Attribution and Legitimacy: Building International Norms for Trust and Accountability in Cyberspace

Mr. Susant Kumar Dash
CSE Department
MITS
Rayagada, Odisha.
susant.disha@gmail.com

Mr. Ramanuja Nayak
CSE Department
MITS
Rayagada, Odisha.
ramanuja.nayak@gmail.com

Jagadish Kadraka
CSE Department
MITS
Rayagada, Odisha.
dulalmelka902@gmail.com

*Abstract-**Attribution in cyberspace has become one of the most pressing challenges in international security, carrying implications that extend far beyond the technical act of identifying malicious actors. Attribution is not merely a forensic process; it is also a political and normative practice that shapes legitimacy, accountability, and the evolution of global governance. While states increasingly issue public attributions and private firms publish technical analyses, little is known about how these practices influence the development of international law and norms in cyberspace. This research addresses that gap by examining attribution as a tool of legitimacy-building in international relations. Drawing upon international law, critical security studies, and norm development theory, the paper explores how attribution practices can reinforce trust among states, deter malicious actors, and establish shared expectations for responsible behaviour in the digital domain.The study argues that attribution should not be seen only as a reactive tool but as a proactive mechanism for shaping international governance. By assessing existing attribution cases and their diplomatic impact, the paper highlights the ways in which attribution contributes to norm construction, influences perceptions of legality, and fosters or undermines trust in multilateral settings. It also considers the risks of politicized or inconsistent attribution practices, which may weaken legitimacy rather than strengthen it. The research proposes that the development of binding international norms for cyberspace must account for attribution as a central element of accountability and conflict prevention. Ultimately, this paper contributes to a deeper understanding of how attribution, when grounded in legitimacy, can serve as a foundation for trust-building and the creation of a stable, rules-based order in cyberspace.***

*Keywords: **Cybersecurity Attribution, Legitimacy, International Norms, Trust-Building, International Law, Cyberspace Governance, Accountability, Conflict Prevention, Global Security, Political Legitimacy, Norm Development, Digital Diplomacy, International Cooperation, Governance Frameworks, Strategic Stability***

I. INTRODUCTION

In an increasingly interconnected world, cyberspace has emerged as a critical domain for state activity, commerce, and social interaction. While the digital environment offers unprecedented opportunities for innovation and collaboration, it also presents unique security challenges. Among these, attribution—the process of identifying the origin of cyber incidents—has become a central concern for states, international organizations, and private actors alike. Attribution is not simply a technical exercise in tracing digital footprints; it is a multidimensional practice with political, legal, and normative implications. The act of attributing a cyberattack to a specific actor carries consequences that extend far beyond cybersecurity, shaping international relations, governance, and global perceptions of legitimacy. Despite its significance, attribution remains an inherently complex and contested process. Technical limitations, the use of sophisticated obfuscation techniques by malicious actors, and the cross-border nature of cyber operations complicate efforts to identify perpetrators with certainty. However, attribution is not solely about accuracy; it also functions as a mechanism through which states and organizations signal accountability, demonstrate due diligence, and influence the behaviour of others in cyberspace. Public attributions by governments or technical reports by private cybersecurity firms can serve as strategic tools to shape norms, establish expectations for responsible conduct, and reinforce the legitimacy of international law in digital contexts.

The political dimension of attribution is particularly significant. Attribution decisions are rarely neutral—they are embedded in broader considerations of state interests, diplomatic leverage, and international reputation. Inconsistent, politicized, or opaque attribution practices can undermine trust and legitimacy, while transparent, evidence-based approaches can enhance cooperation and foster a

sense of shared responsibility. Consequently, understanding attribution as a normative practice, rather than merely a forensic one, is essential for conceptualizing how cyberspace governance can evolve toward a more rules-based order.Existing scholarship has predominantly focused on the technical or operational aspects of attribution, often neglecting its broader implications for international security and norm development. This research seeks to address that gap by analysing attribution as a tool of legitimacy-building in international relations. By examining historical cases of attribution, assessing their diplomatic impact, and situating these practices within frameworks of international law and norm theory, the study explores how attribution can contribute to trust-building, accountability, and conflict prevention. It argues that the proactive and consistent use of attribution has the potential to shape expectations for state behaviour, deter malicious actions, and provide a foundation for developing binding norms in cyberspace.

