impose a staff time cost on an institution for repairing its systems and inconvenience for customers, but there may be little damage to basic systems and no financial loss to the company or customers. Well-written law will ensure that prosecutorial resources are devoted to stopping organized groups of criminals who use email scams to drain the life savings of local pensioners, not to relentlessly pursue a lone activist who, as an act of protest, downloaded and posted public-record local government documents that proved embarrassing to local elected officials.

**Respect due process and the rights of the accused.**

The individuals who participated in the $45 million ATM theft were apprehended and police were able to create a trail of evidence from the video recordings from the ATMs they hit. Since bank robbery is a felony, their activity was illegal. There is no need for a separate law to address the wrongdoing they did.

For a purely white-collar example, there was the noted case in 2006 after Hewlett-Packard hired a team of private investigators to investigate leaks of company information to the media. The investigators contacted various phone companies and impersonated several HP board members and journalists in order to obtain their phone records. The technique, known as pretexting, was in a legal gray area at the time. Even so, the HP executives and private detectives involved in the

---

scheme were all prosecuted under existing state and federal laws that cover wire fraud, illegal acquisition and use of computer data, use of personal identifying information without authorization, identity theft, and conspiracy. The notorious CFAA (which was more limited at the time) did not even come into play.

Even John Kane, who profited from the software glitch in the video poker machines in Las Vegas, has not got off scot-free. He still faces federal wire fraud charges because he used a phone to enlist an associate to successfully exploit the same types of video poker machines in Pennsylvania casinos. Peter Gleick, the scientist who had targeted The Heartland Institute, was forced to resign as chairman of the American Geophysical Union’s Committee on Scientific Ethics.22 While federal prosecutors in Chicago have refused to pursue a criminal case against him, a summary of the criminal case against him is available online23 and his actions continue to attract derision more than 18 months after the incident.24

---


24 See, for example, the collection of posts at meteorologist Anthony Watts’ popular WhatsUpWithThat blog, http://wattsupwiththat.com/tag/peter-gleick/.

Open-ended information gathering and processing should not be used.

Although some data can be important in identifying and combating viruses and malware, much is embedded in operating software and processes. Applications such as email and social networking may provide a gateway for a virus into a system, but the specific information in an application – emails, mailing lists, Web searches, and navigation records – rarely holds any value to forensic investigators. Yet CISPA, the Cybersecurity Act, and the White House executive order would demand their collection without much justification.

CISPA critics said the bill could be used to gather a huge amount of information about users, including their preferences, purchases, beliefs, and habits. Supporters of the bill scoffed, saying the purpose of the bill was to keep people safe and the government would have little interest in, or use for, citizens’ personal information. Those assertions mirrored assurances from the authors and supporters of the PATRIOT Act, the hastily written law that gave the federal government tremendous power to secretly gather private information on U.S. citizens. Although the PATRIOT Act was aimed at counterterrorism more than cybersecurity, the increased protection of the American people was its justification.

Then, in June 2013, news reports disclosed the U.S. National Security Agency, after securing a top-secret warrant from the Foreign Intelligence Surveillance Act (FISA) Court, had been collecting calling data on millions of wireless phone users. Then came reports the NSA’s surveillance program extended to email, Web searches, and other electronic communications. Sweeping as it was, this surveillance was legal under the PATRIOT Act, yet most Americans were shocked to learn the government had used it to such an extent.

In the days that followed the disclosure, the White House and Congress were at a loss to explain why so much information was needed and what value it added to anti-terror efforts.²⁶ Worse still, it now appears the government is willing to misuse its access to confidential information for political purposes. The NSA disclosures followed reports that the Internal Revenue Service had selectively delayed granting non-profit status to citizen groups if the words “Tea Party,” “Patriot,” and “Constitution” – nomenclature that tended to be used by Republican, conservative, or libertarian-leaning political action groups – appeared in the organization’s name. As investigation continued, it became apparent that groups affiliated with Democratic, liberal, or progressive causes were not subject to the same reviews and delays. The pattern suggested the IRS was being used as a political weapon by the party in power to reward its friends and punish its opponents.

The lesson is that lawmakers should be cautious about granting the government a sweeping degree of latitude in collecting and using citizens’ information, especially in the name of security.

security. It is becoming clear that when granted new legal power to use information-gathering or surveillance technology in domestic security, the government will push the limits of the law as far as it can. History tells of President Richard Nixon’s “enemies list,” a group of political opponents he ordered the IRS to audit. Donald Alexander, a commissioner of a more-principled IRS at the time, refused the order.

