DOI 10.5817/MUJLT2024-2-2

OF HACKERS AND PRIVATEERS: THE POSSIBLE EVOLUTION OF THE PROBLEM OF CYBER-ATTRIBUTION *

by

JAKUB VOSTOUPAL † KATEŘINA UHLÍŘOVÁ ‡

The escalating severity of the cyber-attribution problem (a problem with attributing cyberattacks to states that ordered them) poses a significant challenge to international law and cyberspace security. However, amidst worsening international relations, a viable solution remains elusive. To address this predicament, the authors turn to a historical echo of the contemporary practice of employing hacker groups – namely, privateering. After an in-depth examination of this analogy's suitability, they focus mainly on the factors that contributed to the decline of privateering. Their goal is to uncover parallels potentially applicable to mitigating modern challenges posed by state-sponsored cyberattacks and the exploitation of cyber-attribution problem. Among the key identified factors, the most crucial were the emergence of professional cyber-capacities (akin to post-Napoleonic emergence of professional navies) and the disruption of hackers' safe havens. The paper concludes by introducing three prospective scenarios reflecting potential pathways for the future of the cyber-attribution challenges.

KEY WORDS

Cybersecurity, Cyber-attacks, Cyber-attribution, Hacker Groups, Non-state Actor, Privateers

* This article was supported by ERDF project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

† Jakub Vostoupal is a researcher at Institute of Law and Technology at the Faculty of Law, Masaryk University. For correspondence: jakub.vostoupal@law.muni.cz

‡ Kateřina Uhlířová is an assistant professor at the Department of International and European Law at the Faculty of Law, Masaryk University. For correspondence: Katerina.Uhlirova@law.muni.cz

1. INTRODUCTION

The creation of cyberspace and the almost absolute integration of information and communication technologies into our lives marked the beginning of a new era. It provided us with tools to boost the effectiveness of many processes, whether waste disposal, nuclear programs, or healthcare, and therefore, it became an essential part of the worldwide community. However, as a former US President Obama aptly pointed out in the 2010 USA National Security Strategy, "*the very technologies that empower us to lead also empower those who would disrupt and destroy.*"[1]

At first, many states underestimated the perils posed by cyber threats, often attributing them to risks confined primarily to individuals and private companies.[2] However, the cyberattacks on the Estonian government in 2007 debunked this myth and demonstrated that certain types of cyber-attacks can also pose a substantial security threat to states.[3] Moreover, the asymmetric nature of cyberspace does not keep this danger just between the states but also allows non-state actors, primarily hacker groups, to mount successful attacks against otherwise much stronger targets (states).[4] The Colonial Pipeline ransomware attack in 2021 serves as a striking example, highlighting the potential for such entities to disrupt critical infrastructure with relatively minimal skills and resources.[5]

The fact that these attacks pose more than just an opportunity for an academic debate is reflected in both the official positions of states (e.g., the official mandate of the Czech Security and Information Service[6] or of

---

[1] Obama, B. (2010) *US National Security Strategy*. The White House, Washington, p. 27. https://obamawhitehouse.archives.gov/sites/default/files/rss\viewer/national\security\strategy.pdf

[2] Banks, W. (2021) Cyber Attribution and State Responsibility. *International Law Studies* 1039(97), pp. 1040–1041.; Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology* 15(2), pp. 303–309.

[3] Pamment, J. et al. (2019) *Hybrid Threats: 2007 Cyber Attacks on Estonia*. NATO Strategic Communications Centre of Excellence, pp. 66–68. https://stratcomcoe.org/cuploads/pfiles/cyber\attacks\estonia.pdf

[4] Boebert, W. E. (2010) A Survey of Challenges in Attribution. In: *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: The National Academies Press, pp. 42–43. http://www.nap.edu/catalog/12997.html

[5] Turton, W., Riley, M., Jacobs, J. (2021) Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. *Bloomberg.com*. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom; Kolouch, J. et al. Cybersecurity: Notorious, but Often Misused and Confused Terms. (2023) *Masaryk University Journal of Law and Technology* 17(2), pp. 282–285.

[6] This intelligence service actively participates on investigations of various electronic attacks safeguarding, inter alia, critical infrastructure entities. This involves assessing information related to *"threats and risks associated with the operation of strategic information and communication*

the American Cybersecurity and Infrastructure Security Agency[7]) as well as international organisations. For instance, the North Atlantic Treaty Organization (NATO) has incorporated mitigation of cyber threats into its alliance doctrines as well as into its military strategy.[8] Notably, NATO has actively developed cyber warfare capabilities, formally acknowledging "cyberspace" as a fourth domain of warfare during the 2016 Warsaw Summit.[9]

Similarly, the European Commission has issued a Joint Communication to the European Parliament, the European Council, and the Council, aiming to enhance resilience and strengthen capabilities to counter hybrid threats. The rationale behind this initiative lies in recognising that "*hybrid activities by state and non-state actors continue to pose a serious and acute threat to the EU and its Member States. From cyber-attacks that disrupt economies and public services to targeted disinformation campaigns and aggressive military actions*."[10]

Cyberspace did not just challenge the factual power of states and the stability of international society; it also challenged the rule of international law and its application.[11] Even though it is primarily of a customary nature and thus quite flexible and capable of adaptation, the introduction of cyberspace presented a crucial question of whether the current international law can be applied in this global domain or whether a cyber-specific regulation is needed.[12] The *UN Group of Governmental Experts* (UN GGE) concluded in their 2013 report that no substantial reason would preclude the application of international law in cyberspace – a stance acknowledged

systems, the destruction or disruption of which could have a serious impact on the security or economic interests of the Czech Republic." See BIS. Kybernetická bezpečnost. `https://www.bis.cz/kyberneticka-bezpecnost/`

7 See About CISA [online]. *Cybersecurity & Infrastructure Security Agency*. 2024 [accessed 8.1.2024]. `https://www.cisa.gov/about`

8 NATO Standard, AJP-6, Applied Joint Doctrine for Communication and Information Systems, February 2017 `https://www.coemed.org/files/stanags/01\AJP/AJP-6\EDA\V1\E\2525.pdf`

9 NATO Summit Warsaw 2016, 9 July 2016. `https://www.nato.int/cps/en/natohq/events\132023.htm`

10 Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response JOIN/2016/018 final, 6 April 2016.

11 Schmitt, M., Watts, S. (2015) The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare. *Texas International Law Journal*, 50(2–3), pp. 220–222.; Svantesson, D. et al. (2023) On sovereignty. *Masaryk University Journal of Law and Technology*, 17(1), pp. 34–40.

12 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*. UN, 2013. `https://digitallibrary.un.org/record/753055`; Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 94–100.

and endorsed by the General Assembly.[13] However, the ill-received UN GGE report of 2015[14] that sought to restrain the irresponsible use of states' cyber capabilities demonstrated that some states are not yet ready to give up this newfound power nor to clear out the legal uncertainty that currently favours those who exploit it.[15]

This reluctance is particularly evident in the context of one of the key points from the 2013 UN GGE report: "*States must not use proxies to commit internationally wrongful acts*."[16] This refers to the practice of exploiting the inherent anonymity and asymmetricity of cyberspace by using non-state actors to attack and destabilise rivals while at the same time being protected by a plausible deniability from the legal consequences as the link between the non-state actor and a state is very hard to find and prove in cyberspace.[17] In other words, the exploitation of the cyber-attribution problem.[18]

In the context of the law of international responsibility, attribution is one of two constitutive aspects of an international wrongful act and describes a procedure and a set of requirements through which such an act may be linked to a particular state.[19] Identifying the perpetrator then unlocks the possibility of legal repercussions, making attribution a crucial part of the deterrence strategy.[20] Yet, applying the existing rules proved somewhat inefficient in the case of cyberattacks,[21] as the attribution procedure did not account for the

[13] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*, 2013.

[14] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/150*. UN, 2015. `https://digitallibrary.un.org/record/799853`

[15] Schmitt, Watts. (2015) *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, pp. 220–222.; Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2), pp. 216–218.

[16] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*, 2013.

[17] Banks, W. (2021) Cyber Attribution and State Responsibility. *International Law Studies* 1039(97), pp. 1040–1041.

[18] Edwards, B. et al. (2017) Strategic Aspects of Cyberattack, Attribution, and Blame. *Proceedings of the National Academy of Sciences*, 114(11), pp. 2825–2827.

[19] See Article 2 of the Draft Articles on State Responsibility for Internationally Wrongful Acts: Elements of an internationally wrongful act of a State: There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.

[20] Baliga, S., Bueno De Mesquita, E., Wolitzky, A. (2020) Deterrence with Imperfect Attribution. *American Political Science Review*, 114(4), pp. 1155–1157.

[21] As of now, there is no universally agreed definition of cyberattack nor its potential consequences. Cyberattacks can range over a wide spectrum, causing less significant damage, but also damage more than comparable to attacks with conventional weapons, including loss of life (e.g., WannaCry, Stuxnet or the instances of the so-called killware). Nevertheless, as Giles and Hartmann point out, the emerging state practice shows, that the extent of the cyber-attack is not really a predeterminant of attribution (supported by the attribution of

specifics of cyberspace.[22] The sources of the problem may be explicitly found in the requirements on forensic capabilities necessary to identify a responsible individual,[23] the unclear legal requirements on the attribution procedure itself,[24] the impact of extra-legal aspects (mainly political and strategic),[25] and the uncertainty linked with the unspecified standard of proof[26] and evidence disclosure[27]. The combination of these factors has prevented several early major cyber-attacks (e.g., Estonia in 2007,[28] Russia-Georgian War in 2008,[29] Stuxnet in 2010/2012[30]) from ever being attributed. Unsurprisingly, some states, such as the Russian Federation, the People's Republic of China or even the United States of America, have quickly utilised the potential presented by the cyber-attribution problem and began recruiting or at least cooperating with hackers and cybercriminal groups to use them as means of projecting power.[31] Some states even offer those actors "*safe harbours*" – leniency from law enforcement and monetary incentives to take on a mission for the benefit of the said state.[32] These cooperations may be kept at some level of secrecy

cyberattacks against Albania in 2022), and therefore the abstract term cyberattack in its wide meaning is sufficient for the purposes of this paper. See Giles, K., Hartmann, K. (2019) 'Silent Battle' Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. In: Minárik, T. et al. (eds.). *11th International Conference on Cyber Conflict: Silent Battle*. Tallinn: NATO CCD COE Publications, p. 26.; Attack (International Humanitarian Law) [online]. *International Cyber Law: Interactive Toolkit*. 28. 7. 2023 [accessed 10. 1. 2024]. `https://cyberlaw.ccdcoe.org/wiki/Attack\(international\humanitarian\law)`

22 Berghel, H. (2017) On the Problem of (Cyber) Attribution. *Computer - IEEE Computer Society*, 50(3), pp. 84–85.

23 Rid, T., Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies* 38(1–2).

24 Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3).

25 Egloff, F. J., Smeets, M. (2021) Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*. 2021.

26 Davis, J. K. (2022) *Tallinn Paper No. 13 - Developing Applicable Standards of Proof for Peacetime Cyber Attribution*. NATO CCD COE Publications.

27 Aravindakshan, S. (2021) Cyberattacks: A Look at Evidentiary Thresholds in International Law. *Indian Journal of International Law*, 59(1–4).