In this context, the research also considers the challenges posed by divergent state practices, technological limitations, and political sensitivities. The paper highlights the dual role of attribution: as a reactive instrument for identifying cyber threats and as a proactive mechanism for fostering stability and legitimacy in the international system. By emphasizing the interplay between technical capability, legal frameworks, and normative influence, this study offers a comprehensive perspective on how attribution can serve as a cornerstone for international cooperation, strategic stability, and responsible governance in the digital age.

II. LITERATURE REVIEW

1. Attribution in Cyberspace: Technical and Conceptual Perspectives

Attribution in cyberspace refers to the process of identifying the origin of a cyber incident, whether conducted by states, non-state actors, or criminal organizations. Early studies on cyber attribution primarily focused on technical mechanisms, including forensic analysis of malware, tracing Internet Protocol (IP) addresses, and monitoring network traffic (Rid & McBurney, 2012). These studies emphasized the challenges posed by sophisticated obfuscation techniques, such as the use of proxy servers, virtual private networks (VPNs), and anonymization tools, which allow malicious actors to conceal their identity.While technical attribution is necessary for identifying perpetrators, scholars argue that attribution cannot be reduced to a purely technical exercise. It is equally a political and normative practice that influences international perceptions of accountability and legitimacy (Valeriano & Maness, 2015). For instance, the attribution of the Stuxnet attack demonstrated how technical identification intersects with strategic, diplomatic, and normative considerations, as the public assignment of responsibility carries both symbolic and material consequences for state behaviour.

2. Legitimacy and International Law in Cyberspace

Legitimacy is central to the study of international relations and is defined as the acceptance and recognition of actions or rules as appropriate and justified within a particular normative framework (Suchman, 1995). In the context of cyberspace, legitimacy is closely tied to how states perceive the fairness, transparency, and accountability of attribution processes. Public attributions issued by states or independent cybersecurity organizations are a means through which legitimacy is constructed, signalling to the international community that specific actors are responsible for malicious activity.International law provides the formal framework within which attribution operates. Scholars have highlighted that existing treaties, such as the UN Charter, apply principles of sovereignty and state responsibility to cyber operations, yet the absence of binding norms specific to cyberspace creates ambiguity in assigning accountability (Schmitt, 2017). Attribution practices, therefore, fill this normative gap by influencing interpretations of legal responsibility and shaping expectations for state conduct. Attribution, when executed transparently and consistently, can reinforce legal norms, deter future attacks, and promote stability in cyberspace governance.

3. Trust-Building and Norm Development

Norm development theory in international relations emphasizes how repeated practices and shared expectations among states gradually evolve into accepted standards of behaviour (Finnemore & Sikkink, 1998). Attribution plays a critical role in this process. Consistent, evidence-based attribution practices establish precedents for state behaviour, thereby creating informal norms that contribute to trust-building and cooperation.Trust in cyberspace is not merely a diplomatic nicety; it is a prerequisite for coordinated security responses and multilateral governance frameworks. Scholars argue that the selective or politicized application of attribution undermines trust and may exacerbate tensions, while transparent attribution fosters credibility, predictability, and a sense of collective accountability (Kello, 2017). Digital diplomacy initiatives increasingly rely on attribution as a mechanism for signalling commitment to responsible behaviour, thereby strengthening the legitimacy of both national and international governance structures.

4. Challenges and Critiques of Attribution Practices

Despite its potential, attribution is not without limitations. Critics note that the politicization of attribution, inconsistent standards, and reliance on private cybersecurity firms can compromise legitimacy (Geers, 2011). In some cases, states may attribute attacks selectively to advance strategic interests rather than to uphold normative principles. Furthermore, the technical uncertainty inherent in cyber operations introduces the risk of erroneous attribution, which may lead to international disputes or miscalculated retaliatory measures.Additionally, the literature emphasizes the gap between technical capability and normative influence. While advanced forensic techniques enhance confidence in attribution, they do not automatically translate into internationally recognized norms or legal accountability. Therefore, effective attribution requires a

convergence of technical rigor, legal grounding, and diplomatic transparency, highlighting the interdisciplinary nature of the field.

5. Identified Research Gap

Existing literature demonstrates a rich understanding of the technical and legal aspects of attribution; however, there is limited research on the intersection of attribution, legitimacy, and norm development in cyberspace. Most studies treat attribution as either a forensic challenge or a policy tool, without adequately exploring its role as a proactive mechanism for shaping international expectations and trust. This gap underscores the need for research that examines how attribution contributes to norm construction, reinforces accountability, and promotes strategic stability in the digital domain.

