

Impacts of Cyber Security on Geopolitics Nabib Bin Zahid¹



Source: iStock by Getty Images

Introduction

In the contemporary landscape of international relations, cyber security has emerged as a critical factor influencing geopolitics. As nations increasingly rely on digital infrastructure for economic stability and national security, the vulnerabilities associated with cyber threats have profound implications for state behavior and diplomatic interactions. Cyber security encompasses the protection of computer systems and networks from information theft, damage, and disruption, making it a pivotal element in the strategic calculus of nations.³

¹ Nabib Bin Zahid is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). He has completed his B.S.S in International Relations from the University of Rajshahi.

² [Global Communication Network](#)

³ Singer, P. W., & Friedman, A. (2014). *Cyber security and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

The intersection of cyber security and geopolitics is underscored by a series of high-profile cyber incidents that have reshaped global power dynamics. Events such as the Stuxnet attack on Iran's nuclear facilities and the Russian interference in the 2016 U.S. elections exemplify how cyber operations can serve as tools of statecraft, altering the balance of power and challenging traditional notions of warfare.⁴ As cyber capabilities continue to evolve, they not only pose risks to national security but also influence alliances, economic relations, and public perception of governments.

Understanding the implications of cyber security on geopolitics is essential for policymakers and scholars alike. It necessitates a comprehensive examination of how cyber threats are integrated into national strategies and how they affect international cooperation and conflict. As the digital realm becomes increasingly contested, the interplay between cyber security and geopolitics will undoubtedly shape the future of global interactions.

Historical Context

The historical trajectory of cyber security within the realm of geopolitics is marked by significant events that have shaped both state behavior and international relations. One of the earliest examples of state-sponsored cyber operations occurred with the Stuxnet worm, which was designed to disrupt Iran's nuclear program in 2010. This sophisticated cyber-attack not only demonstrated the potential of cyber capabilities in achieving strategic objectives but also marked a turning point in how nations approach warfare.⁵ Stuxnet illustrated that cyber warfare could effectively target critical infrastructure, raising questions about the legality and ethical implications of such actions in international law.

Following Stuxnet, the rise of cyber espionage became increasingly evident, particularly with state actors like Russia and China employing cyber tactics to gain economic and military advantages. The 2015 breach of the U.S. Office of Personnel Management, attributed to Chinese hackers, compromised the sensitive information of millions of federal employees and highlighted the vulnerabilities inherent in national cyber security (US-CERT, 2015)⁶. Such incidents not only

⁴ Lindsay, J. R. (2013). Stuxnet and the Future of Cyber War. *The Washington Quarterly*, 36(2), 45-60. Rid, T. (2013). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5-32.

⁵ Lindsay, J. R. (2013). Stuxnet and the Future of Cyber War. *The Washington Quarterly*, 36(2), 45-60.

⁶ US-CERT. (2015). Data Breach at the U.S. Office of Personnel Management. Retrieved from US-CERT.

underscore the risks associated with cyber vulnerabilities but also reflect a growing trend where nations leverage cyber capabilities to conduct espionage, thereby influencing geopolitical power dynamics.

Moreover, the 2016 U.S. presidential elections serve as a critical case study in the geopolitical implications of cyber security. Russian interference, primarily through social media manipulation and hacking operations, exposed the fragility of democratic processes and raised alarms about the integrity of electoral systems globally.⁷ This event catalyzed discussions about the need for enhanced cyber security measures and reinforced the idea that cyber operations can serve as a means of geopolitical influence, blurring the lines between traditional warfare and modern conflict.

The evolution of non-state actors, such as hacktivist groups, further complicates the cyber security landscape. Groups like Anonymous have utilized cyber tactics to challenge state authority and advocate for political causes, illustrating how non-state actors can impact geopolitical narratives. Their actions often intersect with state interests, creating a complex web of motivations and implications for international relations.⁸

The historical context of cyber security within geopolitics reveals a landscape shaped by significant events and evolving threats. As cyber capabilities continue to advance, understanding this historical trajectory is crucial for comprehending the current challenges and dynamics in international relations.