28 Pamment, J. et al. *Hybrid Threats: 2007 Cyber Attacks on Estonia*. NATO Strategic Communications Centre of Excellence, 2019. `https://stratcomcoe.org/cuploads/pfiles/cyber\attacks\estonia.pdf`

29 Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. `https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf`

30 Connect the Dots on State-Sponsored Cyber Incidents – Stuxnet [online]. *Council on Foreign Relations* [accessed 26. 12. 2023]. `https://www.cfr.org/cyber-operations/stuxnet`

31 APTs & Adversary Groups List - Malware & Ransomware [online]. *Crowdstrike Adversary Universe* [accessed 27. 8. 2023]. `https://adversary.crowdstrike.com/en-US/`

32 Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 99–100.

to allow for plausible deniability of the state, e.g., Iran has tried to mask its involvement in the cyberattacks against Albania in 2022 in such a way.[33]

And even though there has been a significant progress in the forensic capabilities of states allowing for better identification of the perpetrators[34] and the consequent rise in the number of public cyber-attributions since the WannaCry and NotPetya cyberattacks in 2017, these attributions still refrain from using legal terminology and invoking state responsibility.[35] States are, therefore, willing to attribute politically but not apply current customary attribution rules. This reluctance may suggest a profound lack of confidence in the evidence-gathering procedures or even in the legal attribution process as a whole. Some scholars[36] have already criticized the central aspect of the attribution process for the non-state actors controlled by states, the so-called *effective control test*, as being unrealistically stringent and "unsatisfiable" within the context of cyberspace.[37]

However, the focus should not solely be on whether this test is "unsatisfiable" (and Mačák's claim about this is clearly supported by the data from the EuRepoC' and Council on Foreign Relations' Datasets[38]) but also to explore the underlying reasons for its perceived inadequacy. The *effective control doctrine* was established by the International Court of Justice (ICJ) in the 1986 Nic*aragua v. USA case* and reaffirmed in the 2007 *Bosnian Genocide case*.[39] In both instances, the conflicts were primarily land-based,

[33] Microsoft Threat Intelligence. Microsoft investigates Iranian attacks against the Albanian government [online]. *Microsoft Security Blog*. 8. 9. 2022 [accessed 31. 7. 2023]. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

[34] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 520–598.

[35] Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/; Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[36] E.g., Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 420–428.

[37] Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[38] Attribution Tracker [online]. *EuRepoC: European Repository of Cyber Incidents*. 2024 [accessed 18. 5. 2024]. https://eurepoc.eu/attribution-tracker/; Tracking State-Sponsored Cyberattacks Around the World [online]. *Council on Foreign Relations*. 2024 [accessed 7. 2. 2024]. https://www.cfr.org/cyber-operations

[39] *Judgement of the International Court of Justice in the Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) - Merits*. 1986.

an environment where states have historically held significant power.[40] The strictness of the attribution test is therefore understandable in these contexts, as states can exert greater control over non-state actors and forensic evidence can be more readily examined.

We contend that the primary cause of the *effective control doctrine's* ineffectiveness and unsuitability in cyberspace lies in the fundamental differences between land and cyber domains. Specifically, the symmetric nature of land-based conflicts[41] contrasts sharply with the asymmetric nature of cyberspace, and the actors involved in these domains differ significantly. Rather than attempting to apply land-based procedures to cyberspace, we should seek more appropriate analogies—environments where state control is similarly challenged. We propose that the most fitting analogy to cyberspace, one with a sufficient historical legal precedent, is the sea. In this analogy, the practice of states using non-state hacker groups to obscure their involvement in cyberattacks (or to conduct them when the state lacks the necessary capabilities) parallels the historical practice of privateering and the issuance of Letters of Marque in the absence of professional navies.

If this analogy proves to be more suitable, it could offer valuable insights into mitigating the exploitation of cyber-attribution issues by states and predicting the future development of state-sponsored cyberattacks. This is particularly relevant given the current improbability of establishing a cyber-specific treaty or the emergence of a new general customary rule through state practice. Therefore, this article undertakes a thorough examination of this analogy and focuses on the following research questions:

- Are there similarities between the state practices of utilising privateers and non-state hacker groups that would allow drawing inspiration from the historical development as to the evolution of the cyber-attribution problem?
- If so, then based on this analogy, what factors could lead to the resolution or mitigation of the cyber-attribution problem and the exploitative practice of state-sponsored cyberattacks?

`https://www.icj-cij.org/case/70/judgments`; *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. 2007. `https://www.icj-cij.org/case/91/judgments`

[40] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4).

[41] Many states struggle to effectively control cyberspace and the actors within it, whereas these non-state actors find it significantly easier to launch attacks against state interests in the digital realm compared to the physical world.

To offer a comprehensive response, our first step involves thoroughly analysing the compatibility between the historical functioning of the state responsibility and attribution regimes pertinent to privateering practices and the contemporary law of international responsibility. Within both frameworks, we focus on the problems of attributing the acts of non-state actors used by states as proxies. Should our analysis reveal no significant obstacles to employing this analogical comparison, we proceed to explore the parallels between non-state hacker groups and privateers/pirates, specifically focusing on four distinctive areas: the parallels in the subject, the environment, the purpose, and the effect.

Upon confirming that both the legal regimes and relevant subjects are sufficiently similar to warrant working with this analogy and drawing experience from it, we delve into examining key historical milestones of privateering. Our attention is particularly directed towards aspects that contributed to the decline of this once-widely accepted practice that could help us determine the possible future development of the cyber-attribution problem and its exploitation. It is important to add that our focus in this paper does not extend to addressing whether the practice of employing non-state hacker groups should fall under the same legal regime as privateers, as it would diverge from the attribution aspect and delve into a much wider issue, that was already addressed by others.[42]

2. THE RULES OF ATTRIBUTION IN THE ERA OF PRIVATEERS

The law of sovereign responsibility existed for a long time (there are recounts older than 3000 years mentioning these rules from Egypt[43]) and underwent many fundamental changes.[44] In the Roman period (under the *Jus Gentium*), the sovereign responsibility was not unlike the modern due diligence principle – it was constructed as a strict responsibility of the

[42] For more detailed treatise on this matter, see Egloff, F. (2017) Cybersecurity and the Age of Privateering. In: Perkovich, G., Levite, A. E. (eds.). *Understanding Cyber Conflict: Fourteen Analogies*. Washington, DC: Georgetown University Press.; and Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center. http://www.dtic.mil/docs/citations/ADA590294

[43] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4). p. 265.

[44] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, chap. 1. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

collective.[45] The perfect example of its functioning can be found in the consequences of "kidnapping" Helen of Sparta, which served as a *casus belli* for the Trojan War, thus making a whole nation responsible for the act of a prince.[46] The state and its subjects in this period were not understood as separate units, which would allow for the non-attribution of some acts (there was no non-state actor) but a single collective.[47] Moreover, the invoked responsibility could have had only a single output – a reason for war (*casus belli*). The *Jus Gentium* strongly affected the medieval period, especially in the tribal environment.[48] Basically, "*had one member of the tribal entity killed or injured a member of another entity, the whole first entity was responsible and subject to retribution.*"[49] The principle of collective responsibility remained for quite a long time and was not softened until the late Middle Ages (15th century),[50] which meant that it also influenced the rising early practice of privateering[51].[52]

The attempts to stabilise international society caused the strict responsibility (which gave many states excuses to wage war) to decline and give way to a more modern approach based on the fault of the sovereign (about the 17th century).[53] Therefore, the responsibility for the acts of the non-state actors and the consequent procedure of attribution became much more relevant. One of the first authors to introduce this approach was Alberico Gentili, who argued that the casus belli exist only "*in instances in which a private individual has done wrong, and his sovereign or nation has failed to atone for his fault.*"[54]

---

[45] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 278.

[46] Hayes, A. (1925) Private Claims against Foreign Sovereigns. *Harvard Law Review*, 38(5), p. 606.

[47] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 278.

[48] Berman, H. J. (1983) *Law and Revolution: the Formation of the Western Legal Tradition*. Cambridge (Mass.) London: Harvard university press, p. 52.

[49] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 280.

[50] Ibid., p. 281.

[51] The definition and delineation of the terms privateer and pirate and presented in Section 4. For the purposes of sections 2 and 3, even the general understanding of those terms will suffice.

[52] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 566–567.

[53] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 281.

[54] Gentili, A. (1612) *De Iure Belli Libri Tres*. Oxford: The Clarendon Press, p. 104. https://archive.org/details/threebooksonlawo0002ayal/page/n3/mode/2up

This was then further elaborated by one of the most influential authors, thinkers, and philosophers of this period – Hugo Grotius. He completely severed the remaining attachments to the collective responsibility and limited the reach of sovereign responsibility over the non-state actors, as in his view, the primary aspect of international responsibility was fault.[55] As such, acts *ultra vires* were not attributable to the kings, neither were the acts of privateers that "*had seized the property of friends, had abandoned their native land and were wandering at sea without returning even when recalled…*" because the kings "*themselves had not been the cause of the wrongful freebootery and they had not had any share in it…*".[56] By *argumentum a contrario,* the contraction of a privateer (or issuing the *Letter of Marque*[57]) created a bond between the sovereign and the privateer, which made the king responsible for the actions of the privateer as long as he had some degree of power over them.[58]

Grotian take on international responsibility (also in combination with the due diligence principle[59], as in this era, both regimes were somewhat intertwined) is based on two principles: *patientia* and *receptus*.[60] The first term means that "*responsibility ensues if a community or its rulers know of a crime committed by a subject but fail to prevent it if they can and should do so.*"[61] This is one of the reasons why renegade privateers are out of the scope of sovereign responsibility, because if the sovereign "*had also forbidden by laws that friends should be harmed*"[62], he would have taken a stance against the harming act. The *receptus* principle required the king to "*either punish or extradite those who have taken refuge from justice in his realm if he wants to avoid responsibility for their crimes.*"[63] This would be especially grave for rogue privateers, who would lose all safe harbours and risk extradition and execution. If the receptus

[55] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 283.

[56] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger, pp. 433–437.

[57] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 55–56.

[58] Compare with Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), pp. 283–284.

[59] It is important to note that Grotian take on the due diligence principle is based on the link between the sovereign and his subjects, not territory (that is a modern post-Westphalian approach to due diligence). See Ibid., p. 287.

[60] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger, pp. 433–437.

[61] Ibid., p. 523.

[62] Ibid., p. 526.

