Christian DeJong, Daunte Leiran, Matthew Niblock

CSC 445

Dr. Kamel

May 1, 2024

State-Sponsored Cybersecurity Attacks

**Abstract**

This report examines the escalating threat of state-sponsored cyberattacks, which have become a prominent component of modern geopolitical conflicts. By utilizing advanced cyber techniques, governments engage in covert operations to infiltrate, disrupt, and exploit the digital infrastructures of other nations and organizations for strategic gains. This study analyzes these cyberattacks' nature, motivations, and impacts, highlighting their roles in intelligence gathering, economic espionage, and infrastructure sabotage. The research provides a comprehensive overview of historical incidents, current trends, and future threats, emphasizing the necessity for robust cybersecurity measures and international cooperation to mitigate these risks. The findings underscore the need for enhanced cybersecurity protocols and proactive defense mechanisms to protect against the sophisticated and often clandestine cyber operations sponsored by nation-states.

Cyber-warfare—the digital root of many modern conflicts—uses computer networks and technology to target and disrupt nations (*Coro Cybersecurity*). The frequency and intensity of such attacks has only escalated in recent years, with a 600% increase as a result of the COVID-19 pandemic (*Embroker*). This situation has only intensified the embracing of new solutions that allows companies to adapt quickly to this dynamic landscape. “Organizations face a race against time when software developers publicly release patches in response to nation-state vulnerability exploits because opportunistic cybercriminals immediately take action and attempt to infiltrate systems before the patches are applied” (*Coro Cybersecurity*). However, the increased need for development in cyber security does not solely involve companies protecting consumers information, but also governments. However, government action is not entirely comprised of keeping government and economic data safe, but also funding research of government attacks against other countries. State-sponsored cybersecurity attacks occur when a government sponsors or carries out a cyber-attack against another government or organization in a foreign country. The objective of such attacks is to infiltrate computer systems and IT infrastructure, exploit governments and organizations for money, and/or gather intelligence for the state (MRINetwork). State-sponsored attacks involve more resources than regular cyber-attacks and can cause long-lasting damage to a foreign government or business. Cybercriminals can steal intellectual property and military intelligence from a government. Hackers can even penetrate critical infrastructure, such as electricity grids and water systems. Furthermore, “Motivations have diversified, with state-backed groups engaging in cybercriminal activities to generate revenue and fund their ongoing operations. Some APT groups have embraced ransomware attacks, sometimes exploiting the profitability of extorting victims for financial gain but also as a technique of misattribution, disguising stealthy nation-state activity behind a front of common cybercrime” (SentinelOne). Nonetheless, as nations, corporations, and civilians become increasingly reliant on digital infrastructure, the stakes have escalated, making targeted, state-sponsored cyber-attacks a top global security concern. The objective of this research is to analyze these state-sponsored attacks, understand their impact, and investigate potential defensive strategies.

The origins of state-sponsored attacks can be traced back to the early days of computing, usually with intelligence-gathering as its objective. The United States and the Soviet Union engaged in cyber operations to gain access to each other’s classified information during the Cold War in the 1960s and 1970s (*Coro Cybersecurity*). Since then, the 2010s saw an explosion in cybercrime, turning what used to be a small niche industry into a global business. This decade also saw the rise of ransomware, as digital currencies like Bitcoin, the digitization of organizations, and new operating systems gave hackers new avenues and resources for attacks. In 2010, the Stuxnet worm—called the world’s first “digital weapon”—attacked nuclear plants in Iran, sabotaging the country’s uranium enrichment facilities. In the same year, the Zeus Trojan virus was distributed around the world via email in an attack targeting financial services organizations; managing to steal more than $70 million from American banks (*Arctic Wolf*). However, if the 2010s were the decade where cybercrime was finding its footing, the 2020s have seen the ecosystem sophisticate in new ways. In 2020, Russian cyber-attacks on U.S. governmental institutions, foreign intelligence operatives took advantage of a compromised SolarWinds program and invaded an estimated 18,000 private and government-affiliated networks. Granting attackers access to an abundance of information, including financial information, source code, passwords, and usernames. There have been two contributing factors this decade: one is the overall rise in cybercrime driven by new technological advancements, and two is the rapid digitization of organizations turning to the cloud but are doing so faster than their cybersecurity measures can keep up (*Arctic Wolf*). This resulted in cybercrime now valued at a 1.5 trillion-dollar industry and is the number one global business risk. The average cost of a data breach has reached $4.45 million USD; with 82% of breaches involving the cloud, and 24% of attacks comprised of ransomware in 2023 (*Arctic Wolf*). In addition, the balance of AI use is currently in favor of the attackers, with the cybersecurity world struggling to leverage generative AI to keep up with these new capabilities. “Over the last year, the speed, scale, and sophistication of attacks has increased alongside the rapid development and adoption of AI. Defenders are only beginning to recognize and apply the power of generative AI to shift the cybersecurity balance in their favor and keep ahead of adversaries” (*Microsoft Security Blog*,). As we delve into the pervasive and escalating nature of state-sponsored cyberattacks, it becomes imperative to assess the global impact on targeted nations and the consequent responses. These attacks not only exploit the vulnerabilities of national infrastructures but also prompt a multifaceted international reaction encompassing diplomatic tensions and enhanced cybersecurity collaborations.

