Bridging the Divide: A Governance Framework for Public–Private Collaboration in Cybersecurity Attribution

Ms. Nivedita Mohapatra
CSE Department
MITS
Rayagada, Odisha.
niveditamhpt@gmail.com

Mr. Pragnya Ranjan Dash
CSE Department
MITS
Rayagada, Odisha.
dash.pragnya@gmail.com

Mamata Thakur
CSE Department
MITS
Rayagada, Odisha.
Paletipawankumar@gmail.com

*Abstract-**Cybersecurity attribution remains one of the most critical yet unresolved challenges in the field of international security and digital governance. The act of identifying perpetrators behind cyber incidents is not merely a technical exercise but a political, legal, and social process that involves competing narratives, strategic interests, and varying degrees of evidence disclosure. In this complex environment, both state intelligence agencies and private cybersecurity firms have emerged as key producers of attribution knowledge. However, their respective contributions remain largely fragmented, with states often prioritizing secrecy and national security imperatives, while private actors emphasize technical reporting, market credibility, and reputational value. This division has created a persistent gap in attribution practices, resulting in incomplete or biased accounts that undermine trust, transparency, and legitimacy at both domestic and international levels.**This research addresses that gap by advancing a governance-oriented framework for public–private collaboration in cybersecurity attribution. Unlike existing approaches that treat state and private contributions as separate spheres, this study argues for an integrated model where knowledge, resources, and responsibilities are shared without eroding the strategic sensitivities of either side. Drawing upon governance theory, critical security studies, and international relations, the proposed framework conceptualizes attribution as a multi-actor process that requires structured channels of cooperation, institutional safeguards for information exchange, and mechanisms for balancing national security confidentiality with the need for verifiable, reliable evidence.The study critically evaluates current attribution practices, identifying how siloed knowledge creation leads to duplication of efforts, restricted verification, and inconsistencies in public communication of cyber incidents. It further explores the risks of politicization when attribution remains confined to state-centric narratives, as well as the limitations of private sector reporting that often lacks international legitimacy. By analysing these tensions, the paper highlights the need for governance mechanisms that foster trust-building, define clear roles, and establish shared standards of evidence in cyber attribution.*

Keywords: Cybersecurity Attribution, Public–Private Collaboration, Governance Framework, Information Sharing, International Security, Cyber Threats, Knowledge Integration, Legitimacy, Trust, Transparency

I. INTRODUCTION

In the contemporary digital era, cybersecurity has become a central pillar of national security, economic stability, and societal trust. As cyber operations increasingly blur the boundaries between criminal activity, state-sponsored aggression, and covert geopolitical manoeuvring, the ability to attribute cyber incidents to specific actors has emerged as one of the most critical and contested challenges in cybersecurity governance. Attribution—the process of identifying the perpetrators behind a cyberattack—is not only a technical task but also a deeply political and strategic process. The difficulty of achieving accurate attribution stems from the very nature of cyberspace: its anonymity, the ease with which attackers can conceal their identities, and the complex interplay of technical, legal, and diplomatic considerations.The attribution problem is compounded by the fragmented landscape of knowledge creation. On one hand, state intelligence agencies possess extensive resources, advanced surveillance capabilities, and access to classified information that can significantly aid in attribution efforts. However, states are often reluctant to disclose the sources and methods behind their assessments due to national security concerns and geopolitical sensitivities. On the other hand, private cybersecurity firms, including global incident response teams and specialized digital forensics companies, have played an increasingly visible role in producing detailed technical reports on cyber incidents. These private actors often release their findings publicly, contributing valuable knowledge to the broader security community. Yet their analyses are shaped by corporate interests, reputational considerations, and limited access to intelligence data, which may constrain the comprehensiveness and legitimacy of their conclusions.

