The Heritage Foundation

CONGRESSIONAL TESTIMONY

EXAMINING ONGOING CYBERSECURITY THREATS WITHIN THE DEPARTMENT OF THE INTERIOR AND THE NEXUS TO STATE-SPONSORED CYBER ACTORS

Testimony Before
Oversight and Investigations Subcommittee of the Committee on Natural Resources

United States House of Representatives

June 7, 2023

Brian J. Cavanaugh
Visiting Fellow for Cybersecurity, Intelligence, and Homeland Security
The Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy
The Heritage Foundation

My name is Brian Cavanaugh. I am a Visiting Fellow for Cybersecurity, Intelligence, and Homeland Security at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Chairman Gosar, Ranking Member Stansbury, and distinguished Members of the Subcommittee:

In today's digital era, where technology pervades every aspect of our lives, the critical importance of cybersecurity for federal departments and agencies cannot be overstated. As our government increasingly relies on interconnected systems, cloud computing, and data-driven decision-making, the very fabric of our national security, economic stability, and public trust hangs in the balance. The threats we face in cyberspace are relentless, sophisticated, and pervasive, posing a significant challenge to the integrity and resilience of our nation.

Cybersecurity is no longer a mere accessory or an afterthought; it is the cornerstone on which the functioning of our government rests. Federal departments and agencies store and handle vast amounts of sensitive and classified information, ranging from critical infrastructure blueprints and defense strategies to personal records and financial data. Any breach or compromise in these systems can have catastrophic consequences, undermining our national security, eroding public confidence, and jeopardizing the very foundations of our democracy.

The interconnectedness of our digital infrastructure means that a single vulnerability can ripple across multiple agencies, putting not only individual departments at risk but the entire government apparatus as well. The consequences extend beyond bureaucratic headaches; they can disrupt essential services, compromise emergency response systems, bring a halt to the economy, and undermine the trust citizens have placed in their government to protect their interests. The threats we face transcend borders and adversaries, requiring a unified and robust approach to fortify our cyber defenses.

Threat Landscape

The landscape of cyber threats is ever evolving, with adversaries constantly honing their tactics and exploiting vulnerabilities. Nation-states, organized crime syndicates, and even lone actors seek to breach our defenses, steal sensitive information, manipulate data, and wreak havoc on our systems. The realm of cybersecurity demands constant vigilance, adaptability, and a proactive stance to anticipate, detect, and respond to these threats in real time. We cannot afford to be reactive; we must be several steps ahead, pre-empting attacks and safeguarding our digital assets with an unwavering commitment.

The People's Republic of China (PRC) is an adversary of the United States. After a decades-long engagement strategy toward China, we find ourselves embroiled in a New Cold War with an even more capable adversary than the Soviet Union. The threat posed by China to U.S. infrastructure in terms of cyber is significant and complex. The Office of the Director of National Intelligence assesses China currently represents the broadest, most active, and persistent cyber espionage threat to the U.S. government and private-sector networks.

China has long been recognized as a major player in the realm of cyber espionage, and its capabilities and activities continue to evolve and expand. The Chinese government and affiliated entities have been attributed to a wide range of cyber activities, including intellectual property theft, espionage, and targeting critical infrastructure sectors. China's cyber operations pose a serious concern to U.S. infrastructure due to several factors.

First, China has demonstrated a high level of sophistication in its cyber capabilities, employing advanced techniques and tools to breach networks, infiltrate systems, and exfiltrate sensitive data. Their focus on intelligence gathering, particularly related to economic and technological advancements, underscores the potential for significant economic and national security consequences.

Secondly, China's large-scale and persistent cyber campaigns are a cause for alarm. They have been accused of engaging in long-term, strategic cyber operations, targeting a variety of sectors, including government agencies, defense contractors, technology companies, and energy infrastructure. Most recently, Volt Typhoon, a PRC-sponsored hacking group, has been targeting the communications, manufacturing, utility, transportation, construction, maritime, government, information technology and education sectors in the U.S. The breadth and persistence of these campaigns demonstrate a sustained commitment to cyber operations, posing a persistent and evolving threat.

Moreover, China's ability to leverage its vast resources, both in terms of technology and human capital, enhances its cyber capabilities. The country possesses a highly skilled cyber workforce, often supported by state-sponsored initiatives, and has invested heavily in research and development to develop advanced cyber tools and techniques. This combination of talent, resources, and strategic focus amplifies the potential impact of their cyber operations on U.S. infrastructure, especially as the U.S. and China lurch towards an impending conflict over Taiwan and Chairman Xi's vision for a new world order.

