sciendo

Attribution of Cyber Operations: Technical, Legal and Political Perspectives[1]

Jakub Spáčil

Palacký University Olomouc, Czech Republic
jakubspacil@gmail.com

SPÁČIL, Jakub. Attribution of Cyber Operations: Technical, Legal and Political Perspectives. *International and Comparative Law Review*, 2024, vol. 24, no. 2, pp. 150–168. DOI: 10.2478/iclr-2024-0022

Summary: The article deals with the issue of attribution of cyber operations from the technical, legal and political point of view. The first part is devoted to the possibilities of technical attribution, which have increased significantly in connection with the development of technology and the sharing of information about attackers. The second part discusses the issue of legal attribution for purposes of state responsibility under international law, with attention also given to the burden of proof and standard of proof. The third part briefly summarizes the problem of political attribution and the possibility of establishing an international attribution mechanism.

Keywords: attribution, state responsibility, cyber operations, technical attribution, legal attribution, political attribution, cyber forensics

1 Introduction

States are increasingly becoming victims of cyber operations, whether it is simple espionage or more serious attacks against critical infrastructure. Effective defences against these operations require a strict distinction between the crimes of independent individuals and criminal organisations on the one hand, and actions attributable to states on the other.[2] While theoretically every action of an individual or organization is linked to a specific state on the basis of its nationality or place of registration, from the perspective of international law only those actions are attributable to a state in which the state has actively participated in one of the defined ways (e.g. the actions of a state organ or the actions of another entity on the basis of instructions or under the direction or control from the state) – the so-called legal attribution of a conduct.[3]

1 This work was supported by the student project „Legal remedies for defence against cyber operations of non-state actors from the perspective of international law“ (IGA_PF_2023_002) of the Palacky University. The article was supervised by prof. JUDr. Dalibor Jílek, CSc.

2 SKOPIK, Florian and PAHI, Timea. Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity*, 2020, vol. 3, p. 1.

3 INTERNATIONAL LAW COMMISSION. *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. 2001, vol. II, part two, pp. 38 (hereinafter “ARSIWA”).

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

Only conduct that is legally attributable to a state may constitute an internationally wrongful act within the meaning of Article 2 of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts (hereinafter ARSIWA). Proving an internationally wrongful act activates an obligation of the breaching State of cessation of the wrongful act, provision of assurances and guarantees of non-repetition and reparation.[4]

From the perspective of effective defence against cyber operations, however, legal attribution has another important role to play – if other conditions are met, it is a prerequisite for taking countermeasures and acting in self-defence. These two instruments of international law provide the greatest scope for states to take defensive measures in the event that the state becomes a victim of a cyber operation.[5]

Legal attribution is one of the main challenges associated with defending against cyber operations at the international level.[6] Its proper implementation requires sufficient information about the attacker, the cyber operation and the overall context, since, compared to operations carried out in the real world, operations in cyberspace involve a "degree of anonymity orders of magnitude beyond that of a kinetic attack".[7]

Misidentification of an attacker, or missatribution to an innocent state, can lead to escalation with potentially devastating consequences.[8] Cyberspace not only allows attackers to hide their own identity, but can also result in the redirection of attention to an innocent state by, for example, routing data flows through that third state as part of a cyber operation. A similar approach is essentially impossible in the case of conventional attacks. Victim states are therefore challenged in determining the perpetrator of a cyber operation to obtain sufficient relevant information in a limited time, to correctly identify the perpetrator of a malicious cyber operation, and to take effective measures that are nonetheless fully consistent with international law. The technical and legal complexity of attribution and the risks associated with misattribution place the victim state in a difficult situation because, as Payne and Finlay put it, "[g]etting the balance wrong may result in either increased likelihood of escalation of international tension and conflict caused by misdirected retaliation due to flawed

4 ARSIWA, arts. 30 and 31.

5 DEDERER Hans-Georg and SINGER Tassilo. Adverse Cyber Operations: Causality, Attribution, Evidence, and Due Diligence. *International Law Studies*, 2019, vol. 95, p. 456.

6 NGUYEN, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare, *California Law Review*, 2013, vol. 101, no. 4, p. 1104; PRECIADO, Michael. If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure from Cyber Warfare. *Journal of Law & Cyber Warfare*, 2012, vol. 1, no. 1, p. 137.

7 NGUYEN: *Navigating Jus Ad Bellum...*, p. 1104.

8 SKOPIK, PAHI: *Under false flag...*, p. 1; SCHMITT, Michael, N. et al. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, 2017, p. 92.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

attribution or, alternatively, rendering law-abiding states unable to respond to cyber-attack because legal attribution is impossible to establish".[9]

Accurate legal attribution is the result of gathering enough information about a cyber operation, usually a combination of computer data and human intelligence, that in aggregate allows the victim state to conclude with a sufficient degree of certainty (meeting the *standard of proof*) which state (if any) bears international legal responsibility for such a cyber operation.

When talking about attribution of cyber operations, it is necessary to distinguish between three types of attribution: legal, technical and political.[10] From the perspective of international law and the adoption of legal defensive measures (countermeasures, self-defence), legal attribution is key, but it is inextricably linked to technical attribution, since only if it is proven who is behind the cyber operation can conclusions be drawn in relation to legal attribution, i.e. whether there is a relationship between the attacker and the state of origin that would allow attribution of the conduct to the state. Political attribution then forms a separate category, but one that cannot be ignored as most of the public attribution so far constitute a political, not legal attribution.[11]

Research on the issue of attributability of cyber operations can only be truly productive if the phenomenon is examined in its entirety, i.e., taking into account legal, technical and political aspects. Therefore, this article follows this structure. The first subchapter is a more detailed introduction to the issue of attribution and its significance in the context of cyber operations and international law. The second subchapter examines how technical attribution is implemented and whether it provides a sufficient basis for legal attribution. The third subchapter examines legal attribution and its problematic aspects, in particular the standard of proof required and the strength of the relationship that must exist between the conduct of the attacker and the state in order to conclude that the conduct is legally attributable to the state. The fourth subchapter briefly discusses the meaning of political attribution and the relationship between legal and political attribution. The fifth subchapter addresses whether there should be an international institution or organization tasked with authoritatively deciding on the attribution of cyber operation.

