NATO Self-Defense: Is Article 5 the Right Framework for Responding to Sub-Kinetic Cyber Aggression?

Shreyas Kumar[1], Gary Brown[1], Srividhya Ragavan[1], Maddalena Cerrato[1] and Gourav Nagar[2]

[1]Texas A&M University, College Station, TX, USA

[2]Independent Researcher

shreyas.kumar@tamu.edu

Abstract: Cyber aggression presents a significant challenge to traditional frameworks of collective defense, particularly under Article 5 of the NATO Washington Treaty, which obligates member states to respond collectively to an "armed attack." While NATO has acknowledged that cyber incidents may trigger Article 5, ambiguity persists over what constitutes a cyber "armed attack," especially in the absence of kinetic effects. This uncertainty complicates NATO's ability to address increasingly prevalent sub-kinetic cyber threats, such as economic disruption, data manipulation, and interference in democratic processes. Unlike conventional military threats, cyber operations often fall below the traditional threshold of armed conflict while still exerting strategic effects that can destabilize states and alliances. This paper critically examines whether Article 5, in its current form, is adequate for responding to modern cyber threats. Through an analysis of legal thresholds, strategic challenges, and real-world scenarios, it highlights how sub-kinetic cyber aggression blurs the line between peace and conflict, testing NATO's existing frameworks. A key challenge is the lack of a universally accepted definition of what constitutes a cyber "armed attack," leading to inconsistencies in how NATO member states interpret and respond to cyber threats. Additionally, the difficulty of attribution in cyberspace further complicates collective defense efforts, as adversaries often employ proxies, obfuscation techniques, and false flag operations to mask their identities. Key findings underscore that without clearer definitions and adaptive strategies, NATO risks undermining its collective defense principle. To enhance its cyber defense capabilities, NATO must establish precise thresholds and cumulative criteria for cyber aggression, ensuring that sub-kinetic threats do not go unaddressed. Strengthening deterrence mechanisms, improving intelligence-sharing, and fostering consensus among member states will be critical in maintaining NATO's credibility and cohesion. Furthermore, NATO should develop a flexible response framework that considers the cumulative impact of cyber operations rather than relying solely on isolated incidents. By modernizing its collective defense strategy to meet the realities of cyberspace, NATO can better deter and respond to cyber threats, ensuring that Article 5 remains an effective instrument of alliance security in the digital age. This study provides actionable insights into how NATO can navigate the evolving cyber threat landscape while reinforcing its commitment to collective defense.

Keywords: Cyber aggression, Article 5, Sub-Kinetic threats, Cyber warfare, NATO response framework, Global security

1. Introduction

The evolving landscape of cyber threats has challenged traditional notions of national and international security. As cyberspace becomes an increasingly contested domain, state and non-state actors exploit its lack of physical borders to conduct aggressive operations that destabilize economies, disrupt critical infrastructure, and undermine democratic institutions. States have struggled to define and regulate aggressive cyber behavior, and international organizations like NATO face similar challenges. The question of how NATO should respond to cyber aggression is central to this discussion. NATO, a transatlantic defense alliance, was established to provide collective security against armed attacks under the Washington Treaty of 1949. However, as cyber threats grow in sophistication, the alliance faces significant challenges in adapting to this new reality. Article 5 of the treaty—often regarded as NATO's cornerstone—obligates member states to respond collectively to an "armed attack" against any NATO member state. While NATO has acknowledged that Article 5 could apply to cyberattacks, there remains ambiguity regarding the thresholds, criteria, and limits for invoking collective defense in response to sub-kinetic cyber aggression. This uncertainty raises critical questions: How should NATO define and interpret "armed attack" in the context of cyberspace? What qualifies as sub-kinetic cyber aggression, and can economic disruption, data manipulation, or attacks on government processes meet the threshold for triggering Article 5? What operational, legal, and strategic measures are necessary to address these challenges?

This paper explores these questions through a comprehensive analysis of the legal, strategic, and operational dimensions of NATO's cyber defense posture. It evaluates the adequacy of Article 5 in addressing sub-kinetic cyber aggression and proposes pathways to modernize NATO's collective defense framework to account for the unique characteristics of cyber threats. The findings highlight the urgency of establishing clearer thresholds, improved attribution mechanisms, and adaptive strategies to ensure NATO remains capable of defending its members in the digital age.

