Updated: **July, 2022**

Cybersecurity

Summary and Key Talking Points

Policy Proposals

1. Articulate a detailed, bold strategy for deterring and retaliating against cyber aggressors.

2. Continue to invest in U.S. Cyber Command (USCYBERCOM), expand collaboration on cybercrime, and prepare to operate and thrive in zero-trust networks.

3. Reexamine Cybersecurity and Infrastructure Security Agency (CISA), FBI, and USCYBERCOM authorities to ensure that they have all they need to approach our cyber challenges aggressively.

4. Clearly communicate standards that must be met for inclusion in U.S. markets and block foreign technology that creates vulnerabilities in U.S. infrastructure.

Quick Facts

1. Ransomware attacks are going to cost the world approximately $20 billion in 2021—57 times more than the $325 million they cost in 2015.

2. The world will have 3.5 million unfilled cybersecurity jobs by the end of 2021.

3. Health care, information technology, and manufacturing are the top three sectors targeted by hackers.

Power Phrases

Threats the U.S. Faces

- The signs are clear: Cyber warfare is the latest battleground for nations like Russia, China, and, increasingly, non-state actors such as cyber-criminal syndicates.

- The U.S. must prepare for significant cybersecurity threats that jeopardize America's critical infrastructure, business, and online freedom.

Increase Cyber Efforts

- U.S. cybersecurity will ultimately be led by the private sector, which faces the majority of cyber-attacks, and will create solutions.

- The government should support private sector efforts, while leading on issues of foreign policy.

- Cyberspace's dynamic nature must be acknowledged and addressed by policies that are equally dynamic.

The Issue

Nation-state hackers are the most serious cybersecurity challenge the U.S. faces, and Russia and China present the most sophisticated of these cyber threats. In an era of renewed great-power competition, cyber is a new battlefield on which some nation-states are seeking to exploit other nation-states' vulnerabilities. The U.S. has indicted Russians for their efforts to hack such U.S. political entities as the Democratic National Committee. Russian hackers are also believed to be behind multiple cyberattacks that took down portions of Ukraine's electric grid in 2015. Russian intelligence was behind the SolarWinds espionage campaign against U.S. computer networks, compromising the data of the U.S. Departments of Commerce, Treasury, and Homeland Security as well as several *Fortune* 500 companies in one of the largest cyberattacks ever reported.

China has used the theft of commercial intellectual property across many sectors of the economy to jump-start its own economic efforts. For example, Chinese hackers have targeted sensitive cancer research at multiple institutes in the U.S. in addition to other attacks aimed at U.S. intellectual property. Chinese actors have also been identified as being responsible for the Hafnium Microsoft Exchange cyberattacks in 2021. According to FBI Director Christopher Wray, "The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China."

Iran and North Korea are less sophisticated than Russia and China, but they have strong cyber warfare assets that allow them to punch above their geopolitical weight class. The 2012 so-called Shamoon virus unleashed on the Saudi Aramco oil production company, for instance, was a brute-force attack by Iran that destroyed 30,000 computers. In 2019, Iranian hackers continued to target hundreds of universities around the world, including some in the U.S., in an operation named Cobalt Dickens that was designed to steal intellectual property. In October 2021, a group with ties to Iran attempted to hack more than 250 Office 365 accounts. All the targeted accounts were U.S. and Israeli defense technology companies, had a focus on Persian Gulf ports of entry, or were maritime transportation companies with a presence in the Middle East.

North Korea has conducted high-profile cyberattacks against the U.S., the most notable being the attack launched against Sony Entertainment in 2014, allegedly over a movie depicting North Korea in a negative light. The hackers took terabytes of private data and released confidential information, including five undistributed Sony movies, to the public. In 2019, North Korean hackers were suspected of attempting to steal credential information of individuals working on North Korean issues at the United Nations and non-governmental organizations. The regime's cyber guerrilla warfare has stolen classified military secrets, engaged in cyberterrorism, absconded with billions of dollars in money and cybercurrency, held computer systems hostage, and inflicted extensive damage on computer networks.

In addition to these nation-states, cyber criminals, hacktivists, and terrorists all seek to use cyberspace for their own ends. To address these growing threats, the U.S. should leverage the forces of the market and motivate the private sector to make the sort of continual and dynamic investment that is needed to secure the country's diverse cyber networks.