This duality has led to a persistent divide between public and private attribution practices. State-led attribution often lacks transparency and public legitimacy, as accusations are sometimes dismissed as politically motivated when not

accompanied by verifiable evidence. Conversely, private sector attribution, though more transparent in its technical methods, often fails to carry the same weight in the international arena, where states continue to dominate discussions of legitimacy, responsibility, and response. The result is an environment of uncertainty, where attribution remains fragmented, contested, and at times strategically manipulated. This divide undermines the credibility of attribution, weakening its role in deterring malicious actors and fostering accountability in cyberspace.

Addressing this challenge requires moving beyond the traditional siloed approach to attribution. Instead, it necessitates the development of governance frameworks that facilitate meaningful cooperation between state and private actors. Such collaboration must account for the distinct capacities, incentives, and constraints of each side. States bring legitimacy, coercive power, and access to classified intelligence, while private actors contribute technical expertise, forensic methodologies, and the ability to rapidly disseminate findings to global audiences. When considered together, these complementary roles suggest that a governance framework capable of integrating both perspectives could enhance the reliability, transparency, and legitimacy of attribution practices.This paper argues that cybersecurity attribution should be reconceptualized as a shared governance problem rather than as an exclusive domain of either public or private actors. Attribution is not merely a question of assigning blame but a process of constructing knowledge that has consequences for international law, diplomacy, and security policy. Therefore, the development of a governance framework is necessary to align interests, establish mechanisms for trust-building, and create institutional safeguards that balance transparency with confidentiality. The objective of such a framework is not to eliminate the boundaries between state and private contributions but to design structured pathways for collaboration where knowledge can be integrated, verified, and communicated in ways that enhance both reliability and legitimacy.

The significance of this research lies in its potential to address key gaps in current attribution practices. Existing literature has thoroughly documented the challenges of attribution and the roles played by different actors, yet there remains limited exploration of how structured cooperation might be achieved in practice. By drawing from governance theory, critical security studies, and international relations, this study seeks to advance a conceptual model that outlines the principles, mechanisms, and institutional arrangements required to bridge the divide between state and private attribution efforts.
Ultimately, this introduction sets the stage for a deeper exploration of the governance dimensions of cybersecurity attribution. It frames attribution not simply as a technical or intelligence issue but as a problem of coordination, trust, and legitimacy that requires novel approaches to public–private collaboration. In doing so, it highlights the central research question guiding this paper: how can a governance framework be designed to integrate the knowledge and resources of both state and private actors in a way that improves the transparency, reliability, and legitimacy of cyber attribution?

II. LITERATURE REVIEW

The field of cybersecurity attribution has been widely discussed across disciplines ranging from computer science and law to political science and international relations. The literature collectively underscores the complexity of attributing responsibility for cyber incidents and the implications such practices hold for security, governance, and legitimacy in the digital age. However, despite the breadth of scholarship, much of the existing literature remains fragmented, with technical, political, and organizational dimensions often analysed in isolation rather than as interconnected components of a broader governance challenge.

Technical scholarship on attribution has primarily focused on forensic methods and digital evidence analysis. Researchers in this area emphasize the development of tools and methodologies capable of tracing malicious activity back to its origins. Techniques such as traffic analysis, malware reverse engineering, IP tracing, and behavioural analytics have been explored to increase the reliability of technical attribution. While these studies have contributed significantly to advancing the science of attribution, they consistently acknowledge the limitations imposed by the anonymity and obfuscation strategies used by attackers. Scholars note that technical evidence alone often lacks the conclusiveness required for political or legal accountability, as malicious actors frequently exploit proxies, compromised machines, and false flags to disguise their identity. This limitation has led to a growing recognition that attribution cannot be treated as a purely technical exercise.

In parallel, political and international relations scholars have examined attribution as a process deeply embedded in questions of power, legitimacy, and diplomacy. From this perspective, attribution is seen not only as the identification of culprits but also as a performative act through which states construct narratives, signal deterrence, and assert political authority. Literature in critical security studies highlights the inherent politicization of attribution, where states may selectively disclose evidence, exaggerate claims, or withhold information to serve strategic interests. These works stress that attribution practices shape the broader norms of cyberspace governance, influencing how trust, accountability, and international law are perceived. Yet, they also underscore the problem of credibility: when attribution remains confined to state narratives without transparent verification, accusations risk being dismissed as propaganda or politically motivated.

