A Review on International Relations: The impact on nation-state cyberattacks on regional stability and the potential for escalation in the Americas (SDG 16)

Francis Canice Tochukwu Mezue [1] Chibuzor Chidiogo Mezue [2] Maryfine Mayaka [3] Christian Bassey [4]

1.School of Information Technology, Wilmington University, 320 N. DuPont Hwy, New Castle

2.Department of Library of Information Technology, Abia State University Uturu P.M.B 2000, Uturu Abia State, Nigeria.

3.School of Information Technology, Wilmington University, 320 N. DuPont Hwy., New Castle

4.University Security and Networking Engineering, Innopolis, Russia, 1 Universitetskaya Str.

* E-mail of the corresponding author: fmezue001@my.wilmu.edu

Abstract

The increasing frequency and sophistication of nation-state cyberattack have brought to light the vulnerability of the interconnected digital infrastructure that underpins our modern world. In the Americas, this has raised concerns about the potential for widespread disruption and destabilization across the region. Moreover, the asymmetry of cyber capabilities between nation-states has created a power dynamic that could potentially lead to further escalations and conflicts. Furthermore, the multifaceted nature of these cyber threats extends beyond traditional security concerns, encompassing economic, political, and social dimensions. The potential for stolen intellectual property, compromised critical infrastructure, and disinformation campaigns can significantly impact a nation's economy and governance, leading to broader implications for regional stability. As such, the need for a comprehensive and cooperative approach to address nation-state cyber threats in the Americas is paramount. Collaboration on cybersecurity measures, information sharing, and establishing clear guidelines for responsible state behavior in cyberspace are crucial steps to mitigate the risk of escalation and uphold regional stability. Additionally, fostering dialogue and diplomacy among nations in the Americas is essential to build trust and resilience in the face of cyber threats.

Keywords: cyber threats, SDG 16, nation-state, International Organizations; America

DOI: 10.7176/CEIS/15-1-07

Publication date: June 30th 2024

1. Introduction

Cyberattack, perpetrated by nation-states, have become a growing concern for international relations and regional stability (González-Manzano et al., 2022; Data Security Council of India (DSCI), 2023). These cyberattack have the potential to cause significant disruptions and escalations in the Americas, impacting not only the targeted nations but also their neighbouring countries (The Growing Importance of Global Cybersecurity Collaboration, 2023). The rise of nation-state cyberattack has ushered in a new era of geopolitical tension and security challenges. As these attacks transcend physical borders, they pose a substantial threat to the stability and security of nations in the Americas. The interconnectedness of global communication networks and the reliance of modern societies on digital infrastructure have amplified the repercussions of such cyber intrusions (Roberts, 2019) (Tabassum et al., 2018; Systemic Cyber Risk: A Primer, 2022). At the heart of the matter lies the potential for these cyberattack to spark regional instability and trigger escalating conflicts. The intricate web of interconnected alliances and trade relationships in the Americas means that a cyberattack on one nation-state can have cascading effects on its neighbours, leading to a domino effect of disruptions (Warf, 2015).

Furthermore, the clandestine nature of cyber warfare blurs the lines between traditional and non-traditional forms of conflict, complicating the attribution of attacks and raising the spectre of retaliation. This inherent ambiguity contributes to a sense of uncertainty and unpredictability in the realm of international relations, with the potential for miscalculations and unintended consequences (Hartley, 2018). In confronting the complexities of nation-state cyberattack, it is imperative for policymakers and international entities to adopt a comprehensive and proactive approach towards cybersecurity. This approach should encompass measures such as the establishment of international norms and standards for responsible state behaviour in cyberspace (Lewis, 2020; Hurwitz, 2014). Additionally, enhancing cooperation and information sharing among nations can promote early detection and response to cyber threats. These efforts can help build trust and strengthen regional stability in the face of cyber aggression. These measures should be coupled with diplomatic engagement and dialogue to de-escalate tensions and prevent the vicious cycle of cyber arms races. Moreover, it is essential to address the root causes of cyber aggression, including economic inequality, political grievances, and ideological disputes (Chen et al., 2023). By addressing these underlying factors, nations can work towards long-term solutions that promote peace, stability, and resilience in the face of cyber threats. This requires a multi-faceted approach, including diplomatic efforts to establish international norms and agreements on cyber behaviour, cooperation between nations to share information and intelligence (Maulana & Fajar, 2023; 2H 2022 Global Threat Landscape Report: Key Insights for CISOs, 2023)

The impact of nation-state cyberattack on regional stability in the Americas is a pressing concern that requires international cooperation and proactive measures (Chernenko, 2018). to mitigate the potential for escalation and preserve the well-being of nations in the region. In conclusion, the impact of nation-state cyberattack on regional stability in the Americas is a significant challenge that requires urgent attention.

