ATTRIBUTION OF CYBERATTACKS: THE NEED FOR NEW EVIDENTIARY STANDARDS IN INTERNATIONAL LAW

Guram Gvinjilia

PhD in Law, Associate Professor of the Faculty of Law at Caucasus International University
Georgia, Tbilisi
Email: guramgvinjilia@gmail.com

ABSTRACT

In the contemporary era, individuals, private entities, public institutions, and state agencies are increasingly dependent on digital technologies and infrastructures for their daily operations. This reliance on digital systems and data exposes them to vulnerabilities, which can be exploited by malicious actors, both state and non-state, to inflict significant harm. One of the most common forms of causing damage, cyberattacks may target individual users and/or organizations, their impact can extend to the broader security and critical infrastructure of entire States. As a result, there is a growing imperative within the international community to ensure accountability for such attacks and to develop mechanisms that deter future incidents. Within this framework, the attribution of cyberattacks has become a central issue in interstate relations and international legal discourse. The mentioned issue is thoroughly discussed in presented paper, which examines the existing standards of proof and methodologies under the international law of State responsibility, aiming to identify the key advantages, challenges, and prospects of establishing a uniform attribution standard for cyberoperations within the scope of international law.

KEYWORDS: Cyberoperation; Cross-checking; Sliding scale of evidence; State Responsibility.

1. INTRODUCTION

Cyber-attribution involves interconnected political, legal, and technical dimensions. Political attribution entails attributing cyberattacks to States from a foreign policy perspective; legal attribution entails determining legal responsibility under international law and technical attribution entails conducting a forensic investigation to determine the source of an attack.

The process of attribution, encompassing both substantive and procedural dimensions, has been the subject of significant attention from academics, private sector entities, and civil society groups.[1] Political attributions of cyberattacks, which have become increasingly prevalent, play a vital role in upholding strategic stability by supporting deterrence efforts and managing escalation. They also enable States to assign accountability and publicly condemn breaches of cyber norms. Nevertheless, the impact of these attributions may be undermined if they are not backed by adequate and convincing evidence. As a result, such statements often fall short in achieving their intended "naming and shaming" effect.

One way to make it more likely that a particular group or person carried out a cyberattack is to establish specific criteria that States are expected to observe when delivering official communications to the public concerning such attacks. Further attributions of cyberattacks could help to better understand them. However, in order to substantiate attributions, States may be required to reveal the sources and methodologies underpinning their claims, a practice that entails significant risks due to concerns related to confidentiality and the protection of classified information.

The present paper emphasizes the need of properly demonstrating attribution under international law as a condition for getting any sort of remedy. Based on the current international legal standards of proof and methodologies pursuant to law of State responsibility, this paper attempts to determine the type and amount of evidence needed for a state to show attribution for a cyberattack in an international legal forum.

To this end, this article looks at how international evidence standards might be designed to produce credible attributions of cyberattacks to governments. It will examine current evidence-gathering procedures, which will aid in understanding current practice as well as the major concerns at hand. Following that, the primary benefits and challenges of evidence disclosure will be examined. The overview clarifies what obstacles to regulation may exist, as well as why evidentiary criteria are crucial. Finally, based on customary international law, the paper submits that the identified legal standard of evidence will make not only legal, but also legal attributions of cyberattacks more credible and legally sound.

2. CYBERATTACK ATTRIBUTION STANDARD: GENERAL CONSIDERATIONS

2.1. A Sliding Scale of Evidence

The technological novelties give rise to regulation dilemma in international law, featuring the context of cybersecurity - what is the optimal solution: to apply already existing norms of general international law or to cre-

[1] Moynihan, H., 2019, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*. London: Chatham House. [Online] available at: <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/7-conclusions-and-recommendations> [Accessed 6.05.2025. Conclusion].

ate a new one?[2] At present, the application of existing international legal frameworks is mostly adequate. However, when it comes to evidentiary standards for attribution, the insufficient development of international law in this area indicates a need for a combination of current legal norms and newly formulated rules.

For instance, in the context of invoking the right of self-defence, limited State practice indicates that the injured State is expected to satisfy a clear and convincing evidentiary threshold. In cases where cyberoperations escalate to the level of an armed attack, the actions taken in response would be subject to this evidentiary standard, provided it reflects a norm of customary international law. Imposing a stringent threshold for attribution in instances of the most serious cyber incidents aligns with the International Court of Justice's (ICJ) recognition of a sliding scale of evidence[3], which adjusts in proportion to the gravity of the alleged violation. Consequently, attributing a cyberoperation amounting to an armed attack necessitates the most robust evidentiary foundation.[4] The Tallinn Manual adopts a comparable approach based on a sliding scale, asserting that the requisite standard of evidence should correspond to the seriousness of the alleged cyberoperation: "the graver the underlying breach […], the greater the confidence ought to be in the evidence relied upon by a State considering a response […], because the robustness of permissible self-help responses (such as retorsion, countermeasures, a plea of necessity, and self-defence) grows commensurately with the seriousness of a breach."[5]

