E-ISSN: 2997-948X

SemantJournals

American Journal of Religious, Culture, and Archaeological Studies

https://semantjournals.org/index.php/AJRCAS

| Research Article

Cybersecurity as a Pillar of National Security in International Affairs

Maisha Karim

UCSI University, Bangladesh Branch Campus

maishakarim@ucsiuniversity.edu.my

Abstract: The rapid evolution of the digital landscape has elevated cybersecurity to a critical component of national security and a pivotal factor in international relations. This paper explores the role of cybersecurity as a pillar of national security, analyzing its influence on protecting critical infrastructure, safeguarding sovereignty, and shaping geopolitical dynamics. Through a multidisciplinary approach combining security studies and international relations theories, the research highlights the increasing complexity of cyber threats such as espionage, cyberwarfare, and cyberterrorism, which transcend national borders and demand collaborative international responses. The paper also examines the role of cyber diplomacy and global cooperation in addressing these challenges while highlighting the need for clear norms, policies, and trust-building measures. By emphasizing the intersection of cybersecurity and geopolitics, this study provides insights into strategic policy recommendations for enhancing cybersecurity frameworks at national and international levels. The findings underscore the necessity of a proactive and cooperative approach to secure a stable global digital ecosystem.

Keywords: Cybersecurity, National Security, International Relations.

Introduction

In the 21st century, cybersecurity has emerged as an indispensable component of national security, reshaping the ways in which nations safeguard their sovereignty and infrastructure. As societies become increasingly reliant on digital technologies, the potential for cyber threats to disrupt critical systems has grown exponentially. The interconnected nature of global networks means that cybersecurity breaches can have cascading effects across borders, making it a critical focus for international relations (Singer & Friedman, 2014). Unlike traditional threats, cyber threats are invisible, often state-sponsored, and difficult to attribute, presenting unique challenges to national and international security frameworks.

Cybersecurity threats have evolved from simple hacking attempts to complex cyberwarfare tactics involving espionage, sabotage, and disinformation campaigns. Prominent incidents, such as the 2017 WannaCry ransomware attack and the alleged interference in elections through cyber means, illustrate the growing sophistication and impact of these threats (Healey, 2013). The increasing integration of critical infrastructures—such as energy grids, financial systems, and defense networks—with digital technologies further amplifies the risk. For instance, cyberattacks on power grids or financial institutions can destabilize economies and undermine public trust in governance.

Despite the growing recognition of cybersecurity as a strategic priority, many nations struggle to integrate it effectively into their national security doctrines. Internationally, the absence of universally accepted norms and rules governing state behavior in cyberspace has led to a fragmented approach to cybersecurity governance. This lack of cohesion creates vulnerabilities and raises the potential for miscalculation or escalation in cyber conflicts (Nye, 2020). These gaps underscore the need for robust cybersecurity frameworks that address both national and international dimensions.

Hence, this paper seeks to analyze the role of cybersecurity as a cornerstone of national security and its implications for international affairs. It aims to:

1. Examine the integration of cybersecurity into national security strategies
2. Investigate the geopolitical consequences of cyber threats and cyber diplomacy
3. Propose actionable recommendations for strengthening cybersecurity governance at both national and international levels.

Literature Review

Historical Perspective on Cybersecurity in National Security

The integration of cybersecurity into national security paradigms has its roots in the late 20th century when the proliferation of information technology began reshaping defense strategies. The foundational work of scholars like Libicki (1995) highlighted how the digital revolution necessitated a reevaluation of traditional security frameworks, emphasizing the vulnerabilities created by interconnected networks. Over the years, incidents such as the 2007 cyberattacks on Estonia and the Stuxnet operation targeting Iranian nuclear facilities demonstrated the disruptive potential of cyber threats, elevating cybersecurity as a priority in national defense strategies (Rid, 2012). These events marked the transition of cybersecurity from a technical issue to a critical aspect of statecraft and international diplomacy.

Cybersecurity in Contemporary National Security Strategies

Modern national security policies increasingly recognize cybersecurity as a cornerstone of strategic planning. Governments have adopted comprehensive cybersecurity strategies, encompassing the protection of critical infrastructure, countering cyber terrorism, and preparing for cyberwarfare. For instance, the United States has institutionalized cybersecurity through initiatives like the Cybersecurity and Infrastructure Security Agency (CISA) and the European Union has adopted the NIS Directive to ensure network and information security across member states (Lewis, 2018). However, scholars such as Clarke and Knake (2010) argue that despite these advances, many nations remain reactive rather than proactive, leaving critical vulnerabilities unaddressed.