The aim of the article is to answer the following questions based on the analysis of the literature and available state practice: Do current methods of forensic computer analysis allow the identification of a specific attacker with

---

9 PAYNE, Christian and FINLAY, Lorraine. Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *George Washington International Law Review*, 2017, vol. 49, no. 3, p. 566.

10 OSULA, Anna-Maria, KASPER, Agnes and KAJANDER, Aleksi. EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 2022, vol. 16, no. 1, p. 106.

11 TSAGOURIAS, Nicholas and FARRELL, Michael. Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, 2020, vol. 31, no. 3, pp. 945–946.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

a sufficient degree of certainty? What intensity of the relationship between the attacker and the state is required by international law in order to conclude that a cyber operation is legally attributable to that state? Who bears the burden of proof and what is the standard of proof in relation to legal attribution? What is the relationship between legal and political attribution? Is the establishment of an international attribution organisation an appropriate tool to enhance the credibility of legal and technical attribution?

2 Attribution of cyber operations

In 2002, Daniel D. Singer mentioned, that attribution is "the most important practical obstacle to applying the law of jus ad bellum to cyber-attack".[12] He was referring, of course, to legal attribution as a prerequisite to the exercise of the right of self-defense. Over the next two decades, a number of authors made similar points, and in 2012 Handler spoke of the "technical improbability of resolving this challenge in the near future".[13] The fact is, however, there have been significant developments in the field of technical analysis since 2002, and thus in 2018 van der Meer could state that "[i]n the past few years the technical possibilities of cyber forensics have developed rapidly, and indisputable attribution seems to become increasingly feasible".[14] In the section on technical attribution, we look at this issue in detail.

To add context, it should be noted that not all measures against cyber operations are contingent on a demonstration of state responsibility. Attribution is necessary for taking action based on countermeasures and the right of self-defence. However, measures at the level of retorsion or based on the plea of necessity justification can be taken even in the absence of a demonstration of state responsibility (provided, of course, that the other conditions are met).[15] Nevertheless, countermeasures and self-defence are the most significant circumstances precluding wrongfulness, allowing for significant interference with the rights of other States, and in the case of self-defence even with the prohibition on the use of force. It is therefore entirely appropriate to pay attention to this issue, as misattribution could lead to consequences as dire as conventional military conflict.

---

12 SILVER, Daniel, B. Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter. In SCHMITT Michael, N. and O'DONNELL, Brian, T. (eds.). *Computer Network Attack & International Law*. Newport: Naval War College, 2002, p. 76.

13 HANDLER, Stephenie, Gosnell. The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare. *Stanford Journal of International Law*, 2012, vol. 48, no. 1, p. 215.

14 van der MEER, Sico. State-level responses to massive cyber-attacks: a policy toolbox. *Clingendael: Netherlands Institute of International Relations*, 2018, p. 2.

15 See e. g. SPÁČIL, Jakub. Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 2022, vol. 16, no. 2, pp. 215–239.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

A topic that will not be addressed in this article, on the other hand, is the relationship between due diligence and attribution, as this topic received ample attention in other publications.[16]

Before discussing the different types of attribution, it is also necessary to briefly consider terminology. In this paper, the division between technical, legal and political attribution is used because this terminology *prima facie* demonstrates that there is a relationship between these concepts, but at the same time makes it clear that they are not the same. This terminology is, in fact, prevalent in the doctrinal debate.[17] However, some authors use other labels to refer to the same concepts, such as factual attribution[18] , cyber forensics[19] or causality[20] for technical attribution.

3 Technical attribution

Technical attribution can be defined as "using technology to identify a cyber operation's originator".[21] The aim of technical attribution is to identify as accurately as possible the specific device from which the cyber attack was carried out and the individuals, groups or organisations involved.[22] This is based on forensic investigation.[23]

3.1 Historical development

Until recently, technical attribution was considered one of the biggest challenges related to cyber operations. However, this situation has changed in the last few years and technical attribution is becoming more and more possible and credible.[24]

---

16 DEDERER, SINGER: *Adverse Cyber Operations...,* p. 440; SPÁČIL, Jakub. Countermeasures against Cyber Operations: Moving forward?. *International and Comparative Law Review*, 2023, vol. 23, no. 2, pp. 100–102.

17 OSULA, KASPER, KAJANDER: *EU Common Position...*, p. 106. ; TSAGOURIAS, FARRELL: *Cyber Attribution...,* p. 942. GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS. Appendix: International law in cyberspace. [online]. Available at: <https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf> Accessed: 24. 3. 2024.

18 SCHMITT, Michael, N. Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 2017, vol. 8, no. 2, p. 254.

19 BANNELIER, Karine and CHRISTAKIS, Theodore. *Cyber-Attacks: Preventions-Reactions: The Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale, 2017, p. 45.

20 DEDERER, SINGER: *Adverse Cyber Operations...,* p. 436.

21 SCHMITT, Michael, N. Terminological Precision and International Cyber Law. [online]. Available at: <https://lieber.westpoint.edu/terminological-precision-international-cyber-law/> Accessed: 24. 3. 2024.

