DOI 10.5817/MUJLT2020-2-4

MALICIOUS CYBER OPERATIONS, "HACKBACKS" AND INTERNATIONAL LAW: AN AUSTRIAN EXAMPLE AS A BASIS FOR DISCUSSION ON PERMISSIBLE RESPONSES*

by

ERICH SCHWEIGHOFER**,
ISABELLA BRUNNER***, JAKOB ZANOL****

In January 2020, Austria publicly announced that some of its governmental institutions have been hit by a significant malicious cyber operation and that it cannot be denied – at least for the moment – that a state was behind this operation. One month later, the Austrian Foreign Ministry declared the cyber operation to be officially over. While Austria noted that it took "countermeasures" against the operation, it is not entirely clear what it meant by that. This article elaborates the question what response options a state like Austria would have against a malicious cyber operation under the current framework of international law. It, hence, tries to answer when a "hackback" is lawful under international law and when it is not.

KEY WORDS

Countermeasures, Cyber Defense, Cyberspace, Hackback, International Law, Law of State Responsibility, Malicious Cyber Operation

* This contribution is inspired from and supported by both the Austrian *KIRAS-Project ACCSA* (https://www.kiras.at/gefoerderte-projekte/detail/d/accsa-austrian-cyber-crises-support-activities-1/) and the *Center for Intelligence and Security Studies* (*CISS* – https://www.unibw.de/ciss). The project *ACCSA* is financed by the *Austrian Federal Ministry for Transport, Innovation and Technology* and the *Austrian Research Promotion Agency* (*FFG* – https://www.ffg.at/en).

** erich.schweighofer@univie.ac.at, University of Vienna, Department of International Law; Centre for Computers and Law, Austria.

*** isabella.brunner@univie.ac.at, University of Vienna, Department of International Law, Austria.

**** jakob.zanol@univie.ac.at, University of Vienna, Department of International Law; Centre for Computers and Law, Austria.

1. INTRODUCTION

In January 2020, Austria publicly announced that the *Austrian Foreign Ministry* has been hit by a significant malicious cyber operation and that it cannot be denied – at least for the moment[1] – that a state was behind this operation.[2] In February 2020, the *Foreign Ministry* declared the malicious operation to be officially over.[3] While Austria noted that it took "countermeasures" ("*Gegenmaßnahmen*")[4] it is not entirely clear what it meant by that. According to an Austrian blog, technicians managed to get rid of the malware, putting the hacking group "in the defensive".[5] There is no further information available whether Austria considered response options under international law. This leads us to the question what a state – in this case Austria – *could* do (or could have done) in such a case, i.e. what measures would be allowed under the current framework of international law. This contribution, therefore, seeks to shine light on the specific reactions international law allows a state in case it was injured by a wrongful conduct, specifically with respect to wrongful cyber operations. It will, hence, try to answer when a "hackback" is lawful under international law and when it is not.

This contribution defines "hackback" as a measure taken through "cyber means" by a state against the territory of another state to cease a wrongful conduct (in the form of a cyber operation) the former state has been the target of. At the outset, this means that this contribution does not cover questions regarding possible measures of redress of non-state actors that have been the target of malicious cyber operations.

---

1 In a press release, the *Austrian Foreign Ministry* noted that *"the investigation is still ongoing"* about who is behind the "attack", see Austrian Federal Ministry for European and International Affairs. (2020) *Cyber Attack on the Foreign Ministry is Over*. [press release] 13 February. Available from: www.bmeia.gv.at/en/the-ministry/press/announcements/2020/02/cyber-attack-on-the-foreign-ministry-is-over/ [Accessed 19 August 2020].

2 Austrian Press Agency. (2020) *Schwerwiegender Angriff auf IT-Systeme des Außenministeriums*. [press release] 4 January. Available from: https://www.ots.at/presseaussendung/OTS_20200104_OTS0020/schwerwiegender-angriff-auf-it-systeme-des-aussenministeriums [Accessed 19 August 2020].

3 Austrian Federal Ministry for European and International Affairs. (2020) *Cyber Attack on the Foreign Ministry is Over*. [press release] 13 February. Available from: www.bmeia.gv.at/en/the-ministry/press/announcements/2020/02/cyber-attack-on-the-foreign-ministry-is-over/ [Accessed 19 August 2020].

4 Ibid.

5 Moechel, E. (2020) *Vorläufige Bilanz des Cyberangriffs auf das Außenministerium*. [blog entry] 16 February. Radio FM4. Available from: https://fm4.orf.at/stories/2998771/ [Accessed 20 August 2020].

