GUIDE TO THE ISSUES

HOUSE REPUBLICAN POLICY COMMITTEE

ESTABLISHED 1949

DEFENDING AMERICA IN CYBERSPACE

Cyberattacks can cripple institutions from within without leaving a trace. In May 2021, Americans were left sitting in long lines at gas stations following a Russian-based ransomware attack that temporararily shut down Colonial Pipeline, an East Coast fuel pipeline.[1] This attack is only one of the recent high-profile cyber offensives, which pose a "grave" danger to national security.[2]

BACKGROUND

- A cyberattack occurs when an unauthorized user accesses confidential information systems, when system integrity is compromised by unauthorized data manipulation, or when system access is broken by blocking authorized users.[3] A cyberattack may result in theft or manipulation of intellectual property, confidential plans, or personally identifiable information (PII), to name a few.[4] These attacks are costly to both the direct and indirect parties involved.[5] Two of the most dangerous attacks include:
  - **Advanced Persistent Threat (APT):** These attacks use continual and stealth hacking methods to gain access to a system. Once in the system, the goal is to remain inside and undetected for an extended period in order to gain unauthorized information. These attacks are more often carried out against high-value targets due to their laborious nature. They are often, but not exclusively, launched from foreign sources.[6]
  - **Ransomware:** This is malicious software designed to encrypt data files in order to prevent use of data. Then, the cyberattackers require a ransom in exchange for decryption. This ever-evolving techology has been used against governments and critical infrastructure organizations. In 2019, ransomware attacks cost the global economy $11.5 billion and are projected to cost $20 billion in 2021.[7] The Cybersecurity and Infrastructrue Security Agency (CISA), the Federal Bureau of Invesigation, and the U.S. Secret Service provide resources on preventing and addressing ransomeware attacks.[8]

- Cyberattacks threaten U.S. critical infrastructure and are growing in sophistication. There are 16 critical infrastructure sectors identified by CISA"whose assets, systems, and networks…are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[9] These sectors span across healthcare, manufacturing, financial services, government, transportation, and others that impact Americans every day. Each of these sectors is assigned a federal agency to serve as a partner within the federal government, known as a Sector Risk Management Agency, with the goal of ensuring security and resiliency.[10]

- Cyberattacks by foreign adversaries are a threat to national security. China, Russia, Iran and North Korea represent the most active foreign adversaries with the most sophisticated technologies and techniques. China and Russia consistently demonstrate their willingness to launch attacks on public and private sectors in the U.S. to serve their national interests.[11]
  - China notably leverages "increasingly sophisticated" cyberattacks against the U.S. in order to steal data, intellectual property, or PII.[12] The U.S. Intelligence Community's 2021 Annual Threat Assessment reports, "China presents a prolific and effective cyber-espionage threat, possesses substantial

cyberattack capabilities, and presents a growing influence threat."[13] For example, China was attributed with a July 2021 cyberattack against the Microsoft Exchange server which resulted in theft of trade secrets, intelletual property, and other information from several companies and organizations.[14]

- Russia views cyberattacks as a tool to deter opponents, control escalation, and prosecute conflicts.[15] According to the 2021 Annual Threat Assessment, "Russia continues to target critical infrastructure, including underwater cables and industrial control systems."[16] Notably, the Russian Foreign Intelligence Service launched a cyberattack against SolarWinds in 2019,[17] which allowed hackers to spy on the U.S. Government and private companies at an unprecedented scope, scale, and level of sophistication.[18] The full impacts of the attacks are still being assessed.

<u>The U.S. Government works to defend America from threats in cyberspace:</u>

- **U.S. Cyber Command** (CYBERCOM) is the Department of Defense's (DoD) unified military command for cyber operations against American adversaries.[19]
  - CYBERCOM began full operation in May 2010. Its goal is to "direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests."[20] CYBERCOM is directed to secure military capabilities in cyberspace by securing DoD information systems, supporting cyberspace operations, and defending against cyberattacks.[21]
  - CYBERCOM's Cyber Mission Force (CMF) unit was established in 2012 to execute missions and coordinate operations.[22] CMF consists of 133 teams which were fully operational by May 2018.[23]

- **The Cybersecurity and Infrastructure Security Agency** (CISA), within the Department of Homeland Security (DHS), is the U.S. home base for defending against cyber threats and collaborating with the private and public sectors to secure critical infrastructure.[24]
  - CISA is responsible for securing '.gov' networks as well as COVID-19 supply chains and elections.
  - CISA coordinates security efforts with trusted partnerships in public and private sectors. It is at the center of collective defense of critical infrastructure in the U.S. CISA is responsible for helping both private and public sectors to understand and manage cyber risks.[25]

POLICY SOLUTIONS

Congress and security leaders must work to preserve the integrity of U.S. critical infrastructure in the complex domain of cyberspace in order to preserve national security. Congress should conduct oversight and assess the needs of DoD's and DHS's efforts to defend the U.S. from foreign and domestic threats in cyberspace.