Alongside state-centric analyses, another growing body of literature has examined the role of private cybersecurity firms in attribution. With the proliferation of global cybersecurity companies such as FireEye, CrowdStrike, and Kaspersky, private actors have become central to the

production and dissemination of attribution knowledge. Their detailed technical reports and incident analyses often reach global audiences more quickly than official state pronouncements, thereby shaping public understanding of cyber threats. Scholars in this area argue that private attribution contributes to greater transparency and pluralism in knowledge production. However, this literature also points to limitations: private actors may be constrained by commercial interests, may lack access to classified intelligence, and their reports may not carry the same legitimacy in international political arenas as state-led attributions. Furthermore, concerns around intellectual property and client confidentiality restrict the full sharing of technical evidence, reinforcing the partiality of private sector contributions.

Despite the richness of these separate strands of literature, few studies have explored the integration of public and private contributions into a cohesive attribution framework. Governance literature offers some initial insights into models of public–private collaboration in other domains, such as counterterrorism, critical infrastructure protection, and disaster response. These studies emphasize the need for institutionalized channels of cooperation, trust-building mechanisms, and frameworks for balancing security with transparency. However, when applied to cybersecurity attribution, such models remain underdeveloped. Scholars have yet to fully theorize how governance structures might enable cooperation between actors with fundamentally different incentives, levels of authority, and access to information.

The literature also identifies enduring concerns over legitimacy and accountability. Attribution, whether conducted by states or private firms, is ultimately an exercise in constructing knowledge that has real-world consequences for diplomacy, law, and international order. Yet, when attribution practices remain siloed, fragmented, or opaque, they risk undermining confidence in cyberspace governance. Several works call for the establishment of international norms and standards around attribution, but these remain largely aspirational, with little concrete progress achieved. The absence of shared frameworks for verification and information exchange reinforces the gap between public and private contributions, leaving attribution practices vulnerable to politicization, inconsistency, and mistrust.

In summary, the existing literature provides valuable insights into the technical, political, and organizational dimensions of attribution but falls short of offering integrated frameworks that bridge the public–private divide. Technical studies highlight the limits of evidence, political studies emphasize the role of power and legitimacy, and organizational studies reveal the significance of institutional design. Yet, the intersections between these dimensions are underexplored. This research seeks to build upon these existing strands by situating attribution within a governance framework that explicitly addresses the challenges of collaboration between state and private actors. By doing so, it aims to contribute a novel perspective that moves beyond isolated analyses and toward a more holistic understanding of how attribution can be made more transparent, reliable, and legitimate in practice.

III. PROPOSED GOVERNANCE FRAMEWORK

The persistent fragmentation of attribution practices between state and private actors necessitates the development of a structured governance framework that redefines how knowledge is created, validated, and communicated in the realm of cybersecurity. The proposed governance framework is built upon the recognition that attribution is not merely a technical or political process but an inherently collective one that requires collaboration among actors with complementary strengths and differing responsibilities. Rather than positioning states and private cybersecurity firms as competitors in the production of attribution knowledge, the framework conceptualizes them as co-actors within a governance system where mutual trust, structured information flows, and clearly defined roles ensure a balance between transparency and confidentiality.

At the heart of the framework lies the principle of integration without homogenization. States retain their sovereign authority, intelligence-gathering capabilities, and international legitimacy, while private actors maintain their independence, technical expertise, and public credibility. The governance model does not seek to merge these functions into a single authority but instead provides structured pathways for collaboration that allow each actor to contribute to attribution in a manner consistent with their institutional constraints and incentives. This approach acknowledges the asymmetry between state and private contributions but also emphasizes that the effectiveness of attribution depends on their complementarity.