Employing a sliding scale of evidence that aligns with the severity of a cyberattack and the potential response offers some guidance at the extreme end of the spectrum. However, its greatest utility lies in clarifying the intermediate range, where most cyberoperations actually take place. These operations typically fall within the legal framework governing countermeasures.[6] As previously noted, there remains no well-defined consensus on the evidentiary thresholds applicable to state conduct in this domain, aside from the broad expectation that responses must be reasonable.[7]

The sliding scale approach, as supported by both the ICJ and the Tallinn Manual, is grounded in the specific context of legitimizing responsive measures. However, this framework is limited in scope, as it does not address the evidentiary thresholds necessary for other potential objectives of attribution. It offers no guidance regarding the quantity or quality of evidence required for alternative purposes, nor does it assess the scale to which minimum evidentiary standards might apply in those contexts.

---

2 Crootof, R., 2019, Regulating new weapons technology. In: Alcala, R., and Jensen, E.T., eds. The impact of emerging technologies on the law of armed conflict. The Lieber Studies Series. New York: Oxford University Press, p. 24.

3 International Court of Justice, 2007. Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007. I.C.J. Reports 2007, p. 43.

4 International Court of Justice, 2007. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment*, 43, 129.

5 Schmitt, M.N., 2017. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. 2nd ed. Cambridge: Cambridge University Press, p. 82.

6 Tams, C.J., 2010. *Enforcement by Measures Short of Force: Article 49*, in Crawford, J., Pellet, A. and Olleson, S. (eds.) *The Law of International Responsibility*. Oxford: Oxford University Press, p. 1039.

7 Compare. Tallinn Manual 2.0, supra note 3, p. 81; Compare. also Egan, B.J., 2017. International law and stability in cyberspace. Berkeley Journal of International Law, 35 (169), p. 177.

2.2. Stability through Cross-checking

Consider the broader systemic objective of fostering stability and preventing conflict in cyberspace. To serve this aim, attribution claims must be supported by a degree of evidentiary substantiation. Assertions made without accompanying evidence do not contribute to stability. On the contrary, they risk exacerbating tensions and triggering unintended escalation among States. In order to promote a stable cyber environment, the evidence presented should be adequate to enable independent verification or corroboration. Cross-checking is the main issue. Sharing sufficient technical information to allow third parties to assess and validate the attribution enhances its overall credibility.[8] Improving attributions' credibility affects our reality and States' behaviour in cyberspace.

Requirement to attributions to be supported by evidence should stimulate the origin of more well-prepared attributions. States or agencies articulate the grounds for their actions so the latter can be subject to review by courts is understood to encourage better decision-making before the event and responsibility for decisions after.[9]

Establishing a requirement for sufficient evidence that enables cross-checking would provide a baseline standard for the evidentiary support accompanying an attribution. In contrast to the sliding scale approach, which ties evidentiary thresholds to the nature of the responsive measures taken, the verification-based approach functions independently of whether the attributing State opts for a response at all. These two frameworks are not mutually exclusive and can be applied complementarily.[10] In cases involving severe cyberattacks and consequential responses, the sliding scale approach would inherently demand a level of evidence exceeding that required for cross-checking. Conversely, in less grave incidents, cross-checking serves as a minimum evidentiary standard. Even when States rely on public attribution strategies, such as "naming and shaming," they should still be expected to present sufficient evidence to allow for cross-checking of their claims.

Cross-checking may be performed by evaluating the evidence initially disclosed by the first attributing entity, followed by the contributions of subsequent attributors. A benchmark example of evidentiary disclosure is the Mandiant APT1 report, through which Mandiant identified individuals affiliated with the Chinese People's Liberation Army and included detailed technical appendices that enabled third parties to independently verify the attribution.[11] The attribution of the Democratic National Committee (DNC) hack by CrowdStrike was likewise subjected to cross-checking, as several cybersecurity firms conducted independent analyses of the malware and corroborated the findings using key data, such as IP addresses originally disclosed by

8 Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), p. 18.

9 Mashaw, J.L., 2008. Reasoned administration: The European Union, the United States, and the practice of democratic governance. *George Washington Law Review*, 76(99), p. 115.

10 Tsagourias, N. and Buchan, R., 2021, *Research Handbook on International Law and Cyberspace*. 2nd ed. Cheltenham: Edward Elgar, p. 125.

11 Compare. Mandiant, 2013. *APT1: Exposing one of China's cyber espionage units*, p.53. [Online] available at: <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> [Accessed 6.05.2025].