Recommendations

Create a new, bolder strategy for U.S. global efforts in cyberspace. From deterring and retaliating against cyber aggressors to working with allies to reinforce our defenses against cybercrime, the U.S. should craft a new, detailed strategy that directs whole-of-government efforts to protect U.S. interests in cyberspace. This strategy must also take account of the central role the private sector plays and make use of its expertise and skills.

Develop a robust deterrence policy that tailors a proportionate U.S. response to bad actors. Deterrence is in the mind of the adversary, who chooses to alter his behavior if he believes the costs are too high or the benefits are too small. To achieve deterrence in cyberspace, the U.S. must establish a clear pattern of policy and action that leads an actor to rethink his plans. The U.S. has a variety of tools that it can use to retaliate against any sort of cyber aggression: diplomatic naming and shaming, cutting off cooperation, visa restrictions, commercial and financial limitations, sanctions, legal action, trade enforcement tools, action on other military or foreign policy matters, support to dissidents in malicious cyber states, and others that are not considered here. These tools should be used in a way that is tailored to fit the adversary and proportionate to the scale and effects of his aggressive action.

Increase cooperation with allies and partners. Many cyberattacks and incidents cannot be punished, and we may need stronger defenses and cooperation to defeat or mitigate them. The U.S. should therefore pursue deeper technical, legal, and policy cooperation with its allies and partners.

Prepare, along with allies, to fight in the cyber domain. The U.S. and its allies need to develop the tools and capabilities needed to fight in the cyber domain. NATO has taken some steps in this direction, but far more needs to be done. Any future conflict will require offensive and defensive cyber capabilities that are well integrated into U.S. and allied warfighting strategies. Creating such capabilities requires the political will to engage in this new domain as well as the resources to develop the means of engagement.

Require mandatory notification of cyber breaches. Congress can clarify the private sector's responsibilities in the field of cybersecurity by enacting a single requirement to disclose breaches of cybersecurity to the federal government. Any legislation should provide incentives for companies to report hacks when there is still time for the government to help. A federal requirement for disclosure of cybersecurity incidents would be a first step in the improvement of cybersecurity defense.

Share threat information with industry. U.S. government concerns about Chinese technologies and related services cannot be expressed exclusively in classified or other constrained environments. If the U.S. government wants industry to operate in ways that do not provoke or worsen national security concerns, the government must share its telecommunications security concerns in a detailed and easily disseminated manner.

Determine disqualifying factors. The U.S. government should communicate clearly to industry and to America's foreign partners and allies—as well as to the Chinese—exactly which legal frameworks, activities, and business practices will result in exclusion from U.S. 5G infrastructure, services, and other emerging technology integrations. The U.S. also should encourage other nations to adopt these standards as a way to maintain pressure on countries and companies that are working against U.S. and allied interests.

Block vulnerabilities. The U.S. should block any foreign technology from U.S. markets that creates vulnerabilities in critical infrastructure or gives hostile foreign actors "backdoors" to U.S. data. This would put significant pressure on China and others to improve poor security practices. It also would encourage domestic security research in the U.S. that would incrementally improve the safety of the hardware used by the United States as well as the software supply chains into the U.S. The U.S. should encourage the remaining four Five Eyes countries—Australia, Canada, New Zealand, and the United Kingdom—to implement similar exclusionary measures.

Block untrusted companies. The Committee on Foreign Investment in the United States should block foreign companies from U.S. investments if they have a history of producing hardware or software with known vulnerabilities. This would be especially helpful in mitigating the challenge of Chinese investment in and purchase of American start-ups that might embrace poor security practices in return for rapid access to capital.

Prepare for zero-trust networks. Huawei controls approximately 30 percent of the global mobile communications market and could win as much as 50 percent of the global 5G market. Even if the U.S. manages to secure its own wireless networks from foreign spying and interference, the vast majority of networks around the world will be developed and managed by the Chinese. The U.S. defense and intelligence communities must begin to mitigate this threat and develop new networking strategies that will allow the U.S. to operate and thrive in a zero-trust environment on networks that are owned and managed by China or other hostile actors. While it is too soon to cede 5G to challengers, beginning to prepare for worst-case scenarios is only prudent.

Continue to invest in U.S. Cyber Command. Both to strengthen the ability of the U.S. to engage in cyber warfare and to protect Defense Department and critical infrastructure networks, USCYBERCOM should continue to grow and mature into a premier cyberwarfare organization to enhance U.S. offensive and defensive cyber capabilities. These capabilities are important for increasing our ability to deter adversaries.