22 DEDERER, SINGER: *Adverse Cyber Operations...,* p. 436.

23 TSAGOURIAS, FARRELL: *Cyber Attribution...*, p. 942.

24 BANNELIER, CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* p. 45.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

However, this does not mean that the problem has been completely solved.[25] On the one hand, there are the constantly evolving cyber forensic capabilities of the computer specialist and, on the other hand, new techniques and greater vigilance and new technologies and practices on the part of the attackers. Although some authors believe that effective technical attribution is only a matter of time and technology development,[26] it seems more reasonable trust the more skeptical part of the scientific community that expects technical attribution to be one of the major obstacles to legal attribution in the long run.[27] This conclusion stems from the fact that new techniques and practices are being adopted by both sides and, logically, attackers will always be one step ahead at least in some aspects, since it is impossible to create a computer system that does not contain exploitable flaws, and it is often the hackers (whether in the service of the state or not) who discover and exploit these flaws, sometimes with irreversible consequences.

3.2 Process of attribution and evidence

The process of attribution has developed over the years. Each State chooses partially different procedures for determining the perpetrator of a cyber operation, but in the end, the assessment is of similar aspects. This process can be clearly demonstrated, as Tsagourias and Farrell have also done, using the publicly available methodology produced by the United States Office of the Director of National Intelligence (ODNI).[28]

ODNI uses a matrix of five indicators (tradecraft, infrastructure, malware, intent and external sources) to attribute cyber operations. Each indicator is then assigned a value on the scale from "sufficient" to "limited confidence".[29] The technical attribution is based on an analysis of the computer data that was secured in the attack. IT specialists use this data, in conjunction with available information on previous attacks, to determine who carried out the cyber attack, from where, and through what device.[30] They use the above indicators in the following way.

Tradecraft can be defined as "collective behaviour frequently used to conduct cyber attacks, which forms a pattern that can be seen across time and location". Traceable elements of behaviour include procedures (e.g. delivery methods of the malware), personal information (email and social media accounts) or financial information (transactions, bank accounts, crypto wallets). Tradecraft can be considered the most important indicator, but its weight decreases with the release

25 Ibid.

26 DINSTEIN, Yoram. Computer Network Attacks and Self-Defence. In: SCHMITT Michel. N. and O'DONNELL, Brian T. (eds.). *Computer Network Attack & International Law*. Newport: Naval War College, 2002, p. 99.

27 PAYNE, FINLAY: *Addressing Obstacles to Cyber-Attribution...* p. 560.

28 TSAGOURIAS, FARRELL: *Cyber Attribution...*, p. 947; US OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. A Guide to Cyber Attribution. [online] Available at: <https://dl.icdst.org/pdfs/files3/db004a6f55f96c056a23fc4efc6a23ac.pdf> Accessed: 24. 3. 2024.

29 Ibid.

30 TSAGOURIAS, FARRELL: *Cyber Attribution...*, p. 947.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

of information about techniques and procedures, as it allows other entities to mimic the behavior and thus mislead analysts.[31]

Infrastructure refers to communication structures that include domain names, DNS services, IP addresses and so on. The infrastructure can be obtained legally (buy, lease) or illegally (e. g. using infected zombie computers for DDoS attacks). Some actors tend to change infrastructure between or even during cyber operation while others repeatedly use the same systems.[32]

Malware is a malicious software designed to perform a cyber operation. Malware can perform various tasks such as key logging, screen capture, audio recording, remote command and control, and persistent access.[33] Malware can be created *ad hoc* for a particular task or can be used repeatedly for several cyber operations. The malware used may be one of the identifiers of the attacker, but its role cannot be overestimated, especially for publicly available malwares on the dark net.[34]

Intent takes into account whether the cyber operation fits into a broader context, such as an ongoing regional conflict or tensions between states.[35] The existence of a relevant geopolitical context supports the conclusion that an entity is behind the cyber operation, while the absence of such a context argues against its involvement and may indicate, for example, an attempted false flag operation.

Finally, data and information from private industry, the media, academia, and think tanks can serve as an external source of relevant information.

Generally speaking, the evidence from which information about the originator of a cyber attack can be obtained can be divided into two categories – technical data (digital evidence) and intelligence. Technical data includes, for example, IP addresses used, DNS servers, specific code sequences, compiler language, domain names, payment information, infrastructure registration, email and social media accounts, keyboard layout or operating system, language settings.[36] Intelligence consists of information from secret services, diplomatic representatives or other states.[37] Human intelligence can be evidence both for and against the conclusion that a particular state or non-state actor is behind an operation (e.g., information about the planned misuse of another state's computer infrastructure can be evidence in favour of the conclusion that that state was not behind the subsequent attack).[38] For technical (and consequently legal) attribution, it is usually necessary

---

31 Ibid.

32 US OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. *A Guide to Cyber Attribution*...

33 Ibid.

34 TSAGOURIAS, FARRELL: *Cyber Attribution*..., p. 949; DEDERER, SINGER: *Adverse Cyber Operations*..., p. 438.

35 US OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. *A Guide to Cyber Attribution*...

36 NGUYEN: *Navigating Jus Ad Bellum*..., p. 1105; TSAGOURIAS, FARRELL: *Cyber Attribution*..., p. 956.

37 NGUYEN: *Navigating Jus Ad Bellum*..., p. 1105.

38 SCHMITT: *Tallinn Manual 2.0*..., p. 92.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

to use both sources of information simultaneously, as technical analysis alone often does not provide (even with respect to the risk of false flag operations) sufficient information to draw a clear conclusion about the originator of a cyber operation.[39]