CrowdStrike.[12]

Although the U.S. domestic legal system employs a variety of terms to describe evidentiary standards, there remains ambiguity regarding the precise interpretation of these different linguistic expressions.[13] Selecting a single evidentiary descriptor for broader international application may lead to interpretive challenges. The cross-checking standard entails an obligation to disclose supporting evidence that meets a minimum evidentiary threshold. This approach contributes to stability in cyberspace by fostering a shared understanding of attribution claims, thereby reducing the risk of disputes and escalation in the digital domain.

2.3. Attribution as Deterrence

For attribution to contribute effectively to macro-level deterrence, it must involve at least an implicit threat of punitive action, such as the implementation of lawful countermeasures.[14] For such countermeasures to be deemed legitimate under international law, the attributing State must persuade the international community that it has been the target of an internationally wrongful act. Presenting adequate and verifiable evidence to substantiate the attribution strengthens the legitimacy of the claim and, consequently, enhances the credibility of the threatened countermeasures. This, in turn, reinforces the overall deterrent impact of the attribution.

A contemporary approach to establishing micro-level deterrence may involve imposing consequences on specific state-affiliated hacker groups. This objective can be achieved by presenting adequate evidence that allows for cross-checking. In the United States of America, indictments are based on probable cause, while the imposition of sanctions necessitates a reasonable basis.[15] As previously discussed, these domestic thresholds can typically be met through the provision of sufficient evidence enabling cross-checking. When comparing domestic and international evidentiary standards, domestic requirements may exceed those under international law. For instance, the evidentiary threshold needed to establish an individual's criminal liability beyond a reasonable doubt in domestic proceedings might surpass the international requirement of supplying evidence adequate for cross-checking.

Identifying a specific State as responsible for a cyberattack is not a prerequisite for enhancing defensive measures. Strengthening cybersecurity can be achieved through the

12 Compare. Nakashima, E., 2016. Cyber researchers confirm Russian government hack of Democratic National Committee. *Washington Post*, 20 July. [Online] available at: <https://www.washingtonpost.com/world/national-security/cyber-researchers-confirmrussian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html> [Accessed 20.03.2025. Introduction].

13 Addington v. Texas, 441 U.S. 418, 425 (1979).

14 International Law Commission, 2001, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. Yearbook of the International Law Commission, 2001, Vol. II, Part Two. [Online] available at: <https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf> [Accessed 13.05.2025]. - According to the International Law Commission, 2001, *lawful countermeasures* are otherwise unlawful acts that are permitted under international law when taken in response to a prior internationally wrongful act, for the purpose of inducing the responsible state to comply with its obligations (Articles 22 and 49–54 of the Draft Articles).

15 Compare. U.S. Department of Justice, 2025. Principles of federal prosecution. *Justice Manual*, § 9-27.220. [Online] available at: <https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution> [Accessed 7.05.2025].

dissemination of signs of digital breach and additional technical information, even in the absence of a formal public attribution. When an alert merely links the incident to a State in general terms, without identifying a concrete perpetrator, such a statement does not qualify as public attribution. Consequently, it fails to meet the evidentiary threshold required to enable effective cross-checking.[16] However, when an attribution intended to enhance network security explicitly identifies a specific State as responsible, it should be subject to the evidentiary standard necessary to permit cross-checking.

3. INTERNATIONAL LAW STANDARD FOR CYBERATTACK ATTRIBUTION

3.1. Need for Cyberattack Attribution Standard

The absence of established international legal norms governing evidence in the context of cyberspace creates significant obstacles for attributing cyberattacks. Simultaneously, it creates a new opportunity for the development of a dedicated evidentiary *lex specialis*. Progress in this area could be driven by a small number of States either those possessing advanced cyber capabilities or those that have experienced major cyber intrusions - through the adoption or promotion of specific evidentiary standards. This process may lead to forming international customary law for evidentiary standards.[17] The biggest side effects and benefits of evidentiary standard may be providing more clarity to credible attributions requirements and ensuring more transparency about states' behaviour in cyberspace. However, to achieve above-mentioned benefits evidentiary standard requires being part of the customary international law.

The previously discussed requirement to present sufficient evidence to enable cross-checking plays a critical role in the cybersecurity domain, particularly given the limited transparency surrounding State behavior and the fact that significant attribution verification capabilities often reside outside governmental institutions. However, the utility of the cross-checking standard extends beyond cybersecurity.[18] At its core, it reflects the principle of "trust, but verify." Establishing an evidentiary standard that facilitates and encourages verification of State attribution claims, by both state and non-state actors, would enhance the credibility of such claims and promote wider international acceptance of allegations concerning cyberoperations. As a *lex specialis* begins to take shape in the cybersecurity field, it holds the potential to evolve into a broader *lex generalis*, offering clarity on evidentiary standards that have remained ambiguous in non-cyber contexts, such as in past incidents involving disputed State responsibility, including allegations against Iran for the mining of oil tankers and the downing

16 Eichensehr, K., 2016. "Your account may have been targeted by state-sponsored actors": Attribution and evidence of state-sponsored cyberattacks. *Just Security*, 11 January. [Online] available at: <https://www.justsecurity.org/28731/your-account-targeted-state-sponsoredactors-attribution-evidence-state-ponsored-cyberattacks> [Accessed 6.05.2025. Conclusion].