1.1 Addressing the Role of International Organizations

International organizations play a crucial role in addressing the challenges posed by nation-state cyberattack and in promoting regional stability in the Americas. Institutions such as the United Nations and the Organization of American States can serve as platforms for multilateral cooperation and coordination in developing strategies to counter cyber aggression (González-Manzano et al., 2022). These organizations can facilitate the establishment of norms and principles for responsible state behaviour in cyberspace, providing a framework for guiding the conduct of nation-states in the digital domain. Moreover, by fostering dialogue and collaboration among member states, international organizations can contribute to the development of confidence-building measures and information-sharing mechanisms that enhance the collective ability to detect and respond to cyber threats (Morris et al., 2020).

1.2 Strengthening Public-Private Partnerships

Close collaboration between the public and private sectors is essential in bolstering cybersecurity defences and mitigating the impact of nation-state cyberattack. Public-private partnerships can leverage the expertise and resources of both sectors to enhance the resilience of critical infrastructure and digital systems against evolving cyber threats (Ledesma, 2022). By promoting information sharing and best practices, these partnerships can facilitate the implementation of robust cybersecurity measures across industries and organizations, thereby contributing to the overall cyber resilience of the region (Deljoo et al., 2018)

1.3 Emphasizing Capacity Building and Technical Assistance

Investing in the capacity building of nations in the Americas is paramount in strengthening their ability to prevent, detect, and respond to nation-state cyberattack. International assistance programs and technical support initiatives can equip countries with the necessary resources and expertise to enhance their cybersecurity capabilities (Cybersecurity, 2009). By providing training, technology transfer, and other forms of support, the international community can empower nations to fortify their cyber defences and effectively mitigate the impact of cyber incidents on regional stability (Zaman et al., 2021). The impact of nation-state cyberattack on regional stability in the Americas underscores the critical need for a cohesive and collaborative approach among nations and international entities. By addressing the multifaceted dimensions of cyber aggression through international cooperation, public-private partnerships, and capacity building efforts, it is possible to foster greater resilience and mitigate the potential for escalation in the face of cyber threats (Pawlak, 2016). Addressing the root causes of cyber aggression and bolstering cybersecurity measures are pivotal in safeguarding the well-being and security of nations in the Americas, ultimately contributing to the advancement of Sustainable Development Goal 16 on promoting peaceful and inclusive societies for sustainable development (Torres, 2018). The potential for escalation in the Americas.

2. The Potential for Escalation and Unintended Consequences Geopolitical Implications in the Americas

The geopolitical implications of nation-state cyberattack in the Americas have far-reaching effects on the region's stability and international relations. These cyber intrusions not only disrupt the targeted nations but also create a ripple effect that destabilizes neighbouring countries (González-Manzano et al., 2022). The interconnected nature of global alliances and trade relationships means that a cyberattack on one nation-state can lead to a domino effect of disruptions, undermining the overall stability of the region. Moreover, the clandestine nature of cyber warfare blurs the lines between traditional and non-traditional forms of conflict, making it difficult to attribute attacks and escalating the risk of retaliatory actions (Warf, 2014). This ambiguity contributes to a sense of uncertainty and unpredictability in international relations, potentially leading to miscalculations and unintended consequences. In light of these challenges, it is crucial for international entities and policymakers to prioritize comprehensive and proactive cybersecurity measures to address the root causes of cyber aggression (Nkongolo, 2023). By establishing international norms and standards for responsible state behaviour in cyberspace, enhancing cooperation and information sharing among nations, and engaging in diplomatic efforts to prevent cyber escalation, the Americas can work towards long-term solutions that promote peace, stability, and resilience in the face of cyber threats (Cho & Jongpil, 2017). Furthermore, case studies of cyberattack and their fallout can provide valuable insights into the impact of these attacks on regional stability and can inform the development of effective strategies to mitigate their effects (Tabassum et al., 2018). International efforts and initiatives for addressing cyber threats, as well as the role of multinational organizations in promoting cybersecurity, are crucial components in building a resilient and secure environment in the Americas. The potential for escalation and unintended consequences resulting from nation-state cyberattack in the Americas underscores the urgent need for international cooperation and proactive measures to mitigate the impact and preserve the well-being of the nations in the region (2022 Costa Rican ransomware attack, 2022). Addressing these challenges requires a multi-faceted approach that encompasses diplomatic, security, and economic considerations to effectively safeguard regional stability and international relations.