- The Government Accountability Office (GAO) highlights four major areas of vulnerability across the federal government that need improvement, including: (1) establishing and implementing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data." Cyber and information security has been included in GAO's annual *High-Risk List* report since 1997 including the most recent report from 2021.[26]
- The federal government does not have uniform, defined standards of cybersecurity across the federal government. Congress could establish a uniform standard.[27] Congress could also evaluate current cybersecurity requirements across the government to ensure the requirements are simple and unified, so legislators can properly provide oversight.[28]

[1]Dustin Volz. Colonial Pipeline Chief Says Recovery From Ransomware Hack Not Complete. The Wall Street Journal. June 8, 2021. https://www.wsj.com/articles/colonial-pipeline-chief-to-testify-in-senate-panel-on-ransomware-hack-11623144602
[2] High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas. GAO. March 2, 2021. https://files.gao.gov/reports/GAO-21-119SP/index.html
[3]Klon Kitchen and James Di Pane. Cybersecurity: National Policies and Practices for Understanding Hacks and Reducing Vulnerabilities. The Heritage Foundation. July 24, 2020. https://www.heritage.org/cybersecurity/report/cybersecurity-national-policies-and-practices-understanding-hacks-and-reducing
[4] Anna Scherbina. Americans need to know the economic truth about cyber threats. AEI. June 21, 2021. https://www.aei.org/articles/americans-need-to-know-the-economic-truth-about-cyber-threats/
[5] Id. Federal and private sector computer systems are becoming increasingly interconnected with third-party vendors, suppliers, business partners, and customers. This growing connection has expanded the potential for attackers to find exploitable vulnerabilities.
[6]What Is an Advanced Persistent Threat. Kaspersky. https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats and Sarah Maloney. What Is an Advanced Persistent Threat. Cybereason. January 9, 2018. https://www.cybereason.com/blog/advanced-persistent-threat-apt
[77]Klon Kilchen and James Di Pane. Cybersecurity: National Policies and Practices for Understanding Hacks and Reducing Vulnerabilities. The Heritage Foundation. July 24, 2020. https://www.heritage.org/cybersecurity/report/cybersecurity-national-policies-and-practices-understanding-hacks-and-reducing
[8] Ransomware 101. Stop Ransom Ware. https://www.cisa.gov/stopransomware/ransomware-101
[9] Critical Infrastructure Sectors. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/critical-infrastructure-sectors
[10] Sector Risk Management Agencies. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/sector-risk-management-agencies
[11]Klon Kitchen and James Di Pane. Cybersecurity: National Policies and Practices for Understanding Hacks and Reducing Vulnerabilities. The Heritage Foundation. July 24, 2020. https://www.heritage.org/cybersecurity/report/cybersecurity-national-policies-and-practices-understanding-hacks-and-reducing
[12] Chinese Cyber Threat Overview and Actions for Leaders. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/publication/chinese-cyber-threat-overview-and-actions-leaders
[13] Annual Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence. April 9, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
[14]China Cyber Threat Overview and Advisories. Cybersecurity & Infrastructure Security Agency. https://us-cert.cisa.gov/china#chinese
[15] Russia Cyber Threat Overview and Advisories. Cybersecurity & Infrastructure Security Agency. https://us-cert.cisa.gov/russia
[16]Annual Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence. April 9, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
[17]SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response. GAO. April 22, 2021. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
[18] James Di Pane and Travis Sapp. America's Top Cyber Warrior Warns of Growing Threats. The Heritage Foundation. May 31, 2021. https://www.heritage.org/cybersecurity/commentary/americas-top-cyber-warrior-warns-growing-threats
[19] James Di Pane. Cybersecurity: Policymakers Need a Consistent Means to Assess Capabilities. August 25, 2021. https://www.heritage.org/defense/report/cybersecurity-policymakers-need-consistent-means-assess-capabilities
[20] U.S. Cyber Command https://www.cybercom.mil/About/History/
[21] Id.
[22] DOD Fact Sheet: Cyber Mission Force. U.S. Army Cyber Command. February 10, 2020. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/
[23]Id.
[24] Cybersecurity of federal information systems is governed by the Federal Information Security Management Act (FISMA), which gives DHS explicit operational authority for implementation and to set requirements for breach notification for federal agencies. Additionally, the NIST Framework serves as a voluntary set of risk-based best standards and practices to improve cybersecurity. https://www.cisa.gov/about-cisa
[25] About CISA. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/about-cisa
[26] High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas. GAO. March 2, 2021. https://files.gao.gov/reports/GAO-21-119SP/index.html#appendix22
[27] Broadly, cybersecurity is the practice of protecting networks and data from unauthorized users or criminal activity and securing confidentiality, integrity, and proper availability of information and data. Security Tip (ST04-001). Cybersecurity & Infrastructure Security Agency. November 14, 2019. https://us-cert.cisa.gov/ncas/tips/ST04-001 and Dustin Carmack. Admiral Michael Rogers on Confronting the Challenging Cyber LandScape. The Heritage Foundation. September 9, 2021. https://www.heritage.org/cybersecurity/event/admiral-michael-rogers-confronting-the-challenging-cyber-landscape and 2021 Annual Report on Implementation. Cyberspace Solarium Commission. August 2021. https://www.solarium.gov/public-communications/2021-annual-report-on-implementation
[28] Chris Jaikaran. Federal Cybersecurity: Background and Issues for Congress. Congressional Research Service. September 29, 2021. https://www.crs.gov/Reports/R46926?source=search&guid=0cf7bbad06ff46b2a097ab19b3c9e2cf&index=1