However, all these indicators work on a common premise: perpetrators make mistakes and "perfect cyber attack is as elusive as perfect crime".[40] The complexity of cyber operations inevitably leads to the perpetrators making mistakes.[41] For example, due to the number of processes and systems that need to be involved in order to successfully execute a cyber operation, an unintended use of an e-mail address that can be linked to a real person or institution may occur.[42] Another error is the repeated use of the same pieces of code in multiple attacks, which can link even seemingly unrelated cyber operations. For example, the Spanish origin of the Careto spyware was revealed by the use of slang words in the names of some files and folders.[43]

At the same time, however, caution must be exercised, because even in the case of apparent mistakes, there may be a deliberate attempt by the perpetrator to mislead the investigator, and it is therefore necessary to assess all available information in its context and in the overall situation.[44] As Singer aptly put it, "relying on the IP address would be like relying on license plates to identify drivers".[45] The fact that the source of a cyber-attack has been identified in a particular country (for example, by its IP address) is not in itself sufficient proof that that country is behind the operation.[46]

3.3 Partial conclusion

This section explained how and on the basis of what facts it is possible to conclude which device and which person, organisation or group was the perpetrator of the cyber attack. The attribution process has evolved considerably over the last twenty years and it is no longer the case that unequivocal identification of the perpetrator is impossible. Although technical attribution is still an obstacle, the combination of technical data and human intelligence can make it possible to determine with

---

39 DEDERER, SINGER: *Adverse Cyber Operations...,* p. 438; GOEL, Sanjay and NUSSBAUM, Brian. Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. *Journal of the Communications Society*, 2021, vol. 2, no. 1, p. 1091.

40 RID, Thomas and BUCHANAN, Ben. Attributing Cyber Attacks. *The Journal of Strategic Studies*, 2015, vol. 38, no. 1–2, p. 32.

41 TSAGOURIAS, FARRELL: *Cyber Attribution...*, p. 949.

42 Ibid, p. 950; SAALBACH, Klaus-Peter. Attribution of Cyber Attacks. In: REUTER, Christian. (ed.). *Information Technology for Peace and Security*. Springer Vieweg Wiesbaden, 2019, p. 287.

43 RID, BUCHANAN: *Attributing Cyber Attacks...*, pp. 16–17.

44 SCHMITT: *Tallinn Manual 2.0...*, p. 92.

45 SINGER, Peter, W. and FRIEDMAN, Allan. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014, p. 33.

46 OSULA, KASPER, KAJANDER: *EU Common Position...*, pp. 105–106.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

relative precision who is behind a significant share of cyber operations. However, technical attribution does not equate to legal attribution per se.[47]

4 Legal attribution

Legal attribution is based on the law of the state responsibility.[48] It often derives from technical attribution, but while technical attribution answers the questions "Which device was used? Where was it? Who (person, group or institution) was behind it?", legal attribution answers the questions "What is the nature of the relationship between the perpetrator and state? Does the state bear legal responsibility for the conduct of the perpetrator according to international law?".[49] It follows from the above that technical attribution is usually a prerequisite for legal attribution, since if the identity of the perpetrator is not known, it is impossible to assess the potential responsibility of the state for its actions. However, this does not mean that it is necessary to know the exact person acting in order to infer state responsibility, especially if the operation is carried out from state cyber infrastructure (e.g. military base), more on this below.

4.1 Legal framework

Legal attribution of a conduct to a state is not specific to cyber operations. It is one of the two conditions of an internationally wrongful act, the very existence of which is a prerequisite for the activation of secondary obligations of a state, and therefore plays a significant role in the issue of state responsibility under international law.[50] However, unlike other areas of state activities, it poses a significantly greater challenge in the case of cyber operations.

Rules of legal attribution are defined in art. 4 to 11 of ARSIWA. These articles are considered a codification of international law. While all of the rules might be relevant for cyber operations, the focus of this paper will be only on art. 4 and 8 as articles which are the most likely to come into play.

Art. 4 of ARSIWA deals with the conduct of state organs when it stipulates: "(1) The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State. (2) An organ includes any person or entity which has that status in accordance with the internal law of the State." As the commentary to this article explains, "The reference to a State organ covers all the individual or collective entities which make up the organization of the State."[51] In other words, if it is

47 TSAGOURIAS, FARRELL: *Cyber Attribution...*, p. 951.
48 SCHMITT: *Peacetime Cyber Responses...*, p. 254.
49 DEDERER, SINGER: *Adverse Cyber Operations...,* p. 436.
50 ARSIWA, Article 2.
51 ARSIWA, p. 40.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

proven that a cyber operation against another State that constitutes a "breach of an international obligation of the State",[52] was carried out by an organ of that State (e.g. military forces, secret services, governmental institution,...),[53] then such conduct is legally attributable to the State of origin (of the cyber operation) and the victim State may react according to the fact – i. e. invoke countermeasures or even self-defence in the case of an armed attack. A similar rule was also formulated by the Group of Experts for the Tallinn Manual 2.0.[54] In the case of liability under Article 4 of ARSIWA, States are also liable for the actions of an organ *ultra vires*, i.e. when the organ exceeds its authority or acts outside the defined instructions.[55]

It can be concluded that international law is relatively clear in the case of state organs and the greater challenge in this context is thus technical attribution. For example, if it is proven that a military unit specialized in cyber operations is behind the cyber operation, the state's responsibility under international law is clear. In the case of responsibility under Article 8 ARSIWA, however, the situation is different.

A substantial part of cyber operations are not carried out by state authorities, but by non-state actors (individuals, groups or organizations).[56] Even the actions of these actors may be attributable to the state under international law, and in particular under art. 8 ARSIWA. A prerequisite for legal attribution of a conduct of a non-state actor to a state is that the non-state actor "is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[57] The rule was similarly adopted in Tallinn Manual 2.0.[58]

State responsibility in this case derives from the factual (not legal) relationship between the perpetrator (non-state actor) and the state.[59] Typically, this is a situation where the state hires or otherwise arranges for an independent entity to carry out a cyber operation.[60] This may be advantageous for the responsible state given the difficulty of proving its liability and the relatively broad possibilities of denying it. In other words, the responsible state can achieve its objectives in this way (e.g., disrupting another state's electoral processes) while exposing itself to minimal risk of negative consequences.