2.1 Recommendations for Mitigating the Impact of Nation-State Cyberattack

Towards achieving a higher level of efficiency and competitiveness in manufacturing operations, the European Community (EC), European Free Trade Association (EFTA), Australia, Canada, Japan, and the United States (US) founded an international collaborative research programme called Intelligent Manufacturing Systems (IMS) in 1993. This programme consists of six major projects, wherein the fifth one is entitled “Holonic Manufacturing Systems: system components of autonomous modules and their distributed control”. It is important to emphasise that HMS does not represent a new technology, as it is merely a conceptual modelling approach to connect and make use of existing technologies with human interfaces (McFarlane 1995). HMS became one of the first fully endorsed IMS projects in 1997, and so the International HMS Consortium was formed and dedicated to replicate in manufacturing the strengths that holonic systems provide to living organisms and societies. These holonic strengths encompass stability in the face of disturbances, adaptability and flexibility in the face of change, and efficient use of available resources. Succinctly, autonomy and cooperation are known as the prime attributes of HMS (Valckenaers *et al.* 1997; Bongaerts 1998).

2.1.1 Drivers of Nation-State Cyberattack and the Geopolitical Implications in the Americas

The geopolitical implications of nation-state cyberattack in the Americas are multifaceted and extend beyond immediate security concerns. These attacks have the potential to disrupt not only governmental operations but also critical infrastructure, financial systems, and communication networks (Warf, 2015). Such disruptions can have far-reaching consequences, affecting the daily lives of citizens and the functioning of essential services. Furthermore, the use of cyber warfare as a tool for influencing political dynamics and shaping regional power dynamics adds a layer of complexity to international relations. Nation-states may seek to exploit cyber capabilities to exert influence, manipulate public opinion, or undermine the stability of their adversaries (Kramer et al., 2011). This blurring of the lines between traditional and cyber warfare necessitates a re-evaluation of existing frameworks for conflict resolution and response.

2.1.2 Case Studies of Cyberattack and Their Fallout

Examining specific case studies of cyberattack in the Americas provides valuable insights into the varied techniques and motivations employed by nation-states. By analysing past incidents, policymakers and security experts can better understand the tactics and strategies used in cyber warfare (Torres, 2018). Moreover, studying the fallout of these attacks’ sheds light on the broader impact on regional stability, economic activity, and societal resilience. These case studies serve as critical reference points for formulating effective response strategies and identifying vulnerabilities that require mitigation (Brück & Wickström, 2004).

2.1.3 International Efforts and Initiatives for Mitigating Cyber Threats

International cooperation is paramount in addressing the shared challenge of nation-state cyber aggression. Collaborative initiatives aimed at promoting information exchange, capacity building, and joint defence mechanisms are essential for bolstering the resilience of nations in the Americas (Lewis, 2020). Additionally, the alignment of cybersecurity policies and the establishment of response frameworks at the international level can facilitate coordinated action in the event of a cyber crisis. Engaging in joint exercises and simulations to test response protocols can enhance preparedness and foster a cohesive approach to cyber defence (Badamasi & Utulu, 2021).

2.1.4 The Role of Multinational Organizations in Addressing Cybersecurity

Multinational organizations play a crucial role in advancing cybersecurity measures and promoting collective defence against nation-state cyber threats. These organizations can serve as forums for dialogue, knowledge sharing, and the development of best practices for cyber resilience (Pestana, 2023). By leveraging their convening power, multinational organizations can facilitate dialogue between nations, encourage the adoption of cybersecurity standards, and provide technical assistance to less resilient states. Additionally, these organizations can support capacity-building efforts and facilitate the transfer of expertise to strengthen the cybersecurity posture of nations in the Americas (Pestana, 2023). Thus, the complexity of addressing nation-state cyberattack in the Americas demands a holistic approach that encompasses geopolitical considerations, empirical insights from case studies, international cooperation, and the involvement of multinational organizations. By delving into the nuances of cyber aggression and proactive measures, nations can navigate the evolving landscape of international relations and safeguard regional stability (Yau, 2020).

2.1.5 Geopolitical Implications in the Americas: A Closer Look

The geopolitical implications of nation-state cyberattack in the Americas are multifaceted and require a comprehensive analysis. These cyber intrusions have the potential to disrupt not only governmental agencies and critical infrastructure but also the private sector, leading to economic instability and social unrest. Additionally, the implications extend to the geopolitical landscape, as they can strain diplomatic relations and impact trade agreements among nations in the region (Durojaye & Raji, 2022). To fully grasp the gravity of the situation, it is crucial to examine specific case studies of cyberattack in the Americas and their aftermath. By delving into these instances, we can gain insights into the techniques employed by aggressor nations, the vulnerabilities exploited, and the ripple effects on regional stability. Understanding the fallout from these cyber incursions can provide valuable lessons for bolstering defences and resilience against future attacks (Saalman et al., 2023).