[63] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 284.

principle was breached, the king would be held responsible for the crimes of individuals.[64]

During the age of absolutism (the age that witnessed the rise of the Golden Age of Piracy and privateering), the position of a sovereign was said to hold absolute power. With the premise of absolute power over his subjects, such a king should be responsible for any transgressions in light of Grotian ideas. However, this was impractical and unrealistic, as no sovereign had complete control over his lands and subjects, and the concept that a king or a state could not be held responsible for the acts of individuals they did not control grew stronger.[65]

The 18th century (the final period of the Golden Age of Piracy) marked the rise of state responsibility and a slight decline in the doctrine of fault.[66] One of the most influential authors of this period was Christian Wolff, who modified the Grotian concept of the due diligence principle to the point where no sovereign should allow any of its subjects to harm or injure other sovereigns or foreigners.[67] If the ruler fails to uphold this duty, he should punish the offender or compel the perpetrator to repair the loss.[68] He also reflected upon the growing distinction between states and non-state actors in terms of sovereign responsibility and laid down the foundations of the modern take on the attributability of the acts done by non-state actors, as he emphasised that "*the acts of a private citizen are not the acts of the nation to which he is subject, since they are not done as by a subject or so far as he is a subject… The situation is different if he acts by order of the ruler of the state, whom he obeys as a superior.*"[69] Therefore, the concept of control became crucial for the attribution, even though it remained largely unspecified.[70]

2.1. THE SOVEREIGN'S RESPONSIBILITY FOR THE PRIVATEERS' ACTIONS – SUMMARY

To conclude this Section, we find it helpful to briefly summarise the key aspects related to the responsibility for actions carried out by non-state actors, specifically privateers. A privateer's commission (usually cemented by granting the Letter of Marque and Reprisal) creates a bond of responsibility between the state and a non-state actor. The privateers then act as an

64 Ibid.
65 *op. cit.*, pp. 286–287.
66 *op. cit.*, p. 288.
67 Wolff, C. (1995) *Jus Gentium Methodo Scientifica Pertractatum*. Buffalo, NY: Hein, § 317. `https://archive.org/details/jusgentiummethod0002wolf`
68 *op. cit.*, § 318.
69 *op. cit.*, § 315.
70 As demonstrated by the practice of utilization of privateers, see Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 568–571.

extension of the sovereign's power as long as they are loyal and the sovereign has control over them. This control was never entirely clarified by the state practice and thus remained within the limits of an abstract overall control.[71] For instance, a sovereign commissioned a privateer, he could recall the privateer, could unleash him, could name preferred targets, could specify requirements on the conduct of privateers[72], but could not exercise any control over the execution of the privateer's actions on the sea (at best, he could denounce these acts afterwards).[73] Also, should the privateer break the limitations set down by a sovereign, it would not lead to a sovereign responsibility (unless the sovereign has retained control over the privateer and just did not act).[74]

However, the bond between a privateer and a state was not always apparent to an outside observer. In fact, the only times it could be examined was during the sale of his prize (which was usually done in a friendly or at least neutral harbour and thus not entirely helpful for the sake of attribution), when he earned himself a reputation (often interpreted as insufficient), or upon the capture of the said privateer.[75] Typically, a privateer would reveal the Letter of Marque to his adversary only if captured, as it was the only thing distinguishing him from a pirate and thus saving him from quite a gruesome death reserved for pirates (privateers were granted the status of prisoners of war under the law of nations and the consequent protection[76]).[77] In the end, the reputation and the self-interest of privateers themselves allowed for attribution, nothing else.

---

[71] Reminiscing the so-called *overall control* test invoked in the Tadić case by the International Criminal Tribunal for the Former Yugoslavia, see Section 3.1.

[72] In the later times (the turn of the 18th and 19th century), the conduct of privateers was strictly regulated via national laws and under supervision of the national courts. It was also still a highly respected position and the privateer commissions were accepted throughout the world.

[73] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 56–58.; Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 570–571.

[74] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger, pp. 433–437.

[75] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. `https://lthj.qut.edu.au/article/view/1583`; Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), pp. 178–181.; Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 570–571.

[76] Even though the extent of the protection differed greatly throughout the history.

[77] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. `https://lthj.qut.edu.au/article/view/1583`; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 56.

Therefore, the main problem with the responsibility for the privateers' actions was of an evidentiary and enforcing nature. While lacking professional navies, it was problematic at best for many countries to hunt the privateers down and seize them (or kill them in battle) to attribute their actions to any sovereign.[78] At the same time, privateers were the only hope for smaller states to project their power against maritime superpowers such as England and Spain.

3. THE CONTEMPORARY RULES OF ATTRIBUTION

After exploring the relevant parts of the historical development of the sovereign responsibility and attribution rules, it is now imperative to compare them with the contemporary set of attribution rules with an accent on the attribution of non-state actors' acts in cyberspace to find whether these regimes are compatible for the analogy to work with, or not.

The modern state is, de facto, only an abstract construct which has no choice but to act through its organs and individuals, whose actions are then attributed to it according to specific rules. While these rules are primarily customary in nature, their system and function are captured in detail in the codification prepared by the UN Commission on International Law – the Draft Articles on State Responsibility for Internationally Wrongful Acts ("Draft Articles" or "ARSIWA").[79] Experts have no consensus on whether the state responsibility is currently strict or subjective in nature.[80] The Draft Articles do lean towards the strict concept, but the historical idea of fault is not entirely abandoned.[81]

The contemporary conception of international responsibility is based upon the commission of an international wrongful act.[82] That consists

[78] Anderson, J. L. Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*. 1995, vol. 6, no. 2, pp. 175–199; pp. 186–188.; Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6 - 7. https://lthj.qut.edu.au/article/view/1583

[79] Despite the fact that it is only a "Draft", these Articles are widely recognized as binding capture of customary international law, see *Responsibility of States for Internationally Wrongful Acts - Comments and information received from Governments and Report of the Secretary-General (A/71/79)*. General Assembly of the United Nations, 2016. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/112/74/PDF/N1611274.pdf?OpenElement

[80] Haataja, S. (2021) Autonomous Cyber Capabilities and Attribution in the Law of State Responsibility. In: Liivoja, R., Väljataga, A. (eds.). *Autonomous Cyber Capabilities under International Law*. Tallinn, Estonia: NATO CCD COE Publications, pp. 265–266.

[81] *Op. cit.*, pp. 265–266.; Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), pp. 290–292.

[82] Pellet, A. (2010) The Definition of Responsibility in International Law. In: Crawford, J., Olleson, S., Parlett, K. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press, p. 9.; *Draft articles on Responsibility of States for Internationally Wrongful Acts*.

of a breach of an international primary rule (sometimes inappropriately called the objective element of the state responsibility) and the attributability (inappropriately called the subjective element).[83] However, due to the problems with the interpretation and application of both of these elements in the cyber-context (e.g., there is no consensus on what primary rules may be breached by cyber means nor on how intense the breach must be[84,85]), some authors[86] propose to use the due diligence principle (which is nowadays, as opposed to the Grotian era, entirely distinguishable from the traditional "direct" attribution) as a mean of bypassing the controversial aspects of state responsibility.[87] This is caused by the fact that the due diligence principle is not a procedure of assigning responsibility to a state but more of a primary rule of international law, which mitigates the attribution problem.[88] This principle obligates states to prevent events (as it is called in Article 23 of ARSIWA) that could cause harm to other subjects or sovereigns.[89] Therefore, it is not necessary to find any linkage between the state and the act as with

International Law Commission – United Nations, 2001, arts. 1–2. https://legal.un.org/ilc/texts/instruments/english/commentaries/9\6\2001.pdf

83 Brigitte, S. (2010) The Elements of An Internationally Wrongful Act. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press, pp. 200–202.

84 The prevailing view, which is also reflected by the Tallinn Manual 2.0, is the requirement of equivalence of consequences between a cyberattack and a kinetic attack in terms of the use of force. See Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, pp. 84–86. https://doi.org/10.1017/9781316822524

85 The controversy over the breach of primary rule of international law in cyberspace is, however, beyond the limits of this article, and for the remainder of this paper, we will consider this aspect to be fulfilled. See Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, p. 113.https://www.cambridge.org/core/product/identifier/9781139033060/type/book; Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, pp. 84–86.; Schmitt, M. In Defense of Sovereignty in Cyberspace [online]. *Just Security*. 8. 5. 2018 [accessed 28. 6. 2023]. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

86 E.g., Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly* 67(3); Jensen, E. T. (2020) Due Diligence in Cyber Activities. In: Krieger, H., Peters, A., Kreuzer, L. (eds.). *Due Diligence in the International Legal Order*. UK: Oxford University Press. https://doi.org/10.1093/oso/9780198869900.003.0015; Liu, I. Y. (2017) *State Responsibility and Cyberattacks: Defining Due Diligence Obligations*. Rochester, NY. https://papers.ssrn.com/abstract=2907662

87 There is also another way and that is the Plea of Necessity. Same as with the Due Diligence Principle, it has yet to reach a sufficient level of state practice, but nevertheless remains an interesting proposal. See more at Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2).

88 Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly*, 67(3), pp. 645–648.

89 Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, pp. 226 - 227. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

the attribution procedure; it is only necessary to find that the state failed in its obligation to "*frustrate the occurrence of the event as far as lies within its power*".[90] Because of the missing linkage, it is sometimes called indirect responsibility. Any state may demand fulfilment of this obligation from another if it has knowledge about an act in preparation or execution that could compromise its security and originates from a domain of the said state (for example, IT infrastructure).[91]

However, as the application of this principle in cyberspace currently faces not insignificant problems (the lack of the state practice has been called out by several major cyber-powers, who rejected the applicability of this principle in cyberspace, among others the USA[92] and Israel[93]), we shall mainly focus on the process of attribution.[94]

3.1. THE LINK TO ATTRIBUTE

The Draft articles delineate three fundamental constellations of actors concerning attributability. Initially, the focus is on the conduct of state authorities (Article 4) and individuals or entities exercising state power (Article 5)[95]. Actions undertaken by any state organ, whether representative of state power or local government[96], when performed within their official capacity, are attributable to the respective state.[97] The purview of official capacity is extended by Article 7 of ARSIWA, establishing attributability of State organs' actions even in instances of *ultra vires* acts. The same principle

[90] This is not an absolute responsibility, therefore the failure to prevent an undesired outcome is in itself insufficient to conclude the breach of the state's due diligence. See par. 6 Article 23 ARSIWA Commentary.

[91] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, pp. 227–229. https://www.cambridge.org/core/product/identifier/9781139033060/type/book ; Svantesson et al. *On sovereignty*, pp. 40–43.

[92] *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies*. General Assembly of the United Nations, 2021, p. 141. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[93] Schöndorf, R. (2021) Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law Studies*, 97(1). https://digital-commons.usnwc.edu/ils/vol97/iss1/21

[94] For a general overview of issues connected with state responsibility, attribution, or the use of force in cyberspace, see e.g. Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 94–100; or Osula, A. M., Svantesson, D., J. B., Vostoupal, J., Uhlířová, K., et al. (2021) *Cybersecurity Law Casebook 2020*. Brno: Masaryk University.

[95] According to the Tallinn Manual, this could be, for example, a private company in charge of cyber-espionage. See Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, pp. 89–90.

[96] To illustrate, it may be an act of the court, the military or the intelligence service.

[97] This has been confirmed several times by the International Court of Justice, e.g., in the judgments of *Salvador Commercial Company* and *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*.

applies to individuals and entities vested with State power (see Articles 5 and 7 of ARSIWA). Only when the individual in question pursues purely private interests are the relevant acts not attributable to the State. In the *Bosnian Genocide Judgment*, the International Court of Justice (ICJ) further broadened the concept of state organs and persons exercising state power to encompass entities that, while de jure non-state actors, operate in complete dependence and under the absolute control of the relevant state.[98]

In contrast to actors vested with state power, the actions of non-state actors represent a distinct (second) category. The historical development mentioned above, illustrating a gradual lowering of the standard of state responsibility for the non-state actors' actions, resulted in the contemporary principle whereby the actions of non-state actors are typically not attributable to states.[99]

Between these positions lies a more intricate level involving non-state actors operating in dependence on the state[100], with ex-post recognition and adoption of activities by the state (attribution by adoption) or actions of parastatals in cases of fallen governments or the establishment of new states. Such actions are attributable to the states in question under conditions stipulated in ARSIWA, with Article 8 being particularly pertinent. This article states that "*(t)he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is, in fact, acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.*"

It is this very article which emerged as the focal point of the attribution problem, particularly concerning the terms "*instructions*", "*direction*", and "*control*".[101] While the Draft Articles explicitly differentiate between these

[98] *Responsibility of States for Internationally Wrongful Acts - Comments and information received from Governments and Report of the Secretary-General (A/71/79)*, 2016.