III. RESEARCH FRAMEWORK

The research framework for this study is designed to conceptualize the relationship between cyber attribution, legitimacy, trust-building, and the development of international norms. Attribution in cyberspace is not only a technical process but also a multidimensional practice that has implications for international law, political legitimacy, and strategic stability. The framework integrates perspectives from cybersecurity, international relations, and norm development theory, providing a comprehensive lens to analyse the role of attribution in shaping responsible state behaviour.

1. Conceptual Components

The framework consists of four interrelated components:

a. Cybersecurity Attribution

At the core of the framework is the process of identifying the origin of cyber incidents, which involves both technical analysis (forensic investigation, malware analysis, network tracing) and contextual interpretation (intent, scale, and impact of the attack). Attribution is treated as a mechanism for accountability, where the identification of perpetrators serves as a foundation for legitimacy and governance.

b. Legitimacy

Legitimacy refers to the perceived appropriateness and justifiability of attribution actions by the international community. Public attribution statements and technical reports from credible organizations contribute to the perception that states or actors are adhering to accepted norms of behaviour. Inconsistent or politicized attribution can weaken legitimacy, while transparent and evidence-based practices strengthen trust in international governance frameworks.

c. Trust-Building

Trust is a central outcome of legitimate attribution. Transparent and consistent attribution practices enhance mutual confidence among states, deter malicious actors, and foster cooperative mechanisms for cyber defines. Trust-building enables multilateral engagement, facilitates compliance with informal norms, and supports the eventual development of binding rules in cyberspace.

d. Norm Development

Norm development refers to the emergence of shared expectations for state behaviour, based on repeated practices and mutual recognition. Attribution serves as a normative signal, establishing precedents for accountability, responsible conduct, and adherence to international law. Over time, consistent attribution practices contribute to the institutionalization of norms, reinforcing strategic stability and digital diplomacy.

2. Interrelationships Between Components

The research framework emphasizes the causal and feedback relationships among the components:

Attribution → Legitimacy:
Accurate and transparent attribution enhances international legitimacy, signalling adherence to normative expectations.

Legitimacy → Trust-Building:
Legitimacy fosters trust among states, encouraging cooperation and collective cybersecurity measures.

Trust-Building → Norm Development:
Established trust and predictable behaviour facilitate the emergence of informal and eventually formal international norms.

Feedback Loops:
Well-established norms, in turn, reinforce the processes of attribution and legitimacy by providing standards against which cyber incidents are evaluated. Conversely, politicized or inconsistent attribution can undermine legitimacy, weaken trust, and hinder norm formation.

3. Diagrammatic Representation

The conceptual framework can be visualized as a flow diagram:

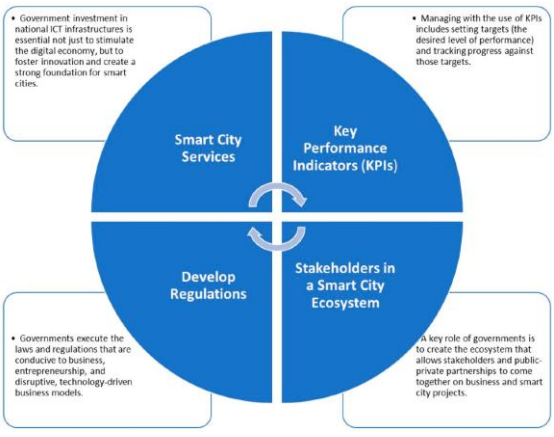

Fig .1. Conceptual Framework Linking Cyber Attribution, Legitimacy, Trust, and Norm Development

[Cybersecurity Attribution] → [Legitimacy] → [Trust-Building] → [Norm Development]

Arrows indicate the direction of influence.The feedback loop demonstrates how norms reinforce attribution practices and legitimacy over time.This framework provides a basis for analysing case studies of attribution and their impact on international trust and norms.

4. Theoretical Basis : The framework draws upon multiple theoretical foundations:

Norm Development Theory (Finnemore & Sikkink, 1998): Explains how repeated state practices become shared expectations.

Legitimacy Theory (Suchman, 1995): Highlights the importance of perceived appropriateness and justification in gaining acceptance.

Cybersecurity Governance Literature: Demonstrates the operational, political, and diplomatic dimensions of attribution in cyberspace.

This integrated framework allows the study to examine attribution not only as a technical or legal process but also as a proactive mechanism that shapes trust, accountability, and international norms.