3. The potential for escalation and unintended consequences

While the focus is often on the immediate impacts of cyberattack, it is essential to also explore the long-term ramifications, including the potential for escalation and unintended consequences. By delving into these potential outcomes, we can better understand the risks associated with retaliatory measures and the need for de-escalation strategies to prevent a spiral of cyber conflicts in the Americas (Cimmino, 2024). Current initiatives and policies addressing nation-state cyberattack in the Americas Examining the existing initiatives and policies in place to address nation-state cyber aggression in the Americas offers valuable insights into the gaps and areas requiring reinforcement (Pestana, 2023). By evaluating the regulatory frameworks, law enforcement capabilities, and information sharing mechanisms, we can identify opportunities to enhance the region's collective cyber defence posture. The need for comprehensive and proactive cybersecurity measures the evolving nature of cyber threats necessitates a proactive and holistic approach to cybersecurity (Odebade & Benkhelifa, 2023). By dissecting the components of comprehensive cybersecurity measures, including risk assessment, incident response protocols, and technological advancements, we can elucidate the requirements for fortifying the resilience of nations in the face of advanced cyber tactics (Ramirez & Choucri, 2020). International norms and standards for responsible state behaviour in cyberspace Establishing international norms and standards for responsible state behaviour in cyberspace is imperative for fostering a stable and secure digital environment (Roche, 2019). Exploring the current state of such norms and examining the challenges in their implementation can provide key insights into the pathway for achieving global cyber stability.

3.1 Addressing underlying factors of cyber aggression

Digging deeper into the underlying factors that drive cyber aggression, such as economic inequality, political grievances, and ideological disputes, is crucial for devising sustainable solutions (Lapierre & Dane, 2020). Understanding the root causes can inform policies aimed at addressing systemic issues and fostering greater stability and cooperation among nations in the Americas. A more profound exploration of the geopolitical, diplomatic, and technical aspects of nation-state cyberattack in the Americas is essential for devising effective strategies to mitigate their impact and preserve regional stability. This thorough examination will serve as a foundation for formulating actionable recommendations to confront the pressing challenge of cyber aggression in the region (Pestana, 2023).

3.1.2 Addressing Nation-State Cyberattack on Regional Stability in the Americas

3.1.2.1 Geopolitical Implications and Complexities of Cyberwarfare

The evolving landscape of nation-state cyberattack presents complex geopolitical implications in the Americas. These cyber intrusions have blurred the boundaries between traditional and non-traditional forms of conflict, challenging the established norms of international relations (González-Manzano et al., 2022). The clandestine nature of cyber warfare further exacerbates the challenge of accurately attributing attacks, leading to an environment of uncertainty and heightened tensions. Analysing specific case studies of cyberattack and their aftermath provides valuable insights into the multifaceted impact of such incidents on regional stability. Examining past cyber intrusions in the Americas can shed light on the cascading effects that permeate across interconnected nations, highlighting the urgency of proactive measures to prevent future escalations (Alimonti, 2022).

3.2 Exploring Historical Incidents of Nation-State Cyberattack in the Americas

Understanding the historical context of nation-state cyberattack in the Americas is crucial for evaluating the patterns, motivations, and impacts of such incidents. An in-depth review of previous cyber intrusions, their targets, and the ripple effects on regional stability will provide valuable insights into the recurring challenges faced by the affected nations (Malafaia, 2015). Investigating the aftermath of prominent cyber incidents, including the responses of the targeted nations and their neighbouring countries, will contribute to a comprehensive understanding of the potential for escalation and the ways in which these attacks have tested regional alliances and cooperation (Zaman et al., 2021). Examining the evolving tactics and strategies employed by nation-states in cyber warfare will offer a nuanced perspective on the adaptive nature of cyber aggression and the challenges it poses for the stability of the region. Additionally, an analysis of the geopolitical implications of these cyber incidents on the power dynamics among nations in the Americas will provide a deeper understanding of the complex interplay between cybersecurity and international relations (Cimmino, 2024).

