Beyond the Battlefield: The Impact of the Russo-Ukrainian War on U.S. Cybersecurity

Introduction

The Russo-Ukrainian War has garnered significant media attention throughout 2022 and 2023. Although the conflict originated in February of 2014, Russia's unexpected invasion of Ukraine from the north and west in February 2022 catapulted the issue into mainstream media focus. As the COVID-19 pandemic receded from headlines, news outlets prioritized Ukraine-related coverage to retain and bolster viewership. In its year-end review, the popular journal Nature identified the conflict as one of the most critical ongoing news stories of 2022, emphasizing its impact on environmental research and its substantial role in the global energy crisis [1]. However, amid research, energy, and destruction discussions, a crucial issue remains underrepresented in the mainstream pipeline: the cybersecurity crisis facing the United States and its allies due to the war. This paper will systematically analyze the emerging threats to U.S. cyber infrastructure in private and public sectors, evaluate the policies and standards implemented to address these challenges, and provide recommendations for future action. Harvard Business Review describes the conflict in Ukraine as presenting "perhaps the most acute cyber risk U.S. and Western corporations have ever faced" [2]. Understanding and addressing these threats is imperative to ensure domestic security and foster resilience.

Catalyst

Russia will not stand by [while its adversaries support Ukraine and level sanctions] but will instead respond asymmetrically using its considerable cyber capability [2].

Private Sector

Private enterprises have emerged as prime targets for nation-state cyber attackers. According to a 2020 study by Hewlett Packard and the University of Surrey, 35% of nation-state cyberattacks focused on businesses and private enterprises, while around 12% targeted government entities [3]. Key world events, such as wars and pandemics, often serve as catalysts for cybercrime. The Russo-Ukrainian War is a prime example of such a catalyst. From the outset, researchers predicted that Russia would retaliate and seek intelligence on Western enterprises in response to punitive measures like heavy sanctions [2]. However, Russia's actions are not unprecedented; they align with intelligence assessments predating the 2022 escalation. A declassified report from April 2021 characterizes Russia as “a power ready to employ various tactics—including influence campaigns, intelligence, and counterterrorism cooperation, military aid and combined exercises, mercenary operations, assassinations, and arms sales—to advance its interests or undermine those of the United States and its allies” [4].

Financial institutions and payment systems are attractive targets for nation-states and their proxies seeking to exert political and ideological influence [5][9]. Although cybercrime in the financial sector has slowed in recent years, the U.S. Treasury's Office of Financial Research warns that Russia's war against Ukraine significantly raises the risk of state-sponsored cyberattacks on the sector [6]. The Cyber Peace Institute shares this assessment, urging financial services to remain on high alert [7]. In response to punitive measures by adversarial governments, powerful nations may retaliate by targeting the financial sector. A Congressional

Research Service report reveals that sanctions have restricted 80% of Russian banking sector assets, with multiple Russian institutions blocked from using the SWIFT payment system [8]. While no public information directly links Russia to attacks on U.S. financial institutions in 2022 or 2023, Russian hackers targeted Costa Rica's Ministry of Finance in April 2022, demonstrating their willingness to exploit financial systems [10]. Despite no major attacks being claimed, numerous breaches of unknown origin plagued financial services and payment systems in 2022 and 2023. For instance, in January 2023, Forbes reported a credential stuffing attack on PayPal users [11], while Flagstar Bank revealed a months-long undetected breach just months prior [12]. Evidently, the sector remains vulnerable to cyber threats. To mitigate risks, banks and payment system operators must strengthen their cybersecurity posture and stay abreast of the latest threats, which currently include ransomware, DDoS, phishing, and insider-related attacks [13].