[99] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, p. 113. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

[100] It is important to add, that when considering private individuals, with or without ties to the state, the Tallinn Manual specifically addresses so-called hacktivists or hackers attacking for patriotic reasons (patriotic hackers). Rule 6 of the Tallinn Manual 1.0 appropriately draws upon Article 8 of ARSIWA, demanding evidence that the individuals in question acted on the instructions of the State or that the State directed their conduct. See Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge ; New York: Cambridge University Press, 2013, pp. 35–38.

[101] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 407–408.; Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press, pp. 110–113.

three categories[102], the practical application often blurs the distinction between the concepts of *direction* and *control*.[103] According to Crawford, *instructions* involve a specific scenario where a state authorises, instructs, and mandates a non-state actor to conduct a particular operation as a de facto "*auxiliary*" – for instance, a private company mandated to support ongoing military operations[104].[105] In contrast, *direction* and *control* encompass broader relationships, with the degree of control over a non-state actor's actions determining an act's attributability.

The ICJ addressed (and tried to clarify) the definition of sufficient control for the attribution of an internationally wrongful act in the case of *Military and Paramilitary Activities in and against Nicaragua*.[106] The ICJ established a stringent *test of effective control*, emphasising that mere support for the activities is insufficient.[107] Instead, the state must actively participate in the planning (beginning), execution, and conclusion of the operation, retaining the ability to terminate the operation itself at all times.[108]

The Tallinn Manual 2.0, aligning with the ICJ's *effective control test* from the Nicaragua case, employs this standard to assess the attributability of cyber-attacks committed by private parties.[109] However, the Nicaragua test is rather old (1986) and does not account for the specifics of cyberspace, making it demand a rather high evidentiary standards and an unrealistic link between hackers and a state.[110] The ICJ had a chance to "update" its approach in 2007 during the Bosnian Genocide case, but it reaffirmed *the effective control*

[102] See par. 7, Article 8 *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries - 2001*. International Law Commission – United Nations, 2001. `http://legal.un.org/ilc/texts/instruments/english/commentaries/9\6\2001.pdf`

[103] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, p. 145. `https://www.cambridge.org/core/product/identifier/9781139033060/type/book`

[104] See Schmitt, M. (2017) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 95–96.

[105] Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press, p. 110.

[106] *Judgement of the International Court of Justice in the Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) - Merits*, 1986, para. 109.

[107] *Op. cit.*, paras 109–110.

[108] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 413.

[109] Schmitt, M. (2017) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 94–99.

[110] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 423–426.

instead[111] and thus gave "*States the opportunity to carry out criminal policies through non-state surrogates without incurring direct responsibility.*"[112]

Except for the unfortunate factual consequences of these judgements, Talmon[113] and Cassese[114] directly criticise the ICJ's research work in examining the state practice (as the ICJ should according to its own rules on the identification of international customary law). Cassese specifically stresses that *"had the Court undertaken a close perusal of such practice, it would have concluded that it indeed supported the 'effective control' test but solely with regard to instances where single private individuals act on behalf of a state, (. . .) international practice uses another test, that of 'overall control', for the attribution to states of acts of organised armed groups acting on behalf of such states."*[115]

The *overall control test*, mentioned by Cassese, was explicitly laid down by the International Criminal Tribunal for the former Yugoslavia in the *Tadić* case.[116] This test is sometimes favoured as a more suitable tool for the digital age. It also better reflects the requirements of control over privateers. Nevertheless, except its rejection by the ICJ,[117] there are also several major impediments to its potential general applicability.[118]

In contrast to the attribution of ultra vires acts of state power permitted by Article 7 of ARSIWA, Article 8 does not extend the same application to non-state actors. Crawford notes that states typically do not assume the risk of non-state actors exceeding their instructions, and such acts then "escape" the reach of attribution.[119] Nevertheless, if the transgression was

[111] *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, 2007, arts. 391–393.

[112] An exempt of the Dissenting Opinion of Vice-President Al-Khasawneh. See *op. cit.*, p. 217.

[113] Talmon, S. (2015) Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion. *European Journal of International Law*, 26(2).

[114] Cassese, A. (2007) The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*. 18(4).

[115] *Op. cit.*, p. 654.

[116] Condorelli, L., Kress, C. (2010) The Rules of Attribution: General Considerations. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press, pp. 229–231.

[117] The rejection by itself may not be devastating for the possibility of application of overall control test, as article 59 of the Statute of the International Court of Justice states that "*the decision of the Court has no binding force except between the parties and in respect of that particular case*". Nevertheless, it is apparent that the ICJ consider its finding as (at least) argumentatively binding and therefore, it is improbable that it would deviate from its reasoning in those cases.

[118] *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, 2007, articles 391–393.

[119] Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press, p. 110.

not accidental or the state continued to exert *effective control* over the non-state actor, the act in question can be attributed to the state.[120]

3.2. RESPONSIBILITY FOR THE ACTS OF THE NON-STATE HACKER GROUPS

The contemporary law of state responsibility represents a logical endpoint in the historical development outlined in Section 2. The separation of responsibility regimes governing the actions of representatives of state power and those of non-state actors has been completed, and the prevailing principle nowadays asserts that states, in general, are not held responsible for the actions of non-state actors. The specific rules outlined in Article 8 and subsequent provisions of ARSIWA serve as an exemption and, consequently, demand a strict interpretation. However, should a state commission or contract a hacker group for a cyberattack, the extent of control it exercises over it may still give rise to the state's responsibility for this group's actions. Therefore, the rule of control remained a primary indicator of attributability, akin to earlier phases delineated in Subsection 2.1). The significant shift lies in the introduction of *the effective control test* and the clear demarcation of the due diligence principle as the way of "indirect" responsibility, distinct from attribution mechanisms.

The effective control test sets a much more rigorous standard compared to the connection required between a sovereign and a privateer. The requirements of this test (especially on factual control and evidence) are probably completely unrealistic for the purposes of attributing cyberattacks to states, and its reaffirmation by the ICJ in the Bosnian Genocide case has provided states with a means to conceal adversarial activities in cyberspace through proxies. Consequently, the problem of cyber-attribution concerning non-state hacker groups extends beyond issues of evidence and enforcement, as was the case of privateers, but also encompasses a fundamental legal challenge. Coupled with the unspecified standard of proof[121] and uncertain requirements on evidence disclosure, legal attribution of cyberattacks orchestrated by hacker groups cooperating with or controlled by the state becomes nearly impossible.[122]

Therefore, after the comparison of said legal regimes, although there are obvious differences, we find no discrepancies serious and complex enough that they would preclude the analogical comparison between the fates of

[120] *Op. cit.*, p. 113.

[121] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), p. 563

[122] Banks, W. Cyber Attribution and State Responsibility. *International Law Studies*. 2021, vol. 1039, no. 97, pp. 1042–1045.;Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 563–566.

privateers and hackers. On the contrary, the parallels between the extent of control necessary for attribution and the nature of the attribution problem in the case of both subjects support the relevance of this comparison, as well as the already proclaimed unsuitability of comparing the land-based and cyber-based regimes of attribution.

4. OF HACKERS AND PRIVATEERS

Having assessed the suitability of the respective responsibility regimes for the purposes of analogical comparison, we proceed to the examination of factual and legal parallels between the sea and cyberspace. But apart from the analysing the similarities between the domains themselves, it is also necessary to delve into the state practices involving the commissioning of privateers and hacker groups. The primary focus of this comparative analysis therefore revolves around several distinct categories – purpose and effect, environment and subject. This categorisation enables a detailed comparison that extends beyond the legal status of both non-state actors. It incorporates considerations of the factual attributes of their respective environments, the geopolitical context, and the specific needs of states employing these techniques.

Before delving further into the subject, it is essential to clarify the terms privateer and pirate. Both terms refer to private individuals employing predatory tactics, attacking commercial targets with armed vessels upon the seas, and sharing similar aims and methods. Consequently, throughout history, these terms have often been conflated.[123] Nonetheless, the primary distinction lies in the fact that privateering was a process sanctioned by a sovereign, which imposed limitations and rules on the conduct of privateers (such as restricting targets to the ships of an enemy nation), whereas piracy was universally recognised as an international crime, posing a threat to international commerce and generally disapproved by all states (pirates were a force uncontrolled by any sovereign, without bounds or loyalties).[124,125]

[123] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 19–20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[124] Ibid.

[125] This can be demonstrated in the interpretation of Com. Still, who refers to piracy as: "a *robbery or forcible depredation on the high seas, without lawful authority, done animo furandi, in the spirit and intention of universal hostility.*" See Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 4 http://www.dtic.mil/docs/citations/ADA590294

However, this theoretical distinction was not consistently reflected in practice until the 17th century.[126]

With the development of maritime law, rules against piracy became clearer and more rigorously enforced. Simultaneously, privateering underwent a transformation, initially being formalised as a tool of international relations and ultimately abolished as an outdated form of warfare.[127,128] Consequently, there is no universally accepted and contemporary legal definition of a privateer[129], while the definition of piracy can be found within Article 101 of the United Nations Convention on the Law of the Sea.[130]

4.1. THE PURPOSE AND THE EFFECT

The first category of comparison focuses on the motivations behind the deployment of privateers and hackers. In the case of privateers, this aspect also serves as an additional distinguishing factor between privateers and pirates, as their purpose significantly impacts their legal status. Privateers were typically commissioned during times of war as a form of supportive measures to intensify attrition against enemies and disrupt their economies.[131] The fact that these activities were "*considered a legitimate*

[126] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 19–20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[127] The Hague Peace Convention VI officially declared armed merchant ships to be in the same category as warships, which ended the special position of privateers.

[128] Ibid.

[129] This means that the practice of privateering has been extinguished, merely transformed (and renamed). The private military companies played a pivotal role in a number of conflicts (e.g., Sierra Leone, Kosovo or Iraq) and are frequently utilized by many states, for instance the USA. See Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), p. 575.

[130] Article 101 reads: Piracy consists of any of the following acts:

> *(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;*
>
> *(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;*
>
> *(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).*

[131] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 566–567.

form of a war-like activity conducted by non-state actors"[132] notably influenced the treatment of those captured. While a captured pirate would almost certainly face trial and execution, a captured privateer was recognised as a prisoner of war under the law of nations [133](and their bond to the sovereign, therefore, protected them).[134,135] Although the rights of the prisoners of war varied significantly throughout history, their legal status was generally more favourable.[136] This contrast was starkly demonstrated in 1582 when nearly 400 combatants from a French raiding party were executed for failing to provide evidence of commission by the French Crown.[137]

While privateers played a pivotal role during times of war, their significance also extended into peacetime through the issuance of "*Letters of Marque*."[138] These private individuals represented a valuable asset not only due to their cost-effectiveness compared to a professional navy (further elaborated in Subsection 4.2)[139] but also because their deployment "*made possible minor acts of war without breaking the general peace existing between nations*,"[140] partly due to the more complicated evidentiary situation for

[132] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 4. http://www.dtic.mil/docs/citations/ADA590294

[133] The expression „the law of nations" has historically more meanings. The older meaning can be understood as „the common law of all nations", and thus „goes back to Jewish, Greek, and Roman Law". The notion „ the law regulating the mutual relations between States" is nowadays expressed in the term „International Law", as coined by the English philosopher Jeremy Bentham. In Idelson, V. R., et al. The Law of Nations and the Individual. *Transactions of the Grotius Society*, vol. 30, Problems of Peace and War, Transactions for the Year 1944, Cambridge University Press, 1944, p. 50.