17 Chinkin, C., 2003. Normative development in the international legal system. In: Shelton, D., ed. *Commitment and compliance: The role of non-binding norms in the international legal system*. Oxford: Oxford University Press, pp. 21, 30.

18 Tsagourias, N. and Buchan, R., 2021, *Research Handbook on International Law and Cyberspace*. 2nd ed. Cheltenham: Edward Elgar, p. 170.

of a U.S. drone.[19]

Developing an evidentiary standard for the public attribution of state-sponsored cyberattacks is distinct from formulating a standard for allegations concerning conduct that does not constitute a breach of international law. A clear example of this distinction is traditional espionage. While such activities are typically in violation of national laws, they are not explicitly prohibited under international law.[20] In cases involving the expulsion of suspected spies, States typically refrain from disclosing the evidence underlying their decisions. The development of a *lex specialis* specifically for cyberattacks would not necessitate a departure from this established practice. Based on above-mentioned reasons, establishing a standard in cybersecurity context would be useful.

3.2. Options for Establishing Cyberattack Attribution Standard

Establishing international law requirement for evidence giving is quite direct process.[21] As it is well known, customary international law requires two elements: state practice and *opinio juris*. In terms of practice, speaking about state-to-state attributions that have been made in recent years, most of them come close to provide sufficient evidence for cross-checking.[22] As a matter of principle, all governmental attributions of cyberoperations should be supported by sufficient evidence to enable verification by other states and non-state actors. This evidentiary support may be presented through various channels, including indictments, sanctions announcements, or official press statements. Regarding *opinio juris*, several States, such as the United States of America, the Netherlands, France and the United Kingdom, have thus far denied the existence of a binding legal obligation to disclose such evidence.[23] However, this stance ought to evolve. Such a shift could occur relatively swiftly and with minimal difficulty. One of the key indicators of *opinio juris* is the issuance of public statements by State representatives affirming that a particular practice is required, permitted, or prohibited under customary international law. Accordingly, States could incorporate references to customary norms in their attribution statements, thereby contributing to the formation or clarification of international legal standards in this area.[24] It is not necessary for all States to agree on a new reality simultaneously; minimal or no objection is often sufficient.

There are States that do not engage in attributions by themselves, but such States may be part of the process by participating in U.N. General Assembly resolutions addressing the

19 Nessa, J.J., 2019. Self-defense in international law: What level of evidence? *Just Security*, 8 July. [Online] available at: <https://www.justsecurity.org/64796/self-defense-ininternational-law-what-level-of-evidence> [Accessed 4.05.2025. Conclusion].

20 Deeks, A., 2014. An international legal framework for surveillance. *Virginia Journal of International Law*, 55(2), p. 309.

21 Korzak, E., 2017. UN GGE on cybersecurity: The end of an era? *Diplomat*, 31 July. [Online] available at: <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.> [Accessed 6.05.2025. Introduction].

22 Smeets, M., 2022, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Oxford: Oxford University Press, p. 123.

23 Tsagourias, N. and Buchan, R., 2021, *Research Handbook on International Law and Cyberspace*. 2nd ed. Cheltenham: Edward Elgar, p. 166.

24 Compare. International Law Commission, 2018. *Draft conclusions on identification of customary international law, with commentaries*. Conclusion 10. [Online] available at: <https://legal.un.org/ilc/reports/2018/2018report.pdf> [Accessed 6.05.2025].

attribution of cyberoperations and the corresponding evidentiary standards.[25] Such resolutions may serve a dual function: they can contribute to the development of customary international law and simultaneously indicate that such legal norms have already emerged, as evidenced by the presence of *opinio juris* among a majority of States.[26] At present, States have the opportunity to engage in one of two active United Nations processes aimed at shaping legal norms for cyberspace: the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE). Both bodies produce reports that may carry relevance for the identification and evolution of customary international law.[27]

Another way to regulate evidence standards is a cybersecurity treaty. However, this idea did not found supporters. Even the United States was against it.[28] However, existence of certain rules would make the process of attribution much easier. If any State is making attribution without necessary evidence provided, it will be apparent that rule of proof has been disregarded. Other way to regulate the subject is establishment the standard of evidence in customary international law. Two steps should be followed in this case: 1) the identification of consistent and widespread State practice, and 2) the presence of a belief that such practice is carried out of a sense of legal obligation (*opinio juris*). While the development of customary norms typically requires time and are shaped by the conduct of States, it remains a significant mechanism for addressing emerging legal challenges.[29] Standards of evidence have the potential to solidify into a norm recognized under customary international law.