The key question in this context is how intense a relationship (degree of control) between a state and a non-state actor is required by international law to make the conduct of the non-state actor legally attributable to the state.

---

52 ARSIWA, Article 2.
53 NGUYEN: *Navigating Jus Ad Bellum...,* p. 254.
54 SCHMITT: *Tallinn Manual 2.0...*, p. 87: "Cyber operations conducted by organs of a State or by persons or entities empowered by domestic law to excercise elements of governmental authority, are attributable to the state."
55 NGUYEN: *Navigating Jus Ad Bellum..., p. 254.*
56 ARSIWA, p. 49.
57 ARSIWA, Article 8.
58 SCHMITT: *Tallinn Manual 2.0...*, p. 94.
59 Ibid, p. 95.
60 ARSIWA, p. 47; SCHMITT: *Peacetime Cyber Responses...*, p. 254.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

International practice has defined two competing standards, namely "effective control" over the conduct and "overall control".[61]

The effective control test was developed by the International Court of Justice (ICJ) in the Nicaragua Case (1986) and subsequently confirmed in the Genocide Convention Case (2007).[62] This test requires a high degree of control on the part of the state over the conduct of the non-state actor ("complete dependence").[63] For example, the mere provision of funds does not constitute a sufficient degree of control to prove legal attribution.[64] Effective control is described in the Tallinn Manual 2.0 as control that "includes both the ability to cause a constituent activities of the operation to occur, as well as the ability to order the cessation of those that are underway".[65]

A competing control standard is the so-called overall control test. This was defined by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the Tadic Case (1999).[66] Compared to effective control, overall control requires a lower degree of interdependence between the conduct of the non-state actor and the instructions of the state, because legal attribution of the conduct to the state can be made "regardless of whether or not the State has issued specific instructions to those individuals". [67]

The existence of these competing tests naturally leads to debates about which one should be applied for legal attribution under international law. Even outside the context of cyber operations, support for both tests can be found, with the main argument for applying the lower standard (overall control) being that the higher standard (effective control) is "too burdensome with respect to the evidence threshold".[68] The fact remains, however, that the ICJ has refused the overall control test in the Genocide Case, thus confirming its previous jurisprudence and the necessity of the existence of effective control to impute state responsibility under art. 8 of ARSIWA.[69] In general, therefore, it can be concluded that although there

---

61 PAYNE, FINLAY: *Addressing Obstacles to Cyber-Attribution...* p. 557.

62 *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, ICJ, Judgement, 27 June 1986 (hereinafter *Nicaragua Case*); *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, ICJ, Judgement, 26 February 2007 (hereinafter *Genocide Convention Case*).

63 HANDLER: *The New Cyber Face of Battle...*, p. 214.

64 The Nicaragua Case; FAIX, Martin and BRUNER, Tomáš. Problém přičitatelnosti jako nástroj lawfare. *Defence & Strategy*, 2018, vol. 18, no. 2, pp. 3–4; VALUCH, Jozef and HAMUĽÁK, Ondrej. Use of Force in Cyberspace. *International and Comparative Law Review*, 2020, vol. 20, no. 2, p. 177.

65 SCHMITT: *Tallinn Manual 2.0...*, p. 96.

66 *Tadić Case (IT-94-1)*, ICTY, Judgement, 15 July 1999, para. 120.

67 Ibid, para. 123.

68 FAIX, BRUNER: *Problém přičitatelnosti...*, p. 4; SVAČEK, Ondřej. Srebrenica: Nicaragua nebo Tadic? K subjektivnímu prvku mezinárodně protiprávního jednání. In. Olomouc: Vydavatelství Univerzity Palackého, 2007, pp. 457–462.

69 Genocide Convention Case, para. 401–407; *see also* PAYNE, FINLAY: *Addressing Obstacles to Cyber-Attribution...* p. 557 and SCHMITT, Michael. N. „Below the Threshold" Cyber Operations:

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

are compelling arguments in favour of the overall control test, the effective control test remains the international law standard.[70]

A follow-up question is whether the effective control test should also be applied in relation to cyber operations. This is because, unlike conventional attacks, cyber operations are significantly more challenging to demonstrate such a high degree of interdependence between the actions of a non-state actor and a state, and at the same time it is significantly easier for non-state actors (given the readily available resources in the form of malware and low personnel and material requirements) to conduct a cyber operation with minimal state involvement.[71] Meanwhile, the standard set by the ICJ in Nicaragua Case requires that effective control be demonstrated in relation to each individual cyber operation that was intended to violate international law, which is extremely challenging for cyber operations.[72] A number of authors therefore take the view that a lower standard (overall control) should be applied in the context of cyber operations, given the specificities of these operations.[73] However, this view does not seem to be reflected in the practice of states. Indeed, when states comment on the issue of attribution, they refer to "effective control" in several cases, but not in any of them to "overall control".[74] Therefore, it should be noted that under current international law, the prerequisite for attribution under art. 8 of ARSIWA is a state's effective control over a particular cyber operation carried out by a non-state actor.

4.2 Burden of proof

Under international law, victim states are not required to disclose the evidence on the basis of which they conclude that a cyber operation is legally attributable to another state.[75] The decision whether to disclose such information in the context of legal attribution and subsequent actions (e.g., taking action based on countermeasures or self-defence) is a sovereign prerogative of each nation state.

The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 2015, vol. 54, no. 1, p. 713.