2. Background

The origins of NATO's collective defense principle stem from the post-World War II era, when mutual defense agreements were essential to deter military aggression, particularly from the Soviet Union. Article 5 of the Washington Treaty enshrined this principle, stating that an attack on one member is considered an attack on all. This provision was designed with kinetic warfare in mind—physical invasions, bombings, and physical destruction. However, the emergence of cyberspace as a strategic battleground introduced new challenges that do not fit within traditional military paradigms. Cyberattacks differ from conventional armed attacks in key ways. They are low-cost, anonymous, and may originate anywhere, and they often target critical infrastructure, private entities, and individuals rather than military assets – all while remaining below the threshold of armed conflict. Examples include ransomware attacks on healthcare systems, disruptions to energy grids, and electoral interference. While not physically destructive, these attacks can cause severe economic, political, and social harm, raising concerns about whether they should be classified as "armed attacks" under Article 5. The 2014 NATO Summit in Wales was a turning point in recognizing cyber threats, with the alliance acknowledging that cyberattacks could trigger Article 5 under certain conditions. However, NATO did not define the specific thresholds that would warrant a collective defense response, leading to strategic and operational ambiguities. The lack of a clear definition means member states may interpret cyber threats differently, potentially leading to inconsistent responses. Moreover, existing international legal frameworks, including Article 51 of the UN Charter, provide no guidance on addressing sub-kinetic cyber aggression, leaving NATO to navigate this evolving threat landscape while ensuring its policies remain aligned with contemporary security challenges.

3. Integrating Cyber Capabilities With Traditional Notions of Security

The integration of cyber capabilities into traditional security frameworks has been widely studied, particularly in national and international security alliances. Research has explored topics such as game theory applications in cybersecurity, cyberattacks' impact on nuclear deterrence, and challenges in crafting effective deterrence strategies. Manshaei et al. (2013) and Zhu and Başar (2015) examine game theory's role in network security and cyber-physical systems, while Lye and Wing (2005) model cyberattacks as stochastic games to optimize defense strategies. Fang, Stone, and Tambe (2015) use security games to address illegal activities, and Roy et al. (2010) survey game theory applications in network security. Pawlick and Zhu (2020) extend these ideas to cyber deception. On cyber-nuclear issues, Gartzke and Lindsay (2017) analyze how cyber operations could weaken nuclear deterrence, while Talmadge (2019) explores escalation risks. These insights are crucial for NATO's cyber defense posture, particularly regarding sub-kinetic cyber threats. Laszka, Vorobeychik, and Koutsoukos (2015) study spear-phishing through game theory, complementing macro-level analyses like Tucker (2019) on cyberattacks' strategic implications. Lin (2016) highlights attribution challenges in deterrence relevant to NATO's Article 5 framework. Studies on nuclear cyber threats include Bunn (2018) on vulnerabilities in nuclear command systems, Futter (2016) on cyber strategies countering nuclear threats, and Acton (2018) on inadvertent escalation risks. Foundational works like Singer and Friedman (2014) on cybersecurity, Schelling (1966) on deterrence, and Zhuang and Bier (2007) on resource allocation provide further context. Waltz (1979) and Huth (1988) contribute to deterrence theory. Policy research, such as Libicki (2009) on cyber deterrence limitations, Clarke and Knake (2010) on cyber defense vulnerabilities, and Koblentz (2014) on cyber-nuclear command integration, emphasize the need for robust policies. Emerging studies like Lin (2015) on cyber conflict termination and Nye (2017) on tailored cyber deterrence reinforce these concerns. In summary, cyber capabilities are reshaping security paradigms. Game theory aids in analyzing cyber threats, while nuclear cyber threat studies stress the need for integrated policies. These insights are crucial for NATO's evolving defense strategies, particularly in addressing cyber threats under Article 5