Theoretical Insights into Cybersecurity and International Relations

Cybersecurity's role in international relations is often analyzed through established theoretical lenses. Realist perspectives emphasize the use of cyber capabilities to project power and deter adversaries, treating cyberspace as another domain for geopolitical competition (Waltz, 2010). Conversely, liberal theories highlight the potential for international cooperation to establish norms and rules for cyberspace, as seen in initiatives like the Budapest Convention on Cybercrime (Nye, 2020). Constructivist scholars focus on the social construction of cyber norms and the role of identity and shared values in shaping state behavior in cyberspace (Tikk-Ringas, 2015). These theoretical insights provide a robust foundation for understanding the multifaceted role of cybersecurity in international affairs.

Challenges and Gaps in Existing Research

Despite growing scholarly interest, several gaps persist in the literature on cybersecurity and national security. First, there is limited empirical research on the long-term effectiveness of cyber deterrence strategies, given the challenges of attribution and escalation (Healey, 2013). Second, the lack of universal norms governing cyberspace has led to fragmented and often contradictory approaches to cybersecurity governance (Singer & Friedman, 2014). Additionally, emerging threats such as artificial intelligence-driven cyberattacks and quantum computing are insufficiently explored in the context of international security (Brunner & Suter, 2009). These gaps underscore the need for interdisciplinary research to address the evolving cyber threat landscape.

Significance of Cybersecurity in International Affairs

The literature underscores that cybersecurity is no longer confined to the realm of national policy but is an integral part of international affairs. Cyber threats often transcend national borders, necessitating coordinated global responses. For instance, initiatives like the United Nations Group of Governmental Experts (UNGGE) and the Global Forum on Cyber Expertise (GFCE) highlight the importance of multilateral collaboration in addressing cybersecurity challenges (Lewis, 2018). However, as Nye (2020) notes, geopolitical rivalries and conflicting interests often hinder such efforts, leaving the global digital ecosystem vulnerable to exploitation.

Theoretical Framework

Security Studies and Cybersecurity

Security studies provide a foundational lens through which the role of cybersecurity in national and international security can be understood. Traditional security paradigms focused on physical threats such as military aggression and territorial disputes. However, the advent of cyberspace has expanded these frameworks to include non-traditional security concerns, including cyber threats (Collins, 2016). Cybersecurity, as a subset of these broader frameworks, emphasizes the protection of critical digital infrastructure and the prevention of malicious cyber activities that can undermine state stability. The Copenhagen School's securitization theory is particularly relevant, as it posits that issues like cybersecurity can be elevated to matters of existential threat, thereby justifying extraordinary measures by states (Buzan, Wæver, & De Wilde, 1998). This theoretical perspective underlines how cybersecurity has been integrated into national security doctrines as a matter of urgency.

Methodology

Realism and the Pursuit of Cyber Power

Realist theories of international relations focus on power dynamics and competition among states, providing a valuable perspective on cybersecurity. In this view, cyberspace is another domain for exercising power, akin to land, sea, air, and space (Waltz, 2010). Realists argue that cyber capabilities can be used to deter adversaries, project power, and gain strategic advantages. States are incentivized to develop offensive and defensive cyber capabilities to protect their interests and counter potential threats. For example, the United States' creation of Cyber Command (USCYBERCOM) exemplifies the realist emphasis on building cyber power to maintain dominance in this critical domain (Healey, 2013). Realist scholars also highlight the risks of escalation and cyber arms races, as states continuously enhance their capabilities to outpace rivals.

Liberalism and Cyber Cooperation

Liberal theories emphasize the potential for cooperation and interdependence in addressing cybersecurity challenges. Cyberspace, as a global commons, requires collaborative governance to ensure stability and security (Keohane & Nye, 2012). Liberalism highlights the role of international institutions and agreements, such as the Budapest Convention on Cybercrime, in fostering collective action and reducing risks. Moreover, the interconnected nature of global networks makes unilateral approaches insufficient, necessitating multilateral frameworks to establish norms and rules for state behavior in cyberspace (Nye, 2020). Liberals also stress the importance of trust-building measures and transparency in mitigating cyber conflicts and enhancing global stability.