The energy sector is another prime target for adversaries such as Russia. In a March 2023 briefing, U.S. DOE CESER Director Puesh Kumar warned that "cyber risks to energy systems continue to increase, from nation-states, criminal actors, and other malicious cyber actors" [14]. His testimony underscores the alarming message in the 2019-2023 Annual Threat Assessment of the U.S. Intelligence Community: the U.S. energy sector is at direct risk of attacks from China and likely Russia as well [14]. In the month following Russia's invasion, the FBI informed CBS News about "network scanning activity" originating from multiple Russia-based IP addresses targeting the U.S. energy sector [15]. Russia has demonstrated its willingness to target or permit its citizens to disrupt U.S. energy services, as seen in May 7, 2021, DarkSide ransomware attack on the Colonial Pipeline Company, likely carried out by Russian hackers [16]. In March 2022, criminal indictments for three Russian FSB officers' highlighted malicious actions against energy infrastructure between 2011 and 2018. These attacks included oil refineries and direct energy providers [17]. While no major attacks attributed to Russia have been observed in 2022 or 2023, proactive measures are being taken to secure the energy sector. For instance, the DOE is funding up to 15 projects focused on cyberattack mitigation, resiliency, authentication, automation, advanced software solutions, and the integration of new technologies [18]. Furthermore, President Biden’s Build Back Better agenda highlights energy resilience as a primary focus of his administration and one of the purposes of the Bureau of Energy Resources [19].

The telecommunications sector is yet another critical area facing heightened risks from adversaries like Russia. Echoing the concerns raised for the financial and energy sectors, the telecom industry is an attractive target for nation-states aiming to disrupt communication channels, steal sensitive information, or monitor communications. The U.S. Intelligence Community's Annual Threat Assessment highlights the risk of cyber threats to the telecommunications sector, identifying both China and Russia as potential aggressors [14]. In 2020, the Russian APT group Sandworm was accused of targeting European telecom companies, demonstrating their willingness to disrupt the industry [20]. In February 2023, Russia attacked communications between NATO forces, and in March, Russian actors used unsuspecting victims and communication equipment to produce pro-Kremlin propaganda [22]. As with the financial and energy sectors, proactive measures are essential to safeguard telecommunications infrastructure. Initiatives such as the FCC's Supply Chain Reimbursement Program aim to reduce risks by identifying and mitigating potential vulnerabilities in the telecommunications supply chain [21]. Moreover, public-private partnerships and collaborations within the industry are crucial for sharing threat intelligence and best practices, ensuring that the telecommunications sector remains resilient in the face of persistent cyber threats.

Addressing cyber threats in the healthcare sector is a matter of life and death. "From small, independent practitioners to large, integrated health systems, cyber-attacks on healthcare records, IT systems, and medical devices have infiltrated even the most protected systems" [22]. Healthcare is an area where Russian hackers have been active, both in the past and present. The Ukraine conflict further encourages such attacks; even unintended attacks may drastically impact this industry. According to an Association of American Medical Colleges report, the U.S. healthcare industry faces three primary cybersecurity concerns: loss of personal information and research, disclosure of government employee records, and collateral damage from other attacks [23]. An example of collateral damage can be observed in the 2017 NotPetya ransomware attack, where pharmaceutical company Merck lost $870 million [24]. American hospitals were also directly affected by infection or the inability to use patient record services like Nuance, which was infected [25]. The invasion of Ukraine has led to healthcare threats that will continue to materialize in 2023. A January report by the Health Sector Cybersecurity Coordination Center states that KillNet, a pro-Russian hacktivist group, is actively attempting to undermine U.S. healthcare sector security through DDoS attacks and data leaks [26]. CISA recommends addressing these attacks by applying patches, enforcing strong authentication such as multi-factor authentication, securing vulnerable services, and providing training [27]. The report also emphasizes the importance of having response plans and a robust security plan as essential components of any cybersecurity program.

The transportation and logistics sector remains vulnerable to cyber threats from Russia despite the efforts of organizations such as the Cybersecurity Infrastructure Security Agency (CISA) and the Transportation Security Administration (TSA), which directly address the industry's cybersecurity concerns [28]. The 2017 NotPetya ransomware attack, for instance, had far-reaching consequences on transportation and logistics companies like Merck [25]. FedEx and Maersk also experienced massive losses. The pro-Russian hacktivist group KillNet, known for targeting the U.S. healthcare sector, also attacked U.S. airports with ransomware in October of 2022 [29]. The growing reliance on autonomous vehicles and the highly fragmented private transportation industry in the United States complicates the coordination of responses to cyber threats. To mitigate these risks, the transportation and logistics sector must prioritize strengthening its cybersecurity posture, sharing threat intelligence and best practices among industry stakeholders, and implementing robust security measures. Proactive approaches can help enhance the sector's resilience in the face of persistent and evolving cyber threats, even with the support of organizations such as CISA and TSA.