3.3. Challenges of Establishing Cyberattack Attribution Standard

Establishing evidentiary standards has some difficulties. Providing evidence on cyberattack is a very hard technical aspect, because most actions in cyberspace do not leave trace.[30] In some cases, States do not want to unveil their sources of information and want them to stay covert. On the contrary, attributions with evidence provided are more legitimate and have more chance to gain support from international commonwealth. There-

25 U.N. General Assembly resolutions generally require the vote of a "majority of the members present and voting." U.N.G.A., *Rules of procedure of the General Assembly, paras 85–86*. [Online] available at: <https://docs.un.org/en/A/520/Rev.19> [Accessed 8.04.2025].

26 International Law Commission, 2018. *Draft conclusions on identification of customary international law, with commentaries*. U.N. Doc. A/73/10, pp. 141; 147–148. [Online] available at: <http://legal.un.org/docs/?path=./ilc/texts/instruments/english/commentaries/1_13_2018.pdf&lang=EF> [Accessed 4.05.2025].

27 Group of Governmental Experts, 2025. *U.N. Office for Disarmament Affairs*. [Online] available at: <https://www.un.org/disarmament/group-of-governmental-experts> [Accessed 4.05.2025]; Open-Ended Working Group, 2025. *U.N. Office for Disarmament Affairs*. [Online] available at: <https://www.un.org/disarmament/open-ended-working-group> [Accessed 4.05.2025]. Compare. also Grigsby, A., 2018. The United Nations doubles its workload on cyber norms, and not everyone is pleased. *Council on Foreign Relations*. [Online] available at: <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased> [Accessed 4.05.2025].

28 Nye, J.S., 2017, Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), p. 54.

29 Brown, G. and Poellet, K., 2012. The customary international law of cyberspace. *Strategic Studies Quarterly*, 6, p. 136.

30 Tsagourias, N. and Buchan, R., 2021. *Research Handbook on International Law and Cyberspace*. 2nd ed. Cheltenham: Edward Elgar, p. 157.

fore, establishing legal standards for providing evidence to enable attribution has more benefits than downsides.

At present, States often refrain from referencing international law when issuing political attributions of cyberattacks. This reluctance stems from the lack of clarity in existing international legal frameworks concerning the evidentiary standards that should be met when accusing another state of committing an internationally wrongful act.[31] In 2015, the UN Group of Governmental Experts tried to establish a necessity to provide the proof while making attribution for cyberattack.[32] Main goal was to avoid political tension between States. However, they had to recognize that this was their will, but not the obligation under international law.[33]

Moreover, there is no uniform approach to attribution among states. It is up to each State to decide whether to give publicity to the case and provide evidence enough to enable attribution. States determine the format, the manner in which evidence is made public, and how attribution is presented.[34] In recent past the United States of America, Canada and United Kingdom agreed to issue a collective condemnation of the activities performed by the cyber espionage group APT29.[35] The latter aimed at various organizations working on Covid-19 vaccine and their goal was to steal information. The joint report concluded, that group of hackers was "almost certainly part of Russian intelligence services."[36] The attribution of this case included facts that justified the claim and had the form of joint advisory.

As it is for now, under international law, States are not legally obligated to disclose evidence in support of their attribution of cyber-operations. That is the reason why forms of attribution differ from each other. It is significant to observe that coordinated attributions involving multiple states or coalition is quite effective and adds some legitimacy to the subject. States like United Kingdom and Netherlands[37] share their position and stressed that political attributions may be made without the need to disclose supporting evidence or reveal its origin. A number of States do not agree with this approach, like Switzerland,

---

31 Green, J.A., 2009. Fluctuating evidentiary standards for self-defence in the International Court of Justice. *International and Comparative Law Quarterly*, 58(1), p. 164.

32 United Nations General Assembly, 2015. *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*. U.N. Doc. A/70/174, p. 13. [Online] available at: <https://undocs.org/A/70/174> [Accessed 26.03.2025].

33 Tallinn Manual 2.0, supra note 3, 83.

34 Eichensehr, K., 2020. The law and politics of cyberattack attribution. *U.C.L.A. Law Review*, 558. Advisory Council of International Affairs, 2011. *Cyber warfare*. AIV/22, p. 15. [Online] available at: <https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare> [Accessed 26.03.2025].

35 United Kingdom's National Cyber Security Centre (NCSC), Canada's Communications Security Establishment (CSE) and United States' National Security Agency (NSA), 2020. *Advisory: APT29 targets COVID-19 vaccine development*. [Online] available at: <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development> [Accessed 3.04.2025].