70 SCHMITT: *Tallinn Manual 2.0...*, p. 96.

71 HANDLER: *The New Cyber Face of Battle...*, p. 214.

72 DEDERER, SINGER: *Adverse Cyber Operations...,* p. 437.

73 HANDLER: *The New Cyber Face of Battle...*, p. 215; TSAGOURIAS, FARRELL: *Cyber Attribution...*, p. 962.

74 GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS: *Appendix: International law in cyberspace...*; UNITED NATIONS. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 of 13 July 2021, UN Doc. A/76/136 [online]. Available at: <https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf> Accessed: 24. 3. 2024 (Norway); IRISH DEPARTMENT OF FOREIGN AFFAIRS. Position Paper On The Application Of International Law In Cyberspace. [online]. Available at: <https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland--National-Position-Paper.pdf> Accessed: 24. 3. 2024.

75 BANNELIER, CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* pp. 46–47.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

That position is also publicly held by a larger number of states, such as Canada (2022),[76] Israel (2020),[77] Italy (2021),[78] Netherlands (2019)[79] or New Zealand (2020)[80]. However, disclosure of the evidence is at least appropriate, for several reasons. Firstly, its publication enhances the legitimacy of any subsequent action taken in the eyes of the international community. At the same time, it reduces the scope for denial and relativisation of attribution by the responsible state. Last but not least, the published evidence can significantly help other states with attribution of other cyber operations, for example, based on information about the infrastructure used. Nor can we overlook the conclusions adopted by the United Nations Group of Governmental Experts (UN GGE) in 2015, according to which, inter alia, "accusations of organizing and implementing wrongful acts brought against States should be substantiated".[81]

These facts, however, do not change the fact that the burden of proof is on the side of the victim state.[82] In other words, the victim state is obliged to prove (although it is not *ex ante* obliged to disclose the evidence) that another state is behind the cyber operation under international law (Articles 4-11 ARSIWA).[83] Although there is no obligation for a state to disclose in advance the evidence on which it has made the legal attribution, it should nevertheless have this evidence, not only because the obligation to prove legal attribution may arise later (see below), but also because misattribution may trigger the victim state's international law liability and also lead to escalation. This raises the question of what standard of proof a state must meet in order to dispatch its burden of proof.

---

76 GOVERNMENT OF CANADA. International Law applicable in cyberspace, international.gc.ca [online]. Available at: <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a9> Accessed: 26. 3. 2024.

77 SCHÖNDORF, Roy. Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law* Studies, 2021, vol. 97, no. 1, p. 405.

78 ITALY. *Italian Position Paper on `International Law and Cyberspace`*. [online]. Available at: <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf> Accessed: 26. 3. 2024.

79 GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS: *Appendix: International law in cyberspace...*

80 DEPARTMENT OF THE PRIME MINISTER AND CABINET, NEW ZEALAND. *The Application of International Law to State Activity in Cyberspace*. [online]. Available at: <https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf> Accessed: 26. 3. 2024;

81 UNITED NATIONS. Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security of 22 July 2015, UN Doc. A/70/174.

82 FAIX, BRUNER: *Problém přičitatelnosti...*, p. 4.

83 DEDERER, SINGER: *Adverse Cyber Operations...,* pp. 439–440.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

4.3 Standard of proof

On the national level, the common law standard of proof scale is clear. The "beyond reasonable doubt" is the highest standard of proof.[84] This is followed by the "preponderance of probability", according to which "the existence of the fact to be proved must be more likely than not".[85] The lowest standard of proof is "prima facie evidence". Civil law jurisdictions usually apply a uniform standard of proof which equates to the judge being "convinced" or "fully convinced".[86]

On the international level, a clear standard of proof is not defined.[87] Even the ICJ has not established the standard of proof that is required in proceedings before it.[88] The ICJ seems to work with a flexible standard of proof depending on how serious the breach of an international legal obligation is.[89] The more serious the breach, the higher the standard of proof.[90]

So what should be the standard of proof for legal attribution of cyber operations? Respecting the approach set by the ICJ, i.e. a flexible scale depending on the intensity of the breach of an international obligation, it is clear that it is necessary to distinguish the standard of proof for countermeasures and for self-defence. The reason for the distinction is that countermeasures cannot justify an interference with peremptory norms of international law, while the right of self-defence is one of the exceptions to the prohibition of the threat and use of force (ius cogens). Thus, in the case of self-defence, the only logical conclusion seems to be the requirement of the highest standard of proof found in the jurisprudence of the ICJ, namely evidence that is fully conclusive.[91] Conversely, for countermeasures, which by definition will always be a less serious violation of international law, one could settle for a lower standard of proof at the level of "preponderance of the evidence".[92]

5 Political attribution

Political attribution derives not from legal or technical considerations (although it may be based on them), but primarily from political considerations. It consists in the public designation of another state (or non-state actor) as the author of a cyber operation carried out by its organs or non-state actors.[93] International law does not stipulate a minimum amount of information (technical data or intelligence)

---

84 Ibid, p. 442.
85 Ibid.
86 Ibid.
87 CRAWFORD, James. *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge: Cambridge University Press, 2002, p. 124.
88 ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*, 2015, vol. 50, pp. 248–249.
89 Ibid.
90 For indepth analysis see DEDERER, SINGER: *Adverse Cyber Operations...,* pp. 442–445.
91 ROSCINI: *Evidentiary Issues...*, p. 250; Genocide Convention Case, para. 209.
92 DEDERER, SINGER: *Adverse Cyber Operations...,* p. 451.
93 SCHMITT: *Terminological Precision...*