4. Methodology

This study employs a multi-faceted approach to evaluate the adequacy of NATO's Article 5 framework in responding to sub-kinetic cyber aggression, combining legal and doctrinal analysis with strategic analysis and scenario-based evaluation to provide a comprehensive understanding of cyber threats and identify pathways for adapting NATO's collective defense posture. The legal and doctrinal analysis focuses on Article 5 of the Washington Treaty and its applicability to cyberattacks, specifically examining how international law defines an "armed attack" in a sub-kinetic context. This includes assessing whether cyber operations can qualify as armed attacks and drawing from legal scholarship and NATO policy documents to clarify ambiguities. The analysis also aims to propose criteria for determining when a cyber event meets the collective defense threshold under Article 5. The strategic analysis involves developing detailed scenarios to evaluate the practical application of Article 5 in cyber contexts. These scenarios include cyberattacks on critical infrastructure, where disruptions to energy

grids, financial systems, or transportation networks in NATO member states are analyzed to determine under which conditions collective defense measures would be justified. Another focus is cyber-enabled disinformation and election interference, examining how cyber campaigns targeting democratic processes can undermine political stability and assessing the strategic and legal implications of responding to such threats. The study also evaluates hybrid warfare scenarios, where cyber aggression is combined with sub-kinetic threats such as economic coercion and disinformation, creating ambiguity that could delay NATO's response. Through this legal and doctrinal analysis and strategic analysis, the study aims to provide a structured approach to understanding cyber threats within the context of NATO's evolving collective defense strategy.

5. Legal Analysis

5.1 Legal Interpretations of "Armed Attack" in Cyberspace

The application of international law to cyberspace remains an area of significant ambiguity for several reasons. Article 51 of the United Nations Charter recognizes the right of self-defense against an armed attack but does not explicitly address cyber operations. Legal scholars, including Lin (2016),, argue that cyberattacks targeting essential state functions— even without causing physical damage—can have profound security implications.

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017) attempts to clarify this issue by interpreting "armed attack" to include cyber operations that result in significant destruction. However, NATO member states have established varied thresholds for what constitutes sufficient grounds for invoking Article 5, creating potential inconsistencies in collective responses. For example, a cyberattack that cripples the financial systems of one state may not be perceived as equally severe by others.

Legal ambiguity is further exacerbated by attribution challenges. Cyberattacks are often anonymized, with adversaries employing proxies or obfuscation techniques to evade detection. Without clear attribution, states may struggle to justify collective defense actions, as highlighted by Manshaei et al. (2013) in their analysis of adversarial behaviors in network security.

Aggressive cyber operations introduce additional uncertainty into NATO's collective self-defense framework. The primary issue is the difficulty of determining which cyber events are functionally equivalent to armed attacks—a determination crucial for attributing responsibility, whether for defensive or offensive actions. The threshold for invoking Article 5 is based on the concept of an "armed attack," which does not translate seamlessly to cyberspace. Additionally, the origin of a cyber operation is far easier to conceal than that of a kinetic attack, complicating efforts to attribute responsibility to a specific state or group. These challenges are explored in more detail in the following sections.

5.2 Cyber Armed Attack

The threshold for invoking Article 5 in the context of cyber aggression challenges the application of Article 5 and may necessitate a new approach to determining what types of aggression permit the lawful use of force in self-defense. The law of war, in various forms, has existed for thousands of years, as noted in The Law of War in Historical Perspective (1998). It has proven remarkably adaptable, evolving alongside shifts in international order and norms, including the rise of strong state sovereignty, democratic principles, world wars, international legal obligations, and the advent of new forms of warfare—such as air warfare and nuclear weapons, as highlighted by Koutroulis (2013). There is broad consensus among international legal scholars, perhaps best represented by the *Tallinn Manual* project, that the law of war will adjust to address cyber threats, as discussed by Schmitt (2017). However, the precise details of how the legal framework adapts to contemporary cyber operations remain elusive across all aspects of cyber conflict.

Cyber capabilities are not merely unique versions of kinetic weapons; some operate in fundamentally different ways. They can disrupt essential services—such as electrical power generation and communications—without physically damaging infrastructure, challenging traditional thresholds for the "use of force" and "armed attack." These capabilities can create strategic effects comparable to kinetic attacks while not necessarily providing a clear legal basis for armed self-defense.

One particularly complex issue is the presence of dual-use malware—code that can be used for espionage or destruction depending on the commands issued. While the use of such malware for espionage is generally accepted under international law, its deployment for destructive purposes could be construed as an act of aggression. Additionally, critical systems can be rendered unusable through operations that destroy or encrypt supporting data. When data is deleted or made inaccessible through encryption, it raises new legal ambiguities because data is virtual rather than physical, complicating the application of traditional international law.

