Cyberspace & Security

Today, hostile nations, criminal groups, and individuals seek to exploit information networks to further a variety of individual, national, and ideological objectives. America's banks, energy sector, and intellectual property are routinely targeted by criminal hackers and foreign governments alike, and a successful attack on U.S. critical infrastructure would directly threaten American citizens' safety, the U.S. economy, and our way of life.

The threat is growing. As people become more dependent on technology, opportunities for crime, espionage, and physical disruption will increase exponentially. This trend will continue unless we are able to foster an environment where cybersecurity is the rule, not the exception.

What should we do?

We need to strengthen the security of our networks in ways that empower the owners of networks to prevent intrusions, give consumers and users confidence that their personal data is private and secure, and allow the

If you read only one thing

Cyber Threats

- America cannot be secure unless its networks are secure and resilient.
- We face cyber threats every day from foreign governments, non-government agents, and criminals.
- As our reliance on technology increases, so does our vulnerability.

Security & Privacy

- Privacy and security are not competing interests; we can do both.
- We should think strategically about the information the government collects and only collect what is necessary.
- Information must be stored, analyzed, and protected in ways that don't compromise its integrity.

government to ensure the integrity of its information while identifying and prosecuting cybercriminals when possible. This can only be done through carefully tailored legislative and executive action, and can only be successful with the buy-in of all relevant actors, most importantly the owners and users of networks.

Four "first principles" should guide all efforts to draft and implement a comprehensive cybersecurity strategy:

- **Cybersecurity enables privacy**—it protects individuals, companies, and governments from malicious intrusions. Today, some contend that greater security means ceding some degree of personal privacy, or vice versa. This is flawed logic. Privacy is security against unwanted intrusions or disturbances. In essence, privacy and cybersecurity not only work together—they are the same.

- **Cyberspace is a public space.** Ownership over the networks and content that make up cyberspace is decentralized and predominantly operated by non-government entities. It is an open, accessible, and user generated domain that grows constantly and organically. Policies to protect it, therefore, must be designed to match and preserve that distributed architecture.

- **Protecting cyberspace is a shared responsibility.** No single entity—whether public or private—has the capacity to secure a domain that extends beyond traditional geographic boundaries. In an era where one weak link in the chain can compromise the security of an entire system, all sectors have a role to play in contributing to common security. Cybersecurity requires coordination and cooperation between federal,

state, local, and private entities.

- **We can secure the networks without suppressing content.** By understanding the distinction between information networks and the content traveling over those networks, we can address the threats to the system while preserving individual privacy and freedom.

Key Issues

The privacy vs. security debate: You can have both. One aspect of privacy is the ability to communicate without third-party access to the contents of your transmission. On the Internet, that third-party might be a cyber-criminal, governments, or other hackers. For this reason, the most secure networks are those with the most robust cybersecurity. And those networks best enable privacy. Both users and the government have a vested interest in a more secure, private internet that protects confidential information and is resilient against malicious intrusions.

Cybersecurity requires partnership between the private and public sectors. The majority of America's critical infrastructure is privately owned and operated. This includes systems vital to the U.S. – everything from power grids to hospitals to financial institutions – whose disruption would have a debilitating effect on our society. The systems we depend on every day are more reliant than ever on networks, but they were often not designed with security in mind. It is important that we begin to protect our networks now.

What we can do

- Craft legislation to protect our critical infrastructure from cyber threats.
- Build a private-public partnership to share cyber threat information.
- Include strong protections for personal privacy.
- Increase our cyber human capital.
- Clarify lines of authority so we can effectively deter and respond to attacks and intrusions.
- Work with the international community so a miscalculation doesn't cause a conflict.
- View the creation of international law on cyber conflict as a source of opportunity to write the rules of the road, not a threat.

Cybersecurity is a weak link in our security. A global cyber arms race is already underway. It is estimated that more than two dozen countries possess a cyber war capability and even more are looking to establish similar capabilities. The head of the NSA's Information Assurance Directorate says countries are using cyber exploitations without "any sense of restraint." Imagine a nation launching a military attack on a U.S. ally while turning off the lights across the Atlantic seaboard, hindering U.S. response. That is just one potential cyber conflict scenario.