This paper will first address the concept of attribution of a wrongful conduct to a state and briefly introduce the reader to the so-called "due diligence principle". In a second step, it will analyse three ways international law allows a reaction (hackback) to a malicious cyber operation endangering a state's territorial integrity: 1) as a lawful countermeasure, 2) as an exercise of the right of self-defence, or 3) as a reaction out of necessity. Given that most cyber operations happen below the threshold of an armed attack[6] (only in case of the latter would a state be able to respond in self-defence[7]), it makes sense to take a look at countermeasures first before addressing self-defensive measures. "Necessity" as a response option should be seen as a last resort, given the high threshold and non-reliance on attribution (on these criteria, see in detail below). Hence it will be dealt with last.

There are many open questions related to these three measures that we cannot all cover in this paper. One, for example, would relate to the extensive debate about the application of international law to cyber operations, and whether some provisions apply or do not apply in the cyber context. For the purpose of this contribution, we align with the larger international community and scholarly opinion that the conventional rules of international law (be it treaty obligations, general principles or custom) apply to cyber operations.[8] We also assume that measures taken in self--defence as well as countermeasures can only be taken against a state and that the initial malicious cyber operation would have to be attributed to that state.[9] Since that latter aspect of attribution is a *conditio sine qua non* of two

---

[6] Guitton, C. (2017) *Inside the Enemy's Computer: Identifying Cyber-Attackers*. London: Hurst & Company, p. 107.

[7] Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945 (1 UNTS XVI). Article 51.

[8] With UNGA Resolution 68/243, the international community endorsed the 2013 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), which acknowledges that *"international law, and in particular the Charter of the United Nations, is applicable"*; see United Nations General Assembly. (2014) *Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Doc A/RES/68/243. New York: United Nations. [online] Available from: https://undocs.org/A/RES/68/243 [Accessed 20 August 2020]; United Nations General Assembly. (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN Doc A/68/98. New York: United Nations. Paragraph 19. [online] Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement [Accessed 20 August 2020].

[9] To the contrary see, however, Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 15; Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17, p. 241.

of the three measures that we will focus on in this contribution, we will start with discussing it first.

2. ATTRIBUTION AND DUE DILIGENCE

Attribution, in general, is the act of *"identifying the agent responsible for the action"*.[10] Usually, experts differentiate between technical, political and legal attribution.[11] All three aspects of attribution need to be seriously taken into account when undertaking a hackback.

Regarding technical attribution, identifying the person acting behind the computer is extremely difficult.[12] The high degree of anonymity in the cyber context, the possibilities of conducting false-flag operations and the difficulties to identify the actors behind multi-stage attacks make it almost impossible to distinguish a particular actor in cyberspace.[13] However, identifying the specific natural person and its relationship to a state is the quintessential prerequisite of legal attribution.[14] Because only if a relationship with a state can be established, the targeted state can take action against the state from which the unlawful conduct originates.

For legal attribution, the *ILC Articles on Responsibility of States for Internationally Wrongful Acts* (hereinafter referred to as *ILC Articles*) are the primary source to determine whose conduct can be attributed

[10] Clark, D. D. and Landau, S. (2011) Untangling Attribution. *Harvard National Security Journal*, 2, p. 1.

[11] *Nicholas Tsagourias* is deemed to be the author of this differentiation, see Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17, p. 234: *"Attribution of cyber attacks is thus a multifaceted process; it has technical, legal and political aspects, with each aspect feeding into the other"*; see also Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 6. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020]: *"In the context of cyberspace, three forms of attribution can be distinguished: Technical attribution* […]*, Political attribution* […and] *Legal attribution* […]*"*.

[12] Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Nicholas Tsagourias and Russell Buchan (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham and Northampton: Edward Elgar Publishing, p. 62.

[13] Brunner, I., Dobric, M. and Pirker, V. (2019) Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards Before the ICJ. *Finnish Yearbook of International Law*, 25, pp. 76–77.

[14] See Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Nicholas Tsagourias and Russell Buchan (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham and Northampton: Edward Elgar Publishing, p. 58.

to a state.[15] The rules of attribution contained therein are widely held to reflect customary international law.[16]

The ILC Articles follow their own legal definition of attribution, which they define as

> *"the operation of attaching a given action or omission to a State."*[17]

For that, the ILC Articles distinguish between conduct of state organs (including *de facto* state organs)[18], and conduct of non-state actors, who – in one way or the other – act for the state.[19] Thus, if there is no sufficient link between the natural person or group of persons and the state, attribution on the basis of the ILC Articles – which regulate the consequences of wrongful *state* behaviour – cannot be established.