The framework begins with the establishment of institutionalized channels for information sharing. Existing literature highlights that one of the primary obstacles to collaboration lies in the reluctance of states to disclose classified intelligence and the hesitancy of private actors to reveal proprietary data. The governance framework proposes a tiered system of information exchange, where sensitive data can be shared selectively under agreed safeguards that protect both national security and corporate confidentiality. For example, states could disclose sanitized intelligence indicators without compromising sources, while private firms could provide anonymized technical analyses without revealing client-specific details. By instituting clear protocols for information sharing, the framework seeks to reduce the mistrust that currently characterizes public–private interactions in attribution.

Equally important to the governance framework is the establishment of verification mechanisms that strengthen the credibility of attribution claims. Attribution has too often been discredited due to accusations of bias, selective evidence disclosure, or manipulation for political purposes. The proposed model introduces multi-actor verification processes in which attribution assessments are cross validated by both state and private actors before being made public. This does not mean that all evidence must be universally disclosed, but that a minimum level of corroboration must be achieved across sectors to ensure reliability. Such verification mechanisms would not only enhance transparency but also protect against the monopolization of attribution narratives by any single actor.

The governance framework further emphasizes the role of trust-building as a cornerstone of collaboration. Trust between states and private firms has been historically weak, shaped by divergent objectives and suspicions of manipulation. To overcome this, the proposed model suggests the institutionalization of regular dialogues, joint task forces, and long-term partnerships that normalize cooperation rather than restricting it to ad hoc responses during crises. Through continuous engagement, public and private actors can establish shared vocabularies, develop common standards of evidence, and create a culture of collaboration that reduces suspicion and strengthens the legitimacy of joint attribution practices.

A critical component of the governance framework is its orientation toward legitimacy in the international arena. Attribution is not simply about assigning technical responsibility but also about shaping international norms and establishing accountability for cyber operations. The framework recognizes that state-led attribution carries diplomatic weight, while private-led attribution contributes to transparency and global visibility. By bringing these together within a governance model, attribution outcomes can be communicated with both political authority and technical credibility, thereby enhancing their acceptance among international audiences. In this sense, the framework is not only a mechanism for collaboration but also a tool for strengthening global cyber governance by ensuring that attribution practices are both trustworthy and legitimate.

Moreover, the framework is designed to be adaptive rather than rigid. Cyberspace is characterized by rapid technological change, shifting threat landscapes, and evolving political dynamics. A successful governance model must therefore incorporate feedback loops that allow attribution practices to be continuously refined. This involves learning from past attribution efforts, incorporating new forensic techniques, and adjusting information-sharing protocols as trust levels evolve. The governance framework, in this way, becomes a dynamic system that grows stronger with experience and adapts to emerging challenges.

Finally, the proposed framework carries significant normative implications. By bridging the public–private divide, it challenges the current tendency to view attribution as either the domain of sovereign states or the marketplace of private firms. Instead, it reconceptualizes attribution as a shared responsibility in which both sectors contribute to the production of reliable, transparent, and legitimate knowledge. This normative shift underscores the importance of collective security in cyberspace, where the integrity of attribution practices cannot be safeguarded by one sector alone.

In sum, the governance framework proposed in this study seeks to transform attribution from a fragmented and contested process into a structured and cooperative endeavour. By institutionalizing information-sharing protocols, establishing verification mechanisms, fostering trust, ensuring legitimacy, and incorporating adaptability, the model provides a theoretical foundation for overcoming the limitations identified in current attribution practices. It positions public–private collaboration not as an optional enhancement but as a necessary condition for achieving credible attribution in a complex and contested digital environment.