6. Strategic Planning

6.1 Positioning Article 5 in the Cyber Age

NATO was formed after World War II to secure the freedom of Western Europe and guard it against aggression. Since NATO's formation in 1949, it has grown from the original twelve members to 32, including a number of states formerly part of the USSR or Soviet Bloc, as noted by NATO Member Countries (2024). In Article 5 of the eponymous treaty, member states agree that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all, and consequently they agree that, if such an armed attack occurs, each of them … will assist the Party or Parties so attacked by taking … such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area" (North Atlantic Treaty, 1949).

NATO also recognizes the role of the UN Security Council (UNSC) in its exercise of collective self-defense. Paragraph 2 of Article 5 requires NATO to report to the UNSC if an armed attack occurs and all measures taken in response. NATO acknowledges the UN's important role in the international system by also noting that NATO's actions will terminate "when the Security Council has taken the measures necessary to restore and maintain international peace and security." In a nod to the reality of global politics, this clause acknowledges NATO's commitment to a critical global institution while leaving itself free to pursue self-defense if the UNSC is unable to take effective action in a particular case because of the veto of a permanent member of the Security Council.

Article 5 has only been invoked once—after the 9/11 terrorist attacks against the US in 2001 (What is NATO, 2024). Although it is unlikely that NATO members were considering the possibility of cyber attacks in 1949, nothing in the language of Article 5 limits the definition of "armed attack" to sub-kinetic cyber aggression. The 2007 cyber aggression against Estonia first triggered discussion within NATO about how cyber threats fit into the alliance's collective defense framework, as noted by Herzog (2011) and Laasme (2011).

Although the Estonia incident ultimately did not trigger Article 5, it spurred further discussion across NATO about how cyber incidents could trigger the mutual self-defense obligation. In 2014, NATO specified that cyber defense was part of core NATO defense. NATO's cyber posture developed further, leading it to note in 2021 that all malicious activities, including those that individually might not rise to the level of an armed attack, could fall within Article 5—thereby prompting the alliance to act based on an assessment of the cumulative effect, as highlighted by Wiedemar (2023).

The 2021 statement arguably defines the term "armed attack" under Article 5 more broadly than under international law but has raised concerns that any number of sub-kinetic cyber actions that are otherwise below the threshold of armed conflict could henceforth be patched together to elevate to the level of an armed conflict.

6.2 The Role of Attribution and Credibility in Cyber Defense

Attribution uncertainty remains a core challenge in cyber conflict, as attackers often conceal their identities to evade retaliation. Lin (2015) and Libicki (2009) argue that inaccurate attribution weakens deterrence by reducing the credibility of retaliatory threats. For NATO, developing shared attribution mechanisms and technologies among member states is essential for strengthening collective security. Attribution also plays a crucial role in maintaining NATO's deterrence posture, as adversaries may exploit inconsistencies in responses to test the alliance's resolve (Clarke & Knake, 2010). Two primary approaches can help address this challenge. First, NATO should establish a coordinated attribution framework by integrating technological tools, intelligence-sharing, and standardized protocols to reduce vulnerabilities and enhance cyber defense. Second, the alliance should develop a damage-containment protocol to mitigate cyber incidents and prevent escalation. Attribution difficulties overshadow all aspects of cyber operations, as identifying responsible actors with sufficient certainty is essential for lawful countermeasures, armed self-defense, or public attribution.[1] Unlike kinetic attacks, which can often be traced to specific state actors, cyber operations create significant challenges in assigning responsibility. Most cyber incidents remain unattributed, placing the burden on the victim to determine responsibility. International law imposes limited obligations on states to disclose evidence supporting attribution

[1]Under international law countermeasures are defined as state actions "that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation." International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (2001), Part 3, Chap. II, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries - 2001, p. 128. In other words, (non-forcible) state actions that would normally be unlawful can be rendered lawful if taken for the purpose of ending unlawful conduct by the targeted state.

claims (Schmitt, 2017). The extent of evidence disclosure is discretionary, influenced by a state's relative power, alliance dynamics, and the severity of the cyber incident. While many states maintain strategic ambiguity, the UK has taken a clearer position, with Attorney General Jeremy Wright (2018) asserting that nations are not obligated to reveal their own cyber operations. States may withhold evidence to protect intelligence sources and methods (Wirtz, 2010). However, a recent trend has seen greater transparency, with the US, UK, Netherlands, and allied nations publicly attributing cyber operations to state actors like China and Russia (The White House, 2021; The Guardian, 2021). Hybrid warfare, which combines conventional, cyber, and informational tactics, further complicates NATO's collective defense doctrine. The 2007 cyberattacks on Estonia highlighted the difficulty of addressing such threats within traditional military frameworks. Hybrid tactics deliberately create ambiguity, making NATO's collective defense responses more complex (Singer & Friedman, 2014). To counter hybrid threats effectively, NATO must balance investments in cyber defense with traditional military capabilities (Zhuang & Bier, 2007). Additionally, collective defense should encompass responses to disinformation campaigns, economic coercion, and other non-kinetic tactics, ensuring a comprehensive approach to modern security challenges.