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

that would be necessary for political attribution.[94] It is at the sole discretion of the state whether or not it assesses that it is politically advantageous for it to make public (or semi-public or private) political attribution. Political attribution has no legal consequences per se, but can legitimize for example retorsion measures (e. g. expulsion of diplomats, travel bans, freezing of assets, cancelling bilateral visits,...). In other words, a strict distinction must be made between legal and political attribution, as each has different assumptions and consequences.[95]

In public attribution, states generally do not specify whether it is legal or political attribution and it is necessary to base the assessment of what type of attribution is involved on the language used and the measures the victim state takes in response to the cyber operation (whether it is mere retorsion or countermeasures or even self-defence). Thus, for example, if states state that a cyber operation was "government-sponsored" or "state-sponsored" and identify a particular state, this is certainly political attribution, but it cannot be inferred from this terminology that it should also be legal attribution.[96] The fact is that although public attribution of a conduct to a state is becoming more and more common, for the time being it is always political and not legal attribution.[97] States are familiar with the terminology of legal attribution, and therefore it is to be expected that if indeed the public designation of another state as the author of a cyber operation were to give rise to international legal consequences, this terminology would be used.[98] In particular, one would expect reference to ARSIWA and the use of legally relevant language including references to direction and control, effective control, conduct of an organ of the state and so on.

6 International attribution mechanism

In order to make the analysis of attribution of cyber operations complete, it is also necessary to briefly mention the debate on the creation of an international attribution mechanism. Some states have promoted the idea of establishing an international mechanism similar to the Organisation for the Prohibition of Chemical Weapons Technical Secretariat, which would have sufficient technical and professional capacity to carry out reliable and independent technical and legal attribution (to states or non-state actors).[99] However, this proposal is opposed by a number of states which stress that attribution "includes not only technical and legal but also political considerations" and therefore decisions on attribution

94 Ibid.

95 IRISH DEPARTMENT OF FOREIGN AFFAIRS: *Position Paper On The Application Of International Law In Cyberspace...*

96 TSAGOURIAS, FARRELL: *Cyber Attribution...*, p. 954.

97 Ibid, 946.

98 See overview of the national positions on attribution of cyber operations which demonstrates that the legal language is widely used by the states: https://cyberlaw.ccdcoe.org/wiki/Attribution.

99 Ibid.; SHANY, Yuval and SCHMITT, Michael, N. An International Attribution Mechanism for Hostile Cyber Operations?. *Hebrew University of Jerusalem Legal Studies Research Paper Series No. 20–16*, 2020, pp. 3, 12.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

should remain the exclusive right of individual states.[100] The fact is that, while a conventional military operation carried out by one state against another state is such a significant infringement of sovereignty that it necessarily requires a response from the victim state, in the case of cyber operations it may be advantageous for the victim state (e.g. in view of its own technological inadequacies or the potential risks associated with the disclosure of a cyber attack) to avoid public attribution. It is therefore a legitimate argument that public (or semi-public) attribution should be a matter of discretion of the victim state.

On the other hand, the establishment of an independent body could, through the concentration of technical and professional expertise, benefit technologically less equipped states that do not currently have effective technical means to carry out technical attribution. The involvement of these states could lead to the establishment of a broad international practice and thus to the stabilization of the application of international law norms relating to legal attribution in the cyber context.[101]

There are many arguments for and against the establishment of an international attribution mechanism.[102] However, in the absence of broader international support, its establishment is highly unlikely at this time and attribution, whether legal or technical, will for the foreseeable future remain a sovereign prerogative of national states.

7 Conclusion

The aim of this paper was to analyze the different aspects of attribution of cyber operations – technical, legal and political.

It can be concluded that the identification of the perpetrator of a cyber operation is becoming increasingly more common, at least from a technical point of view. The growing technological capacity of states, coupled with the rising amount of information on cyber attacks (infrastructure, procedures and other digital traces), now make it possible to detect the perpetrators of a substantial part of cyber operations with a relatively high degree of certainty, and it is no longer the case that technical attribution is almost impossible.

However, in order to establish liability under international law, a relationship between the specific person, group or organisation that carried out the cyber operation and the state is also required. The prerequisites for legal attribution are established by customary international law and codified in art. 4 to 11 of ARSIWA. In terms of cyber operations, art. 4 and 8 are the most important, with the former setting out rules for the responsibility of states for the actions of their organs and

100 Ibid.

101 BANKS, William. Cyber Attribution and State Responsibility. *International Law Studies*, 2021, vol. 97, p. 1071.

102 SHANY and SCHMITT: *An International Attribution Mechanism...,* p. 14; *see also* MUELLER, Milton et al. Cyber Attribution: Can a New Institution Achieve Transnational Credibility?. *The Cyber Defense Review*, 2019, vol. 4, no. 1, pp. 115–116.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

the latter setting out rules for the responsibility of states for the actions of non-state actors that are nonetheless under their direction or control. The standard still in place for imposing liability under art. 8 is the so-called effective control test developed by the ICJ in 1986, which requires a very high degree of state control over individual cyber operations. The application of this test even in the context of cyber operations is confirmed by the current practice of states and therefore it cannot be expected that this standard will be lowered in the foreseeable future to, for example, the overall control test defined by the ICTY in 1999, despite the fact that demonstrating effective control remains a significant challenge in the case of cyber operations.

Attention was also paid to the burden of proof and standard of proof. Current international law does not impose an obligation on states to disclose the evidence on the basis of which they have concluded that a particular state is responsible for a cyber operation, although soft-law instruments already enshrine this obligation. However, in the event of a court proceeding, presumably before the ICJ, the victim state would bear the burden of proof, and would be obliged to meet a standard of proof, the precise definition of which international law does not yet contain. Nevertheless, it can be inferred from the jurisprudence of the ICJ that the standard of proof required in proceedings before it is fluid and depends on the intensity of the breach of the international law obligation. For less intense breaches, a lower standard of proof at the level of "preponderance of the evidence" is sufficient, while for the most serious breaches (e.g. interference with *jus cogens*), the highest standard at the level of "fully conclusive" evidence must already be insisted upon.