Fig. 2. Below:

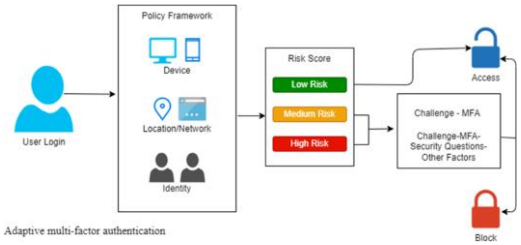

Fig. 2. Attribution as a Mechanism for Trust and Norm Development in Cyberspace

IV. METHODOLOGY

This study adopts a qualitative, theory-driven research design to investigate the role of cyber attribution in establishing legitimacy, fostering trust, and contributing to the development of international norms. The research emphasizes an analytical and interpretive approach, focusing on the theoretical and normative implications of attribution in cyberspace rather than the technical intricacies of cyberattacks. A qualitative design is particularly suited for exploring complex interactions between technical, legal, and political dimensions, allowing for an in-depth understanding of how attribution practices influence perceptions of accountability and responsible state behaviour in the international domain.

The study relies exclusively on secondary data sources to ensure a comprehensive and interdisciplinary examination. These sources include technical reports and analyses from established private cybersecurity firms, which provide insights into attribution methodologies and their reception in the international community. Official statements, public attributions, and white papers issued by governments are utilized to contextualize the political and legal dimensions of cyber incidents. Additionally, international legal frameworks, including relevant treaties, United Nations resolutions, and scholarly interpretations of state responsibility in cyberspace, serve as normative reference points for assessing legitimacy and accountability. Peer-reviewed academic literature in the domains of cybersecurity governance, norm development, international law, and political science provides the theoretical grounding for the study, while verified media accounts supplement empirical understanding by documenting state responses and international reactions to major cyber incidents.

To examine attribution as a normative and legitimacy-building mechanism, the study employs a purposive case study approach. Cases are selected based on their strategic significance, the availability of credible attribution statements, and evidence of normative impact on international behaviour. Illustrative examples include the Stuxnet cyberattack of 2010, the WannaCry ransomware incident of 2017, and the SolarWinds supply chain attack of 2020. These cases demonstrate the interplay between technical attribution, political legitimacy, and the emergence of shared expectations for state conduct in cyberspace.

The analytical strategy combines thematic, comparative, and interpretive approaches to understand the broader implications of attribution practices. Thematic analysis is used to identify patterns in attribution processes, legitimacy claims, and trust-building mechanisms. Comparative analysis allows for the examination of similarities and differences across cases, highlighting the consistency or variation in attribution practices and their normative consequences. Interpretive analysis facilitates an understanding of the political, legal, and normative dimensions of attribution, emphasizing the role of legitimacy and trust in shaping international norms and governance structures.

The methodology is closely aligned with the conceptual framework presented in Figure 1, which links cyber attribution, legitimacy, trust-building, and norm development. Attribution serves as the initiating mechanism, legitimacy functions as the evaluative dimension, trust-building represents the relational outcome, and norm development constitutes the cumulative effect. The framework guides case selection, data interpretation, and the analysis of relationships among key constructs, ensuring that the study systematically addresses its research objectives.

Despite its strengths, the methodology is subject to certain limitations. Reliance on secondary sources may introduce bias or incomplete information, and confidential state information regarding attribution processes may not be publicly accessible. Moreover, the qualitative nature of the study does not allow for the quantification of the effectiveness of attribution practices in preventing cyber

incidents. Nonetheless, the methodology provides a robust theoretical basis for understanding the interplay between attribution, legitimacy, trust, and the evolution of international norms in cyberspace.

V. ANALYSIS AND DISCUSSION

The analysis examines how cyber attribution functions not merely as a technical process but as a strategic and normative instrument that influences international legitimacy, trust, and norm-building. Drawing upon selected cases, the study demonstrates the interplay between these elements and highlights the mechanisms through which attribution shapes international governance in cyberspace.

1. Attribution as a Legitimacy-Building Tool

In the selected cases, attribution serves as a mechanism for establishing legitimacy. For instance, the Stuxnet incident illustrates how public attribution, even if implied or widely acknowledged, signalled adherence to normative expectations regarding state conduct in cyberspace. The act of attribution, whether performed by states or independent cybersecurity firms, functions as a public declaration of accountability. By framing cyber incidents within an evidentiary and normative context, attribution communicates to the international community that responsible actors are being held accountable. The legitimacy derived from transparent and evidence-based attribution reinforces the credibility of both state and non-state actors in the cyber domain.