As this paper goes to press, reports were emerging that the U.S. government had been pressuring major Internet firms into disclosing customer account passwords, a process that would have required many firms to pro-actively decrypt them out of customer-confidential data.\textsuperscript{27} In other words, the government, in an insatiable appetite for citizen information, was demanding that private companies violate their own policies on customer security and, quite literally, hack their own customers.

\textbf{Vague cybersecurity regulatory “frameworks” are unnecessary.}

As this \textit{Policy Brief} goes to press, the only new cybersecurity initiative in force is Obama’s executive order. As it was issued in February 2013, most observers believe it’s too early to tell whether it will engender additional complexity or cost for private-sector companies.

\begin{quote}
When granted new legal power to use information-gathering or surveillance technology in domestic security, the government will push the limits of the law as far as it can.
\end{quote}

The vagueness of the executive order remains its chief defect. To a certain degree it is merely an executive order to create another executive order. In its analysis of the order, the security research and consulting firm Forrester Research notes there is a lack of clear directives for how private-sector companies should implement the framework and no indication of how complex the task would be.\textsuperscript{28} Nor does the executive order specify any plan to address cybersecurity at the international diplomatic level to work with governments that may be behind some of the cyberattacks.

The Obama executive order is just the latest of many security “frameworks” imposed in recent years. Others include standards set forth in legislation such as the Federal Information Security Management Act (FISMA), general joint industry standards such as the National Institute of Standards and Technology’s 800-53 document, and specific industry standards such as those developed by the Federal Energy Regulatory Commission. Layering yet another framework on top of those will create additional challenges, and if all the regulations can’t be aggregated and streamlined, they stand to become red-tape headaches rather than useful measures.


The private sector should take the lead.

In cybersecurity, the government ought to remove the plank from its own eye before addressing the splinter in the private sector’s. Although data breaches occur throughout the commercial, industrial, education, and government sectors, government consistently has been among the most vulnerable to losing large amounts of information. In 2011, although federal, state, and local government agencies were the target of 11 percent of U.S. data breaches, those breaches combined represented 44 percent of all private and confidential records exposed that year.29

The source of most breaches generally is poor stewardship of information. Computer disks containing sensitive data have been lost or misrouted. Government-employee laptops that should never have been removed from their offices have been stolen. Documents that should be shredded are discarded with everyday trash.

Compared to government, the private sector has lost relatively little information, data, or money to computer hacking. Even the global ATM hackers did not attempt to tap individual user accounts because they knew they would be detected in a matter of minutes. Instead they targeted the pool of funds that banks collectively make available for prepaid ATM cards. Banks expect this fund to be drawn down by millions of dollars daily, which is why it took so long for the heist to be detected.

Private owners have strong incentives to invest in effective cybersecurity. Owners are always better at protecting their own property than are third parties with less personally at stake. Proprietary information is the lifeblood of a company; loss of data hurts it competitively. Not only is there a loss of company information, but loss of customer information can bring civil penalties and lawsuits and long-term damage to customer trust.

The government, by contrast, has no such proprietary interest in protecting data. When millions of Social Security numbers were compromised because an employee lost a laptop,30 the government officials most responsible for the security gap faced no danger of financial loss or career setback. Since the government has a monopoly on certain services that require information collection (tax collection, benefits payments, drivers licensing, etc.) it doesn’t risk losing customers, business, or profits. All angry taxpayers can do is complain to their congressmen.

That’s why the government should be taking cybersecurity cues from the private sector, not creating mandates for the private sector to follow. The ground-up, best-practices approach of the


private sector is able to keep up with threats as they evolve. Private-sector companies already regularly exchange data on malware, viruses, and other cyberthreats. Companies such as Symantec and McAfee build their success on being able to provide up-to-the-minute software to deflect each new type of attack. No one is working in a vacuum. The overall focus is on detecting the latest new problem and devising a solution that works.

Government mandates, on the other hand, are poorly suited for dealing with rapidly changing threat scenarios. They take time to develop and are subject to the political process, which inherently involves caution and compromise. Instead of rapidly addressing a changing set of circumstances, the focus becomes a matter of pleasing as many parties as possible. The result tends to settle on the least common denominator – which itself creates problems because instead of incenting companies to do the best possible job at cybersecurity, mandated regulations allow them to get away with doing only what the law demands.

**Protect civil liberties and privacy.**

Since the nation’s founding, its most important organizing principle has been to maintain civil law and order within a structure of limited government powers and respect for individual rights. There is no reason this balance needs to be adjusted to favor state power at the expense of individual rights in combating computer crime or defending the nation’s information systems from foreign attack.