The Geopolitical Dynamics of Cybersecurity

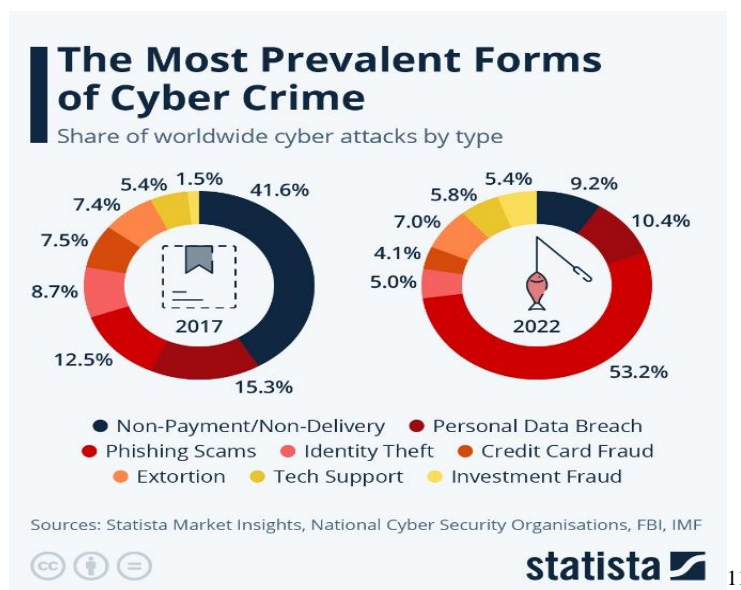
The current landscape of cyber security is characterized by a complex interplay among major global actors, particularly the United States, China, and Russia, each applying distinct strategies to enhance their cyber capabilities while engaging in cyber operations against one another. This rivalry not only reflects broader geopolitical tensions but underscores the growing significance of cyber security as a strategic asset.

The United States has positioned itself as a leader in cyber security, significantly investing in both defensive and offensive capabilities. The establishment of U.S. Cyber Command (USCYBERCOM) in 2010 marked a pivotal shift in military strategy, recognizing cyberspace as

⁷ Mueller, R. S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. U.S. Department of Justice.

⁸ Denning, D. E. (2015). The Ethics of Cyber Conflict. *Journal of Military Ethics*, 14(1), 1-20.

a domain of warfare.⁹ Recent U.S. cyber security policies emphasize deterrence and proactive measures. The 2021 Executive Order on Improving the Nation's Cyber Security aimed to fortify federal cyber security defenses following high-profile incidents such as the SolarWinds cyber-attack, which exposed vulnerabilities across multiple government agencies and private sectors. Additionally, the 2021 Colonial Pipeline ransomware attack disrupted fuel supplies across the Eastern U.S., prompting discussions on the need for enhanced resilience against cyber threats.¹⁰



Source: Statista

China, conversely, adopts an assertive approach to cyber security, viewing it as essential to national security and economic advancement. The Chinese government has been implicated in numerous cyber espionage operations aimed at acquiring intellectual property and sensitive data from foreign entities. For instance, the Microsoft Exchange Server hack in early 2021, attributed to a Chinese state-sponsored group, compromised thousands of organizations globally, further illustrating China's aggressive cyber tactics. Moreover, China's 2020 Cyber Security Law emphasizes state control over the internet while promoting the development of domestic technologies to reduce reliance on foreign systems.¹²

⁹ <https://www.washingtonpost.com/news/checkpoint/wp/2017/08/18/president-trump-announces-move-to-elevate-cyber-command/>

¹⁰ <https://www.cnn.com/2021/05/10/politics/colonial-ransomware-attack-explainer>

¹¹ <https://cdn.statcdn.com/Infographic/images/normal/30870.jpeg>

¹² Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Russia's cyber security strategy is characterized by a combination of offensive operations and disinformation campaigns. The Russian government has utilized cyber capabilities to influence elections and create discord, as seen in the 2020 U.S. presidential elections, where Russian interference was again reported.¹³ The 2021 ransomware attack on the JBS meat processing plant, attributed to a Russian cybercriminal group, underscored the threats posed by ransomware and the geopolitical implications of cybercrime.¹⁴ Such incidents reflect Russia's broader hybrid warfare strategy, blending cyber operations with traditional military tactics.

The rise of non-state actors further complicates the cyber security landscape. Groups such as REvil and other ransomware syndicates have demonstrated the ability to disrupt critical infrastructure, often operating with relative impunity. The 2021 Kaseya attack, which affected numerous businesses worldwide, exemplifies the pervasive threat posed by organized cyber criminals. Their actions not only challenge state authority but also strain international relations, as nations grapple with the need for coordinated responses to these evolving threats.