36 Ibid.

37 Government of the Netherlands, 2019. *Letter to the Parliament on the international legal order in cyberspace*, 26 September. [Online] available at: <https://www.rug.nl/cf/onderzoek-gscf/research/research-centres/dataresearchcentre/pdfs/351564-okp-blog-post2.pdf> [Accessed 20.03.2025]. Wright, J., 2018. Cyber and international law in the 21st century. *UK Government*, 23 May. [Online] available at: <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [Accessed 20.03.2025].

who has provided detailed report of a cyber incident, without any further actions, including political attribution.[38] The amount of evidence provided while making attribution varies according to country and the manner in which attribution is presented itself. In the United States of America for political attribution mainly is used form of less detailed press release,[39] but Department of Homeland Security or FBI uses more detailed technical text.[40]

3.4. Establishing Cyberattack Attribution Standard: A Way Forward

The advantage of convincing States to present evidence while making attribution is prevention of false accusations. False accusations can be harmful for both sides in different ways. In 2015, the United States attributed the cyber intrusion into the Office of Personnel Management to the People's Republic of China (PRC).[41] Accusations were made without any evidence, so Chinese side called this claims a speculation.[42] In such situations, lack or absence of evidence may be very harmful and have decisive effect on the outcome.

Establishing international law standards in other areas is necessary. The latter approach may yield a more favorable outcome, as the evidentiary requirements under existing international law are even less well-defined in cases that fall below the threshold of an armed attack. Most cyberoperations beneath this threshold may still amount to a use of force or constitute other breaches of international law, such as infringements on the principle of non-intervention.[43] In such circumstances, attribution entails an accusation of a breach of international law. These accusations should be substantiated by evidence sufficient to permit cross-checking by other actors. Where a victim State reasonably asserts that an internationally wrongful act has occurred, it may be justified in adopting countermeasures. The assertion of such a violation alters the legal relationship between the States concerned. Consequently, the provision of evidence supporting both the occurrence and attribution of the initial wrongful act becomes essential

38 GovCERT.ch, 2016. *APT Case Ruag: Technical Report*. MELANI: GovCERT. [Online] available at: <https://perma.cc/2XKP-4FAX> [Accessed 25.03.2025].

39 U.S. Department of Homeland Security, 2016. *Joint statement from the Department of Homeland Security and Office of the Director of National Intelligence on election security*, 7 October. [Online] available at: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> [Accessed 24.04.2025].

40 Cybersecurity & Infrastructure Security Agency, 2018. *Russian government cyber activity targeting energy and other critical infrastructure sectors - Alert (TA18-074A)*, 15 March. [Online] available at: <https://us-cert.cisa.gov/ncas/alerts/TA18-074A> [Accessed 24.04.2025].

41 Eichensehr, K., 2020. Cyberattack attribution and international law. *Just Security*, 24 July. [Online] available at: <https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law> [Accessed 22.03.2025. Conclusion].

42 Ministry of Foreign Affairs of the People's Republic of China, 2015. *Foreign Ministry spokesperson Hong Lei's regular press conference on June 5, 2015*, 5 June. [Online] available at: <https://time.com/3910897/office-personnel-management-hack/?utm_source=chatgpt.com> [Accessed 22.03.2025].

43 Goodman, R., 2017. International law and the US response to Russian election interference. *Just Security*, 5 January. [Online] available at: <https://www.justsecurity.org/35999/international-law-response-russian-election-interference> [Accessed 6.05.2025. Conclusion]. Hollis, D., 2016. Russia and the DNC hack: What future for a duty of non-intervention? *Opinio Juris*, 25 July. [Online] available at: <http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/> [Accessed 6.05.2025. Introduction].

for evaluating the legality of the countermeasures taken in response.[44]

The credibility of the State providing evidence and relationship with the attributed State can affect the amount of evidence required to enable cross-checking.[45] The development of a clear legal standard requiring sufficient evidence to allow for cross-checking reduces the influence of geopolitical rivalry and reputational considerations in the attribution process. Although international law imposes obligations primarily on States, non-governmental entities engaging in attribution activities are also expected to adhere to its norms, principles and the standard for evidence-giving as well.[46] Standards for providing sufficient evidence to enable cross-checking should stay unchanged for nongovernmental attributors as well. This condition would help ensure that attributions made by non-governmental actors contribute to a common and coherent understanding of State conduct in cyberspace, thereby promoting greater stability and reducing the risk of conflict through enhanced transparency.