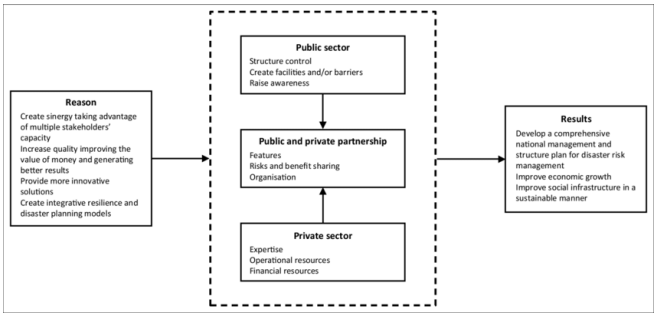

Fig. 1. Conceptual Governance Framework for Public–Private Collaboration

IV. METHODOLOGY

The methodological foundation of this study is primarily theoretical and conceptual, drawing from interdisciplinary perspectives across governance theory, cybersecurity studies, and international relations. Given the sensitive nature of attribution, where empirical access to state intelligence and proprietary corporate data is restricted, this research employs a conceptual modelling approach to develop a governance framework that can later be operationalized through empirical studies. The methodology rests on three pillars: analytical review of existing attribution practices, conceptual integration of governance principles, and the design of a model that incorporates public–private collaboration as its central organizing logic.

The first step in this methodological process involves an analytical review of current attribution practices across both state and private domains. This analysis synthesizes existing cases of cyber attribution, such as state declarations attributing cyber operations to adversaries and private sector reports identifying malicious campaigns. The review does not attempt to resolve the truth claims of individual cases but instead examines how attribution is produced, verified, and communicated. By mapping the practices of each actor, this stage identifies structural asymmetries: states often operate within classified environments, limiting transparency, while private firms emphasize open technical reporting but lack political authority. The methodological contribution here is to frame attribution not as isolated acts but as recurring patterns that reveal systemic gaps in collaboration.

Building on this analytical foundation, the second step involves conceptual integration. Governance theory provides a useful lens for rethinking attribution as a collective action problem that requires coordination between actors with different capacities and interests. The methodological approach draws on models of public–private cooperation in other sectors—such as counterterrorism, financial regulation, and disaster response where information sharing, trust-building, and role differentiation have been critical to success. By abstracting key principles from these domains and adapting them to the unique characteristics of cyberspace, the study develops a theoretical architecture for collaboration in attribution. This conceptual integration emphasizes adaptability, multi-level governance, and the importance of legitimacy as guiding principles.The third step in the methodology involves the design of a conceptual model for governance. This model is not intended as a rigid blueprint but as a dynamic framework that can be adapted to different national contexts and institutional arrangements. The model outlines the roles of public and private actors, the channels through which information can flow, the mechanisms by which verification is achieved, and the safeguards that protect sensitive data. The methodological choice to focus on conceptual modelling reflects the recognition that cyber attribution cannot be addressed through purely empirical methods alone, given the political sensitivities involved. Instead, theoretical modelling provides a foundation that can guide subsequent empirical validation through case studies, simulations, or pilot collaborations.

Finally, this methodological approach incorporates an evaluative dimension. The governance framework developed in this study will be assessed against three criteria: reliability, transparency, and legitimacy. Reliability refers to the capacity of the framework to produce consistent and accurate attribution outcomes; transparency relates to the ability of actors to understand and, where possible, verify the attribution process; and legitimacy refers to the acceptance of attribution outcomes by both domestic and international audiences. By evaluating the framework against these criteria, the study seeks to ensure that the proposed model not only addresses theoretical gaps but also has practical relevance for real-world implementation.In summary, the methodology employed in this study combines analytical review, conceptual integration, model design, and evaluative assessment to develop a governance framework for public–private collaboration in cybersecurity attribution. While grounded in theory, this approach provides a structured pathway for future empirical research, where the model can be tested, refined, and institutionalized through practical application