3.3 Technological Landscape and Cybersecurity Challenges in the Americas

A detailed exploration of the technological landscape and cybersecurity challenges in the Americas is essential for comprehending the vulnerabilities. The complexity and severity of nation-state cyberattack on regional stability go beyond immediate disruptions to digital infrastructure (COHA, 2011). These attacks have the potential to infiltrate critical systems such as energy grids, financial institutions, and governmental operations, thereby undermining the very foundations of national security and economic stability. The interconnectedness of these systems means that a cyberattack on one sector can have cascading effects, impacting multiple aspects of a nation's functioning and extending beyond its borders to neighbouring countries (Petratos, 2018). This interconnected vulnerability underscores the need for a multifaceted approach to cybersecurity that addresses not only technical defences but also the underlying geopolitical and socioeconomic factors driving cyber aggression (Chen et al., 2023). In addition to the immediate impact on stability, nation-state cyberattack also have broader implications on international norms and the rule of law in cyberspace. The lack of established boundaries and regulations in this domain complicates the response to cyber intrusions, creating a vacuum where state-sponsored attacks can occur with impunity (Shin et al., 2018). The absence of clear guidelines for responsible state behaviour in cyberspace further amplifies the potential for miscalculations and unintended escalations. Addressing this issue requires a concerted effort to establish international norms and standards that define acceptable behaviour in the cyber realm and outline repercussions for violations (Thomas, 2017). Furthermore, the clandestine nature of cyber warfare introduces challenges in accurately attributing attacks to their sources, leading to difficulties in holding perpetrators accountable. This ambiguity can fuel distrust and suspicion among nations, exacerbating regional tensions and hindering efforts to build cooperative mechanisms for preventing and mitigating cyber threats (Goel, 2020). Developing robust mechanisms for attribution and accountability is essential for fostering trust among nations and creating a framework for cooperation in addressing cyber aggression. Ultimately, the impact of nation-state cyberattacks on regional stability and the potential for escalation in the Americas demand a holistic strategy.

3.4 The need for comprehensive and proactive cybersecurity measures

Exploring the potential for escalation in the Americas due to nation-state cyberattack requires a comprehensive understanding of the geopolitical dynamics and the evolving landscape of cyber warfare (González-Manzano et al., 2022). The interconnectedness of nations in the region and the reliance on digital infrastructure demand a nuanced approach to addressing these challenges. To delve deeper into the complexities of this issue, it is essential to analyse the historical context of international relations in the Americas and how it shapes the current landscape of cyber aggression (Bolgov, 2020). The legacies of past conflicts and alliances have a significant impact on the dynamics of cyber warfare in the region, influencing the motives and strategies of nation-states. Moreover, a detailed examination of the technological advancements and capabilities of different nations in the Americas is crucial to assess the potential for escalation in the event of a cyberattack (Cimmino, 2024). Understanding the asymmetries in cyber capabilities and the competitive dynamics can shed light on the vulnerabilities and motivations driving such attacks. Furthermore, it is imperative to consider the role of non-state actors and proxy entities operating within the region. These actors often exploit the ambiguity of cyberspace to carry out malicious activities on behalf of nation-states, adding layers of complexity to the already intricate web of cyber threats (Durojaye & Raji, 2022). In addition to proactive cybersecurity measures, a deeper analysis of the socioeconomic and political factors underlying cyber aggression is necessary. By examining issues such as economic inequality, political grievances, and ideological disputes, a more holistic understanding of the root causes of cyber conflicts can be attained, paving the way for sustainable solutions that address the fundamental drivers of instability (Cho & Chung, 2017). To effectively mitigate the potential for escalation and preserve regional stability, it is crucial for policymakers and international entities to integrate these nuanced insights into their strategies and collaborations. By doing so, it is possible to foster a more resilient and secure environment in the face of evolving cyber threats (Shackelford et al., 2014).

4. **The Human Cost of** Cyberattack

Beyond the geopolitical and security implications, it is crucial to consider the human cost of nation-state cyberattack. These attacks can have far-reaching consequences for individuals and communities, disrupting essential services, compromising personal data, and undermining trust in governmental institutions (Pattnaik et al., 2023). The psychological impact on individuals affected by cyberattack, whether directly or indirectly, cannot be overstated.

4.1 Addressing the Legal and Ethical Dimensions

In the realm of international relations, there is a pressing need to address the legal and ethical dimensions of nation-state cyberattack. Existing international laws and norms pertaining to cyberspace are still evolving, and there is a lack of consensus on how to attribute and respond to cyber intrusions carried out by nation-states (Saunders, 2023). As such, it is imperative for policymakers and legal experts to engage in meticulous discussions aimed at establishing frameworks for accountability and proportionate responses to cyber aggression.