[134] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 56.

[135] This is also the reason why privateers were motivated to provide the means of attribution – their commission.

[136] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 56.

[137] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583

[138] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, p. 20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[139] Tabarrok, A. (2007) *The Rise, Fall, and Rise Again of Privateers*, p. 566.

[140] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, p. 20 http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

the purposes of the attribution.[141] Although the term "*Letters of Marque and Reprisal*" is often used interchangeably with privateering, these letters were originally issued only during peacetimes, providing employment for privateers who would otherwise be idle during times of peace.[142]

The primary purpose of privateers during peacetimes is captured in the very name of the legal instrument commissioning their services, as it stems from two traditional laws – marque and reprisal. The law of *Marque* allowed a private individual to cross the border between two sovereigns and their domains, and the law of *Reprisal* gave the right to seek retribution or restitution for perceived harm that would be otherwise unsatisfied.[143] Therefore, by issuing letters combining these two rights, states authorised private individuals "*to take recompense from the citizens of another* (state) *for a legally recognised grievance.*"[144]

Hence, for sovereigns, privateers presented a relatively cost-effective tool, deployable against adversaries during both times of war and peace, offering a means to project sovereign power without overtly violating the general peace. For several states, privateers also represented the sole means of naval warfare, considering professional navies were prohibitively expensive and challenging to monitor for an extended part of history.[145] And while controlling privateers, similar to managing mercenary companies on land, typically posed quite a few challenges, they proved to be a pragmatic choice during the absence of professional navies.

The primary purpose of privateers was to intensify the attrition and disrupt adversarial economies, trade, international relations, and overall power projection. However, it would be a mistake to downplay the economic impact of their deployment, as privateers shared a percentage of their loot with the sovereign and thus often provided states with much-needed income.[146]

---

[141] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 4 - 5. https://lthj.qut.edu.au/article/view/1583

[142] Cooperstein, T. M. (2009) *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*. Rochester, NY, pp. 223–225. https://papers.ssrn.com/abstract=1406677

[143] *Op. cit.*, p. 223.; Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, p. 20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[144] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 5. http://www.dtic.mil/docs/citations/ADA590294

[145] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), p. 575.

[146] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 21 - 24. http://www.jstor.org/stable/10.2307/

Comparing these historical aspects with the contemporary employment of Advanced Persistent Threat (APT) and other hacker groups reveals striking similarities in their goals and effects. Given the significant understaffing and high costs associated with professional cyber-capacities,[147] hacker groups offer a viable means of projecting power in cyberspace during both times of war[148] and peace[149]. Furthermore, numerous instances of cyberattacks demonstrate their use for asset destruction,[150] economic disruption,[151] destabilisation of countries and international relations,[152] espionage,[153] support for military operations,[154] and general power projection.[155] The WannaCry attack also exemplifies the second face of cyberattacks' economic importance, showcasing how they can generate income for the responsible state.[156]

j.ctv2nxkpmw; Rodger, N. A. M. The Law and Language of Private Naval Warfare. *The Mariner's Mirror*. 2014, vol. 100, no. 1, pp. 11–13.

147 The Urgency of Tackling Europe's Cybersecurity Skills Shortage [online]. *Microsoft: EU Policy Blog*. 23. 3. 2022 [accessed 17. 2. 2023]. https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/; (ISC)2. *Cybersecurity Workforce Study*. 2022. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx; Svantesson et al. *On sovereignty*, pp. 52–63.

148 E.g., the cyberattack on Georgian governmental infrastructure during the Russia-Georgian war of 2008. See Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf

149 The majority of other attacks, e.g., Estonian cyberattacks of 2007, Stuxnet, WannaCry or NotPetya.

150 E.g., Stuxnet and NotPetya.

151 E.g., WannaCry and Petya.

152 E.g., the cyberattacks against Estonia in 2007, the cyberattacks against Albania in 2022 or the ransomware campaign against hospitals during COVID-19 pandemics. See e.g., Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology* 15(2).

153 E.g., SolarWinds.

154 The cyberattacks against Georgian governmental infrastructure during the Russia-Georgian war of 2008 and the KASAT hack (hacks against Ukraine in 2022).

155 This aspect is especially apparent in the work of the Equation Group (USA) or in the cyberattacks mounted under the control of the Russian Federation, as these attacks sometimes need to remind their targets of the cyber-capabilities of the aggressor. See e.g., Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf

156 Bossert, T. Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – The White House [online]. *The White House - Press Briefings*. 19. 12. 2017 [accessed 22. 11. 2023]. https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/; Bendiek, A., Schulze, M. Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW. *SWP Research Paper*. 2021, pp. 20–23. https://www.swp-berlin.org/10.18449/2021RP11/; Global Research and Analysis Team of Kaspersky Lab. WannaCry and Lazarus Group – the missing link? [online]. *Kaspersky*

And while hacker groups also pose challenges in terms of control, they stand as the next best alternative in the absence of professional expert capacities. Therefore, it is evident that in the category of purpose and effect, the practices of deploying privateers and hackers are analogous.

4.2. THE ENVIRONMENT – THE RISE TO POWER

In the second subsection, our focus shifts to a comparative analysis of the distinctive characteristics of high seas and cyberspace, elucidating the factors contributing to the ascendancy of both privateers and hackers to power.

In contrast to land, both the high seas and cyberspace present environments that defy easy governance and border demarcation. Non-state actors can relatively easily access both domains (both skill- and resource-wise), which both guarantee a certain degree of anonymity. These aspects hinder the states' monitoring and enforcement capabilities, thus amplifying the demands on effective governance. Consequently, states exert a much weaker presence in these environments, creating opportunities for private individuals and organisations (such as East India Company or Google and Facebook).

These dynamics are aptly illustrated by the factors leading to the zenith of privateering during its golden age in the 18th century (also known as the Golden Age of Piracy). While the importance and respectability of the privateering practice grew throughout history (mainly in the Middle Ages), it was the surge in maritime trade, particularly with the exploration of America and the East Indies, that catapulted privateering to unprecedented heights.[157] The competition among European powers, particularly Spain and England, for dominance in the New World pushed many naval powers to augment their naval capabilities beyond their national arsenals (especially after the defeat of the Spanish Armada in 1588) and lesser powers, that lacked the resources and capabilities to deploy a respectable navy, to employ at least private contractors to extend their power projection and impede the hegemonic progress of colonial powers.[158]

The constant conflicts between naval superpowers during the wars to control East and West Indies presented lucrative opportunities for

- *SecureList*. 15. 5. 2017 [accessed 7. 1. 2024]. https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/

[157] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 35–41. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[158] Rodger, N. A. M. The Law and Language of Private Naval Warfare. *The Mariner's Mirror*. 2014, vol. 100, no. 1, pp. 11–13.; Anderson, J. L. (1995) *Piracy and World History: An Economic Perspective on Maritime Predation*, pp. 189–194.

privateers.[159] The abundance of lucrative prizes, coupled with diminishing naval threats (as the navies were either shattered, weary or preoccupied with the conflict), resulted in an influx of privateers so vast that it was impossible to employ all of them even during the peacetimes, which prompted many of them to turn to piracy (e.g., after the end of the Spanish Succession Wars in 1713, there was an evident upsurge in pirate activity in the Caribbean).[160] And despite draconian law enforcement attempts by the English in the 1720s (mass hangings in the Atlantic ports), piracy persisted due to states' inability to sustain such efforts for longer periods of time and target safe havens.[161]

As noted in the previous subsection, a pivotal aspect of the environment fostering privateer activity was the absence of professional forces capable of opposing and bringing them to justice.[162] As Still points out, "*for the better part of human history, the primary method for dealing with maritime pirates and privateers was individual avoidance and self-defence.*"[163] States, unable to effectively address the issue, adopted a laissez-faire approach to maritime trade, and many either paid foreign privateers to spare their ships or employed their own to redirect the problem towards their enemies.[164]

Considering all these factors within the broader geopolitical context, it becomes evident that states played a crucial role in ushering in the golden age for both privateers and pirates through their laissez-faire approach or outright utilisation.[165] As the alternatives and solutions appeared either too costly or in direct contradiction with the strategic goals of a sovereign, most states were somewhat reluctant to refrain from the practice of privateering.[166] And because most of the naval powers used these private individuals to bolster their strength at sea, abolishing this practice would disadvantage any

[159] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583

[160] Kraska, J. (2011) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*. Santa Barbara, Calif: Praeger, p. 30.

[161] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7. https://lthj.qut.edu.au/article/view/1583

[162] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 575–576.

[163] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 3. http://www.dtic.mil/docs/citations/ADA590294

[164] Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), p. 187.

[165] Cooperstein, T. M. (2009) *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, pp. 223–224.

[166] Ibid.

state that would do so.[167] Thus, the equation was relatively simple – states tolerated the suffering of their subjects as long as others suffered more.

Therefore, it is evident that the environments of the sea and cyberspace have much in common. The presence of states, their power, and their capacity to monitor and enforce their will within both of these environments was/is much weaker compared to their power over land.[168] Both promise a certain degree of anonymity, they both are problematically divided by borders that would directly limit states' interests (resulting in the direct conflict of those interests), and they are both relatively easy to access for individuals. Both of these also exhibit a certain degree of asymmetry, enabling private individuals to challenge the power of other sovereigns to some extent.[169]

As states recognised their lack of skills and professional capacities even in cyberspace, some collaborated with cybercriminal hacker groups. These partnerships, promising safe haven and preferential treatment from law enforcement, impeded the prosecution of cyber-criminals from specific countries.[170] Consequently, many states, even in cyberspace, adopted a regime of *avoidance* and *self-defence* (meant generally, not in the sense of UN Charter), which severely lowered the threat level faced by hacker groups.[171] Moreover, collaborations with hacker groups, even among permanent UN Security Council members, hinder discussions and the political will to effect meaningful changes and enhance security in cyberspace.[172,173]

---

[167] Rodger, N. A. M. The Law and Language of Private Naval Warfare. *The Mariner's Mirror*. 2014, vol. 100, no. 1, pp. 9–13.

[168] In case of limitations of sovereigns' power within cyberspace, see Polčák, R., Svantesson, D. J. B. (2017) *Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[169] Spector, P. (2017) In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–222.

[170] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. pp. 96–99.