Public Sector

The public sector plays a vital role in maintaining national security, public safety, and the overall functioning of society, making it an attractive target for adversarial nation-states like Russia. Cyber threats to public sector critical infrastructure, such as public transportation, water and wastewater systems, emergency services, and e-government services, pose significant risks to the United States. Russian-sponsored cyberattacks on public sector infrastructure can lead to disruptions in essential services, compromise sensitive information, and undermine public trust in government institutions.

The nation's critical infrastructure spans across both public and private sectors, making it a complex and challenging target for defending against nation-state attackers, particularly from Russia. In January 2022, just before the escalation of the Ukraine conflict, the NSA, CISA, and FBI issued a joint cybersecurity advisory addressing the threat Russia poses to U.S. critical infrastructure. The report urges the cybersecurity community, especially critical infrastructure network defenders, to adopt a heightened state of awareness, conduct proactive threat hunting, and implement recommended mitigations to reduce the risk of compromise or severe business degradation [30]. Given the vast and diverse nature of critical infrastructure, protection strategies must be tailored to each specific industry. CISA, in collaboration with its partners, works diligently to provide guidance and recommend legislation to ensure the protection of various critical infrastructure sectors. One example is the Dams Sector, which encompasses over 90,000 dams in the U.S. and delivers essential water retention and control services. CISA collaborates with sector partners to safeguard these assets from natural disasters, human-caused incidents, and technological events [31]. By working closely with industry partners, CISA aims to strengthen the resilience and security of the nation's critical infrastructure against potential cyber threats from Russia and other adversaries.

The realm of national security is an area where we may find limited public or sourced information about cyberattacks from Russia. Nevertheless, intelligence agencies, government contractors, and other sensitive entities hold a wealth of valuable data that Russia could potentially use against the U.S., its allies, and to disrupt alliances. For instance, in April 2023, the release of a relatively small amount of classified material had a profound impact on international relations. Reports from CNN and BBC revealed that sensitive information about the U.S. presence in Ukraine, surveillance on allies, and foreign governments' views on supporting the war effort were all exposed[32][33]. One way to mitigate these risks is by ensuring that policymakers hold entities accountable and enforce adherence to established standards. However, even with the best policies in place, unforeseen challenges may arise due to the rapid evolution of cyber threats and innovative attack strategies. Given the capacity of such information to undermine international relations and erode trust among U.S. citizens, it is highly likely that an ongoing and highly secretive cyber battle is taking place to protect each nation's interests and secure leverage in the global landscape.

Foreign powers and their role in election interference have been a contentious topic in recent years. According to a YouGov survey in November 2022, 53% of Americans considered it somewhat or very likely that foreign countries would interfere in their elections, with 61% of respondents identifying Russia as the most probable culprit [34]. A partially redacted report from the Select Committee on Intelligence covering Russian interference in the 2016 election reveals that Russia has a history of attempting to meddle in its adversaries' elections. The report states, "the Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure," but adds that "there is no evidence that votes were changed in any way" [35]. Nevertheless, merely sowing discord among the public regarding election outcomes serves as a potent attack strategy, as highlighted in the report.

To further its interests in Ukraine and on the global stage, Russia might attempt to create confusion within the election system again or, even worse, find a way to influence election outcomes directly. U.S. intelligence and defense agencies are committed to preventing such attacks. The Department of Homeland Security asserts, "A secure and resilient electoral process is a vital national interest and one of our highest priorities" [36]. In the next section, we will examine some of the legislation, standards, and procedures implemented and in development. The key takeaway, however, is that elections are a sensitive area that Russia could exploit to divert attention from the Ukraine conflict and incite civil unrest.