Constructivism and Cyber Norms

Constructivist approaches provide an alternative lens by focusing on the social construction of norms, identities, and shared understandings in cyberspace. Constructivists argue that states' behaviors in cyberspace are shaped not only by material capabilities but also by ideas, norms, and identities (Tikk-Ringas, 2015). For instance, efforts by the United Nations Group of Governmental Experts (UNGGE) to establish norms of responsible state behavior in cyberspace reflect constructivist principles. These norms, such as refraining from targeting critical infrastructure during peacetime, are designed to create a shared understanding of acceptable conduct (Lewis, 2018). Constructivist scholars also emphasize the importance of non-state actors, such as tech companies and civil society, in shaping the governance of cyberspace.

Integrated Approach to Cybersecurity

Given the complexity of cyberspace, a single theoretical lens is often insufficient to fully capture the multifaceted role of cybersecurity in national and international security. An integrated approach that draws on insights from security studies, realism, liberalism, and constructivism offers a more comprehensive understanding. While realism highlights the competitive aspects of cyber capabilities, liberalism and constructivism underscore the importance of collaboration and normative frameworks. This synthesis allows policymakers and scholars to address the dual challenges of cyber conflict and cooperation effectively.

Key Issues in Cybersecurity and National Security

The Expanding Cyber Threat Landscape

Cyber threats have become increasingly sophisticated, diverse, and disruptive, posing significant challenges to national security. Modern cyberattacks range from ransomware and data breaches to advanced persistent threats (APTs) targeting critical infrastructure. For example, the 2017 WannaCry ransomware attack affected over 200,000 systems across 150 countries, causing widespread disruptions in healthcare and transportation sectors (Kshetri, 2018). Similarly, the SolarWinds attack in 2020 demonstrated the ability of state-sponsored actors to infiltrate supply chains and compromise sensitive government networks (Lewis, 2021). The scale and complexity of these threats highlight the urgency of developing robust cybersecurity defenses to protect national assets and citizens.

Critical Infrastructure Vulnerabilities

Critical infrastructure, including energy grids, financial systems, healthcare networks, and defense systems, is increasingly dependent on digital technologies. This interdependence makes them attractive targets for cyberattacks, as disruptions can have catastrophic consequences for national stability. For instance, the 2021 Colonial Pipeline ransomware attack in the United States disrupted fuel supplies across the East Coast, underscoring the vulnerabilities of critical infrastructure to cyber threats (Perlroth, 2021). Governments worldwide are implementing measures to address these risks, such as the European Union's NIS Directive, which mandates cybersecurity measures for essential services (European Commission, 2020). However, the lack of standardized practices and coordination across sectors remains a significant challenge.

Cyber Sovereignty and Jurisdictional Challenges

Cybersecurity raises complex issues related to state sovereignty and jurisdiction in the digital age. Cyberattacks often originate from one country and target another, creating legal and diplomatic challenges in attribution and response. The principle of cyber sovereignty, which emphasizes a state's control over its digital space, often conflicts with the transnational nature of cyberspace (Chander, 2017). Countries like China and Russia advocate for cyber sovereignty to justify restrictive internet governance policies, while others argue for a more open and collaborative approach (Nye, 2020). This divergence hampers the establishment of global norms and regulations, leaving cyberspace as a contested domain.

Cyber Deterrence and Attribution

Unlike conventional warfare, where the origins of attacks are often identifiable, the anonymity of cyberspace makes attribution a significant challenge. The difficulty of accurately attributing cyberattacks complicates the implementation of deterrence strategies, as states may hesitate to retaliate without concrete evidence of responsibility (Rid & Buchanan, 2015). Cyber deterrence also requires capabilities that balance defensive measures with offensive readiness, a controversial approach that raises ethical and legal concerns. For example, the Stuxnet attack on Iran's nuclear facilities showcased the effectiveness of offensive cyber operations but also set a precedent for future cyber conflicts (Farwell & Rohozinski, 2011).

Emerging Technologies and Cyber Threats

The rapid development of emerging technologies, such as artificial intelligence (AI), quantum computing, and the Internet of Things (IoT), introduces new dimensions to cybersecurity threats. AI-driven cyberattacks can enhance the speed and precision of attacks, while IoT devices create an expanded attack surface for adversaries (Kshetri, 2021). Quantum computing, once fully realized, has the potential to break current encryption standards, rendering traditional cybersecurity measures obsolete (Mosca, 2018). Policymakers and researchers must address these emerging threats by investing in innovation and anticipating future vulnerabilities.