However, as already noted above, the difficulty does not lie in the legal realm, it lies within *proving* the sufficient link to the state: If a cyber operation originates from an IP address situated within the territory of state A, this information still does not provide us with which actor is actually behind the wrongful cyber operation. With its press release of 4 January 2020, Austria seems to suggest that it was indeed able to identify the origins of the "attack".[20] Unfortunately, however, it did not release any further information – let alone evidence – that would back up its position that a state actor could be behind the operation.

Given the fact that attribution of a wrongful conduct to a state tends to be very difficult, some scholars suggest to apply the so-called "due diligence" principle also in the cyber context: If a direct link to a state cannot be established, but it can be proven that the cyber operation derives

---

[15] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[16] See e.g. Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Tsagourias, N. and Buchan, R. (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham and Northampton: Edward Elgar Publishing, p. 58.

[17] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. P. 36 (Commentary to Article 2, paragraph 12). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[18] Cf. op. cit., Article 4.

[19] Cf. op. cit., Articles 5, 8 and 11.

[20] Austrian Press Agency. (2020) *Schwerwiegender Angriff auf IT-Systeme des Außenministeriums*. [press release] 4 January. Available from: https://www.ots.at/presseaussendung/OTS_20200104_OTS0020/schwerwiegender-angriff-auf-it-systeme-des-aussenministeriums [Accessed 19 August 2020].

from a specific location on the territory of another state, state responsibility should arise on the basis that that other State violated its due diligence obligation.[21] Here, it must be highlighted that the state can merely be held responsible for acting negligently, not for the initial malicious cyber operation itself.[22]

The *"due diligence principle"* was most famously referred to in the *Corfu Channel* judgment of the ICJ, which notes that it is

> *"every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States"*.[23]

Therefore, this means that states cannot escape international responsibility by merely noting that they did not do it if they knew that malicious conduct was exercised through some (non-state or foreign state) actor on their territory. They can thus at least be held responsible for knowing about the malicious conduct and not taking appropriate action to counter it.

Some scholars suggest that this principle constitutes a general principle of (international) law,[24] which also applies to cyber activities.[25] Both *Tallinn Manuals*[26] have included a due diligence rule similar to the *Corfu Channel dictum*.[27] Along the same lines, *Recommendation 13(c) of the 2015 Report of the United Nations Group of Governmental Experts on Developments*

---

[21] Cf. Henriksen, A. (2015) Lawful State Responses to Low-Level Cyber-Attacks. *Nordic Journal of International Law*, 84 (2), p. 335; we have not seen Austria claim a violation of "due diligence" (yet).

[22] There is a suggestion in the literature, however, that a state should be held responsible for the initial act if it acted negligently, see, *inter alia*, Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International & Comparative Law Quarterly*, 67, p. 643. There is no basis in international law, however, which would support such an argument.

[23] Judgment of 9 April 1949, *Corfu Channel (United Kingdom v. Albania)* (Merits), ICJ Reports 4, p. 22; The due diligence principle is said to have its origins in the Island of Palmas Arbitration, which notes the following: *"Territorial sovereignty* […] *involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war"*, see Award of 4 April 1928, *Island of Palmas Case (Netherlands v. United States of America)*, Reports of International Arbitral Awards, United Nations, Vol. II, p. 839.

[24] See Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, pp. 23, 27; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 30; Koivurova, T. (2010) Due Diligence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 2 (*Bannelier-Christakis* and the *Tallinn Manual 2.0* call it a general principle of international law, *Koivurova* calls it a general principe of law).

[25] Schmitt, M. N. (2015) In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum*, 125, p. 68; Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 27; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 31.

in the Field of Information and Telecommunications in the Context of International Security (hereinafter referred to as *UNGGE*)[28] notes that

> *"States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs [Information and Communication Technologies]"*.[29]

This is significant, as the report reflects the opinion of governmental – and thus states' – experts on the application of international law to cyberspace. It is important to note, however, that the reference in the report is merely framed as a non-binding recommendation.[30] This suggests that it is far from clear that this principle is a stand-alone principle inducing obligations on states "in its own right" in the cyber context.[31] Austria has made it clear that it perceives the due diligence obligation to be *"a legally binding obligation under international law"*.[32] Given that we seek to shine light

---

[26] Both *Tallinn Manual 1.0* and *2.0* provide guidance for policy advisors and governmental legal experts on how international law applies to cyberspace. They contain cyber specific rules, which were agreed upon by an international group of experts and have been written under the auspices of the *NATO Cooperative Cyber Defence Centre of Excellence*.