While the Office of the Director for National Intelligence noted Russia's cyber operations during the Ukraine war fell short of the pace and impact they had expected, Russia continues to pose cyber threats to the U.S. Putin is particularly focused on improving Russia's ability to target critical infrastructure, including underwater cables and operational technologies. It appears that Russia's belief in demonstrating the ability to compromise such infrastructure during a crisis achieves the goal of influencing foreign policy outcomes.

Iran has demonstrated a willingness to conduct aggressive cyber operations on critical infrastructure, such as water treatment facilities, and their expertise is improving at an alarming pace. While their approach to cyberattacks remains opportunistic, it does not diminish the susceptibility of U.S. critical infrastructure owners, particularly as Tehran believes it must prove to itself that they can push back against the West.

Cyber operations from North Korea have matured and are capable of causing temporary, limited disruptions of some critical infrastructure networks and disrupting business networks in the U.S. The North Korean cyber program emphasizes cybercrime, focusing on financially motivated cyber operations, such as conducting cryptocurrency heists—with on such heist obtaining $625 million. However, cyber actors linked to North Korea have conducted espionage efforts against a range of organizations and continue to focus on cyber espionage geared towards advancing Pyongyang's military programs.

Another threat that often goes unmentioned is transnational organized criminals whose ransomware attacks continue to execute high-impact ransomware attacks, extorting funds, disrupting critical services, and exposing sensitive data. Critical infrastructure such as health care, schools, emergency services, and manufacturing continue to experience attacks aimed at disrupting services. The cost of ransomware attacks is taking its toll on insurance markets, price increases and a hesitation of new insurance carriers in the market are systemic of an out-of-control problem set.

What Is at Risk

The growing trend of digital transformation within federal departments and agencies brings immense benefits but also amplifies the risks. The adoption of emerging technologies such as artificial intelligence, Internet of Things, and cloud computing introduces new attack surfaces and vulnerabilities that must be addressed with utmost urgency. For its part, the Department of the Interior (DOI) houses enormous amounts of data on its digital infrastructure. Whether it relates to sustaining the health and productivity of public lands, the development of U.S. Outer Continental Shelf energy and mineral resources, or enhancing the quality of life of American Indians, Indian tribes, and Alaska Natives, the DOI must safeguard the data, resources, and infrastructure it utilizes to deliver its mission.

As noted in a recent Office of Inspector General (OIG) report, lackadaisical policies and procedures enabled the OIG to hack 21 percent of active user passwords at the DOI using basic and inexpensive means. Of the 18,000-plus accounts hacked, 362 accounts were senior U.S. government employees and 288 accounts had elevated privileges. Identifying and authenticating users is a fundamental security control. The OIG was able to demonstrate that the front door to the DOI has been left unlocked by its employees.

With over 1,600 structures on the outer continental shelf (OCS) responsible for a significant portion of U.S. domestic oil and gas production and at least 187 offshore wind farms currently being developed for energy production, the Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE) must proactively address cybersecurity risks. Modern exploration and production methods are increasingly reliant on remotely connected operational technology, a known vulnerability for cyberattack. A successful cyberattack on offshore energy infrastructure could cause physical, environmental, and economic harm. The effects of a cyberattack could resemble those that occurred in the 2010 Deepwater Horizon disaster or cause market-moving disruptions to energy production or transmission.

In the context of cybersecurity, the interconnected dependencies of critical infrastructure mean that a breach or compromise in one sector can have far-reaching consequences across multiple sectors. The ripple effect of such an attack can cause widespread disruption, economic losses, and potentially endanger public safety. The risk of interconnected dependencies lies in the fact that critical infrastructure sectors are often interdependent and share common underlying systems and technologies. This means that a vulnerability or compromise in one sector can be exploited to gain unauthorized access or disrupt operations in another sector. For instance, a successful cyberattack on a Bureau of Land Management system could potentially impact the operations of a U.S. Geological Survey system or even a Department of Commerce system.

Flaw in Current Approach

The U.S. government's approach to cybersecurity has its flaws, from a lack of prioritization and chasing trends and buzzwords, to its approach to the private sector and its soft response to U.S. government employees entrusted with access to systems and data. Addressing these four areas would represent a marked improvement for the government sector of critical infrastructure.