Global Collaboration and Governance Challenges

The transnational nature of cyberspace necessitates global collaboration to address cybersecurity challenges effectively. Initiatives such as the Budapest Convention on Cybercrime and the United Nations' Group of Governmental Experts (UNGGE) aim to establish international norms and frameworks for responsible state behavior in cyberspace (Lewis, 2018). However, geopolitical rivalries, differing priorities, and conflicting views on cyber sovereignty hinder progress toward cohesive governance. For instance, while Western nations emphasize the importance of openness and cooperation, authoritarian regimes advocate for stricter controls over cyberspace (Chander, 2017). Bridging these divides is essential to achieving a secure and stable global digital environment.

Cybersecurity in International Affairs

Cyber Diplomacy and Multilateral Cooperation

Cybersecurity has become a critical issue in international diplomacy, with states increasingly engaging in multilateral efforts to address cross-border cyber threats. Institutions such as the United Nations and regional organizations like the European Union have taken steps to foster dialogue and cooperation in cyberspace. For instance, the United Nations Group of Governmental Experts (UNGGE) has sought to establish norms of responsible state behavior in cyberspace, including commitments to refrain from targeting critical infrastructure during peacetime (Nye, 2020). Similarly, the Budapest Convention on Cybercrime serves as a framework for international collaboration in combatting cybercrime, although it faces criticism from nations outside its framework, such as Russia and China, for reflecting Western-centric values (Chander, 2017). Despite these efforts, geopolitical rivalries and conflicting interests often undermine the progress of cyber diplomacy.

Result

Geopolitics and Cyber Power Dynamics

Cyberspace has become a battleground for geopolitical competition, with states leveraging cyber capabilities to assert dominance and influence. Nations such as the United States, China, and Russia have developed sophisticated offensive and defensive cyber strategies, reflecting the realist view of cyberspace as a domain for power projection (Waltz, 2010). Cyber espionage and cyberattacks are increasingly used as tools of statecraft to achieve strategic objectives without engaging in conventional warfare. Notable examples include allegations of election interference by Russia in the United States and the use of cyber tools by China to access intellectual property from Western firms (Lewis, 2021). These actions exacerbate tensions among major powers and raise the stakes for conflict in the cyber domain.

Challenges in Establishing Cyber Norms

The establishment of global norms for cybersecurity governance has proven to be a complex and contentious process. While there is broad agreement on the need for rules governing state behavior in cyberspace, significant differences remain regarding their scope and enforcement. Western nations generally advocate for open and transparent cyberspace governance, emphasizing human rights and the free flow of information. In contrast, authoritarian regimes prioritize cyber sovereignty, which allows for greater state control over internet activities within their borders (Chander, 2017). This ideological divide hinders the development of universal norms, leaving the global digital ecosystem vulnerable to fragmentation and exploitation.

Global Cybersecurity Cooperation and Trust-Building

Efforts to foster global cybersecurity cooperation face numerous challenges, particularly in the areas of trust-building and accountability. Trust deficits among states, fueled by frequent allegations of state-sponsored cyberattacks, make it difficult to achieve meaningful agreements (Rid & Buchanan, 2015). Initiatives such as confidence-building measures (CBMs) aim to address this issue by promoting transparency and communication among nations. For example, the Organization for Security and Co-operation in Europe (OSCE) has implemented CBMs to reduce the risk of misunderstandings and escalation in the cyber domain (Lewis, 2018). However, the success of these initiatives depends on the willingness of states to prioritize collective security over individual strategic advantages.

The Role of Non-State Actors in Cybersecurity Governance

Non-state actors, including technology companies, non-governmental organizations, and academic institutions, play a crucial role in shaping cybersecurity governance. These entities often possess the technical expertise and resources necessary to address complex cyber challenges. For instance, tech giants like Microsoft and Google have advocated for global cybersecurity standards and invested in securing critical digital infrastructure (Bradshaw & DeNardis, 2018). Additionally, multi-stakeholder initiatives, such as the Global Forum on Cyber Expertise (GFCE), bring together governments, private sector actors, and civil society to share knowledge and promote best practices (Nye, 2020). However, the inclusion of diverse stakeholders also introduces challenges in balancing competing interests and ensuring equitable decision-making.