Policies, Standards, Guidelines, Frameworks and More

In this section, we will highlight some of the various policies, standards, guidelines, frameworks, etc., established to address cyber risks in many of the industries discussed earlier, including financial services, telecommunications, healthcare, transportation, and the public sector. These policies and standards aim to provide guidance to help organizations manage and mitigate cybersecurity threats while also promoting collaboration between the public and private sectors. By understanding and implementing these measures, organizations across different industries may better safeguard against potential cyber threats from adversaries like Russia. However, as with any legislation, it can become dated. Therefore, new guidance must be drafted to ward off the threats of the ever-changing cybersecurity landscape.

The table below displays information on the policies, standards, and frameworks that existed before the conflict reignited in February 2022.

Item	Creation Date	Industry	Purpose
National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)	2014	Broad	“The CSF is a voluntary framework comprising standards, guidelines, and practices to promote critical infrastructure protection” [37].
CISA (Agency)	2018	Broad	“CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience” [38]. CISA produces guidelines and practices on

			current and emerging threats. They work closely with states and private enterprises.
Executive order 13800	2017	Broad	“EO 13800 focuses Federal efforts on modernizing Federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies” [39].
Health Insurance Portability and Accountability Act (HIPAA)	1996	Healthcare	“HIPAA is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge” [40].
FCC Supply Chain Reimbursement Program	2020	Communicat-ions	The FCC’s Supply Chain Reimbursement Program aims to help telecommunications providers remove and replace equipment and services that pose a national security risk in their networks, ensuring a more secure telecommunications infrastructure [21].
Gramm-Leach-Biley Act	1999	Finance	“The FTC Safeguards Rule requires covered companies to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information” [41].
CISA’s Election Infrastructure Security Resource Guide	2020	Elections	The guide provides guidelines on best practices for election infrastructure [42].

As cyber risks continue to evolve amidst the ongoing Ukrainian conflict, several developments, and recently enacted policies are addressing cyber challenges across various industries. For critical infrastructure sectors like telecommunications, financial services, and energy, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law in March 2022. This legislation requires companies in these sectors to report significant cyber incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, facilitating improved information sharing and threat intelligence [43].

In the realm of IoT security, the National Institute of Standards and Technology (NIST) has released guidance for IoT device manufacturers on building secure devices through the NISTIR 8259 series [44]. To enhance election security, proposed bills such as the Secure Elections Act and the Election Security Act focus on upgrading election systems, implementing risk-limiting audits, and improving information sharing between federal and state agencies [45][46]. Lastly, to address the growing demand for skilled cybersecurity professionals, initiatives like the Cybersecurity Skills Integration Act have been introduced, seeking to establish grant programs that encourage the integration of cybersecurity education into post-secondary degree programs [47].

Based on the line of inquiry this paper has taken so far, it appears that although not every industry is entirely resilient against Russian cyberattacks, overall major attacks (at least those publicly disclosed) are minimal. This may suggest (but not provide correlation) that the implemented policies, standards, and proactive measures taken by various industries are helping to mitigate the impact of potential cyber threats from adversaries like Russia. However, it is crucial to remain vigilant and continuously adapt to the evolving threat landscape to protect critical infrastructure and sensitive information.

Discussion for the Future

In addressing the ongoing and evolving cyber threats, particularly those posed by Russia, it is essential to concentrate on several key areas that will shape the future of cybersecurity and resilience.

- Strengthening collaboration: Enhanced cooperation between public and private sectors, as well as international partners, is vital for sharing threat intelligence, best practices, and resources. Such collaboration will help develop comprehensive strategies to protect critical infrastructure and promote collective security.

- Cybersecurity education and workforce development: Investing in education and workforce development will build a strong foundation for future cybersecurity experts. A robust and knowledgeable workforce is crucial for responding effectively to emerging threats and securing our digital landscape.

- Encouraging innovation: Supporting research and development initiatives and fostering collaboration between academia and industry will drive innovation in cybersecurity technologies. Cutting-edge solutions can proactively address emerging threats, ensuring our defenses evolve alongside potential risks.