The contemporary cyber security landscape is defined by state actors' strategies and the disruptive actions of non-state entities. As geopolitical tensions rise, the implications for international relations will grow, highlighting the need for a nuanced understanding of this critical field.

Strategic Approaches to Cyber security Amid Geopolitical Turbulence

The future of cyber security is poised to be profoundly influenced by evolving technological advancements, shifting geopolitical dynamics, and the increasing interdependence of global systems. As nations enhance their cyber capabilities, the importance of establishing robust international norms and collaborative frameworks becomes critical to mitigate threats and foster stability in the digital domain.

One of the foremost challenges facing the cybersecurity landscape is the rapid pace of technological innovation. Emerging technologies such as artificial intelligence (AI) and quantum computing present both opportunities and vulnerabilities. AI can enhance threat detection and response capabilities, yet it also enables more sophisticated cyber-attacks. Incidents, such as the use of AI-driven phishing attacks, exemplify how adversaries can exploit these advancements to

¹³ Mueller, R. S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. U.S. Department of Justice.

¹⁴ <https://www.cbsnews.com/news/jbs-ransom-11-million/>

deceive and manipulate targets. As such, nations must prioritize the development of resilient systems that can adapt to these emerging threats.

Geopolitical tensions will further shape the future of cyber security. The ongoing rivalry between the U.S. and China, particularly in the realms of technology and trade, has significant implications for cyber security policies. The U.S. has increasingly sought to counter China's influence through initiatives like the Clean Network program, aimed at securing telecom infrastructure and protecting sensitive data from foreign adversaries.¹⁵ As these tensions escalate, the potential for cyber conflict between major powers remains a pressing concern, necessitating proactive measures to prevent miscalculations and escalation.

Furthermore, the rise of ransomware attacks poses a critical challenge to global security. High-profile incidents, such as the Colonial Pipeline and JBS attacks, have underscored the vulnerabilities in critical infrastructure and the economic implications of cybercrime.¹⁶ Governments are increasingly recognizing the need for public-private partnerships to enhance resilience and response capabilities. The establishment of frameworks that facilitate information sharing and collaboration among stakeholders will be essential in addressing the evolving threat landscape.

International norms and agreements will also play a crucial role in shaping the future of cyber security. Efforts to create a global framework for responsible state behavior in cyberspace, such as the United Nations discussions on cyber security norms, are gaining traction.¹⁷ These initiatives aim to establish guidelines that promote stability and reduce the likelihood of cyber conflicts. However, achieving consensus among nations with differing interests remains a formidable challenge.

The future of cyber security is intricately linked to technological advancements, geopolitical dynamics, and the need for international cooperation. As nations navigate this complex landscape, developing adaptive strategies and fostering collaborative frameworks will be essential to enhance security and stability in the digital domain.

¹⁵ <https://2017-2021.state.gov/the-clean-network/>

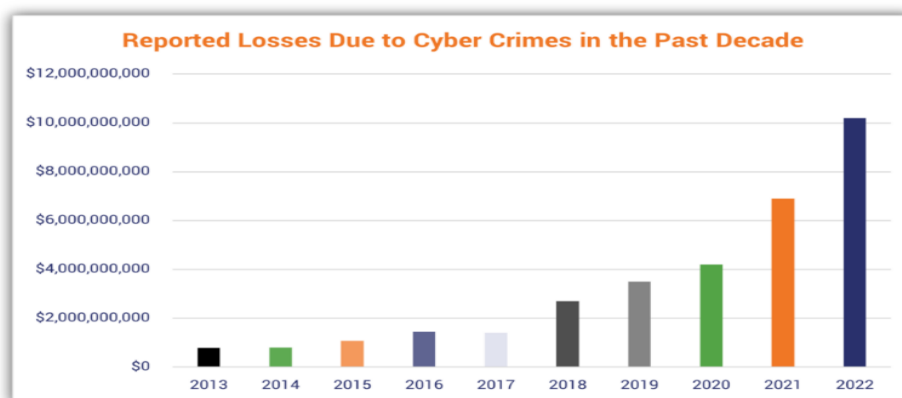
¹⁶ <https://www.cnn.com/2021/05/10/politics/colonial-ransomware-attack-explainer>,
<https://www.cbsnews.com/news/jbs-ransom-11-million/>

¹⁷ UN. (2021). "Developments in the Field of Information and Telecommunications in the Context of International Security." Retrieved from un.org

The Role of International Cooperation in Cybersecurity

International cooperation is essential for addressing the multifaceted challenges posed by cybersecurity threats. As cyber-attacks increasingly transcend national borders, collaborative efforts among nations, organizations, and private sectors become crucial to enhancing collective security and resilience.