The lack of prioritization of risk within the U.S. government is a significant hindrance to its efforts in cybersecurity. Effective cybersecurity requires a strategic and risk-based approach, where resources and efforts are allocated based on the level of risk posed by various threats and vulnerabilities. However, when risk is not adequately prioritized, several detrimental consequences arise: resource allocation inefficiency, a reactive approach to threats, inadequate risk assessments, misallocation of efforts, and a lack of accountability.

To overcome these challenges, it is crucial for the U.S. government to prioritize risk as a fundamental component of its cybersecurity strategy. This requires a comprehensive understanding of the threat landscape, thorough risk assessments, and the establishment of clear priorities based on potential impacts and likelihood of occurrence. By prioritizing risk, the government can allocate resources effectively, adopt a proactive approach, and ensure accountability in its cybersecurity efforts, ultimately strengthening the resilience of its systems and protecting national interests.

One sign that the government is misallocating efforts is its willingness to chase after cybersecurity buzzwords or new trends. While it is no secret that technology is rapidly developing and evolving, this does not mean that the U.S. government can erratically chase after the shiny object. Instead, the U.S.

government should find ways to close the detection gap, something alluded to by the IBM Security Cost of a Data Breach Report 2022. According to the report, the average time to identify and contain a data breach is 287 days, with malware being undetected for an average of 180 days on systems.

The U.S. government's model for addressing cybersecurity is a flat-footed and clumsy approach that keeps them in a constant state of response and recovery—awaiting alerts from the private sector and then managing messaging. Instead of waiting for the private sector to decide to share information, the U.S. government must become forward leaning, and take meaningful steps toward addressing the risk and mitigating cyber threats to our critical infrastructure. This includes engaging with small businesses and start-ups that are driving innovation in cybersecurity. Procurement practices must evolve and foster innovation, especially in the tech sector. Flexibility in requirements, streamlined and agile procurement-process adoption, and incorporation of pilot programs and testbeds would be a great start.

The risk of interconnected dependencies within critical infrastructure highlights the urgent need for robust cybersecurity measures, including personal accountability. From a repercussion perspective, we all have a role to play in vigilance, and just like how resilience starts with the individual, so, too, does the responsibility of cybersecurity. The U.S. government needs to take a firm stance on accountability at the employee level. U.S. government employees are central, important, and have immense power. With that must come responsibility—with the expectation that they become lead adopters in proven security methods. Cyber and information technology policies need to be treated as seriously as those regarding the unauthorized disclosure of sensitive information.

A More Resilient Future

To address the threat posed by China and other cyber adversaries, the U.S. government must take proactive measures to enhance cybersecurity efforts. We must strike a delicate balance between harnessing the power of innovation and securing our digital infrastructure, employing robust encryption, multi-factor authentication, and comprehensive threat intelligence to counter the evolving threat landscape. Moreover, to address the critical importance of cybersecurity for federal departments and agencies, we must prioritize infrastructure by risk, focusing on closing the detection gap and strengthening personal accountability.

Investing in research and development of innovative cybersecurity technologies and techniques is crucial to stay ahead of evolving threats. This includes leveraging technologies such as artificial intelligence, machine learning, and behavioral analytics to detect and respond to cyber threats in real time. While investing in cutting-edge technologies and cultivating a highly skilled cybersecurity workforce, we must promote a culture of cybersecurity awareness and resilience at all levels of government.

Robust cybersecurity practices, threat intelligence sharing, investment in defense technologies, and collaboration with international partners are vital components of a comprehensive strategy to mitigate the risks posed by China's cyber activities to U.S. infrastructure.

The value of cybersecurity for federal departments and agencies cannot be underestimated. It is the shield that safeguards our nation's secrets, ensures the smooth functioning of our government, and preserves the trust and confidence of the American people. We must rise to the challenges that lie ahead, fortifying our defenses, embracing innovation securely, and forging a united front against the ever-present and evolving threats in cyberspace. Our future, our security, and the integrity of our democracy depend on it.

* * * * * * * * * * * * * * * * * * *

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2022, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2022 operating income came from the following sources:

Individuals 78%
Foundations 17%
Corporations 2%
Program revenue and other income 3%

The top five corporate givers provided The Heritage Foundation with 1% of its 2022 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position of The Heritage Foundation or its board of trustees.