- Implementing best practices: Adopting proven best practices across critical infrastructure sectors can significantly improve their resilience against cyber threats. Consistent implementation of these practices will reduce the attack surface and minimize potential damage.

- Enhancing response and recovery capabilities: Developing robust incident response and recovery capabilities is essential for minimizing the impact of cyberattacks. Well-defined plans, regular drills, and effective response mechanisms can help organizations quickly recover from cyber incidents.

- Promoting responsible state behavior: Encouraging the establishment of international norms and agreements on responsible state behavior in cyberspace can help create a more secure and stable global cyber environment. Such norms will reduce the likelihood of escalation and foster a shared understanding of acceptable behavior among nations.

- Standardizing audits and accountabilities for established cyber regulations and protocols with penalties for violations.

Conclusion

In conclusion, the Ukrainian conflict has brought to the forefront the critical importance of securing our nation's infrastructure against cyber threats. While this paper has provided a general overview of the key areas of concern within critical infrastructure in both private and public sectors, it is by no means comprehensive. It is evident that cyber threats will continue to evolve, and it is vital to remain vigilant and proactive in protecting against them. Even when this conflict is over, there will be further catalysts, and Russia will remain an adversary.

References

[1] “Nature's biggest news stories of 2022,” *Nature News*, 15-Dec-2022. [Online]. Available: https://www.nature.com/articles/d41586-022-04384-y. [Accessed: 05-May-2023].

[2] P. R. Kolbe, M. R. Morrow, and L. Zabierek, “The cybersecurity risks of an escalating Russia-Ukraine conflict,” *Harvard Business Review*, 24-Feb-2022. [Online]. Available: https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict. [Accessed: 05-May-2023].

[3] HP Wolf Security, “Nation states, Cyberconflict and the Web of Profit: HP threat research,” HP Wolf Security, 18-May-2021. [Online]. Available: https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/. [Accessed: 05-May-2023].

[4] “Annual Threat Assessment of the US Intelligence Community,” 09-Apr-2021. [Online]. Available: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. [Accessed: 05-May-2023].

[5] “Financial Sector Cybersecurity: Cybersecurity and governance,” CSIS, 2023. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/financial-sector. [Accessed: 05-May-2023].

[6] D. Chiella, H. Hamandi, and R. Leung, “Five risk areas that financial regulators should watch in 2023,” Office of Financial Research, 07-Mar-2023. [Online]. Available: https://www.financialresearch.gov/the-ofr-blog/2023/03/07/five-risk-areas-that-financial-regulators-should-watch-in-2023/. [Accessed: 05-May-2023].

[7] “Financial and Insurance Activities,” *Cyberattacks Impact and Harm on the Financial sector | CyberPeace Institute*, 2023. [Online]. Available: https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/financial. [Accessed: 05-May-2023].

[8] “Russia’s war on ukraine: Financial and trade sanctions - congress,” *Congressional Research Service*, 22-Feb-2023. [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF12062. [Accessed: 05-May-2023].

[9] R. Iyengar, “US braces for Russian cyberattacks as Ukraine conflict escalates. here's how that might play out | CNN business,” *CNN*, 24-Feb-2022. [Online]. Available: https://www.cnn.com/2022/02/24/tech/russia-ukraine-us-sanctions-cyberattacks/index.html. [Accessed: 05-May-2023].

[10] “Significant cyber incidents: Strategic technologies program,” *CSIS*, Mar-2023. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. [Accessed: 05-May-2023].

[11] D. Winder, “Thousands of PayPal accounts breached-is yours one of them?,” *Forbes*, 21-Jan-2023. [Online]. Available: https://www.forbes.com/sites/daveywinder/2023/01/19/thousands-of-paypal-accounts-hacked-is-yours-one-of-them/?sh=73ef3da73a6b. [Accessed: 05-May-2023].

[12] “Data breach notifications,” *Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches*, 2022. [Online]. Available: https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml. [Accessed: 05-May-2023].