State-sponsored cyber-attacks target many different industries. The most affected industries are manufacturing, government agencies, energy, and transportation. For example, a Chinese hacking group known as Volt Typhoon compromised the U.S. Department of Energy, Environmental Protection Agency, and Transportation Security Agency. The same group also compromised several countries’ state cybersecurity agencies. (CSISPRC) These industries are often targeted by nation-states to gain leverage over other countries or sabotage their operations. This leverage often comes in the form of intellectual property, private information and data, and government and trade secrets. Espionage is the term used to refer to this kind of cyber-attack. Information that is commonly targeted is military intelligence, especially between warring countries, but it can include business’ data and confidential files. (CHECK) Espionage has been especially prevalent in the war between Russia and Ukraine, especially as Russia continues to launch offensive cyber-attacks on Ukraine and its allies in an effort to gain the upper hand in the war. Nation-states conduct a special kind of attack known as economic espionage, which is when information is stolen and used for the attacker’s monetary gain or the victim’s financial loss. Billions of dollars are lost every year because of cyber-attacks on the supply chain, which disrupts the manufacturing and distribution of countless companies’ products, and from theft of intellectual property. There have been estimates in the hundreds of billions of dollars lost from U.S. companies due to Chinese cyber espionage. (SentinelOne) Some cyber-attacks are carried out without any intention of informational or monetary gain, however. Disruption and sabotage attacks are cyber-attacks with a goal of disrupting critical infrastructure and services of a nation-state. These kinds of attacks are commonly launched on infrastructure that is essential to all industries, such as power grids and transportation networks. This kind of sabotage can lead to financial loss, public inconvenience, and industrial disruption. (SOPHOS) Ukraine recently carried out an attack like this when they compromised Russia’s largest water utility plant by deleting 50 terabytes of data, while encrypting over 6,000 computers to deny Russian workers access to the systems. This attack was in retaliation to Russian hackers disabling Ukraine’s largest mobile network, which supplied internet to over 24 million Ukrainians. The Russian-backed hackers are said to have crippled over 10,000 computers and 4,000 servers in their attack. (CSIS) These attacks do not give the nations any kind of information, but they prevent the other nation from carrying out important operations.

As stated earlier, state sponsored cyber security attacks are a growing problem for many countries across the world. Because of this the US Government has implemented agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), established in 2018. Within this agency there are certain divisions such as cybersecurity and infrastructure security. These divisions include a cybersecurity division, infrastructure security division, emergency communications division, risk management division, and a few more, but this paper will focus primarily on the ones named above. The cybersecurity division (CSD) focuses on fortifying the nation’s cyber defenses against immediate threats and vulnerabilities. They coordinate cyber incident response, provide cybersecurity tools and guidance, and work with stakeholders to enhance cybersecurity resilience. In terms of importance, this is at the top of the list. The infrastructure security division (ISD) is responsible for safeguarding the nation's critical infrastructure, including physical assets like buildings, transportation systems, and utilities such as energy. This division works to identify vulnerabilities, work with critical infrastructure owners, and support infrastructure resilience efforts. The emergency communications division (ECD) oversees programs and initiatives aimed at ensuring reliable and effective communication during emergencies and disasters. Similarly to the ISD, they coordinate with critical partners to enhance emergency communication capabilities. The national risk management center/division (NRMC) focuses on identifying and prioritizing strategic risks to the nation's critical infrastructure. They conduct risk assessments, develop mitigation strategies, and facilitate collaboration between government and industry stakeholders to address systemic risks. One of the primary functions of CISA is to manage the National Cybersecurity Protection System (NCPS). The NCPS is a system that delivers capabilities like intrusion detection, analytics, and information sharing. The system contains features aimed at CISA's cybersecurity assignment, including hardware, software programs, methods, and services. Perhaps the most important feature of the system is EINSTEIN. It serves as an early caution gadget and offers improved situational recognition of intrusion threats to federal civilian executive department (FCEB) networks. NCPS abilities divide into 4 sections: Intrusion Detection, Analytics, Information Sharing, and Intrusion Prevention. Intrusion Detection, facilitated by EINSTEIN 1 and 2, employs a passive, signature-based sensor grid to reveal network visitors, enhancing CISA's intelligence of threats. Analytics offer gear for compiling and reading cyber pastime facts throughout multiple security enclaves. Information Sharing permits the exchange of incident records amongst CISA analysts and companions, focusing on collaboration and performance. CISA integrates privateness protections into all its programs, including NCPS, undertaking Privacy Impact Assessments to minimize dangers and ensure transparency in compliance with privacy ideas. Along with services like CISA and NCPS, policies and acts are also put in place to protect government security. An important policy that was implemented was the FISM Act. The FISMA, or the Federal Information Security Management Act, is an important piece of legislation in the United States aimed at safeguarding federal government information systems and data. Enacted in 2002, it provides a comprehensive framework for managing cybersecurity risks within federal agencies. At its core is the Risk Management Framework, which guides agencies through a structured process of categorizing information systems, selecting and implementing security controls, assessing security posture, authorizing systems, and continuously monitoring for threats. FISMA mandates security controls and guidelines outlined by the National Institute of Standards and Technology (NIST), emphasizing the importance of confidentiality, integrity, and availability of government information. Oversight and compliance activities ensure agencies are effectively implementing cybersecurity measures, with roles and responsibilities assigned to various stakeholders to oversee and enforce security protocols. Through FISMA, federal agencies strive to protect sensitive information, mitigate cybersecurity risks, and maintain the government systems in the face of evolving threats.