CONCLUSION

Attribution of cyberattacks is relevant tool to maintain stability through deterrence. Attribution serves as a mechanism for identifying and publicly condemning conduct that breaches established norms of responsible behavior in cyberspace. Nowadays, States provide some level of evidence to enable attribution, but this action comes from their domestic policies and there is no international law standards or regulations. The majority of potential evidentiary standards could eventually be governed by customary international law. However, the development of such norms requires time. The emergence of customary law depends on a consistent and widespread State practice of presenting a defined threshold of evidence to support attribution, accompanied by a sense of legal obligation (*opinio juris*) in doing so. All this process will prevent States from shifting their practices and become more consistent while making attributions. Next step for attribution should be cross-checking process and all this system will make political attributions and statements more verifiable and transparent at the same time. The latter would promote greater stability both within cyberspace and across the broader international legal order.

BIBLIOGRAPHY:

Used Literature:

1. Brown, G. and Poellet, K., 2012. The customary international law of cyberspace. *Strategic Studies Quarterly*. (in English)
2. Chinkin, C., 2003. Normative development in the international legal system. In: D. Shelton, ed. *Commitment and compliance: The role of non-binding*

44 Compare. International Law Commission (ILC), 2001. *Draft articles on responsibility of states for internationally wrongful acts, with commentaries*. Articles 49–54, particularly Article 52.

45 Finnemore, M. and Hollis, D., 2020. Beyond naming and shaming: Accusations and international law in cybersecurity. *European Journal of International Law*, p. 19.

46 Rid, T. and Buchanan, B., 2015, Attributing Cyber Attacks, *Journal of Strategic Studies*, 38(1–2), pp. 14, 35.

norms in the international legal system. Oxford: Oxford University Press. (in English)
3. Crootof, R., 2019. Regulating new weapons technology. In: R. Alcala and E.T. Jensen, eds. *The impact of emerging technologies on the law of armed conflict*. The Lieber Studies Series. New York: Oxford University Press. (in English)
4. Deeks, A., 2014. An international legal framework for surveillance. *Virginia Journal of International Law*. (in English)
5. Egan, B.J., 2017. International law and stability in cyberspace. *Berkeley Journal of International Law*. (in English)
6. Finnemore, M. and Hollis, D., 2020. Beyond naming and shaming: Accusations and international law in cybersecurity. *European Journal of International Law*. (in English)
7. GovCERT. ch, 2016. *APT Case Ruag: Technical Report*. MELANI: GovCERT. [Online] available at: <https://perma.cc/2XKP-4FAX> [Accessed 25.03.2025]. (in English)
8. Government of the Netherlands, 2019. *Letter to the Parliament on the international legal order in cyberspace.* [Online] available at: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace?> [Accessed 20.03.2025]. (in English)
9. Green, J.A., 2009. Fluctuating evidentiary standards for self-defence in the International Court of Justice. *International and Comparative Law Quarterly*. (in English)
10. International Law Commission, 2001. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. Yearbook of the International Law Commission, 2001, Vol. II, Part Two. [Online] available at: <https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf> [Accessed 13.05.2025]. (in English)
11. International Law Commission, 2018. *Draft conclusions on identification of customary international law, with commentaries*. Conclusion 10. [Online] available at: <https://legal.un.org/ilc/reports/2018/2018report.pdf> [Accessed 6.05.2025]. (in English)
12. International Law Commission (ILC), 2001. *Draft articles on responsibility of States for internationally wrongful acts, with commentaries*. (in English)
13. Mandiant, 2013. *APT1: Exposing one of China's cyber espionage units*. [Online] available at: <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> [Accessed 6.05.2025]. (in English)
14. Mashaw, J.L., 2008. Reasoned administration: The European Union, the United States, and the practice of democratic governance. *George Washington Law Review*. (in English)
15. Nye, J.S., 2017. Deterrence and Dissuasion in Cyberspace, *International Security*, 41(3). (in English)
16. Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. *Journal of Strategic Studies*. (in English)
17. Schmitt, M.N., 2017. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. 2nd ed. Cambridge: Cambridge University Press. (in English)
18. Smeets, M., 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Oxford: Oxford University Press. (in English)
19. Tams, C.J., 2010, *Enforcement by Measures Short of Force: Article 49*, in Crawford, J., Pellet, A. and Olleson, S. (eds.) *The Law of International Responsibility*. Oxford: Oxford University Press. (in English)
20. Tsagourias, N. and Buchan, R., 2021. *Research Handbook on International Law and Cyberspace*. 2nd ed. Cheltenham: Edward Elgar. (in English)
21. United Nations General Assembly, 2015. *Report of the Group of Governmental Experts on developments in the field of*

information and telecommunications in the context of international security. U.N. Doc. A/70/174. [Online] available at: <https://undocs.org/A/70/174> [Accessed 26.03.2025]. (in English)