[13] O. Gulyas and G. Kiss, “Cybersecurity threats in the banking sector,” *IEEExplore*, May-2022. [Online]. Available: https://ieeexplore-ieee-org.offcampus.lib.washington.edu/stamp/stamp.jsp?tp=&arnumber=9804140&tag=1. [Accessed: 05-May-2023].

[14] P. Kumar, “Testimony of director puesh kumar office of cybersecurity, energy ...,” 23-Mar-2023. [Online]. Available: https://www.energy.senate.gov/services/files/7C2EC274-467C-4444-BD14-D4F11E474492. [Accessed: 06-May-2023].

[15] C. Herridge and N. Sganga, “Russia exploring options for potential cyberattacks on U.S. Energy Sector, FBI warns,” *CBS News*, 22-Mar-2022. [Online]. Available: https://www.cbsnews.com/news/russia-cyberattacks-us-energy-fbi-warning/. [Accessed: 05-May-2023].

[16] “Colonial Pipeline Cyber Incident,” *Energy.gov*, May-2021. [Online]. Available: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident. [Accessed: 05-May-2023].

[17] “Tactics, techniques, and procedures of indicted state-sponsored Russian cyber actors targeting the energy sector: CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, 24-Mar-2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a. [Accessed: 05-May-2023].

[18] “Doe announces $45 million for next-generation cyber tools to protect the power grid,” *Energy.gov*, 17-Aug-2022. [Online]. Available: https://www.energy.gov/articles/doe-announces-45-million-next-generation-cyber-tools-protect-power-grid. [Accessed: 05-May-2023].

[19] “Energy - United States Department of State,” *U.S. Department of State*, 04-Nov-2021. [Online]. Available: https://www.state.gov/policy-issues/energy/. [Accessed: 05-May-2023].

[20] O. Gazis, “NSA warns of new cyberattacks by Russian military hackers,” *CBS News*, 28-May-2020. [Online]. Available: https://www.cbsnews.com/news/national-security-agency-cyberattack-sandworm-russia-hackers/. [Accessed: 05-May-2023].

[21] “Protecting against national security threats to the communications supply chain through FCC programs,” *Federal Communications Commission*, 13-Mar-2023. [Online]. Available: https://www.fcc.gov/supplychain. [Accessed: 05-May-2023].

[22] “Healthcare and Public Health Sector: CISA,” *Cybersecurity and Infrastructure Security Agency CISA*. [Online]. Available: https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector. [Accessed: 05-May-2023].

[23] S. Weiner, “How the war in Ukraine threatens hospital cybersecurity - and what to do about it,” *AAMC*, 24-May-2022. [Online]. Available: https://www.aamc.org/news/how-war-ukraine-threatens-hospital-cybersecurity-and-what-do-about-it. [Accessed: 05-May-2023].

[24] A. Greenberg, “The untold story of notpetya, the most devastating cyberattack in history,” *Wired*, 22-Aug-2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [Accessed: 05-May-2023].

[25] A. Greenberg, “How the worst cyberattack in history hit American Hospitals,” *Slate Magazine*, 05-Nov-2019. [Online]. Available: https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html. [Accessed: 05-May-2023].

[26] “January 30, 2023 TLP:Clear Report: 202301301200 - hhs.gov,” 30-Jan-2023. [Online]. Available: https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf. [Accessed: 06-May-2023].

[27] “Russian state-sponsored and criminal cyber threats to critical infrastructure: CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, 18-Apr-2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a#:%7E:text=Responding%20to%20Cyber%20Incidents. [Accessed: 05-May-2023].

[28] “GAO-22-105103, critical infrastructure protection: Agencies need to ...,” *gao.gov*, Feb-2022. [Online]. Available: https://www.gao.gov/assets/gao-22-105103.pdf. [Accessed: 06-May-2023].

[29] A. Eich, “Killnet: Russian Hacktivists DDoS US Airports, Government Websites,” *University of Hawaii - West Oahu*, 18-Oct-2022. [Online]. Available: https://westoahu.hawaii.edu/cyber/uncategorized/killnet-russian-hacktivists-ddos-us-airports-government-websites/. [Accessed: 05-May-2023].