In conclusion, state-sponsored cyberattacks pose a significant threat to global security, targeting industries and critical infrastructure for espionage, economic gain, or sabotage. The escalating frequency and sophistication of these attacks underscore the urgent need for robust defensive strategies and international cooperation. Efforts such as the establishment of agencies like the Cybersecurity and Infrastructure Security Agency (CISA) in the United States demonstrate a commitment to fortifying cyber defenses. Policies like the Federal Information Security Management Act (FISMA) provide a framework for managing cybersecurity risks within government agencies. Moving forward, addressing these challenges requires investment in advanced cybersecurity technologies, collaboration between governments and private sector entities, and strengthening international norms governing cyberspace. By adopting a proactive and coordinated strategy, nations can minimize the impact of cyber threats and safeguard digital infrastructure in a digital world.

Works Cited

“2024 Must-Know Cyber Attack Statistics and Trends.” *Embroker*, 4 Jan. 2024, www.embroker.com/blog/cyber-attack-statistics/.

Arctic Wolf. “History of Cybercrime.” *Arctic Wolf*, 19 Apr. 2024, arcticwolf.com/resources/blog/decade-of-cybercrime/.

CHECK. “Nation-State Level Cyberattacks.” Check Point Software, [www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/nation-state-level-cyberattacks/#:~:text=Espionage%3A%20Espionage%20is%20a%20common](http://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/nation-state-level-cyberattacks/#:~:text=Espionage%3A%20Espionage%20is%20a%20common).

CISA. “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA.” Www.cisa.gov, 7 Feb. 2024, www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

CISAPRC. “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, 18 Apr. 2024, [www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a](http://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a).

CSIS. “Significant Cyber Incidents | Center for Strategic and International Studies.” Www.csis.org, 2024, [www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents](http://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents).intri

“Divisions & Offices: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/about/divisions-offices.

Imi. “State Sponsored Cyber Warfare.” *Identity Management Institute®*, IMI https://www.identitymanagementinstitute.org/app/uploads/2021/03/logo-.jpg, 9 May 2023, identitymanagementinstitute.org/state-sponsored-cyber-warfare/.

Intelligence, Microsoft Threat. “Staying Ahead of Threat Actors in the Age of Ai.” *Microsoft Security Blog*, 27 Feb. 2024, www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/.

MRINetwork. “Why State-Sponsored Cyber Attacks Are a Global Threat.” *MRINetwork*, 18 Jan. 2024, mrinetwork.com/hiring-talent-strategy/why-state-sponsored-cyber-attacks-are-a-global-threat/.

“National Cybersecurity Protection System: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, [www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system](http://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system).

SentinelOne. “The New Frontline of Geopolitics: Understanding the Rise of State-Sponsored Cyber Attacks.” *SentinelOne*, 3 Apr. 2024, www.sentinelone.com/blog/the-new-frontline-of-geopolitics-understanding-the-rise-of-state-sponsored-cyber-attacks/.

SOPHOS. “Threat Actors Explained: Motivations and Capabilities.” SOPHOS, [www.sophos.com/en-us/cybersecurity-explained/threat-actors](http://www.sophos.com/en-us/cybersecurity-explained/threat-actors).

“What Are State-Sponsored Cyberattacks?” *Coro Cybersecurity*, 1 Feb. 2024, [www.coro.net/blog/what-are-state-sponsored-cyberattacks](http://www.coro.net/blog/what-are-state-sponsored-cyberattacks).‌

‌