Political attribution, which *de facto* replaces legal attribution in current practice, has not been left out of the picture. Indeed, when discussing the responsibility of states for cyber operations against other states, victim states choose language from which legal attribution cannot be inferred, and these statements thus remain mere political proclamations that may legitimise retorsion measures but do not justify possible countermeasures that would infringe on the rights of other states on the basis of countermeasures or the right of self-defence.

Finally, the possibility of creating an international attribution mechanism was also discussed. Such a mechanism could help to eliminate some of the problems associated with attribution (e.g. the technical inadequacy of some states or the lack of credibility of attribution due to the non-disclosure of evidence). However, the creation of such a mechanism is currently not supported by states, which consider attribution to be a sovereign prerogative of a nation state that they are not willing to relinquish.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

List of references

BANKS, William. Cyber Attribution and State Responsibility. *International Law Studies*, 2021, vol. 97, pp. 1039–1072.

BANNELIER, Karine. and CHRISTAKIS, Theodore. *Cyber-Attacks: Preventions-Reactions: The Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale, 2017, 88 p.

CRAWFORD, James. *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge: Cambridge University Press, 2002, 428 p.

DEDERER, Hans-Georg and SINGER, Tassilo. Adverse Cyber Operations: Causality, Attribution, Evidence, and Due Diligence. *International Law Studies*, 2019, vol. 95, pp. 430–466.

DINSTEIN, Yoram. Computer Network Attacks and Self-Defence. In: SCHMITT, Michael, N. and O'DONNELL, Brian, T. (eds.). *Computer Network Attack & International Law*. Newport: Naval War College, 2002, pp. 99–119.

FAIX, Martin and BRUNER, Tomáš. Problém přičitatelnosti jako nástroj lawfare. *Defence & Strategy*, 2018, vol. 18, no. 2, pp. 79–94.

GOEL, Sanjay and NUSSBAUM, Brian. Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. *Journal of the Communications Society*, 2021, vol. 2, no. 1, pp. 1082–1093.

HANDLER, Stephenie, Gosnell. The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare. *Stanford Journal of International Law*, 2012, vol. 48, no. 1, pp. 209–237.

MUELLER Milton et al. Cyber Attribution: Can a New Institution Achieve Transnational Credibility?. *The Cyber Defense Review*, 2019, vol. 4, no. 1, pp. 107–122.

NGUYEN, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare, *California Law Review*, 2013, vol. 101, no. 4, pp. 1079–1129.

OSULA, Anna-Maria, KASPER, Agnes and KAJANDER, Aleksi. EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 2022, vol. 16, no. 1, pp. 89–123.

PAYNE, Christian and FINLAY, Lorraine. Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *George Washington International Law Review*, 2017, vol. 49, no. 3, pp. 202–206.

PRECIADO, Michael. If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure from Cyber Warfare. *Journal of Law & Cyber Warfare*, 2012, vol. 1, no. 1, pp. 99–154.

RID, Thomas and BUCHANAN, Ben. Attributing Cyber Attacks. *The Journal of Strategic Studies*, 2015, vol. 38, no. 1–2, pp. 4–37.

ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*, 2015, vol. 50, pp. 233–275.

SAALBACH, Klaus-Peter. Attribution of Cyber Attacks. In: REUTER, C. (ed.). *Information Technology for Peace and Security*. Springer Vieweg Wiesbaden, 2019.

SHANY, Yuval and SCHMITT, Michael, N. An International Attribution Mechanism for Hostile Cyber Operations?. *Hebrew University of Jerusalem Legal Studies Research Paper Series No. 20–16*, 2020.

SCHMITT Michael, N. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 2015, vol. 54, no. 1, pp. 697–732.

SCHMITT, Michael, N. et al. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017, 638 p.

SCHMITT, Michael, N. Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 2017, vol. 8, no. 2, pp. 239–280.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

SCHMITT, Michael, N. Terminological Precision and International Cyber Law. [online]. Available at: <https://lieber.westpoint.edu/terminological-precision-international-cyber-law/> Accessed: 24. 3. 2024.

SCHÖNDORF, Roy. Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law* Studies, 2021, vol. 97, no. 1, pp. 395–406.

SILVER, Daniel, B. Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter. In: SCHMITT, Michael, N. and O'DONNELL, Brian, T. (eds.). *Computer Network Attack & International Law*. Newport: Naval War College, 2002, pp. 73–97.

SINGER, Peter, W. and FRIEDMAN, Allan. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014, 320 p.

SKOPIK, Florian and PAHI, Timea. Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity*, 2020, vol. 3, pp. 1–20.

SPÁČIL, Jakub. Countermeasures against Cyber Operations: Moving forward?. *International and Comparative Law Review*, 2023, vol. 23, no. 2, pp. 86–110.

SPÁČIL, Jakub. Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 2022, vol. 16, no. 2, pp. 215–239.

SVAČEK, Ondřej. Srebrenica: Nicaragua nebo Tadic? K subjektivnímu prvku mezinárodně protiprávního jednání. In. Olomouc: Vydavatelství Univerzity Palackého, 2007.

TSAGOURIAS, Nicholas and FARRELL, Michael. Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, 2020, vol. 31, no. 3, pp. 941–967.

VALUCH, Jozef and HAMUĽÁK, Ondrej. Use of Force in Cyberspace. *International and Comparative Law Review*, 2020, vol. 20, no. 2, pp. 174–191.

van der MEER, S. State-level responses to massive cyber-attacks: a policy toolbox. *Clingendael: Netherlands Institute of International Relations*, 2018, 8 p.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)