Hackers are targeting intellectual property (IP). Businesses today store their intellectual property in digital form, making them a target for industrial cyber espionage. Stolen IP damages American competitiveness and, over time, costs American jobs. Recently, U.S. intelligence officials publicly accused China of stealing American business secrets. Former Homeland Security Secretary Janet Napolitano estimated that the annual cost of global cyber crime is $114 billion.

Cybersecurity means protecting personal information as well as intellectual property and state secrets. With the development of smart phones, online banking, and other digital services, we are all becoming more dependent on computers. But greater connectivity means a greater "attack surface" for criminals to try to exploit. In 2012, 12 million American households had at least one person who was the victim of identity theft. Two-thirds of those victims had their credit card information stolen and misused. In 2012, the Justice Department reported that identity theft cost Americans $24.7B, while burglary, motor vehicle, and property theft combined only cost $14B. The increased risk that comes with the convenience of digital technology requires us to be more vigilant in protecting our data.

Key Fact

Critical infrastructure sectors include (but are not limited to):

- Banking & Finance
- Chemical production
- Communications
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water treatment & distribution

Attacks that target personal information can come from other sources with other motives, too. Malicious hackers recently targeted the personal computers of retired Admiral Mike Mullen, former Chairman of the Joint Chiefs of Staff, as a way to access sensitive information without having to break U.S. government security. The Wall Street Journal reported that the Mullen episode was just the latest in a series of incidents against "former senior U.S. officials."

Attribution in cyberspace is challenging. This is a tremendous benefit for democracy and human rights activists, journalists, and others who might be targeted by authoritarian governments or other bad actors around the world. But for efforts to fight cyber crime, prevent terror attacks, ensure data integrity and confidentiality, or conduct business in a networked environment, it is also an enormous challenge. If you catch someone red-handed attempting to break into a vault, you know who the culprit is. But if you catch someone attempting to steal money or information digitally, you might not know what country they are in, let alone who they are.

The lines of authority on cybersecurity within the federal government are not clear. The responsibility for protecting American networks and researching new technologies is spread across multiple agencies and congressional committees. The military is in charge of protecting the .mil domain and DHS is in charge of protecting .gov; however, no agency has a clear mandate to protect .com or .org, despite the fact that most of our critical infrastructure is a part of these domains. The Chairman of the Federal Energy Regulatory Commission recently said, "If I had a cyber threat that was revealed to me in a letter tomorrow, there is little I could do the next day to ensure that that threat was mitigated effectively by the utilities that were targeted." Because of

Key Fact

The Attribution Problem

One of the biggest challenges of cybersecurity is knowing who is behind an intrusion or attack. Unlike a conventional intelligence gathering or military activity, it is often much harder to prove who is behind a breach. This makes a cyber attack tempting tool to employ, and makes developing an appropriate response difficult. Improving our ability to track down the source of an intrusion and mitigating the effects on the targeted network will improve our deterrence capacity. A potential hacker is less likely to invest the time and resources to breach a network if they know they will be tracked down and the system will continue to operate effectively.

outdated legal authorities, the government is constrained in its ability to help companies protect their networks.

The Department of Defense is expanding its defensive and offensive capabilities. DoD suffers millions of probes each day by "malicious" cyber actors on its networks. In testimony before Congress, General Keith Alexander, Commander of U.S. Cyber Command, stated "modern forces cannot operate without reliable networks, [so] we will invest in advanced capabilities to defend them even in contested environments."

The Department of Defense is investing $3 billion per year to develop capabilities and conduct offensive operations consistent with U.S. principles and existing legal structure—including the law of armed conflict. DoD is also investing in human resources to develop and retain a skilled workforce.

Both international and domestic law affect cyberspace. International law is especially problematic because there is no treaty or agreed upon set of norms for how countries should conduct themselves in cyberspace. This lack of established law means that nations and non-government entities are able to harass and attack each other in cyberspace with few or no repercussions. The Russian Federation, one of the worst offenders in cyberspace, has attacked nearby nations on numerous occasions, while pretending the attacks come from "patriotic hackers" unaffiliated with the Russian military. This trend will only get worse and the U.S. has yet to push for a firm set of international norms.