[27] Schmitt, M. N. (ed.). (2013) *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, p. 26, Rule 5, stipulates that *"*[a] *State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States"*; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 30, Rule 6, stipulates that *"*[a] *State must exercise due diligence in not allowing its territory, or territory or cyber infra-structure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States"*.

[28] The UNGGE is a group of governmental experts tasked with, *inter alia*, identifying how international law applies in cyberspace. It convened 5 times since 2004 and is currently convening for the 6th time until 2021.

[29] United Nations General Assembly. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN GAOR 70th Session, Item 93, UN Doc A/70/174. New York: United Nations, p. 8, paragraph 13(c). [online] Available from: https://undocs.org/A/70/174 [Accessed 20 August 2020].

[30] United Nations General Assembly. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN GAOR 70th Session, Item 93, UN Doc A/70/174. New York: United Nations, p. 8, paragraph 13.

[31] The Netherlands, e.g. *"regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act"*, but they also acknowledge that not all states share this view; see Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 4. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020].

[32] Government of Austria. (2020) *Austrian Statement on Rules, Norms and Principles for Responsible State Behaviour*, p. 2 (delivered on 17 June at the Informal OEWG June Consultations).

on Austria's perspective and also because we are convinced that this is the right decision, we will follow this assumption.

Next to that, there are a couple of other questions regarding the application of this principle to cyber operations:

Firstly, as the due diligence principle is an obligation of conduct, not result,[33] the content of the obligation needs to be assessed on a case-by-case basis.[34] For example, there seem to be differing views whether this obligation also contains an obligation to prevent.[35] While the *Tallinn Manual 2.0* notes that its experts agreed that

> *"the due diligence principle does not encompass an obligation to take material preventive steps"*,[36]

other scholars disagree. *Bannelier-Christakis*, for example, notes that the due diligence principle indeed also encompasses a duty of prevention.[37] Thus, it is not clear what kind of obligations are expected in the cyber context from each state in a given case.[38]

Secondly, questions remain regarding the knowledge requirement of the due diligence principle. On the one hand, how can an injured state prove that a state had knowledge about a specific cyber operation? It could be argued that as that latter state exercises exclusive control over its territory, it will be almost impossible for the injured state to establish enough evidence that that state knew about the situation.[39] On the other hand, does "constructive knowledge" (i.e. the state *should* have known

---

[33] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 26; Koivurova, T. (2010) Due Diligence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 8; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 49.

[34] See Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58, p. 116: *"*[D]*ue diligence is a standard of care, a general clause, not a specific rule to be immediately applied; it requires a judgement of value of what could and should have reasonably be done under the circumstances* [… It] *is a relative and circumstantial term, since the judgement on it must take account of all the circumstances of the particular case; judgment thus always takes place in concreto; the judgment is also necessarily flexible"*.

[35] See Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 32; Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58, p. 123; on the other hand, denying a duty of prevention, see Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 32.

[36] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 32, paragraph 5.

[37] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, pp. 23, 30.

about the situation) suffice in order to claim a violation of the due diligence principle? Here, again, there seem to be diverging views.[40]

While Austria seems convinced of the principle's binding nature, it has not (yet) clarified its view on the specific questions raised above. It has, however, endorsed South Korea's proposal on the implementation of *Recommendation 13(c) of the 2015 GGE Report* in its statement in June 2020 at informal consultations of the OEWG, noting that

> *"a state which has been notified by another state about an ICT incident on its territory and has thus knowledge about it must take all reasonable steps to cease the incident and mitigate its adverse consequences for other states."*[41]

To conclude, the due diligence principle appears to be a useful tool to establish responsibility for those acts which occurred on a state's territory and of whose harmful nature the state knew about. Austria itself has not made use of this principle for the January 2020 incident. However, if a state succeeds in establishing the responsibility of another state for a malicious

---

[38] France, the Netherlands and Estonia advocate a "reasonability test", but do not specify what can be seen as "reasonable" and what not; see Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 10. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020]; Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 4. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020]; Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020].

[39] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 29, who terms this a "probatio diabolica".