[171] This is further worsened by the inefficient sanctions aimed at the individual hackers, that can be easily avoided should the hackers refrain from travelling into extraditing countries. See Goldsmith, J. (2017) The Strange WannaCry Attribution [online]. *Lawfare*. [accessed 21. 11. 2023]. https://www.lawfaremedia.org/article/strange-wannacry-attribution; Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/

[172] Analogically, see keynote by Johanna Weaver for the CyCon 2022 Conference, accessible here: https://www.youtube.com/watch?v=O8eFiJaNzRU\&list=PLV8RTnZwQxcmajmJOMBlXByxJpzy9qD3c\&index=29

[173] The similarity of both environments may be of analogical significance even at this point, as it is crucial to understand that it was the states who exploited the privateering practices the most, that brought forth the golden age of the privateers and pirates through safe havens, preferential treatments and laissez-faire approach. It is likely that utilising cybercriminal groups may have similar consequences. See Osula, A.-M., Kasper, A. and Kajander, A. (2022)

As previously discussed, both cyberspace and the maritime environment are well-suited for projecting power anonymously and destabilizing rivals without crossing the threshold of war. The nature of the relationship between a state and non-state actors such as hacker groups and privateers, which we will explore in the following subsection, differs qualitatively from that with entities like mercenary companies on land. Unlike mercenaries, these non-state actors do not require extensive support and control to achieve significant levels of damage or power projection; in some cases, merely unleashing them is sufficient. Additionally, the inherent characteristics of these environments (i.e., the relatively limited state presence) further complicate the process of gathering evidence, particularly for states with weaker intelligence capabilities.

The fact that there are states aware of this complexity is aptly illustrated by the varying levels of state involvement in cyberattacks as outlined by Jason Healey in his 2012 article.[174] He categorizes state involvement on a spectrum: "*State-prohibited, State-prohibited-but-inadequate, State-ignored, State-encouraged, State-shaped, State-coordinated, State-ordered, State-rogue-conducted, State-executed and State-integrated.*"[175] For instance, the 2007 cyberattacks against Estonia likely fell between the State-shaped and State-coordinated levels, both of which are insufficient to meet *the effective control test* for legal attribution. It is evident that if states can execute a sufficiently damaging cyberattack with a level of control that does not meet the threshold for legal attribution, they are likely to pursue such tactics. Alternatively, they may integrate private hacker groups into the state apparatus to further complicate attribution.[176] Overall, due to the asymmetric natures of the environments (cyberspace and sea), states find it unnecessary to exert the same level of control and support as in traditional cases, such as the *Nicaragua* case.

EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1).

[174] Healey, J. (2012) *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. Atlantic Council – Cyber Statecraft Initiative. `https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212\ACUS\NatlResponsibilityCyber.PDF`

[175] Ibid.

[176] The State-integrated level by Healey is specific in this matter as the level of control and support are relatively high but the states involvement is still hidden by the obscurity provided by the integration, because the integration is seldom made on a legal level (e.g., the actor behind the WannaCry attack or APT 28 and 29 were once probably stand-alone hacker groups, but later integrated into the state apparatus, effectively obscuring the level of control the state has over them).

4.3. THE SUBJECT – A PRIVATE INDIVIDUAL WITH MEANS AND MOTIVATION

The final comparative category between hackers and privateers focuses on the subject aspect.

Privateers were typically recruited from among private individuals possessing the requisite resources, such as an armed vessel with a crew, a specific skill set, and a particular motivation driven by the desire for wealth.[177] Typically, they had already established a reputation for themselves, distinguishing them in the eyes of state representatives and proving their value as an asset for the state. This reputation might have been gained through various means, even including harassing the state's subjects, which in turn motivated the state to bribe or employ them against its enemies instead, especially if it lacked the power to bring such an individual to justice.[178]

Privateers were primarily motivated by financial gains[179], often compensated by piece (captured or sunk ships and cargo), ransom from prisoners, and a portion of the loot (with a percentage going to the commissioning sovereign).[180] Nonetheless, the privateering profession, even in the absence of professional navies, was inherently risky and a loyalty to a sovereign offered some crucial benefits, primarily the guaranteed safe havens, which reduced the threat level privateers faced and offered a place to repair and regroup.[181,182] The rise of the pirates and privateers would have been impossible without these bases of operations throughout the Caribbean, Mediterranean or East Indies.[183] These bases of operation also severely

[177] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 19–24, 35–39 and 59–66. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[178] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 567–570.

[179] Even though some also pursued this profession from a sense of patriotic duty or a sadistic pleasure.

[180] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 59–66. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[181] The safe havens or harbours were not an exclusive aspect of privateering, pirates also used these bases, nevertheless, privateers' access to the safe harbours of their master were guaranteed. See Cartwright, M. (2021) Pirate Havens in the Golden Age of Piracy [online]. *World History Encyclopedia*. [accessed 14. 1. 2024]. https://www.worldhistory.org/article/1844/pirate-havens-in-the-golden-age-of-piracy/

[182] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 59–66. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[183] Cartwright, M. (2021) Pirate Havens in the Golden Age of Piracy [online]. *World History Encyclopedia*. [accessed 14. 1. 2024]. https://www.worldhistory.org/article/1844/pirate-havens-in-the-golden-age-of-piracy/

diminished the effectiveness of deterrence.[184] From the criminological and psychological point of view, people are deterred from anti-social acts mainly because of the fear of punishment or the high probability of failure.[185] Therefore, the effectiveness of punitive deterrence is primarily influenced by the probability of arrest and conviction and the severity of punishment.[186] Therefore, the combination of a relatively low risk of arrest guaranteed by the existence of safe havens with high monetary gains could not serve as a capable deterrence.[187]

In comparison, hackers are usually also recruited from among the private individuals already organised with like-minded colleagues and typically with a cybercriminal background and reputation, akin to privateers.[188,189] These groups possess the necessary skills, knowledge, and equipment, with their own techniques, tactics, and processes, and while primarily motivated by financial gains, some hackers may also harbour a sense of patriotism or destructive tendencies.[190] States cooperating with such actors may establish specific rules of conduct, promising leniency from law enforcement as long as the hacker groups avoid targeting the citizens of the cooperating states[191] and offering a safe haven against foreign law enforcement and intelligence agencies in exchange for occasional execution of cyberattacks more or less specified by the government or intelligence services.[192]

[184] This aspect is crucial for the factors impacting cyber-deterrence.

[185] Jervis, R. et al. (1989) *Psychology and deterrence*. Baltimore (Ma.) London: The John Hopkins university press, pp. 34–37.

[186] Baliga, S., Bueno De Mesquita, E., Wolitzky, A. (2020) Deterrence with Imperfect Attribution. *American Political Science Review*, 114(4), pp. 1155–1157.

[187] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 8. `https://lthj.qut.edu.au/article/view/1583`

[188] That is apparent with most of the top 20 APT listed by CrowdStrike, see *APTs & Adversary Groups List - Malware & Ransomware*.

[189] The relationship between privateers and pirates is essentially analogous to the one between state-sponsored hacker groups and cybercriminal groups.

[190] Horsley, E. (2020) State-Sponsored Ransomware Through the Lens of Maritime Piracy. *Georgia Journal of International & Comparative Law*, 47(3), pp. 671–673.; Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure [online]. *Cybersecurity and Infrastructure Security Agency*. 9. 5. 2022 [accessed 15. 1. 2024]. `https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a`

[191] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 96–99.

[192] Holt, T. J. et al. (2023) Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*, 22(4), pp. 826–828; Osawa, J. (2017) The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review*, 24(2), pp. 114–118.

Both non-state actors typically engage in activities below the threshold of war, aiming to cause harm without disrupting the general peace.[193] However, hackers and privateers differ in an essential aspect – the physical risks of their endeavours. Privateers had to be physically present (ergo, not in the safe haven) during raids, increasing the likelihood of capture or harm (consequently increasing also the motivation of presenting valid commission and thus attributing their activities to a sovereign). In contrast, hackers do not need to compromise their security in such a way. Should they refrain from travelling, they are relatively safe from most targeted sanctions.[194] Yet, most of them still travel, which may present the aggrieved state with the possibility of apprehension, such as in the case of Roman Seleznev, who was apprehended by the USA in Maldives in 2013.[195] Nevertheless, the effectiveness of safe harbours is undeniably higher for hackers (inter alia due to the anonymous and global nature of the internet), complicating attribution more than in the case of privateers.

Based on the analogies found throughout the examined categories, it is reasonable to assume that the practice of utilising hacker groups is sufficiently similar to the practice of commissioning privateers (effectively making the practice of utilising hacker groups "cyber-teering"). Even though we have found differences (such as the extent and effectivity of the safe haven in case of hackers), which may further complicate the evolution of the cyber-attribution problem, analysing factors that contributed to the decline of privateering may offer valuable insights into addressing, mitigating, and potentially resolving the cyber-attribution problem associated with "state-sponsored" hacker groups[196]. Therefore, we now proceed to analyse these factors in the next section, where we also examine their potential relevance for the modern age analogy.

[193] Horsley, E. (2020) State-Sponsored Ransomware Through the Lens of Maritime Piracy. *Georgia Journal of International & Comparative Law* 47(3), pp. 671–673.

[194] Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/.

[195] Layne, N. (2017) Russian Lawmaker's Son gets 27 Years Prison in U.S. hacking case. *Reuters*. https://www.reuters.com/article/idUSKBN17N2GZ/; Russian Cyber-Criminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for $50 Million in Online Identity Theft and $9 Million Bank Fraud Conspiracy [online]. *United States Department of Justice, Office of Public Affairs*. 30. 11. 2017 [accessed 29. 12. 2023]. https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible

[196] We use this term to encompass more than just APT groups – there are also groups, who are not as advanced or who cooperate only rarely. Unfortunately, we know of no term that would describe such a subject.

5. HIC SUNT DRACONES

The 19th century marked the decline of the privateering practice, initially apparent in shifting policies around the turn of the century[197] and later, in 1856, also legally, with the enactment of the Paris Declaration Respecting Maritime Law.[198]

It is crucial to emphasise that privateering was a widely employed practice by the end of the Golden Age, and piracy was a necessary and somewhat tolerated complement. The initial crack in this paradigm emerged during the American conflicts with the Barbary States in 1801, coupled with a general weariness and dissatisfaction with paying tributes to these states.[199] This development shattered the idealised view of privateers and exposed the inadequacy of suppressing their activities. Following America's lead, other European powers adopted similar strategies to deal with foreign corsairs and privateers, collectively bringing an end to the dominance of Barbary privateering in the Mediterranean.[200] Additionally, the French colonisation of key strongholds for the Barbary states in the 1830s further contributed to the cessation of the Barbary privateer threat.[201]

Although the American-Barbary conflicts served as a guide for Europe, the transformative shift did not come until the Napoleonic Wars, albeit in an ironic fashion. The conflict's extent and intensity forced most participating powers to equip professional navies, thus lowering the demand for privateers.[202] Furthermore, following the wars, the British Royal Navy found itself with surplus capacity and a newfound role of a naval hegemon. Leveraging their considerable naval strength, the British Royal Navy found, for the first time in history, that it was powerful enough to counter the threat of pirates and foreign privateers and thus enforced the so-called *Pax Britannica*.[203] In this endeavour, the Royal Navy actively participated in global anti-piracy and anti-slavery initiatives to safeguard international

[197] Rubin, A. P. (1988) *The Law of Piracy*. Honolulu.: University Press of the Pacific Hunolulu, p. 216. https://archive.org/details/lawofpiracy63rubi

[198] Stark, F. R. (1987) *The Abolition of Privateering and the Declaration of Paris*. New York: Columbia University.

[199] Kraska, J. (2011) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*, pp. 25–26.

[200] *Op. cit.*, pp. 26–27.

[201] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7. https://lthj.qut.edu.au/article/view/1583

[202] Kraska, J. (2011) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*, p. 31.