6.3 Role of the UN Security Council

While NATO plays a central role in collective defense, the UN Security Council (UNSC) is also implicated under Article 5 of the NATO Treaty. Paragraph 2 of Article 5 mandates that any armed attack and resulting measures be reported to the UNSC, which is responsible for restoring and maintaining international peace and security. This clause underscores the UNSC's role in legitimizing NATO's collective defense actions, promoting transparency, accountability, and alignment with international law. However, the effectiveness of the UNSC is often constrained by the geopolitical dynamics of its permanent members (P5), whose veto powers can obstruct consensus, particularly in cases of cyber aggression where attribution remains uncertain. The UNSC's ability to respond swiftly and effectively to cyberattacks remains questionable, as its historical focus has been on traditional kinetic conflicts rather than digital threats. The lack of precedents in handling cyber incidents raises concerns about whether the UNSC has the necessary expertise and mechanisms to address cyber-specific security challenges. Given these limitations, revising Article 5 to include alternative measures—such as empowering NATO or a specialized international body to respond to cyber incidents—could ensure more timely and effective action without reliance on UNSC intervention.

In conclusion, while the UNSC is essential for legitimizing NATO's actions, evolving cyber threats demand enhanced coordination, clearer reporting norms, and more adaptable response mechanisms. Revisiting Article 5 to address the UNSC's limitations in cyberspace could significantly strengthen NATO's ability to maintain international peace and security in the digital age.

7. Case Study: NATO's Challenges in Responding to a Cyberattack on a Member Nation

In 2007, Estonia, a NATO member since 2004, experienced a series of unprecedented and coordinated cyberattacks. Following a political dispute with Russia over the relocation of a Soviet-era monument, Estonian government websites, banks, and media outlets were targeted by Distributed Denial of Service (DDoS) attacks. These attacks disrupted critical infrastructure, causing widespread economic and social disturbances and marking one of the first major instances of state-sponsored cyber aggression. Despite Estonia's NATO membership, the alliance faced significant challenges in responding to the incident. At the time, NATO had no clearly defined protocols for addressing cyberattacks under its Article 5 collective defense clause. The ambiguity surrounding the definition of an "armed attack" in Article 5, particularly in the context of non-kinetic actions, meant that the cyberattacks on Estonia did not meet the threshold for triggering a collective defense response. Instead, NATO provided technical assistance and policy recommendations, exposing the limitations of the existing framework in addressing cyber threats.

This case highlights two key issues: first, the need for NATO to strengthen its preparedness for future cyber aggression, and second, the challenges posed by attribution, which must be addressed with greater urgency. The attacks were conducted through botnets and other proxy mechanisms, complicating efforts to establish definitive proof of Russian state involvement. As mentioned earlier, attribution remains a critical obstacle in responding to cyber incidents, as adversaries often exploit anonymity to evade direct accountability. The Estonia case also underscored a broader challenge: the necessity of building consensus among NATO members. Collaborating with academic experts who can highlight the severity of cyberattacks and their implications for both national and collective security is essential to achieving this consensus. The 2007 incident sparked discussions on NATO's role in cyber defense, making this a pivotal moment to enact structural and doctrinal

changes. However, these discussions must now translate into concrete policy developments by engaging experts from both technical and policy fields. The Estonia attacks ultimately led NATO to recognize cyberspace as a domain of operations in 2014 and acknowledge that significant cyberattacks could trigger Article 5. Nevertheless, the incident also exposed a persistent gap in NATO's operational readiness. This example underscores the need for NATO to establish clear thresholds and response mechanisms for cyberattacks. As cyber threats continue to evolve, NATO must balance the flexibility required to address emerging challenges with the necessity of maintaining cohesion among its member states. Without well-defined policies and capabilities, NATO risks being perceived as incapable of fully protecting its members in the digital age.