Domestic law and American conduct within its own sovereign

> We can't let Russia and China use cyber crime as an excuse to limit Internet freedom.

territory have been continual challenges for lawmakers. As with international law, the body of domestic law is still "catching up" to technology. While the court systems struggle to adapt laws to modern contexts, law enforcement agencies are finding themselves deluged by the massive influx of cybercrime. This gap has helped contribute to cyber crime becoming the most profitable criminal enterprise both domestically and internationally.

Our domestic cybersecurity policy will have international human rights consequences. Due to of the global use of U.S. platforms like Google and Facebook, U.S. cybersecurity laws affect people outside of our borders. Other countries may also look to us to justify their own security policies. If the same policies we establish for network monitoring to prevent, for instance, child pornography, could be used by an authoritarian country to monitor political dissidents, we can assume they will cite our example to justify their programs. Individual freedom in the 21st century is closely tied to how we govern and use digital technology. And, while the internet can play a powerful role in increasing global human freedom, it can also be manipulated to suppress individual rights and personal privacy.

The Policy Landscape & Recommendations

Critical infrastructure owners should meet baseline security standards. Just as a fence is required around the perimeter of a nuclear

power plant, computer networks linked to critical infrastructure must be protected. America's national security leaders have repeatedly called for baseline security standards. The government should work with the private sector to develop a set of standards that are flexible enough to adapt to a changing threat environment and resilient enough to keep many would-be intruders out. One weak link in the chain is all an intruder needs to breach a network and potentially cause catastrophic damage.

The Obama Administration's Executive Order on cybersecurity was a good first step in terms of identifying best practices for critical infrastructure owners and operators. The next step is for the Administration and Congress to work with the private sector to ensure owners and operators of major private sector enterprises are incorporating best practices. When necessary, the government should provide incentives for business to do so.

Security standards must be flexible to adapt to evolving threats. Legislating a specific security measure would be counterproductive—it will be outdated by the time the legislation is passed. Instead, laws in this area should require the most critical networks to meet baseline standards for security. Those measures should be developed in partnership with private sector stakeholders and adoption should be incentivized. Implementation of those standards should also be technology-neutral in order to adapt to a nimble enemy and new technology.

Effectively fighting against cyber threats requires a national partnership to share information. If a business is hacked, sharing how it happened and who might be responsible helps other businesses and the government. This kind of information is vital to understanding current and developing threats and protecting networks against them.

> If regulations are too specific, they will stifle new & creative solutions to our security problems. But they are essential to keeping us safe.

But not all information sharing is alike. There are real concerns about who information is shared with, in what form, and what can be done with it. The private sector should be encouraged to share information with the federal government. This will allow for proper oversight and accountability—and will enable information to be shared across an industry. The federal government should also share threat information in a consumer-friendly way with the private sector and the public, so that businesses and individuals can improve resilience.

Limited liability protection must be offered to private entities

For private owners and operators to come forward with cyber threat information without fear of legal reprisal or damage to their reputation, they must be offered limited liability protection. This protection should be carefully crafted to incentivize sharing without weakening privacy, consumer, or anti-trust protections. It should also not be so broad as to allow companies to share user's private information, because faith in data privacy is critical to a successful networked economy.

Robust privacy protections must be built into all legislation. Any policy, whether legislative or executive, must clearly define the purposes for which shared information can be used. Information must also be handled extremely carefully in order to safeguard personal privacy and civil liberties. Sharing digital signatures is important for assessing the threat environment and improving security, but information should first be scrubbed of content that would identify individuals before it is shared.

Education and human capital investment are an essential and cost effective way to promote security. Cybersecurity is not just a technical problem. In a world where the most common network password is "123456," the person sitting at his or her desk remains the weakest link

Key Fact

Humans remain the weakest link in the security of most networks, so training and education are critical.

in the system. By increasing technology and security education at every level, we can improve security and competitiveness. This requires us to build a "culture of security": making sure individual users are part of the security solution, ensuring security is ingrained into the work of hardware and software manufacturers, and informing institutional investors and shareholders of the material risks of cyber theft to companies.

Improve private sector relations and cyber acquisition policy. Cybersecurity, as a field, is continuously evolving. Tomorrow's threats may look very different than today's. In this environment, it is critical that the U.S. government is able to work well with technological innovators to keep up with rapid developments. In addition, many of our defense procurement policies are too slow to keep up with changes.