[203] Ibid.

trade.[204] Dwan et al. also add that during this era, "*the British treated international law more like guidelines than actual rules, as best demonstrated by their practice in counter piracy operations. Further, this period in which British naval dominance ended piracy is significant because of the way in which it blurred British Imperial Law with international law.*"[205]

The cornerstone of British success lay in strategically targeting and blockading safe pirate anchorages and notorious safe havens, effectively nullifying the primary security feature for both pirates and privateers.[206] Moreover, legal mechanisms supporting privateers' income, such as the rights of ransom and parole, gradually eroded, eventually leading to their outlawing.[207] As governmental capacities strengthened, including heightened capabilities for monitoring the high seas, the privateering system became increasingly perceived as inefficient (and unprofitable for the privateers).[208] It is crucial to emphasise that throughout history, privateering has never been an ideal solution. Due to fiscal constraints, it had served as a makeshift alternative to professional navies, being a cheaper yet more challenging-to-control option that rarely aligned precisely with government objectives.[209] To add insult to injury, in the 19th century, privateers also emerged as direct competitors with states' navies in hiring sailors (and were typically more proficient in that, worsening their relations with professional capacities).[210]

The rise of professional navies, both in strength and professionalism, coupled with their growing animosity toward privateers, increased risks of apprehension and death in the era of *Pax Britannica*, the destruction of safe

[204] Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), p. 189.; Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7. https://lthj.qut.edu.au/article/view/1583

[205] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7 - 8. https://lthj.qut.edu.au/article/view/1583

[206] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 572–573;Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 8. https://lthj.qut.edu.au/article/view/1583

[207] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 572–573.

[208] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 57–58.

[209] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), p. 575.; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 59.

[210] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 59.

havens, and a decline in potential financial gains[211], collectively rendered the privateer practice obsolete and unprofitable for states and privateers alike.[212] The formal abolition of this practice in 1856 through the Paris Declaration was already more of a declaratory in nature.[213]

6. LESSONS OF THE PAST

As established in Section 4.2, most sovereign powers still lack sufficient capabilities to manage the cybercrime problem entirely.[214] Instead of addressing it directly, certain states, such as the Russian Federation, attempt to exploit the situation by harnessing these individuals against rivals, leveraging their capabilities within cyberspace's weakly monitored and governed environment.[215] However, drawing from the historical example of privateers, this exploitative approach, combined with the laissez-faire approach of many other states, could potentially lead to a golden age of cybercriminals and cyberattacks. Such a scenario can potentially severely destabilise not only cyberspace but also international relations.[216] Moreover, contemporary society is even more dependent on the availability of cyberspace[217] than it was on the high seas and maritime trade.

The utilisation of hacker groups exploits the cyber-attribution problem to detrimentally impact the interests of strategic rivals, causing harm to their assets and crippling economies, all while avoiding a disturbance to general peace. This situation is relatively unlikely to change in the foreseeable future, as although the frequency of attributions is increasing, states hesitate to invoke international responsibility and enforce relevant consequences.[218]

---

[211] Not only because of the abolition of the rights to ransom and parole, but also because of the rising percentage of the loot that was supposed to be sent to the commissioning sovereign. See Kraska. *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*, p. 30.

[212] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 575–576.; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 59–60.

[213] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 55–56.

[214] For example, the cybersecurity of the public and private sectors in the Czech Republic is far from ideal. It is so because of many reasons, one being the inability of the public sector to draw experts into their fold. However, these problems are beyond the scope of this paper.

[215] *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022.

[216] Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2), pp. 216–222.; Kolouch et al. *Cybersecurity: Notorious, but Often Misused and Confused Terms*, pp. 291–298.

[217] Evident, e.g., in Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology* 15(2), pp. 305–321.

[218] Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. `https:`

Furthermore, exploiting the cyber-attribution problem typically lies in the hard-to-prove link between hackers and the state in question. Akin to privateers, state-sponsored hackers may only disclose this link if captured. However, their motivation to do so is much lower than in the case of privateers providing valid *Letters of Marque*, as mere cybercriminals do not face death sentences (unlike pirates). The situation's complexity is further compounded by the global reach of cyberattacks and the extensive safe haven protection afforded to state-sponsored hacker groups.

The historical excursion presented above illustrates that the attribution problem in the case of privateers was not resolved directly, nor was the solution of a legal nature. Instead, the relevance of the privateers' attribution problem diminished together with the factual decline of the privateering practice. Considering current developments, it is rather unlikely that history would not repeat itself in the case of state-sponsored hacker groups, despite the increasing frequency of political attributions since 2017.[219,220]

However, the historical analogy effectively highlights that as long as there are safe havens for hackers, cybercrime and state-sponsored cyberattacks are likely to persist and even grow.

Therefore, based on the historical parallels, the future development of the cyber-attribution problem and "cyber-teering" practice appears to be heading in one of three potential directions:

1) **Unification of the State Practice Leading to a Cyber-specific Customary Rule of Attribution**: The trend of political attributions of cyberattacks may persist, gradually contributing to the reformation of the unused rules of the attribution (i.e., *the effective control test*). The unification of state practices could lead to the formation of cyber-specific customary rules along the lines of maritime attribution standards, which would be better tailored to the unique needs of states in cyberspace. This renewed applicability might result in more

//www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/; Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 94–100.

[219] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 530–533.

[220] That is closely related to the geopolitical context, as political attributions utilizing naming and shaming strategy are relatively meaningless in the relationship of strategic rivals (such as North Korea and the USA). See Goldsmith. *The Strange WannaCry Attribution*.; Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/

frequent invocations of state responsibility, potentially stabilising the international situation.

2) **Emergence of Sufficient Professional Cyber-capabilities**: The current practice of political attributions may remain too diverse and thus fail to create a cyber-specific customary rule due to varying state interests. The number (and severity of consequences) of state-sponsored cyberattacks could increase, further destabilising cyberspace and international relations. This scenario could lead to a conflict or a major cyber-incident with catastrophic consequences, which might force states to invest in the preparation of professional cyber-capacities[221], improving their capabilities to monitor and govern cyberspace. The possibility of not only identifying the perpetrator but also striking back could then serve as a basis for cyber-deterrence. With the emergence of such capabilities on a sufficient level[222], the need to employ hacker groups could diminish, akin to the decline observed in privateering.[223]

3) **Stabilisation through Destabilisation**: As mentioned in Section 3, not every state desires the cyber-attribution problem to be resolved. There are those who exploit it and benefit from the more restrained approach of (primarily) Western states.[224] However, with the worsening of these problems of applied cyber legalism and overall security situation, even Western states may abandon the high road and adopt the same tactics (exploitation of the cyber-attribution problem).[225] The ensuing worsening of international relations, stability of international society and security in cyberspace (*the destabilisation aspect*) could eventually

[221] There are already many projects trying to improve the education of cybersecurity expert capacities, such as the project SPARTA (see `https://www.sparta.eu/`), however, the capabilities of the states to produce a sufficient number of those experts and employ them in the public sector are still rather limited.

[222] Many states have already a cyber-capacities within their armies and intelligence services, nevertheless, similarly to the relationship between navies and privateers, their numbers are not yet sufficient to deter and effectively fulfil any of the states' goals.

[223] These official capacities could either accept and adapt to cyber-attribution problem (and thus create a new state practice), or completely resign on it and leave the attribution only in the political level without legal constrains (paradoxically also creating new state practice).

[224] Schmitt, M. Three International Law Rules for Responding Effectively to Hostile Cyber Operations [online]. *Just Security*. 13. 7. 2021 [accessed 16. 1. 2024]. `https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/`

[225] Kello, L. (2021) Cyber Legalism: Why It Fails and What to do about It. *Journal of Cybersecurity*, 7(1), pp. 2–3; Schmitt, M. Three International Law Rules for Responding Effectively to Hostile Cyber Operations [online]. *Just Security*. 13. 7. 2021 [accessed 16. 1. 2024]. `https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/`.

lead to a consensus among states on the need for regulation, reminiscent of the Paris Declaration, bringing the cyber-attribution back within the scope of the law and constraining the use of cyberattacks (*the stabilisation aspect*). To minimise the risks of full escalation, it might be necessary to implement a particular set of rules balancing this destabilising campaign, such as the multi-level attribution-cyberteering concept and reinstitution of Letters of Marque proposed by Still.[226] A vital component of this destabilisation campaign should also involve targeting and "blockading" (DDoS and infrastructure destruction) hackers' safe havens and the states supporting them, as Harašta and Bátrla suggested.[227] By doing so, such a campaign could not only disrupt the cybercriminal environment but also influence the most relevant states. This scenario is based upon the premise that the political will to improve the situation may only emerge when the *general annoyance* becomes too substantial to ignore.

7. CONCLUSION

In this article, we have argued that the inadequacies of contemporary cyber-attribution legal procedures stem from the misguided attempt to apply standards developed for land-based conflicts to an environment that more closely resembles the high seas, primarily due to the lower level of control that states exert over these domains. This perspective offers a compelling parallel to the practice of obscuring states' involvement[228] in cyberattacks by employing hacker groups – privateering. To explore this analogy, we examined the historical practices of employing privateers and hackers, aiming to derive insights into the challenges posed by state-sponsored cyberattacks and the exploitation of the cyber-attribution problem. Our analysis revealed significant parallels across various dimensions, including purpose, effect, environment, and the nature of non-state actors, supporting the validity of drawing comparisons between cyberspace and the high seas, and justifying the application of historical analogy for inspiration. Consequently, we analysed the factors that led to the decline of privateering, seeking insights that could be applied to mitigate the issues associated

[226] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 3. `http://www.dtic.mil/docs/citations/ADA590294`, pp. 24–25.

[227] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 99–100.

[228] Or utilizing capabilities that would otherwise be inaccessible for the said state.

with cyber-attribution and the modern-day equivalent of privateers – "cyber-teers."

Our analysis revealed that the resolution of the privateering problem (and associated attribution problems) was not achieved by means of law but by the change of doctrine, which is unfortunately the probable course even in the case of cyber-attribution.[229] The factors instrumental to the decline of privateers that could also potentially mitigate the practice of state-sponsored cyberattacks and exploitation of cyber-attribution problem involve the emergence of professional state capacities (rendering the use of hard-to-control and unreliable privateers or hackers less necessary and profitable), destruction, disruption or denial of safe havens and the consequent decline of the risk/gain profitability for the non-state actors. In combination with technological advancements like the thorough implementation of *security by design and default* approaches throughout the market, these factors may cause or at least contribute to the decline of the cyber-teering practice.

Concluding our exploration, we introduced three prospective scenarios based on contemporary developments and historical analogies. These scenarios encompass the emergence of cyber-specific rules of attribution and the enhancement of legal aspects of cyber-deterrence, the development of professional cyber-capacities of states following a major cyber-incident or even a conventional conflict (such as in the case of the post-Napoleonic era) enhancing the factual aspects of cyber-deterrence, and stabilisation through destabilisation. These scenarios or their combination reflect potential pathways for the evolution of the current situation, offering a perspective on addressing the challenges in the realm of state-sponsored cyberattacks and cyber-attribution.

LIST OF REFERENCES

[1] Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), pp. 175–199.

[2] Aravindakshan, S. (2021) Cyberattacks: A Look at Evidentiary Thresholds in International Law. *Indian Journal of International Law*, 59(1–4), pp. 285–299.

[3] Baliga, S., Bueno De Mesquita, E., Wolitzky, A. (2020) Deterrence with Imperfect Attribution. *American Political Science Review*, 114(4), pp. 1155–1178.

[4] Banks, W. (2021) Cyber Attribution and State Responsibility. *International Law Studies*, 1039(97), pp. 1040–1072.