4.2 Strengthening Cyber Resilience

A critical aspect of mitigating the impact of nation-state cyberattack is to enhance the cyber resilience of nations in the Americas (Taddeo, 2020). This involves not only fortifying technical defences but also investing in the capacity building of cybersecurity professionals and fostering a culture of cyber hygiene and awareness among the general populace. By bolstering the resilience of critical infrastructure and government systems, nations can better withstand and recover from cyber incidents, thereby mitigating the potential for widespread destabilization (Data Security Council of India (DSCI), 2023).

4.3 A Call for Enhanced Multilateral Cooperation

Given the transnational nature of cyber threats, it is imperative to emphasize the importance of enhanced multilateral cooperation in addressing the impact of nation-state cyberattack (Taddeo, 2017). Collaborative frameworks that facilitate the sharing of best practices, intelligence, and technological resources can significantly strengthen the collective defence posture of nations in the region. Moreover, fostering dialogue and building consensus on norms of responsible state behaviour in cyberspace through multilateral forums can lay the groundwork for a more stable and secure digital environment (Jaishankar, 2022).

5.0 Conclusion

In conclusion, addressing the threat of nation-state cyberattack on regional stability in the Americas necessitates a multi-faceted approach. The interconnected nature of modern societies and the potential for cascading effects from cyber intrusions underscore the urgency of this issue. International cooperation and proactive measures are crucial for mitigating the potential for escalation and preserving the well-being of nations in the region. By fostering dialogue, establishing norms for responsible state behaviour in cyberspace, and addressing underlying factors driving cyber aggression, the international community can work towards building resilience and promoting peace and stability in the face of cyber threats. It is imperative for policymakers and stakeholders to prioritize cybersecurity as a fundamental component of international relations in the digital age.

References

Alimonti, V. (2022, December 25). “Hacking Governments and Government Hacking in Latin America: 2022 in Review.” *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2022/12/hacking-governments-and-government-hacking-latin-america-2022-year-review

Badamasi, B., & Utulu, S. C. A. (2021, August 22). “Framework for Managing Cybercrime Risks in Nigerian Universities.” *arXiv*. https://arxiv.org/pdf/2108.09754.pdf

Baronchelli, A. (2018, October 20). “Conflict in Cyber-Space: The Network of Cyber Incidents, 2000–2014.” *Peace Economics, Peace Science and Public Policy*, 24(1), 29-59. https://doi.org/10.1515/peps-2018-0028

Bolgov, R. (2020, April 1). “The UN and Cybersecurity Policy of Latin American Countries.” *IEEE*. https://doi.org/10.1109/icedeg48599.2020.9096798

Brück, T., & Wickström, B. (2004, June 1). “The economic consequences of terror: guest editors' introduction.” *European Journal of Political Economy*, 20(2), 293-300. https://doi.org/10.1016/j.ejpoleco.2004.03.004

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Chundong, G. (2023, February 23). “Exploring the global geography of cybercrime and its driving forces.” *Humanities & Social Sciences Communications*, 10(1), 1-12. https://doi.org/10.1057/s41599-023-01560-x

Chernenko, E. (2018, February 9). “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms. Council on Foreign Relations.” https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

Cho, Y., & Chung, J. (2017, August 5). “Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity.” *Pacific Focus*, 32(2), 290-314. https://doi.org/10.1111/pafo.12096

Cimmino, J. (2024, February 12). “The competition for influence in the Americas is now online. Atlantic Council.” https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-competition-for-influence-in-the-americas-is-now-online/

COHA. (2011, December 23). “The Internet and Latin America: The Rise of the Virtual World and Emerging Cyber Security Issues. Council on Hemispheric Affairs.” https://www.coha.org/the-internet-and-latin-america-the-rise-of-the-virtual-world-and-emerging-cyber-security-issues/

Cybersecurity. (2009, August 1). “Organization of American States.” https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

Data Security Council of India (DSCI). (2023, January 1). https://www.dsci.in/content/international-cooperation

Deljoo, A., Engers, T. V., Koning, R., Gommans, L., & Laat, C. D. (2018, August 1). “Towards Trustworthy Information Sharing by Creating Cyber Security Alliances.” *IEEE*.
https://doi.org/10.1109/trustcom/bigdatase.2018.00213

Dorn, A. W., & Webb, S. (2019, January 1). Cyberpeacekeeping. International Journal of Cyber Warfare and Terrorism, 9(1), 11-21. https://doi.org/10.4018/ijcwt.2019010102

Durojaye, H., & Raji, O. (2022, January 1). Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure. arXiv. https://doi.org/10.48550/arxiv.2212.08036

Goel, S. (2020, January 1). “How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. Connections. *The Quarterly Journal,* 19(1), 87-95. https://doi.org/10.11610/connections.19.1.08