Develop a unified national cyber strategy, and a group that can effectively oversee its implementation. There has been a great deal of effort in the last few decades to establish the vision of the US cyber strategy; however, as of today there has yet to be a clear and defined cyber strategy that properly unifies effort among the government's department and agencies, the private sector, and the international community. The current method of ensuring that the US government is abiding by the various visions and goals set forth by the Administration is through self-reporting – a technique that may work for less complex issues but has increasingly proven to be inadequate for the cross cutting and massive issues in the cyber realm. The Administration should draft a document that unifies its ten "sub" cyber strategy documents, establishes clear and measurable objectives and goals for the various departments and agencies, ensures that there is public sector buy-in for relevant sections, and creates an empowered agency or organization to oversee its implementation.

Continue to increase supply chain security. Our national security systems rely on parts that are manufactured all over the world. The proliferation of counterfeit parts threatens to adversely impact our military readiness. In 2011, Congress strengthened the inspection regime for imported electronic parts and ensured the U.S. government will not have to pay for counterfeit parts supplied by contractors. Congressional committees continued to investigate and report on supply chain threats in 2012. They should continue to provide oversight in this area.

Establish international norms on the use of the internet. In 2012, Russia, Iran, and China submitted draft rules to the United Nations on internet governance as part of an update to the 1988 Telecoms Treaty. Their draft favored greater censorship and state control over the internet. Western nations refused to sign, instead desiring a multi-stakeholder approach that enables governments, businesses, and NGOs to all have a role in internet governance. We should not allow countries like Russia, Iran, and China to twist cybersecurity arguments to make the internet more authoritarian, and less open.

Establish international security norms and eliminate cyber safe havens. Currently, there are no clear rules of international engagement for cyber warfare. As a result, a miscalculation could become a flashpoint, triggering a clash between countries. We need to establish cyber war norms and a better means for signaling intentions to potential opponents. We also need to build international law enforcement partnerships and frameworks to combat global cyber crime.

Key Players

The Private Sector. Cyber crime costs hundreds of billions of dollars each year. The private sector is the first line of defense, protecting its networks and intellectual property. Most critical infrastructure is also owned and operated by industry. U.S. companies need to be proactive in defending their networks.

The Department of Homeland Security. The civilian cabinet department responsible for domestic cybersecurity, including protection of the '.gov' domain.

The Department of Defense. The National Security Agency and U.S. Cyber Command play critical roles in defending the nation against cyber attacks. The NSA is responsible for designing the security systems that protect federal networks and collecting intelligence. DoD is in charge of protecting '.mil' domains and national security systems. The Department also develops offensive capabilities and is finalizing new rules of engagement for cyber operations.

The Department of State. The State Department is responsible for negotiating international frameworks through which governments can collaboratively fight cyber crime and cyber terror.

The Federal Bureau of Investigation. The FBI is responsible for investigating cyber incidents domestically and conducting forensics and counterintelligence.

In 30 seconds...

Recommendations of the House Cybersecurity Task Force

- Adopt incentives to encourage private companies to improve security.
- Consider carefully targeted critical infrastructure regulations.
- Create a third-party clearinghouse to facilitate information sharing between public and private sectors.
- Establish legal protections for sharing information.
- Update existing cyber laws to reflect changes in technology.
- Clarify legal authorities to allow for more effective national protection.

The Department of Commerce. The National Institute for Standards and Technology (NIST) within Commerce works with the private sector to establish a cybersecurity framework.

Key Terms

Cyberspace. The domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures.

Cyber attack. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber intrusion. An incident of unauthorized access to data or an automated information system.

Cyber exploitation. Stealing information that would otherwise be kept confidential and is resident on or transiting through a computer system or network.

Malware. A software program that is designed to exploit or damage a computer system.

Virus. A malicious program or a piece of code that is loaded on to a computer server through the internet or copied from a disk, storage device, or another computer.

Worm. A type of virus that replicates itself and travels to other computer hosts without human assistance.

Spear-phishing. Targeted emails that trick users into giving up their user names and passwords.

Trojan horse. A program that is hidden within another, benign program and used to gain access to a computer or network. Once accepted, it can damage or allow a third party to take over the network remotely.