Recent incidents highlight the urgent need for such cooperation. The 2020 SolarWinds cyber-attack, attributed to Russian state-sponsored actors, compromised numerous U.S. government agencies and private companies, revealing vulnerabilities in supply chain security. This incident underscored the interconnected nature of global cyber security, prompting calls for a unified international response to mitigate similar threats in the future.



18

Source: The SSL Store

One significant initiative aimed at fostering international collaboration is the Global Forum on Cyber Expertise (GFCE). Established in 2015, the GFCE seeks to enhance global Cyber security capacity through cooperation and knowledge sharing among countries and organizations.¹⁹ By facilitating dialogue and promoting best practices, the GFCE aims to build a more resilient global cyber ecosystem.

Moreover, the European Union's Cyber Security Strategy for the Digital Decade emphasizes the importance of collaboration among member states and with international partners. The strategy outlines initiatives to strengthen cyber security resilience and response capabilities, including the

¹⁸ <https://www.thessslstore.com/blog/wp-content/uploads/2023/10/cybercrime-statistics-reported-losses-past-decade-1024x618.png>

¹⁹ GFCE. (2021). "Global Forum on Cyber Expertise." Retrieved from gfce.org.

establishment of the European Cyber Security Agency (ENISA) to support cross-border cooperation.²⁰ Such frameworks are vital for addressing threats that often originate from outside national jurisdictions.

Another notable example of international cooperation is the Budapest Convention on Cybercrime, which provides a framework for countries to collaborate in combating cybercrime. As of 2023, 66 countries have ratified the convention, enabling law enforcement agencies to work together more effectively in investigating and prosecuting cybercriminals.²¹ This treaty highlights the necessity of legal frameworks that facilitate cooperation across borders in the digital space.

However, achieving effective international collaboration in cyber security is fraught with challenges. Differing national interests, regulatory frameworks, and levels of technological advancement can hinder cooperative efforts. The geopolitical rivalry between major powers, particularly the U.S. and China, complicates the establishment of unified cyber security norms, as both nations often pursue conflicting strategies. The role of international cooperation in Cyber security is paramount in addressing the evolving landscape of threats. By fostering collaboration through existing frameworks and developing new initiatives, nations can enhance their collective security and resilience against cyber threats.

Emerging Trends in Cybersecurity

Emerging trends in cybersecurity reflect the growing sophistication of threats and the need for innovative solutions. The rise of zero trust architecture emphasizes continuous verification of users and devices, mitigating risks from internal and external threats.²² Additionally, the integration of artificial intelligence in threat detection enhances response times and predictive capabilities. Furthermore, the increasing prominence of ransomware as a service (RaaS) underscores the democratization of cybercrime, making it accessible to a broader range of attackers.²³ These trends necessitate adaptive strategies for organizations to remain resilient.

²⁰ European Commission. (2020). "EU Cyber security Strategy for the Digital Decade." Retrieved from ec.europa.eu.

²¹ Council of Europe. (2023). "Convention on Cybercrime." Retrieved from coe.int

²² Rose, S., et al. (2020). "Zero Trust Architecture." NIST Special Publication 800-207.

²³ FBI. (2021). "Ransomware as a Service." Retrieved from [FBI.gov](https://fbi.gov).

Conclusion

In an era marked by rapid technological advancements and escalating geopolitical tensions, the imperative for robust cyber security measures has never been more critical. As cyber threats evolve in sophistication and scale, nations must prioritize international cooperation to establish a cohesive defense framework. The interplay between state and non-state actors highlights the necessity for adaptive strategies that address both current vulnerabilities and emerging risks. Initiatives such as the Global Forum on Cyber Expertise and the Budapest Convention provide essential platforms for collaboration, yet challenges remain in aligning diverse national interests and regulatory environments. By fostering a culture of shared responsibility and resilience, countries can mitigate potential cyber threats and enhance global stability. Ultimately, a unified approach to cyber security not only protects individual nations but also strengthens the international community against the pervasive and evolving landscape of cyber threats. Embracing this collaborative ethos is essential for securing a safer digital future.