Cybersecurity as a Catalyst for International Stability

Despite the challenges, cybersecurity has the potential to serve as a catalyst for international stability when approached collaboratively. Establishing norms, enhancing capacity-building efforts, and promoting trust among nations can mitigate the risks of cyber conflict and foster a more secure global digital environment. Initiatives such as the Paris Call for Trust and Security in Cyberspace demonstrate the potential for inclusive and cooperative approaches to cybersecurity governance (Lewis, 2021). As cyberspace continues to evolve, the need for innovative and adaptable strategies to address its challenges will remain paramount.

Policy Implications and Recommendations

Strengthening National Cybersecurity Strategies

Governments must adopt proactive measures to enhance their national cybersecurity frameworks. This includes investing in advanced technologies, such as artificial intelligence (AI) and quantum-resistant encryption, to counter emerging threats (Kshetri, 2021). Public-private partnerships are essential for securing critical infrastructure, as the private sector owns and operates much of the digital infrastructure in many countries. For example, initiatives like the U.S. Cybersecurity and Infrastructure Security Agency (CISA) demonstrate the benefits of collaboration between government agencies and private companies to address vulnerabilities and respond to incidents (Perlroth, 2021). Governments should also prioritize workforce development to address the global shortage of cybersecurity professionals, which remains a critical bottleneck in implementing effective security measures.

Discussion

Promoting International Cyber Norms and Agreements

The establishment of global cyber norms is essential for reducing the risk of conflicts and ensuring responsible state behavior in cyberspace. Policymakers should work through international platforms such as the United Nations, the G20, and regional organizations to build consensus on issues such as prohibiting cyberattacks on critical infrastructure and ensuring the integrity of global supply chains (Nye, 2020). Efforts like the Budapest Convention on Cybercrime provide a useful starting point for addressing cybercrime, though its adoption must be broadened to include non-signatory states like China and Russia (Chander, 2017). Developing a universally accepted framework for cyber attribution will also improve accountability and deter malicious actors.

Enhancing Cyber Diplomacy

Cyber diplomacy should be prioritized as a core element of international relations to mitigate geopolitical tensions and foster trust among nations. Confidence-building measures (CBMs), such as regular communication channels and joint cyber exercises, can reduce the risk of misunderstandings and escalation in cyber conflicts (Rid & Buchanan, 2015). Additionally, states should establish bilateral and multilateral agreements to promote transparency in cyber operations and share intelligence on emerging threats. For instance, the European Union’s cybersecurity cooperation mechanisms offer a model for enhancing information sharing and aligning cybersecurity policies across nations (European Commission, 2020).

Developing Resilient Critical Infrastructure

Policymakers must focus on improving the resilience of critical infrastructure to withstand and recover from cyberattacks. This includes conducting regular vulnerability assessments, implementing stringent security protocols, and adopting advanced monitoring systems to detect potential threats in real time (Lewis, 2018). Governments should also incentivize private sector investments in cybersecurity through tax benefits and grants, ensuring that even small and medium-sized enterprises (SMEs) have the resources to protect their systems. Furthermore, national incident response plans must be regularly updated and tested to ensure readiness in the face of large-scale cyber incidents.

Integrating Emerging Technologies into Cybersecurity

Emerging technologies such as AI, blockchain, and quantum computing offer both opportunities and challenges for cybersecurity. Policymakers should invest in research and development to harness these technologies for enhancing security while addressing their potential risks. For instance, AI can improve threat detection through predictive analytics, but it also raises concerns about AI-driven cyberattacks (Kshetri, 2021). Quantum computing's potential to break current encryption standards underscores the urgency of developing quantum-resistant cryptographic methods (Mosca, 2018). Governments and research institutions must collaborate to ensure that technological advancements contribute to a secure and stable digital ecosystem.

Addressing Global Cybersecurity Inequality

Cybersecurity capacity varies significantly across nations, with many developing countries lacking the resources and expertise needed to address cyber threats. International organizations and developed nations should prioritize capacity-building initiatives to bridge this gap. Programs like the Global Forum on Cyber Expertise (GFCE) provide technical training, funding, and policy guidance to enhance cybersecurity capabilities in under-resourced regions (Nye, 2020). Ensuring equitable access to cybersecurity tools and knowledge will not only protect vulnerable nations but also strengthen global cybersecurity resilience as a whole.