22. U.N. General Assembly resolutions generally require the vote of a "majority of the members present and voting." U.N.G.A., *Rules of procedure of the General Assembly, paras 85-86. [Online] available at:* <https://docs.un.org/en/A/520/Rev.19> [Accessed 8.04.2025]. (in English)
23. U.S. Department of Justice, 2025. Principles of federal prosecution. *Justice Manual*. [Online] available at: <https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution> [Accessed 7.05.2025]. (in English)

Internet Resources:

1. Cybersecurity & Infrastructure Security Agency, 2018. *Russian government cyber activity targeting energy and other critical infrastructure sectors - Alert (TA18-074A)*, 15 March. [Online] available at: <https://us-cert.cisa.gov/ncas/alerts/TA18-074A> [Accessed 24.04.2025]. (in English)
2. Eichensehr, K., 2020. Cyberattack attribution and international law. *Just Security.* [Online] available at: <https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law> [Accessed 22.03.2025]. (in English)
3. Eichensehr, K., 2020. The law and politics of cyberattack attribution. *U.C.L.A. Law Review*. Advisory Council of International Affairs, 2011. *Cyber warfare*. AIV/22. [Online] available at: <https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare> [Accessed 26.03.2025]. (in English)
4. Eichensehr, K., 2016. Your account may have been targeted by state-sponsored actors: Attribution and evidence of state-sponsored cyberattacks. *Just Security*. [Online] available at: <https://www.justsecurity.org/28731/your-account-targeted-state-sponsoredactors-attribution-evidence-state-ponsored-cyberattacks> [Accessed 6.05.2025]. (in English)
5. Goodman, R., 2017. International law and the US response to Russian election interference. *Just Security.* [Online] available at: <https://www.justsecurity.org/35999/international-law-response-russian-election-interference> [Accessed 6.05.2025]. (in English)
6. Grigsby, A., 2018. The United Nations doubles its workload on cyber norms, and not everyone is pleased. *Council on Foreign Relations.* [Online] available at: <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased> [Accessed 4.05.2025]. (in English)
7. Group of Governmental Experts, 2025. *U.N. Office for Disarmament Affairs*. [Online] available at: <https://www.un.org/disarmament/group-of-governmental-experts> [Accessed 4.05.2025]. (in English)
8. Hollis, D., 2016. Russia and the DNC hack: What future for a duty of non-intervention? *Opinio Juris.* [Online] available at: <http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/> [Accessed 6.05.2025]. (in English)
9. Korzak, E., 2017. UN GGE on cybersecurity: The end of an era? *Diplomat.* [Online] available <https://www.rug.nl/cf/onderzoek-gscf/research/research-centres/dataresearchcentre/pdfs/351564-okp-blog-post2.pdf > [Accessed 6.05.2025]. (in English)
10. Ministry of Foreign Affairs of the People's

Republic of China, 2015. *Foreign Ministry spokesperson Hong Lei's regular press conference on June 5, 2015.* [Online] available at: <https://time.com/3910897/office-personnel-management-hack/?utm_source=chatgpt.com> [Accessed 22.03.2025]. (in English)

11. Moynihan, H., 2019. *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*. London: Chatham House. [Online] available at: <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/7-conclusions-and-recommendations> [Accessed 6.05.2025] (in English)
12. Nakashima, E., 2016. Cyber researchers confirm Russian government hack of Democratic National Committee. *Washington Post*. [Online] available at: <https://www.washingtonpost.com/world/national-security/cyber-researchers-confirmrussian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html> [Accessed 20.03.2025]. (in English)
13. Nessa, J.J., 2019. Self-defense in international law: What level of evidence? *Just Security*. [Online] available at: <https://www.justsecurity.org/64796/self-defense-ininternational-law-what-level-of-evidence> [Accessed 4.05.2025]. (in English)
14. Open-Ended Working Group, 2025. *U.N. Office for Disarmament Affairs*. [Online] available at: <https://www.un.org/disarmament/open-ended-working-group> [Accessed 4.05.2025]. (in English)
15. United Kingdom's National Cyber Security Centre (NCSC), Canada's Communications Security Establishment (CSE) and United States' National Security Agency (NSA), 2020. *Advisory: APT29 targets COVID-19 vaccine development*. [Online] available at: <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development> [Accessed 3.04.2025]. (in English)
16. U.S. Department of Homeland Security, 2016. *Joint statement from the Department of Homeland Security and Office of the Director of National Intelligence on election security*. [Online] available at: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> [Accessed 24. 04.2025]. (in English)
17. Wright, J., 2018. Cyber and international law in the 21st century. *UK Government*. [Online] available at: <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [Accessed 20.03.2025]. (in English)

Judicial Practice:

1. Addington, v. Texas, 441 U.S. 418, 425 (1979). (in English)
2. International Court of Justice, 2007, Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007, I.C.J. Reports 2007. (in English)
3. International Court of Justice, 2007. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment. (in English)