González-Manzano, L., Fuentes, J. M. D., Ramos, C., Sánchez, Á., & Quispe, F. (2022, June 29). “Identifying Key Relationships between Nation-State Cyberattack and Geopolitical and Economic Factors: A Model.” *Security and Communication Networks*, 2022, 1-11. https://doi.org/10.1155/2022/5784674

Greiman, V. (2019, October 5). “The Winds of Change in World Politics and the Impact on Cyber Stability.” *IGI Global.* https://www.igi-global.com/gateway/article/246332

Hartley, D. S. (2018, January 1). “An Ontology for Unconventional Conflict. Understanding Complex Systems.” https://doi.org/10.1007/978-3-319-75337-9

Hurwitz, R. A. (2014, September 3). “The Play of States: Norms and Security in Cyberspace.” *American Foreign Policy Interests*, 36(5), 322-331. https://doi.org/10.1080/10803920.2014.969180

Jaishankar, D. (2022, June 21). “In Cybserspace, Actions—Not Words—Define Norms — ORF America.” *ORF America*. https://orfamerica.org/newresearch/cybermilitaryconflictintensified

Kramer, F. D., Wentz, L., & Januar, Y. (2011, March 1). “Cyber Influence and International Security.” *University of Nebraska Press eBooks*, 343-361. https://doi.org/10.2307/j.ctt1djmhj1.19

Kshetri, N., & DeFranco, J. F. (2020, September 1). “The Economics of Cyberattack on Brazil.” *IEEE Micro*, 40(5), 19-26. https://doi.org/10.1109/mc.2020.2997322

Lapierre, K. R., & Dane, A. V. (2020, December 1). “Social Advantages and Disadvantages Associated with Cyber Aggression-Victimization: A Latent Class Analysis.” *Computers in Human Behaviour,* 113, 106497. https://doi.org/10.1016/j.chb.2020.106497

Ledesma, K. D. (2022, November 25). “Why the public and private sectors must join forces to address cyber risk for national security.” *The Hill*. https://thehill.com/opinion/cybersecurity/3750096-why-the-public-and-private-sectors-must-join-forces-to-address-cyber-risk-for-national-security/

Lewis, J. A. (2020, November 5). “A Necessary Contest: An Overview of U.S. Cyber Capabilities.” *Project MUSE*. https://muse.jhu.edu/article/754911

Malafaia, T. C. (2015, May 17). Resenha de “cyber conflict: competing national perspectives”. *Conjuntura Austral*, 6(29), 97-97. https://doi.org/10.22456/2178-8839.52761

Mariarosaria, T. (2017, September 19). “Deterrence by Norms to Stop Interstate Cyber Attacks - Minds and Machines.” *Minds and Machines,* 27(4), 665-687. https://doi.org/10.1007/s11023-017-9446-1

Maulana, Y. I., & Fajar, I. (2023, March 25). “Analysis of Cyber Diplomacy and its Challenges for the Digital Era Community.” *Aptikom Journal of Intelligent Systems and Data Informatics.* https://aptikom-journal.id/itsdi/article/download/587/243

Morris, D., Madzudzo, G., & García-Pérez, A. (2020, August 1). “Cybersecurity threats in the auto industry: Tensions in the knowledge environment.” *Technological Forecasting and Social Change*, 159, 120102. https://doi.org/10.1016/j.techfore.2020.120102

Nkongolo, M. (2023, January 1). “Navigating the complex nexus: cybersecurity in political landscapes.” *arXiv*. https://doi.org/10.48550/arxiv.2308.08005

Odebade, A. T., & Benkhelifa, E. (2023, January 1). “A Comparative Study of National Cyber Security Strategies of ten nations.” *arXiv*. https://doi.org/10.48550/arxiv.2303.13938

Pattnaik, N., Nurse, J. R. C., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023, January 1). “It's more than just money: The real-world harms from ransomware attacks.” *arXiv*. https://doi.org/10.48550/arxiv.2307.02855

Pawlak, P. (2016, February 1). “Capacity Building in Cyberspace as an Instrument of Foreign Policy.” *Journal of Cyber Policy*, 1(1), 63-78. https://doi.org/10.1111/1758-5899.12298

Pestana, R. (2023, July 25). “Cybersecurity: The Next Frontier of U.S.-China Competition in the Americas.” *Americas Quarterly.* https://www.americasquarterly.org/article/cybersecurity-the-next-frontier-of-u-s-china-competition-in-the-americas/

Petratos, P. (2018, December 1).” Systemic Cyber Risks and Defense: Valuation, Innovation and Strategic Implications.” *Management Communication Quarterly*, 32(1), 110-116. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1060&context=mca