Give USCYBERCOM additional statutory authority. Congress should clarify that U.S. Cyber Command's authority under the fiscal year (FY) 2019 National Defense Authorization Act goes beyond election interference and extend USCYBERCOM's statutory authorization to include a wide range of cyber operations that can deter or degrade the ability of adversaries to attack critical U.S. infrastructure. Although the President has constitutional authority to carry out offensive cyber operations, additional statutory authority would send a clear signal to allies and adversaries alike that there is political support for offensive cyber operations.

Continue to delegate authority to operating agencies. Instead of restoring the Obama Administration's paralysis by analysis, President Biden and his National Security Council should retain the Trump Administration's approach and drive operating agencies to establish deterrence below the threshold of armed conflict. Siloed infighting among competing agencies and discussions of intelligence-collection gains and loss analysis should not be allowed to dominate consideration of proper and necessary responses. Policymakers should be clear-eyed with respect to the time, resources, and potential loss of technical capability that are needed to plan and execute offensive cyber operations as well as the level of their impact and the time it may take for an adversary to reconstitute. This framework should rely on metrics that enable the proper evaluation of risk and reward as well as the effect of actions and their long-term impacts.

Identify additional domestic law enforcement authorities and capabilities. The Department of Justice, including the Federal Bureau of Investigation, should review additional capabilities or authorities that may be needed to target and disrupt known ransomware and, when possible, recover illicit gains from criminals' financial networks.

Consider ending the "dual-hat" relationship between the National Security Agency and USCYBERCOM. Currently, the NSA director is a four-star military officer who also serves as commander of USCYBERCOM. Initially, USCYBERCOM relied on the NSA for its capabilities, but President Trump elevated USCYBERCOM to an independent unified command in 2018, and the committee-passed Intelligence Authorization Act for Fiscal Year 2022 sets a road map for termination of the dual-hat arrangement. Congress should continue its oversight efforts while working with the Administration, NSA, and USCYBERCOM to evaluate whether this relationship should be ended. The dual-hat role is an enormous job for any one person, and separating the two organizations would help to prevent intelligence gain-loss considerations from dominating discussions of offensive cyber operations (although it might also lead to overlapping capabilities). In addition, if the dual-hat arrangement were ended, the director of the NSA—like the directors of the National Geospatial-Intelligence Agency and the National Reconnaissance Office—could be a civilian official.

Deepen collaboration on cybercrime among like-minded nations. The U.S. should look to create an acceptance for active cyber defenses that are not harmful and allow better attribution of and intelligence on cyber threats. Laws and tools from the organized crime arena, such as the Racketeer Influenced and Corrupt Organizations Act (RICO), should be expanded to cover transnational criminal organizations involved in cybercrime.

Expand cybercrime cooperation beyond current signatories of the Budapest Convention. The U.S. should create a cyber forum of the Financial Action Task Force (FATF) that combats money laundering and the financing of terrorism. While they need not abide by all terms of the Budapest Convention, non-signatory countries should still be encouraged to take reasonable actions against cybercrime. Nations that do not assist in international cybercrime investigations or that do little to stop cybercrime within their territories should be considered non-cooperative and face repercussions from members of the new cyber task force.

Encourage the private development of cybersecurity supply chain ratings and accreditation. Such a framework would contain different tiers or ratings for different levels of accreditation, ranging from minimal overview of a company's supply chain to in-depth analysis of specific products' supply chains. Consumers would find the additional information provided by these various levels of accreditation helpful when making risk-based decisions, and producers would find such accreditation valuable for sales, thus connecting security and a profit incentive. Instead of mandating cybersecurity solutions, the U.S. government should collaborate with the private sector. One way to encourage the adoption of this system would be to require government agencies that deal with large amounts of sensitive data or that have security-related duties to purchase technology only from organizations that are accredited by this ratings system.

Improve sensitive government and military cyber supply chain procedures. U.S. Government Accountability Office (GAO) reports and news accounts indicate that the government needs to improve its supply chain procedures for technology products. Such improvements should include the requirement that no technology for use in U.S. national security systems may be purchased from Chinese companies. Additionally, government agencies should be required to consider supply chain ratings when adding technology goods to their acquisition processes.

Enhance cyber resilience. Relevant agencies should consider using hardware that monitors itself for hardware attacks and other redundancies in critical government systems. Though such hardware is likely to be more expensive, this premium would help the U.S. to protect its most important systems. Agencies with systems that are less sensitive should consider expanding cloud computing to gain access to rapidly scalable and available computer resources as a way to enhance resilience and continuity of operations at low cost.