8. Recommendations

A more structured approach to cyber response strategies would better address the challenges cyber operations pose to NATO's self-defense framework. The ambiguity surrounding the application of Article 5 in cyberspace complicates NATO's decision-making and increases the risk of unintended escalation. NATO should refine its understanding of what constitutes an "armed attack" in cyberspace by identifying critical systems whose compromise would likely trigger an Article 5 response, defining specific levels of disruption that warrant various countermeasures, and establishing guidelines on how the cumulative effects of cyber operations—considering scope, duration, and intensity—might lead to escalation (Schmitt, 2017). Strengthening strategic communication is also essential, as demonstrated by the Vilnius Summit Communiqué (2023), which explicitly addressed cyber threats from Russia and China. Further policy statements should clarify NATO's stance on gray zone cyber activities, outline red lines, enhance coordination among member states, and ensure cyber policies evolve with emerging threats. Additionally, NATO should adopt a flexible, tiered response mechanism to cyber incidents, ensuring proportionate and effective measures ranging from retorsion and countermeasures, such as diplomatic and economic actions, to active cyber defense operations aimed at neutralizing threats before escalation, and in extreme cases, military responses where cyber aggression warrants kinetic retaliation. Enhancing NATO's cyber resilience is equally critical, requiring improved intelligence-sharing, joint cyber exercises, and stronger public-private partnerships to safeguard critical infrastructure. By implementing these measures, NATO can reduce ambiguity in its cyber response strategy, strengthen deterrence, and minimize escalation risks, ensuring its defense framework remains effective in the face of persistent cyber threats.

9. Discussion

Our research builds on and extends the existing literature on NATO's collective defense posture in the cyber age, particularly the challenges associated with sub-kinetic cyber aggression. By critically analyzing the adequacy of Article 5 in responding to such threats, this study makes several unique contributions to the field. Unlike similar studies—such as those by Futter (2016), and Libicki (2009)—our work takes a comprehensive, alliance-wide perspective, emphasizing the need for NATO to adapt its defense posture to address legal, strategic, and operational challenges in the cyber domain. By integrating real-world scenarios and policy recommendations, this study offers actionable insights that bridge existing gaps in the literature. For instance, our analysis of hybrid warfare incorporates lessons from Estonia's 2007 cyber-attacks, highlighting the need for a coordinated response framework—an aspect largely absent from prior research. This integration of theory, real-world examples, and practical strategies from an interdisciplinary perspective establishes our study as a distinctive

10. Conclusion

NATO and its member states have long refrained from specifying which types of cyber operations, and which systems and objects, if targeted, would most likely trigger an armed response, relying instead on the concept of "strategic ambiguity" (Stoltenberg, 2018). The rationale behind this approach was that explicitly defining red lines would enable adversaries to operate just below the threshold, effectively restraining NATO's ability to respond. However, events over the past decade have exposed a critical flaw in this strategy—when states fail to define the boundaries, their adversaries will do so for them. This approach has been remarkably ineffective in countering cyber-enabled influence operations, where international law remains ambiguous and cyberspace offers highly effective and easily accessible capabilities. NATO's adversaries have already exploited this ambiguity, raising the threshold by using cyber capabilities to influence elections and implant malware with destructive potential in critical infrastructure (CISA, 2024; NATO, 2023). These operations would likely have violated any stated threshold, but now the lack of a meaningful response appears to have pushed the threshold for triggering self-defense even higher. This was likely not the intended result of the policy of strategic ambiguity. By issuing clearer statements, NATO could help discourage future aggression and more effectively signal its intent to adversaries, reducing the risk of escalation through miscalculation.

Ethics statement: Ethical clearance was not required for the research.

References

Acton, J.M., (2018). Cyber warfare and inadvertent escalation. Daedalus, 147(2), pp.133-147.

Betts, R.K., (1987). Nuclear blackmail and nuclear balance. Brookings Institution Press.

Bunn, M., (2018). Nuclear cyber threats. Bulletin of the Atomic Scientists, 74(4), pp.205-211.

Clarke, R.A. and Knake, R.K., (2010). Cyber war: The next threat to national security and what to do about it. HarperCollins.

Do, Q., Tran, T. and Zhou, Y., (2017). Game theory for cyber security: A survey. arXiv preprint arXiv:1701.01562.

Fang, F., Stone, P. and Tambe, M., (2015). When security games go green: Designing defender strategies to prevent poaching and illegal fishing. Proceedings of the 24th International Joint Conference on Artificial Intelligence (IJCAI), pp.2589-2595.