[40] See e.g. Schmitt, M. N. (ed.). (2013) *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, p. 28, paragraph 11: *"The International Group of Experts could not achieve consensus as whether this rule applies if the respective State has only constructive ('should have known') knowledge"*; see, however, Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 41, which says that *"*[t]*he International Group of Experts agreed that knowledge encompasses constructive knowledge for the purposes of this Rule"*; see also Bannelier-Christakis, K. (2014) Cyber Diligence: A Low--Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, pp. 29f, arguing in favour of the "constructive knowledge" theory; see also Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58, pp. 123–124.

[41] Government of Austria. (2020) *Austrian Statement on Rules, Norms and Principles for Responsible State Behaviour*, p. 2 (delivered on 17 June at the Informal OEWG June Consultations).

cyber operation – be it through attributing the wrongful conduct directly to the state or through proving the state's violation of the due diligence principle, the question now is how the targeted state can react to it. As explained above, international law allows specific measures.

In principle, in the case of countermeasures and measures taken in self-defence the targeted State must know *who* is the perpetrator of the wrongful act (note, that in case of a violation of the due diligence principle, the wrongfulness relates to the state acting in negligence, and not in committing the wrongful act itself).

Thus, we will first start with addressing countermeasures (as the least "intervention-intensive" measure), followed by self-defense and end with the measure for which attribution to a state is not necessary: the exceptional plea of necessity.

3. HACKBACK AS A COUNTERMEASURE

A state may take a countermeasure against a state who has committed an internationally wrongful act, in order to induce the state to comply with its international obligations.[42] These countermeasures would be, in general, unlawful, if they were not undertaken as a reactive measure to the initial wrongful act.[43] Thus, in order to take a countermeasure, the initial act must be in violation of international law.

Countermeasures need to be distinguished from retorsions: Retorsions are lawful, but unfriendly acts, whereas countermeasures are unlawful acts,

[42] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. Article 49. [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[43] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 128 (Commentary to Part Three, Chapter II, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020]; note that if a state wrongfully assumes that, let's say, state A was behind an operation and takes a counter-measure against state A, but it turns out that state B was actually behind the act, the injured state has committed an internationally wrongful act whose wrongfulness would not be precluded; see UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 130 (Commentary to Article 49, paragraph 3). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

whose unlawfulness is, however, precluded if they are a reaction to another violation of international law.[44]

In the context of hackbacks, three violations are of particular interest: 1) the violation of the prohibition to use force, 2) the violation of the prohibition of intervention and 3) the violation of the rule of sovereignty [in case one assumes that this is a stand-alone rule of international law applicable in cyberspace.[45] Austria has made it clear in its speech on international law at the February session of the so-called *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (hereinafter referred to as *OEWG*) that it believes that it is a rule, and not merely a principle, and also suggested that the cyber operation against the *Foreign Ministry* might be a violation of sovereignty[46]]. Other works have dealt with these questions in detail, thus the focus of this paper is on the reactions to the *violation* of these primary obligations.[47]

There are certain procedural and substantive conditions that need to be fulfilled in order for a state to be entitled to undertake a countermeasure. First and foremost, if we follow the traditional view on countermeasures as stipulated by the ILC Articles, they are "non-forcible"[48], meaning that any countermeasure must not cross the threshold of use of force.[49] Within

---

[44] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 128 (Commentary to Part Three, Chapter II, paragraph 3). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[45] To the contrary see the speech by UK Attorney General *Jeremy Wright*, noting that there is no principle of sovereignty in cyberspace. Wright, J. (2018) *Cyber and International Law in the 21st Century*. London. [online] Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 20 August 2020].

[46] See Government of Austria. (2020) *OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security: Statement by Austria on International Law*. New York, p. 1 (delivered on 11 February at the second substantive session of the OEWG).

[47] See e.g. Roscini, M. (2014) *Cyber Operations and the Use of Force*. Oxford: Oxford University Press; Brunner, I., Dobric, M. and Pirker, V. (2019) Proving a State's Involvement in a Cyber--Attack: Evidentiary Standards Before the ICJ. *Finnish Yearbook of International Law*, 25; Schmitt, M. (2014) "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 54.

[48] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 129 (Commentary to Part Three, Chapter II, paragraph 6). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[49] See op. cit., Article 50(1)(a): *"Countermeasures shall not affect: (a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations"*; additionally, countermeasures must also not violate fundamental human rights obligations of the state, see op. cit., Article 50(1)(b).

the literature different approaches exist on how to determine what measures can be considered "forcible" and are therefore prohibited by Article 2(4) UN Charter.[50] A very reasonable approach by *Dinniss* is to assess whether the act in question resulted in a "physical consequence" – hence, in *"destruction of physical property, injury or loss of lives"*.[51] In that case, the act is to be considered a use of force. *Schmitt* also includes a *"serious loss of functionality"*,[52] which is helpful in case a massive amount of data is deleted and can only be recovered with great difficulty and immense technical skill. Otherwise, or when the

> *"physical results are too minimal or too removed from the chain of causation"*,

it cannot be presumed that Article 2(4) UN Charter is violated.[53] If a state were thus to defend itself against DDoS attacks without causing any physical consequences against the wrongful state (such as by blocking IP addresses from which the attacks are held to originate) this will not constitute a use of force.