Facts + Figures

FACT: Cyberattacks and espionage are costly both for the U.S. and for the global economy.

- Estimated global losses from cybercrime were just under $1 trillion for 2020, and the COVID pandemic provided new opportunities for cyberattacks.
- The top three targets for hackers from 2019–2020 were health care, manufacturing, and information technology.
- Multiple firms project that by 2020, 30 billion devices will be connected to the "Internet of things," a huge growth in devices that connect more and more of our daily life to the World Wide Web.
- The cyber-insurance industry is already estimated to be worth well over $3 billion and will provide a market mechanism for quantifying cyber risks and encouraging companies to improve their security.

FACT: China, Iran, North Korea, Russia, and hacking groups working with these countries continually attack U.S. economic interests and critical infrastructure. The United States must implement an all-tools-of-national-power approach to dealing with these bad actors.

- In March 2021, China targeted Microsoft's exchange server software, causing a massive worldwide cyber breach exposure.

- In 2020, hackers linked to Russia's Foreign Intelligence Service used a SolarWinds update to install malicious software that allowed hackers to gain access to accounts across multiple U.S. Cabinet agencies.
- The U.S. Department of Justice indicted three North Korean hackers for conspiring to steal and extort more than $1.3 billion in cash and cryptocurrencies.
- Facebook revealed that it has tracked and at least partially disrupted a long-running Iranian hacking campaign that used Facebook accounts to pose as military recruiters, reeling in U.S. targets with convincing social engineering schemes before sending them malware-infected files or tricking them into submitting sensitive credentials to phishing sites.
- According to Verizon's most recent *Data Breach Investigations Report*, cyber espionage against government networks is up 168 percent in year-over-year data breaches; 79 percent of the external hacks are by state-affiliated hackers.

Additional Resources

Dustin Carmack and Michael Ellis, "For Cybersecurity, the Best Defense Is a Good Offense," Heritage Foundation *Backgrounder* No. 3670, November 10, 2021.

Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat," Heritage Foundation *Special Report* No. 247, September 2, 2021.

James Di Pane, "Cybersecurity: Policymakers Need a Consistent Means to Assess Capabilities," Heritage Foundation *Backgrounder* No. 3651, August 25, 2021.

Dustin Carmack, "Biden Administration Needs to Take the Kid Gloves Off When Reacting to China's Cyberattacks," Heritage Foundation *Commentary*, July 21, 2021.

Dustin Carmack, "U.S. Response to Cyberattacks? It Must Be More Than Just Biden's 'Off Limits' List," Heritage Foundation *Commentary*, July 9, 2021.

Dustin Carmack, "Fighting Back Against Cyber Attackers," Heritage Foundation *Commentary*, June 18, 2021.

Michael Ellis, "Time for a National Cyber Incident Disclosure Requirement," Heritage Foundation *Issue Brief* No. 6081, May 20, 2021.

Dustin Carmack and Chad F. Wolf, "How to Strengthen America's Cyberdefenses," Heritage Foundation *Commentary*, March 18, 2021.

James Di Pane, "Should Cyber Command and the NSA Have Separate Leadership? How to Decide," Heritage Foundation *Backgrounder* No. 3403, May 2, 2019.

Riley Walters, "Federal Cyber Breaches in 2017," Heritage Foundation *Issue Brief* No. 4804, January 3, 2018.

Riley Walters, "Private Sector Cyber Incidents in 2017," Heritage Foundation *Issue Brief* No. 4803, January 3, 2018.

David Inserra, "Cybersecurity Beyond U.S. Borders: Engaging Allies and Deterring Aggressors in Cyberspace," Heritage Foundation *Backgrounder* No. 3223, July 14, 2017.

Paul Rosenzweig, Steven P. Bucci, and David Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense," Heritage Foundation *Backgrounder* No. 3188, May 5, 2017.

David Inserra, James Jay Carafano, Charles D. Stimson, Steven P. Bucci, David Shedd, and Paul Rosenzweig, "Encryption Commission: Making Sense of Critical Policy Options," Heritage Foundation *Issue Brief* No. 4531, March 18, 2016.

Steven P. Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, March 28, 2013.

James L. Gattuso, "Ensuring Cybersecurity: More Red Tape Is Not the Answer," Heritage Foundation *Issue Brief* No. 3626, June 5, 2012.