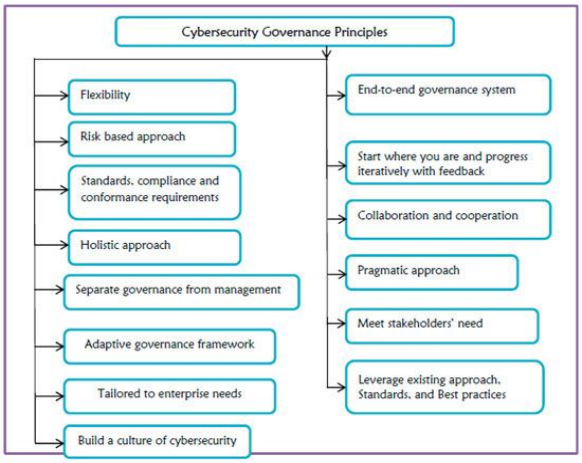

Fig. 2. Current Fragmentation of Attribution Practices

V. ANALYSIS AND DISCUSSION

The proposed governance framework for public–private collaboration in cybersecurity attribution must be evaluated not only as a conceptual model but also in terms of its ability to address the structural challenges identified in the literature. The analysis presented here demonstrates how the framework mitigates the deficiencies of current attribution practices, enhances the credibility of attribution outcomes, and contributes to the broader goals of international cyber governance.

The first critical issue concerns the problem of fragmentation between state and private attribution practices. As previously discussed, states often operate in secrecy, relying on classified intelligence and withholding evidence for strategic reasons, while private actors focus on transparency in technical reporting but lack political legitimacy. This separation has resulted in attribution claims that are frequently contested or dismissed, undermining their deterrent value. The governance framework addresses this fragmentation by providing structured pathways for information exchange, ensuring that knowledge from both domains can be integrated without compromising confidentiality or commercial sensitivities. Through tiered channels of cooperation, sanitized intelligence indicators can complement technical forensic analyses, resulting in attribution narratives that are both credible.

Third, the governance framework must be understood in terms of its role in trust-building. Trust between states and private firms has historically been minimal, shaped by suspicion, divergent incentives, and the lack of institutionalized cooperation. The framework proposes a model of sustained collaboration rather than crisis-driven, ad hoc engagement. Regular dialogues, joint task forces, and structured partnerships create opportunities for developing common standards of evidence, shared vocabularies, and long-term cooperation. Over time, such institutionalized practices can build the trust necessary for effective collaboration, replacing suspicion with confidence and reinforcing the legitimacy of shared attribution outcomes.

The broader implications of this analysis extend to the development of international norms for cyberspace governance. Attribution is not only about identifying perpetrators but also about shaping the rules of acceptable behaviour in cyberspace. The governance framework contributes to norm-building by establishing standards for evidence, cooperation, and communication that can inform global discussions on cyber responsibility. In doing so, it provides a foundation for the gradual emergence of shared international norms around attribution, which could play a critical role in reducing conflict and promoting accountability in the digital domain.

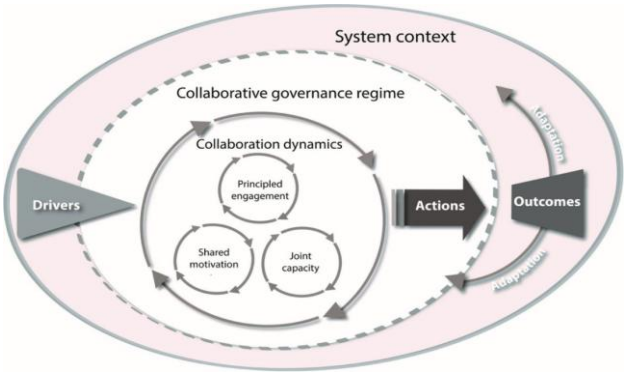

Fig. 3. Current Fragmentation of Attribution Practices

In conclusion, the analysis demonstrates that the governance framework addresses the central challenges of fragmentation, credibility, trust, legitimacy, and adaptability in cybersecurity attribution. By conceptualizing attribution as a shared governance problem rather than a contested space, the framework transforms attribution from a fragmented and mistrusted process into a cooperative and credible endeavour. Its significance lies not only in improving the reliability of attribution but also in advancing the broader objectives of sustainable and legitimate governance in cyberspace.