Ramirez, R., & Choucri, N. (2020, October 11). “Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review.” *arXiv*. https://doi.org/10.48550/arXiv.2010.05156

Roberts, M. J. (2019, February 1). “The Cyber Threat and Globalization: The Impact on U.S. National and International Security.” *Journal of Strategic Security,* 12(1), 82-86. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1716&context=jss

Roche, E. M. (2019, April 3).” The search for global cyber stability.” *The Journal of Politics & International Affairs,* 7(1), 63-82. https://doi.org/10.1080/15228053.2019.1636570

Saalman, L., Dovgal, L. S., & Su, F. (2023, November 1). “Mapping Cyber-related Missile and Satellite Incidents and Confidence-building Measures”. *Russian Journal of Military History*, 2023(2), 1-15. https://doi.org/10.55163/rjmh1479

Saunders, B. (2023, April 4). “Advancing Cyber Norms Unilaterally: How the U.S. Can Meet its Paris Call

Commitments." *Belfer Center*. https://www.belfercenter.org/publication/advancing-cyber-norms-unilaterally-how-us-can-meet-its-paris-call-commitments

Sedaghat, M., & Gini, M. M. (2019, May 9). "Cyber-attacks Based on Legal Requirements and International Relations of Governments." *BIREX: Bina Ekonomi,* 9(1), 1-20. https://bircu-journal.com/index.php/birex/index

Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014, January 1). "How Businesses Can Promote Cyber Peace." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

Shin, Y. Y., Lee, J., & Kim, M. (2018, March 1). "Preventing State-Led Cyberattack Using the Bright Internet and Internet Peace Principles." *Journal of the Association for Information Systems,* 19(3), 152-181. https://doi.org/10.17705/1jais.00488

Carnegie Endowment for International Peace. (2022, March 7). "Systemic Cyber Risk: A Primer. "https://carnegieendowment.org/publications/86531

Tabassum, A., Mustafa, M. S., & Al-Maadeed, S. (2018, March 1). "The need for a global response against cybercrime: Qatar as a case study." In *2018 International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). https://doi.org/10.1109/isdfs.2018.8355331

Taddeo, M. (2017). "Deterrence by Norms to Stop Interstate Cyber Attacks." *Minds and Machines*, 27(3), 387-392. https://doi.org/10.1007/s11023-017-9446-1

Taddeo, M. (2020). Norms and Strategies for Stability in Cyberspace. In M. S. Shaikh (Ed.), "Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security" (pp. 53-65). *IGI Global.* https://doi.org/10.1007/978-3-030-29145-7_3

The Growing Importance of Global Cybersecurity Collaboration. (2023, June 18). LinkedIn. https://www.linkedin.com/pulse/growing-importance-global-cybersecurity-collaboration-chuck-brooks

The Political Cybersecurity Blindfold in Latin America. (2023, April 25). Lawfare. https://www.lawfareblog.com/political-cybersecurity-blindfold-latin-america

Thomas, E. (2017, November 13). "Taming the 'Wild West': The Role of International Norms in Cyberspace." *E-International Relations*. https://www.e-ir.info/2017/11/13/taming-the-wild-west-the-role-of-international-norms-in-cyberspace/

Toapanta, S. M. T., Jaramillo, J. M. E., & Gallegos, L. E. M. (2019, December 18). "Cybersecurity Analysis to Determine the Impact on the Social area in Latin America and the Caribbean." *In Proceedings of the 20th International Conference on Information Technology (ICIT 2019)* (pp. 1-6). https://doi.org/10.1145/3375900.3375911

Torres, D. (2018). "Cybersecurity and cyber defense for Venezuela: an approach from the Soft Systems Methodology." *Complex & Intelligent Systems,* 4(3), 213-226. https://doi.org/10.1007/s40747-018-0068-x

Warf, B. (2014). "Cyberwar: A new frontier for political geography." *Political Geography,* 46, 89-90. https://doi.org/10.1016/j.polgeo.2014.07.010

Yau, H. (2020, September 5). "Evolving Toward a Balanced Cyber Strategy in East Asia: Cyber Deterrence or Cooperation?" *East Asia: An International Quarterly,* 37(3), 265-285. https://www.worldscientific.com/doi/abs/10.1142/S1013251120400111

Zaman, G. K., Hossain, Z., Urmi, S. S., & Taher, K. A. (2021, February 27). "Cyber-Partnership and Cyber-Alliance - Options for Developing Nations. In *2021 International Conference on ICT for Sustainable Development (ICT4SD)* (pp. 1-7). https://doi.org/10.1109/icict4sd50815.2021.9396966