Futter, A., (2016). The dangers of using cyberattacks to counter nuclear threats. Arms Control Today, 46(7), pp.22-28.

Gartzke, E. and Lindsay, J.R., (2017). Thermonuclear cyberwar. Journal of Cybersecurity, 3(1), pp.37-48.

Herzog, S., (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), pp.49-60.

Huth, P.K., (1988). Extended deterrence and the outbreak of war. American Political Science Review, 82(2), pp.423-443.

Koblentz, G.D., (2014). Cyber operations and nuclear command and control systems. The Nonproliferation Review, 21(3-4), pp.373-394.

Koutroulis, V., (2013). Martens Clause. Oxford Bibliographies.

Kumar, S., Niranjan, M., Nagar, G., Tripathi K. and Peddoju S., 2025. Humanizing Cyber War: Proposal for a Geneva Convention Equivalent for Cyber Warfare. 20th International Conference on Cyber Warfare and Security (ICCWS), 28-29 March, Williamsburg, Virginia, USA.

Laszka, A., Vorobeychik, Y. and Koutsoukos, X., (2015). Filtering spear-phishing attacks using game theory. Proceedings of ACM CCS.

Libicki, M.C., (2009). Cyberdeterrence and cyberwar. RAND Corporation.

Lin, H., (2015). Escalation dynamics and conflict termination in cyberspace. Strategic Studies Quarterly, 9(1), pp.46-70.

Lindsay, J.R., (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), pp.365-404.

Lye, K.W. and Wing, J.M., (2005). Game strategies in network security. International Journal of Information Security, 4(1), pp.71-86.

Manshaei, M.H., Zhu, Q., Alpcan, T., Başar, T. and Hubaux, J.P., (2013). Game theory meets network security and privacy. ACM Computing Surveys (CSUR), 45(4), pp.1-39.

NATO Member Countries, (2024). Available at: https://www.nato.int/cps/en/natohq/topics_52044.htm#coldwar.

North Atlantic Treaty, (1949). Article 5 (4 Apr 1949). Available at: https://www.nato.int/nato-welcome/#:~:text=Collective%20defence.

Nye, J.S., (2017). Deterrence in cyberspace. International Security, 41(3), pp.44-71.

Pawlick, J. and Zhu, Q., (2020). Game theory for cyber deception. Springer Nature.

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, (2024). CISA (7 February 2024).

Roy, S., Ellis, C., Shiva, S., Dasgupta, D. and Shandilya, V., (2010). A survey of game theory as applied to network security. Proceedings of the 43rd Hawaii International Conference on System Sciences.

Schelling, T.C., (1966). Arms and influence. Yale University Press.Cambridge University Press.

Schmitt, M.N. (ed.), (2017). State responsibility. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Section 1, para. 13.

Singer, P.W. and Friedman, A., (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Stoltenberg, J., (2018). Provides details of NATO's cyber policy. Atlantic Council (16 May 2018).

Talmadge, C., (2019). Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today. Journal of Strategic Studies, 42(6), pp.864-887.

The Gray Zone, (2015). USSOCOM White Paper (9 September 2015). Available at: https://specialforcestraining.info/docs/GrayZones-USSOCOM-WhitePaper9Sep2015.pdf.

The Law of War in Historical Perspective, (1998). International Law Studies, Vol. 72.

Tucker, P., (2019). Cyber battles, nuclear outcomes? Dangerous new pathways to escalation. Arms Control Today, 49(9), pp.20-27.

UK Attorney General Jeremy Wright, (2018). Cyber and international law in the 21st century (23 May 2018). GOV.UK.

Waltz, K., (1979). Theory of international politics. Addison-Wesley.

Wiedemar, N., (2023). NATO and Article 5 in cyberspace. Center for Security Studies, No. 323 (May 2023).

Wirtz, J., (2010). The sources and methods of intelligence studies. In: L.K. Johnson (ed.), Oxford Handbook of National Security Intelligence (2 Sept 2010).

Zhu, Q. and Başar, T., (2015). Game-theoretic methods for robustness, security, and resilience of cyber-physical control systems: Games-in-games principle for optimal cross-layer resilient control systems., 35(1), pp.46-65.

Zhu, Q., Chen, Y., Sinopoli, B. and Başar, T., (2012). Optimal resilient sensor placement with constraints. International Conference on High Confidence Networked Systems, pp.1-8.