To ensure this balance, all cybersecurity legislation should contain language requiring the existence of a clear and present danger as a basis for requests for access to third-party information. There should be a way to expedite due process, as there is with search warrants and subpoenas, but this should be conducted through conventional state and federal courts. Foreign Intelligence Surveillance Act warrants, as the law’s name implies, should apply only to foreign intelligence threats. Government agencies should not be going to FISA to obtain secret warrants to spy on U.S. citizens.

No private company, entity, or individual should be coerced or pressured to turn over information without due process. Compliant parties should not be rewarded with funding, waivers, or special consideration for which noncompliant parties would be ineligible.

The government should be allowed to collect personally identifiable information only when demonstrably necessary, and access should be strictly limited. For example, data should be anonymized by default. The government should have to present a clear argument explaining why the information should not remain anonymous in any particular case. Collected data also should be subject to “time-to-live” limits – it should be erased or deleted after a certain period unless it


is clearly marked as evidence in a criminal case. Extensions to these time-to-live deadlines should be rare and subject to judicial review.

Government should respect the contract process. Private-sector companies should remain legally liable for any damages that result from a breach of personally identifiable data they have agreed to keep confidential. Likewise, citizens should have some form of legal redress if personally identifiable data are compromised or improperly used while in government care.

Conclusion

Threats to the nation’s cybersecurity are real, but none of the national government’s proposed responses – CISPA, the Cybersecurity Act, or the White House executive order – will be effective. They are too vague, duplicate or overlap with existing laws, and grant sweeping powers to the government to gather and process information on citizens without discrete limits that respect legal due process required by the Constitution.

Vaguely written computer crime laws give prosecutors too much discretion, as in the case of the Computer Fraud and Abuse Act being used against Internet entrepreneur and activist Aaron Swartz. When it comes to information-gathering, government tends to push the envelope on what the law permits, as seen by its use of the PATRIOT Act to conduct surveillance on millions of telephone customers.

Effective cybersecurity policy begins with the understanding that computer and data security is an extension of physical security, which traditionally has been the responsibility of the property owner. The government can be effective in apprehending and prosecuting criminals, but it’s not needed or competent to establish best practices for preventing most cybercrime.

Laws against cybercrime must target real wrongdoing and define specific actions that are illegal or proscribed. Various types of cybercrime already are illegal. Current legislation should be reviewed and, if necessary, amended before rushing to enact new laws. Any new cybersecurity law should specify limits and protocols on the collection of personally identifiable information, require anonymization by default, and incorporate provisions requiring timely deletion or disposal of data if they are not needed for a specific prosecution.

The threat of state-sponsored cyberattacks should be met through communication of clearly stated response options the United States will consider against an aggressor, with deterrence the principal aim, in addition to international diplomacy and cooperation with allies.

Cybersecurity is a dimension of domestic law enforcement and national defense. Time-proven strategies can be brought to bear in response. With rational thought and measured response, the security of the U.S. information infrastructure and assets can be maintained without granting vast new police, prosecutorial, and extrajudicial powers to the state.
About the Author

Steven Titch is a policy analyst at Reason Foundation focusing on telecommunications, the Internet, and information technology. He is also a policy advisor to The Heartland Institute. He served as managing editor of InfoTech & Telecom News, published by The Heartland Institute, and provides strategic market research and analysis as a private consultant. His columns have appeared in Investor’s Business Daily, Total Telecom, and America’s Network, among others.

Titch was co-founder and executive producer of Security Squared, a business-to-business Web publication covering IT convergence in physical security and surveillance. He also has written for the ISSA Journal, a publication of the International Systems Security Association, a global organization of IT security professionals. Previously, Titch was editor of Network-Centric Security and director of editorial projects for Data Communications magazine. He also has held the positions of editorial director of Telephony, editor of Global Telephony magazine, Midwest bureau chief of Communications Week, and associate editor-communications at Electronic News.

About The Heartland Institute

The Heartland Institute is a national nonprofit research and education organization. Founded in Chicago, Illinois in 1984, Heartland’s mission is to discover, develop, and promote free-market solutions to social and economic problems. Its activities are tax-exempt under Section 501(c)(3) of the Internal Revenue Code.

Heartland is headquartered in Chicago, Illinois and has a full-time staff of 31 and a 2013 budget of $6 million. It is supported by the voluntary contributions of approximately 8,000 supporters. For more information, please visit our Web site at www.heartland.org, call 312/377-4000, or write to The Heartland Institute, One South Wacker Drive #2740, Chicago, Illinois 60606.