Conversely, inconsistent or politicized attribution can erode legitimacy. The WannaCry ransomware attack demonstrated that divergent interpretations of responsibility, combined with geopolitical sensitivities, may lead to contested legitimacy, undermining trust among states and complicating multilateral responses. These observations suggest that legitimacy is contingent not only on the accuracy of attribution but also on the transparency and consistency of the practice.

2. Trust-Building Through Attribution

Trust in cyberspace emerges when attribution practices are perceived as fair, consistent, and impartial. The analysis reveals that transparent attribution facilitates mutual confidence among states, encouraging cooperation in cyber defence and collective norm enforcement. In the SolarWinds supply chain attack, coordinated attribution reports by multiple cybersecurity entities and government agencies provided a basis for international collaboration, demonstrating the role of attribution in establishing trust.

The feedback loop between legitimacy and trust is critical. Legitimate attribution strengthens trust, which in turn encourages adherence to emerging norms. When trust is undermined by opaque or politicized attribution, the ability to develop consistent behavioural expectations and shared governance mechanisms diminishes. These dynamic underscores the importance of attribution as a proactive tool for shaping normative behaviour, rather than merely reacting to cyber threats.

3. Attribution and Norm Development

The study highlights attribution's role in norm construction within cyberspace. Repeated, transparent, and credible attribution practices contribute to the gradual institutionalization of norms, establishing shared expectations for responsible behaviour. The selected cases indicate that attribution serves as both a signalling mechanism and a normative reference point. Over time, these practices can evolve into informal norms, which may later influence the formation of binding international agreements.

Attribution also functions as a corrective mechanism, deterring future malicious actions by creating reputational and diplomatic consequences. However, norm development is contingent upon consistency, multilateral recognition, and adherence to shared principles. Without these conditions, attribution may fail to produce lasting normative effects, potentially leading to fragmented governance and strategic instability.

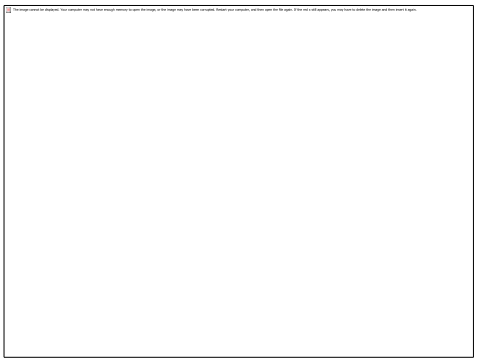

Fig . 3. Case Study Mapping

VI. EXPECTED RESULTS

The study is expected to demonstrate that cyber attribution plays a central role in shaping legitimacy, trust, and the development of international norms in cyberspace. It is anticipated that the analysis will reveal a clear relationship between the accuracy, transparency, and consistency of attribution practices and the perception of legitimacy among states. Attribution that is evidence-based and publicly communicated is likely to be associated with higher legitimacy, fostering trust and reinforcing expectations for responsible behaviour in cyberspace.The research is also expected to highlight the role of attribution as a proactive mechanism for norm development. Consistent and credible attribution practices are likely to contribute to the establishment of shared expectations for state conduct, gradually influencing informal norms and potentially guiding the evolution of binding international agreements. Conversely, attribution practices that are politicized, inconsistent, or opaque are expected to undermine legitimacy, diminish trust, and impede the development of cohesive normative frameworks.

Through the case study analysis, the study is anticipated to identify patterns and best practices in attribution that enhance accountability and promote strategic stability. These patterns may include coordinated attribution by multiple actors, transparent disclosure of evidence, and adherence to recognized legal and normative standards. Furthermore, the research is expected to demonstrate that trust-building is both an outcome of legitimate attribution and a critical facilitator for the institutionalization of norms, forming a positive feedback loop that reinforces responsible behaviour over time.

Ultimately, the study is expected to contribute to a theoretical understanding of how attribution, when grounded in legitimacy, can serve as a foundational tool for governance in cyberspace. It will provide insights into how states and international actors can utilize attribution strategically, not only as a reactive measure in response to cyber threats but as a deliberate mechanism to foster trust, accountability, and the evolution of shared international norms.