[30] “Understanding and mitigating Russian state- sponsored cyber threats to ...,” *media.defense.gov*, 11-Jan-2022. [Online]. Available: https://media.defense.gov/2022/Jan/11/2002919950/-1/-1/1/JOINT_CSA_UNDERSTANDING_MITIGATING_RUSSIAN_CYBER_THREATS_TO_US_CRITICAL_INFRASTRUCTURE_20220111.PDF. [Accessed: 06-May-2023].

[31] “Critical Infrastructure Sectors: CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, 2023. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. [Accessed: 05-May-2023].

[32] J. M. and A. R. Paul Adams, “What the leaked Pentagon documents reveal - 8 key takeaways,” *BBC News*, 15-Apr-2023. [Online]. Available: https://www.bbc.com/news/world-us-canada-65238951. [Accessed: 05-May-2023].

[33] N. Bertrand and K. Atwood, “Leaked Pentagon documents provide rare window into depth of US intelligence on allies and foes | CNN politics,” *CNN*, 10-Apr-2023. [Online]. Available: https://www.cnn.com/2023/04/09/politics/pentagon-leaked-documents-us-spying-allies-foes/index.html. [Accessed: 05-May-2023].

[34] “The economist/yougov poll,” *YouGov*, 2022. [Online]. Available: https://docs.cdn.yougov.com/pyh97ixj6q/econTabReport.pdf. [Accessed: 06-May-2023].

[35] “REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE WITH ADDITIONAL VIEWS,” *intelligence.senate.gov*. [Online]. Available: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf. [Accessed: 06-May-2023].

[36] “Election security,” *Election Security | Homeland Security*, 25-Apr-2023. [Online]. Available: https://www.dhs.gov/topics/election-security. [Accessed: 05-May-2023].

[37] “Getting started,” *NIST*, 21-Apr-2023. [Online]. Available: https://www.nist.gov/cyberframework/getting-started. [Accessed: 05-May-2023].

[38] “About Cisa: CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, 2023. [Online]. Available: https://www.cisa.gov/about. [Accessed: 05-May-2023].

[39] “Executive order on strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, 2023. [Online]. Available: https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure. [Accessed: 05-May-2023].

[40] “Summary of the HIPAA privacy rule,” *HHS.gov*, 19-Oct-2022. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. [Accessed: 05-May-2023].

[41] H. Vedova and T. F. T. C. O. of Technology, “Gramm-Leach-Bliley Act,” *Federal Trade Commission*, 31-Mar-2023. [Online]. Available: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act. [Accessed: 05-May-2023].

[42] “ELECTION INFRASTRUCTURE SECURITY RESOURCE GUIDE ,” *cisa.gov*, Sep-2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/cisa_election-security-resources-guide-Sept-2020_0.pdf. [Accessed: 06-May-2023].

[43] “Cyber incident reporting for critical infrastructure act of 2022 (CIRCIA): CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, 2022. [Online]. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia. [Accessed: 05-May-2023].

[44] M. Fagan, K. Megas, K. Scarfone, and M. Smith, “Foundational cybersecurity activities for IOT device manufacturers,” *CSRC*, 29-May-2020. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8259/final. [Accessed: 05-May-2023].

[45] “S.2593 - 115th Congress (2017-2018): Secure Elections Act,” *congress.gov*, 22-Mar-2018. [Online]. Available: https://www.congress.gov/bill/115th-congress/senate-bill/2593. [Accessed: 06-May-2023].

[46] “S.1540 - 116th congress (2019-2020): Election security act of 2019,” *congress.gov*, 16-May-2019. [Online]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/1540. [Accessed: 06-May-2023].

[47] “H.R.9259 - Cybersecurity Skills Integration Act - Congress.gov,” *congress.gov*, 31-Oct-2022. [Online]. Available: https://www.congress.gov/bill/117th-congress/house-bill/9259?s=1&r=1. [Accessed: 06-May-2023].