[229] Kello, L. (2021) Cyber Legalism: Why It Fails and What to do about It. *Journal of Cybersecurity*, 7(1), pp. 2–3.

[5] Bendiek, A., Schulze, M. (2021) Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW. *SWP Research Paper*. https://www.swp-berlin.org/10.18449/2021RP11/

[6] Berghel, H. (2017) On the Problem of (Cyber) Attribution. *Computer - IEEE Computer Society*, 50(3), pp. 84–89.

[7] Berman, H. J. (1983) *Law and Revolution: the Formation of the Western Legal Tradition*. Cambridge (Mass.) London: Harvard university press.

[8] Boebert, W. E. (2010) A Survey of Challenges in Attribution. In: *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: The National Academies Press, pp. 41–52. http://www.nap.edu/catalog/12997.html

[9] Bossert, T. (2017) Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – The White House [online]. *The White House - Press Briefings*. [accessed 22. 11. 2023]. https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

[10] Brigitte, S. (2010) The Elements of An Internationally Wrongful Act. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press. Oxford Commentaries on International Law.

[11] Cartwright, M. (2021) Pirate Havens in the Golden Age of Piracy [online]. *World History Encyclopedia*. [accessed 14. 1. 2024]. https://www.worldhistory.org/article/1844/pirate-havens-in-the-golden-age-of-piracy/

[12] Cassese, A. (2007) The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*, 4, pp. 649–668.

[13] Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly*, 67(3), pp. 643–668.

[14] Condorelli, L., Kress, C. (2010) The Rules of Attribution: General Considerations. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press. Oxford Commentaries on International Law.

[15] Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf

[16] Cooperstein, T. M. (2009) *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*. Rochester, NY. https://papers.ssrn.com/abstract=1406677

[17] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

[18] Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press.

[19] Davis, J. K. (2022) *Tallinn Paper No. 13 - Developing Applicable Standards of Proof for Peacetime Cyber Attribution*. NATO CCD COE Publications.

[20] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2). https://lthj.qut.edu.au/article/view/1583

[21] Edwards, B. et al. (2017) Strategic Aspects of Cyberattack, Attribution, and Blame. *Proceedings of the National Academy of Sciences*, 114(11), pp. 2825–2830.

[22] Egloff, F. (2017) Cybersecurity and the Age of Privateering. In: Perkovich, G., Levite, A. E. (eds.). *Understanding Cyber Conflict: Fourteen Analogies*. Washington, DC: Georgetown University Press, pp. 231–247.

[23] Egloff, F. J., Smeets, M. (2021) Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, pp. 1–32.

[24] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 520–598.

[25] Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/

[26] Gentili, A. (1612) *De Iure Belli Libri Tres*. Oxford: The Clarendon Press. Carnegie Classics of International Law. https://archive.org/details/threebooksonlawo0002ayal/page/n3/mode/2up

[27] Giles, K., Hartmann, K. (2019) 'Silent Battle' Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. In: Minárik, T. et al. (eds.). *11th International Conference on Cyber Conflict: Silent Battle*. Tallinn: NATO CCD COE Publications, pp. 23–36.

[28] Global Research and Analysis Team of Kaspersky Lab. WannaCry and Lazarus Group – the missing link? [online]. *Kaspersky - SecureList*. 15. 5. 2017 [accessed 7. 1. 2024]. https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/

[29] Goldsmith, J. (2017) The Strange WannaCry Attribution [online]. *Lawfare*. [accessed 21. 11. 2023]. https://www.lawfaremedia.org/article/strange-wannacry-attribution

[30] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger.

[31] Haataja, S. (2021) Autonomous Cyber Capabilities and Attribution in the Law of State Responsibility. In: Liivoja, R., Väljataga, A. (eds.). *Autonomous Cyber Capabilities under International Law*. Tallinn, Estonia: NATO CCD COE Publications, pp. 260–290. NATO CCDCOE Publications.

[32] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 93–115.

[33] Hayes, A. (1925) Private Claims against Foreign Sovereigns. *Harvard Law Review*,38(5), pp. 599–621.

[34] Healey, J. (2012) *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. Atlantic Council – Cyber Statecraft Initiative. https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212\ACUS\NatlResponsibilityCyber.PDF

[35] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), pp. 265–306.

[36] Holt, T. J. et al. (2023) Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*, 22(4), pp. 825–848.

[37] Horsley, E. (2020) State-Sponsored Ransomware Through the Lens of Maritime Piracy. *Georgia Journal of International & Comparative Law*, 47(3), p. 669.

[38] (ISC)2. *Cybersecurity Workforce Study*. 2022. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[39] Jensen, E. T. (2020) Due Diligence in Cyber Activities. In: Krieger, H., Peters, A., Kreuzer, L. (eds.). *Due Diligence in the International Legal Order*. UK: Oxford University Press, p. 0. https://doi.org/10.1093/oso/9780198869900.003.0015

[40] Jervis, R. et al. *Psychology and deterrence*. Baltimore (Ma.) London: The John Hopkins university press, 1989. Perspectives on security.

[41] Kello, L. (2021) Cyber Legalism: Why It Fails and What to do about It. *Journal of Cybersecurity*, 7(1), pp. 1–15.

[42] Kolouch, J. et al. (2023) Cybersecurity: Notorious, but Often Misused and Confused Terms. *Masaryk University Journal of Law and Technology*, 17(2), pp. 281–305.

[43] Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology*, 15(2), pp. 301–341.

[44] Kraska, J. (2021) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*. Santa Barbara, Calif: Praeger. Contemporary Military, Strategic, and Security Issues.

[45] Layne, N. (2017) Russian Lawmaker's Son gets 27 Years Prison in U.S. hacking case. *Reuters*. https://www.reuters.com/article/idUSKBN17N2GZ/

[46] Liu, I. Y. (2017) *State Responsibility and Cyberattacks: Defining Due Diligence Obligations*. Rochester, NY. https://papers.ssrn.com/abstract=2907662

[47] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 405–428.

[48] Microsoft Threat Intelligence. (2022) Microsoft investigates Iranian attacks against the Albanian government [online]. *Microsoft Security Blog*. [accessed 31. 7. 2023]. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

[49] Obama, B. (2010) *US National Security Strategy*. The White House, Washington. https://obamawhitehouse.archives.gov/sites/default/files/rss\viewer/national\security\strategy.pdf

[50] Osawa, J. (2017) The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review*. 24(2), pp. 113–131.

[51] Osula, A.-M., Agnes Kasper, Aleksi Kajander. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 89–123.

[52] Pamment, J. et al. (2019) *Hybrid Threats: 2007 Cyber Attacks on Estonia*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/cyber\attacks\estonia.pdf

[53] Pellet, A. (2010) The Definition of Responsibility in International Law. In: Crawford, J., Olleson, S., Parlett, K. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press. Oxford Commentaries on International Law.

[54] Polčák, R., Svantesson, D. J. B. (2017) *Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[55] Rid, T., Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1–2), pp. 4–37.

[56] Rodger, N. A. M. (2014) The Law and Language of Private Naval Warfare. *The Mariner's Mirror*, 100(1), pp. 5–16.

[57] Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[58] Rubin, A. P. (1988) *The Law of Piracy*. Honolulu.: University Press of the Pacific Hunolulu. https://archive.org/details/lawofpiracy63rubi

[59] Schmitt, M. (2018) In Defense of Sovereignty in Cyberspace [online]. *Just Security*. [accessed 28. 6. 2023]. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

[60] Schmitt, M. (2021) Three International Law Rules for Responding Effectively to Hostile Cyber Operations [online]. *Just Security*. [accessed 16. 1. 2024]. https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/

[61] Schmitt, M. (2017) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

[62] Schmitt, M. (2013) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge ; New York: Cambridge University Press.

[63] Schmitt, M., Watts, S. (2015) The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare. *Texas International Law Journal*, 50(2–3), pp. 189–232.

[64] Schöndorf, R. (2021) Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law Studies* 97(1). https://digital-commons.usnwc.edu/ils/vol97/iss1/21

[65] Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2), pp. 215–239.

[66] Spector, P. (2017) In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–223.

[67] Stark, F. R. (1897) *The Abolition of Privateering and the Declaration of Paris*. New York: Columbia University.

[68] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[69] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center. http://www.dtic.mil/docs/citations/ADA590294

[70] Svantesson, D. et al. (2023) On sovereignty. *Masaryk University Journal of Law and Technology*, 17(1), pp. 33–85.

[71] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review* 11(4), pp. 565–577.

[72] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 55–62.

[73] Talmon, S. (2015) Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion. *European Journal of International Law*, 26(2), pp. 417–443.

[74] Turton, W., Riley, M., Jacobs, J. (2021) Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. *Bloomberg.com*. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

[75] Wolff, C. (1995) *Jus Gentium Methodo Scientifica Pertractatum*. Buffalo, NY: Hein. The Classics of International Law 13. https://archive.org/details/jusgentiummethod0002wolf

[76] APTs & Adversary Groups List - Malware & Ransomware [online]. *Crowdstrike Adversary Universe* [accessed 27. 8. 2023]. https://adversary.crowdstrike.com/en-US/

[77] (2023) Attack (International Humanitarian Law) [online]. *International Cyber Law: Interactive Toolkit*. 28. 7. 2023 [accessed 10. 1. 2024]. https://cyberlaw.ccdcoe.org/wiki/Attack(international_humanitarian_law)

[78] (2024) Attribution Tracker [online]. *EuRepoC: European Repository of Cyber Incidents*. [accessed 18. 5. 2024]. https://eurepoc.eu/attribution-tracker/

[79] Connect the Dots on State-Sponsored Cyber Incidents – Stuxnet [online]. *Council on Foreign Relations* [accessed 26. 12. 2023]. https://www.cfr.org/cyber-operations/stuxnet

[80] (2001) *Draft articles on Responsibility of States for Internationally Wrongful Acts*. International Law Commission – United Nations. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[81] (2001) *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries - 2001*. International Law Commission – United Nations. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[82] (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*. https://digitallibrary.un.org/record/753055

[83] (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/150*. UN. https://digitallibrary.un.org/record/799853

[84] *Judgement of the International Court of Justice in the Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) - Merits*. 1986. https://www.icj-cij.org/case/70/judgments

[85] *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. 2007. https://www.icj-cij.org/case/91/judgments

[86] (2021) *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies*. General Assembly of the United Nations. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[87] (2016) *Responsibility of States for Internationally Wrongful Acts - Comments and information received from Governments and Report of the Secretary-General (A/71/79)*. General Assembly of the United Nations. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/112/74/PDF/N1611274.pdf?OpenElement

[88] (2017) Russian Cyber-Criminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for $50 Million in Online Identity Theft and $9 Million Bank Fraud Conspiracy [online]. *United States Department of Justice, Office of Public Affairs*. 30. 11. 2017 [accessed 29. 12. 2023]. https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible

[89] (2022) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure [online]. *Cybersecurity and Infrastructure Security Agency*. 9. 5. 2022 [accessed 15. 1. 2024]. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

[90] (2022) The Urgency of Tackling Europe's Cybersecurity Skills Shortage [online]. *Microsoft: EU Policy Blog*. 23. 3. 2022 [accessed 17. 2. 2023]. https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/

[91] (2024) Tracking State-Sponsored Cyberattacks Around the World [online]. *Council on Foreign Relations*. [accessed 7. 2. 2024]. https://www.cfr.org/cyber-operations