Encouraging a Multistakeholder Approach

Given the complexity of cybersecurity challenges, a multistakeholder approach involving governments, private companies, academia, and civil society is essential. Policymakers should create inclusive forums that allow diverse voices to contribute to cybersecurity governance. Non-state actors, such as technology companies, play a critical role in implementing security measures and advocating for global standards (Bradshaw & DeNardis, 2018). Encouraging collaboration across sectors will result in more comprehensive and effective policies that address the multifaceted nature of cybersecurity threats.

Conclusion

The integration of cybersecurity into national security and international affairs reflects the growing significance of the digital realm in contemporary geopolitics. As cyber threats become more sophisticated and widespread, they present challenges that transcend national borders, affecting critical infrastructure, state sovereignty, and global stability. This paper has highlighted the multifaceted nature of cybersecurity, emphasizing its role as both a source of conflict and a potential avenue for collaboration among nations. Key findings underscore the necessity of proactive and comprehensive strategies to address cyber threats. At the national level, governments must invest in advanced technologies, foster public-private partnerships, and develop resilient critical infrastructure to mitigate vulnerabilities. Internationally, the establishment of norms, trust-building measures, and multilateral cooperation is essential for fostering a secure and stable global digital ecosystem. Emerging technologies such as artificial intelligence, blockchain, and quantum computing present both opportunities and challenges, necessitating innovative approaches to cybersecurity governance. Moreover, addressing global disparities in cybersecurity capacity is crucial for ensuring that all nations, regardless of their resources, are equipped to defend against cyber threats. While significant obstacles remain, including geopolitical rivalries and differing views on cyber sovereignty, the path forward lies in collaborative and inclusive policymaking. By embracing a multistakeholder approach and prioritizing transparency and accountability, the international community can navigate the complexities of cyberspace and create a foundation for peace and security in the digital age. Ultimately, cybersecurity is not just a technical challenge but a strategic imperative that demands coordinated action at all levels. The recommendations outlined in this paper aim to guide policymakers, scholars, and practitioners in addressing these pressing challenges and harnessing the potential of cybersecurity as a pillar of national and international security. Through sustained efforts, a resilient and cooperative global digital environment can be achieved, benefiting nations and individuals alike.

References

1. Buzan, B., Wæver, O. and De Wilde, J., 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.
2. Bradshaw, S. and DeNardis, L., 2018. The globalization of trust in cyberspace governance. *Global Policy*, 9(1), pp.79–90.
3. Chander, A., 2017. *The Electronic Silk Road: How the Web Binds the World Together in Commerce*. Yale University Press.
4. Clarke, R.A. and Knake, R.K., 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.
5. Collins, A., 2016. *Contemporary Security Studies*. Oxford University Press.
6. European Commission, 2020. *Directive on Security of Network and Information Systems (NIS Directive)*. Available at: https://ec.europa.eu/ [Accessed 23 December 2024].
7. Farwell, J.P. and Rohozinski, R., 2011. Stuxnet and the future of cyber war. *Survival*, 53(1), pp.23–40.
8. Healey, J., 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
9. Keohane, R.O. and Nye, J.S., 2012. *Power and Interdependence*. Longman.
10. Kshetri, N., 2018. *Cybersecurity and Cyberwarfare: What Everyone Needs to Know*. Oxford University Press.
11. Kshetri, N., 2021. Cybersecurity and the Internet of Things: Vulnerabilities, threats, intruders, and countermeasures. *Elsevier*.
12. Lewis, J.A., 2018. *Cybersecurity and Critical Infrastructure Protection*. Center for Strategic and International Studies.
13. Lewis, J.A., 2021. The SolarWinds attack and the threat of cyber espionage. *Cyber Defense Review*, 6(2), pp.89–105.
14. Libicki, M., 1995. What is information warfare? *Institute for National Strategic Studies*. Available at: https://ndupress.ndu.edu/ [Accessed 23 December 2024].
15. Mosca, M., 2018. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), pp.38–41.
16. Nye, J.S., 2020. *The Regime Complex for Managing Global Cyber Activities*. Belfer Center for Science and International Affairs.
17. Perlroth, N., 2021. *This Is How They Tell Me the World Ends: The Cyber Weapons Arms Race*. Bloomsbury.
18. Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), pp.4–37.

19. Singer, P.W. and Friedman, A., 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

20. Waltz, K.N., 2010. *Theory of International Politics*. Waveland Press.