Denial-of-service attack. One of the oldest and most common types of cyber attacks. Denial-of-service attacks are designed to overload the target and disrupt its operations.

Logic bomb. A program that lies dormant until triggered by a specific event—such as a date or time—and then activates, disrupting or damaging the system.

Zero-day exploit. An attack that exploits a security hole before the vulnerability is known. The attack occurs on "day zero", before the developer is aware of the hole, leaving the developer no time to prepare a patch or fix for the problem.

Botnet. A group of computers that has been infected by malicious software and is controlled remotely.

Encryption. The act of encoding a message so that only authorized entities can access the message content.

Man-in-the-middle attack. A method of intercepting messages between two entities by pretending to be an authorized recipient of passed information.

Going Deep: Background & Context

The genie is out of the bottle on cyber attacks. State-on-state cyber attacks have now been publicized, which could lead to a proliferation of events. However, there are no mutually agreed upon rules to govern when an attack is appropriate. Until we agree on these principles, attacks may be used more frequently. For example, beginning in the Bush administration and accelerating during the Obama administration, Israel and the U.S. worked together to develop and implement a worm to disrupt and damage Iran's nuclear program. Originally introduced through a thumb drive (Iran's Natanz nuclear facility has no connections to the Internet), the worm caused nuclear centrifuges to spin out of control and sometimes self-destruct. For a time, Iran believed this was caused by an error on the part of Iranian engineers. The Stuxnet worm escaped, though, and became public in 2010 when an Iranian engineer connected his laptop to the Natanz facility and later reconnected with the Internet.

Edward Snowden's disclosers sparked a nationwide debate over the government's monitoring of internet and phone traffic for national security purposes. In May 2013, Snowden, an American contractor at the National Security Agency, leaked millions of highly classified documents that revealed an extensive global surveillance program, purportedly used by the U.S. for counterterrorism purposes. The Snowden leaks continue to directly influence the conversation about how to balance privacy and security in an era of rapidly evolving technology.

Several countries are employing offensive cyber capabilities to breach U.S. corporate and military systems. Businesses lose between $6 and $20 billion each year because of cyber theft. In January 2014, White House Cyber Security Coordinator Michael Daniel warned that, "[Security] compromises are becoming inevitable…Companies need to build [cybersecurity and the risk of cyber espionage] into their business plans."

A bipartisan group of senators began writing legislation in 2008 and it was brought to a vote in the Senate in 2012. The Chamber of Commerce opposed the bill—which included voluntary security standards for industry—arguing "a light touch can become very prescriptive." The bill failed in the Senate when the minority argued they were not being given the opportunity to offer amendments to the bill—even though their amendments included a repeal of health care legislation.

In 2013, the House of Representatives passed a bill focused only on information sharing. Business groups pushed back against comprehensive proposals and the House pursued a narrower bill. Privacy

groups and the Obama Administration, however, advocated against it on the grounds that it allowed personal information to be shared with the government without sufficiently limiting its use.

After Congress failed to act, the President signed an Executive Order to improve U.S. cybersecurity. In his 2013 State of the Union, President Obama announced an Executive Order instructing the Federal government to explore ways, within existing authorities, to share cyber threat information with private entities and develop—in consultation with the private sector—cybersecurity best practices for U.S. critical infrastructure. All of this should be done, as mandated in the 2013 Executive Order, with "senior agency officials for privacy and civil liberties" to ensure that we do not erode individual rights in the name of security. In February 2014, the Executive Order framework was released, announcing a voluntary program of best practices that private entities can incorporate at their own discretion.

In March 2014, the U.S. Department of Commerce announced a plan to make the Internet Corporation for Assigned Names and Numbers (ICANN) a fully independent body. ICANN has served as the contractor responsible for managing the system of numbers and names that computers use to find each other on the internet. By making ICANN fully independent, the Commerce Department will ensure that the internet continues to be administrated by a multi-stakeholder, non-governmental body. This transition will weaken support for attempts by other countries to exert greater state control over the internet, like the 2012 effort by Russia, Iran, and China to put internet governance under the authority of the United Nations. Far from giving up U.S. control of the internet, as some pundits have suggested, making ICANN fully independent preserves the free nature of the internet, and heads off

further attempts by authoritarian regimes to establish state dominance over the internet within national borders.