VI. EXPECTED RESULTS

The proposed governance framework is expected to demonstrate that effective collaboration between public and private actors in cybersecurity attribution can significantly reduce fragmentation, enhance the credibility of attribution claims, and foster greater legitimacy in the international arena. By integrating classified state intelligence with the technical expertise of private cybersecurity firms through structured cooperation, the framework is anticipated to produce more reliable and transparent attribution outcomes. Furthermore, it is expected to strengthen trust between stakeholders, create standards for evidence verification, and contribute to the establishment of shared norms for cyberspace governance. Ultimately, the research envisions that the adoption of such a framework will not only improve attribution practices but also advance broader objectives of accountability, deterrence, and stability in the digital domain.

Fig. 3 .Anticipated Benefits of the Governance Framework

CONCLUSION

Cybersecurity attribution has long been recognized as one of the most contested domains in digital governance, where technical complexity intersects with political sensitivity and strategic interests. This paper has examined the persistent divide between state-led and private-sector attribution practices, identifying how their siloed approaches weaken the transparency, reliability, and legitimacy of attribution outcomes. The analysis has demonstrated that attribution cannot be fully trusted when monopolized by state narratives that often remain opaque, nor can it be universally accepted when driven solely by private actors whose findings, although technically transparent, lack political authority. The failure to bridge this divide risks perpetuating a cycle of mistrust, contested claims, and weakened accountability in cyberspace.

The governance framework proposed in this study offers a structured response to these challenges by reconceptualizing attribution as a shared governance problem rather than as a zero-sum contest of authority. Through the integration of public and private contributions, the framework outlines how attribution can move beyond fragmentation toward collaborative and credible outcomes. By introducing institutionalized information-sharing protocols, mechanisms for joint verification, and processes for sustained trust-building, the framework creates a cooperative architecture that balances the secrecy required for national security with the transparency necessary for international legitimacy.A central insight of this research is that the effectiveness of attribution is not determined solely by technical capability or political authority but by the credibility of the process through which knowledge is produced. The governance framework seeks to create this credibility by combining the strengths of both sectors while mitigating their individual limitations. States bring legitimacy, diplomatic leverage, and access to classified intelligence, whereas private actors contribute technical expertise, independent analysis, and the ability to engage diverse audiences. When these capacities are aligned through structured cooperation, attribution outcomes become more resilient against scepticism, manipulation, and bias.

The conclusion also points to the broader implications of this research for the governance of cyberspace. Attribution practices are more than just responses to malicious

incidents; they play a fundamental role in shaping the norms of responsible behaviour and accountability in the digital domain. A collaborative governance model not only strengthens the credibility of individual attribution claims but also contributes to the gradual establishment of international standards for evidence, transparency, and responsibility. In this way, the framework provides a normative pathway for enhancing global trust, reducing the politicization of cyber incidents, and promoting stability in an increasingly contested digital environment. While this study has been primarily theoretical, it establishes a foundation for future research and policy experimentation. Empirical testing of the framework through case studies, pilot programs, or simulations would provide valuable insights into its feasibility and adaptability in real-world contexts. Moreover, the model invites comparative exploration across different national systems, examining how diverse political, legal, and cultural contexts may shape public–private collaboration in attribution. Such research would further refine the framework and contribute to its practical implementation as part of the evolving architecture of cyber governance.

In conclusion, this paper underscores the urgent need to move beyond fragmented approaches to attribution and toward a cooperative system that reflects the interconnected nature of cyberspace. By bridging the divide between public and private actors, the proposed governance framework represents a significant step toward more reliable, transparent, and legitimate attribution practices. It reaffirms that the future of cybersecurity governance depends not only on technological advancement but also on the ability to design institutions and frameworks that foster collaboration, build trust, and uphold accountability in the digital age.

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.
- 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.
- Fider, 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.

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