CONCLUSION

This study has explored the multifaceted role of cyber attribution in shaping legitimacy, trust, and the development of international norms within the domain of cyberspace. Attribution is not merely a technical exercise in identifying the origin of cyber incidents; it is a complex normative and political practice with far-reaching implications for international governance. By analysing the theoretical and practical dimensions of attribution, the study emphasizes its function as a mechanism for establishing accountability, fostering trust among states, and contributing to the emergence of shared expectations for responsible behaviour.

The research demonstrates that legitimacy is central to the effectiveness of attribution. Transparent, evidence-based, and consistent attribution practices enhance the credibility of the actor issuing the attribution, thereby fostering trust and cooperation in the international arena. Conversely, politicized, opaque, or inconsistent attribution can undermine legitimacy, erode trust, and impede the development of cohesive norms. Through this lens, attribution emerges as a proactive tool for shaping state behaviour, rather than merely a reactive response to cyber threats.

The study's conceptual framework highlights the interconnectedness of attribution, legitimacy, trust, and norm development. Attribution initiates a chain of normative influence: it establishes accountability, reinforces legitimacy, facilitates trust-building, and ultimately contributes to the institutionalization of norms. Case studies, including Stuxnet, WannaCry, and SolarWinds, illustrate the practical significance of these relationships, demonstrating how attribution practices influence international perceptions, diplomatic responses, and the evolution of normative expectations.

By integrating technical, legal, and normative perspectives, this research contributes to a more holistic understanding of cybersecurity governance. It underscores the importance of coordinated, transparent, and credible attribution practices as foundational elements for the creation of stable, rules-based order in cyberspace. The study also highlights the dual role of attribution as both a reactive mechanism for accountability and a proactive instrument for norm-building, offering a pathway toward enhanced strategic stability and responsible state conduct.

Finally, this research identifies areas for future exploration, including the formalization of attribution standards, the potential integration of multilateral verification mechanisms, and the examination of attribution's impact on digital diplomacy and conflict prevention. By emphasizing the normative dimension of attribution, the study provides a theoretical foundation for policymakers, cybersecurity practitioners, and scholars seeking to strengthen governance, trust, and accountability in the rapidly evolving domain of international cyberspace.

.REFERENCES

- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58.
- Betz, D. J., &Stevens, T. (2013). *Cyberspace and the state: Toward a strategy for cyber-power*. Routledge.
- Brantly, A. F. (2018).*The decision to attack: Military and intelligence cyber decision-making*. University of Georgia Press.
- Buchanan, B. (2020).*The hacker and the state: Cyber-attacks and the new normal of geopolitics*. Harvard University Press.
- Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, Omega, and Kubernetes. *Communications of the ACM, 59*(5), 50–57.
- Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance, 6*(2), 22–30.
- Clarke, R. A., & Knake, R. K. (2019).*The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin.
- Dunn Cavelty, M., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review, 15*(1), 37–57.
- Egloff, F. J. (2022). Attribution of cyberattacks: A framework for analysis. *Journal of Cyber Policy, 7*(1), 1–24.

- Fidler, M. (2017). Cyber deterrence and international law. *American Journal of International Law Unbound, 111*, 87–91.
- Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law, 110*(3), 425–479.
- Guitton, C. (2013). Cyber insecurity as a national threat: National security, private sector actors and public policy. *Journal of Cyber Policy, 1*(1), 25–41.
- Healey, J. (2011). The spectrum of national responsibility for cyberattacks. *Brown Journal of World Affairs, 18*(1), 57–70.
- Klimburg, A. (2017).*The darkening web: The war for cyberspace*. Penguin Press.
- Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and national security*. Potomac Books.
- Maurer,T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1-2), 4–37.
- Singer, P. W., & Friedman, A. (2014).*Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- Stevens, T. (2016).*Cyber security and the politics of time*. Cambridge University Press.
- Taddeo, M. (2017). Trusting cyber security.*Ethics and Information Technology, 19*(1), 1–13.
- Thomas, D. R., Antkiewicz, M., & Verhulst, S. (2018). Public–private partnerships for cyber resilience: A literature review. *Journal of Cyber Policy, 3*(3), 355–379.
- Tsagourias, N., & Buchan, R. (2015). Cyber interventions and international law. In *Research Handbook on International Law and Cyberspace* (pp. 439–458). Edward Elgar.
- Valeriano, B., & Maness, R. C. (2018).*Cyber strategy: The evolving character of power and coercion*. Oxford University Press.
- Zegart, A. (2022).*Spies, lies, and algorithms: The history and future of American intelligence*. Princeton University Press.