The *Tallinn Manual 2.0*, on the other hand, viewed the limitation not to use force when responding with a countermeasure a "contentious issue" and thus decided not to address this limitation in a Rule.[54] Given the explicit wording of the ILC Articles, the note in the ILC Articles' Commentary that the obligation to refrain from the threat or use of force when taking countermeasures is "sacrosanct",[55] and the lack of state practice[56] in favour to digress from this obligation, we stick to the ILC Articles' assessment

---

[50] See Shackelford, S. J., and Andres, R. B. (2011) State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, 42, p. 993.

[51] Dinniss, H. (2014) *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, p. 74.

[52] Schmitt, M. (2020) *Cyber Operations Against Vaccine R & D: Key International Law Prohibitions and Obligations*. [blog entry] 10 August. EJIL:Talk!. Available from: www.ejiltalk.org/cyber-operations-against-vaccine-r-d-key-international-law-prohibitions-and-obligations/ [Accessed 20 August 2020].

[53] Dinniss, H. (2014) *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, p. 74.

[54] See Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 125.

[55] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 131 (Commentary to Article 50, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

rather than the *Tallinn Manual's*. Moreover, the ICJ explicitly noted in its *Nicaragua* judgment, that

> *"a use of force of a lesser degree of gravity* [as an armed attack] *cannot* […] *produce any entitlement to take* [collective] *countermeasures involving the use of force."*[57]

Admittedly, however, the opinion that forcible countermeasures are lawful was only shared by the minority of the experts of the *Tallinn Manual*.[58]

Second, Article 52(1)(b) ILC Articles foresees a notification requirement of the injured state to the responsible state that it decides to take countermeasures and a requirement to offer negotiations with the latter state.[59] In case of urgent countermeasures, however, there is no such requirement according to Article 52(2) ILC Articles.[60] The question is what constitutes *urgency* in that context. France seems to interpret *urgency* quite broadly, arguing that urgent countermeasures may be taken whenever

> *"there is a need to protect* [the victim state's] *rights"*.[61]

---

[56] Rather to the contrary, see Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 8. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020]; Wright, J. (2018) *Cyber and International Law in the 21st Century*. London. [online] Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 20 August 2020]; Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020]; Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 7. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020].

[57] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)* (Merits), ICJ Reports 14, p. 117, paragraph 249; UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 132 (Commentary to Article 50, paragraph 5). [online] Available from: https://legal.un.org/ilc/texts/instrument/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[58] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 125–126, paragraph 12.

[59] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. Article 52(1)(b). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[60] Op. cit., Article 52(2) notes: *"Notwithstanding paragraph 1 (b), the injured State may take such urgent countermeasures as are necessary to preserve its rights."*

The *Tallinn Manual 2.0* notes that

> *"if notification of intent to take a countermeasure would likely render that measure meaningless"*

there is also no requirement to notify. The Group of Experts argued that such a case, despite not being urgent *per se*, would be analogous to urgent countermeasures.[62] Also, the majority of experts rejected the existence of a requirement to offer negotiation before conducting the countermeasure.[63]

Another important aspect to bear in mind is the proportionality requirement as stipulated in Article 51 ILC Articles. It poses an "essential limit" for states wishing to react to an internationally wrongful act through countermeasures.[64] The proportionality requirement is particularly important to consider when a victim state is taking countermeasures against a state which has violated its due diligence obligation but did not itself commit the internationally wrongful act (concerning the debate whether the due diligence principle poses a legal obligation on states, see above). Article 51 ILC Articles clearly stipulates in this context that both the gravity of the act and the rights in question need to be taken into account when assessing which countermeasure would be proportionate to the act. Thus, the way a state is able to react to the violation of a state's obligation to act with due diligence obviously differs compared to a state's reaction to a violation of e.g. the prohibition of the use of force or intervention.

Closely linked to the proportionality requirement is the view of the legality of *collective* countermeasures. Estonia has recently voiced its opinion that it believes that states may also take such *collective*

---

[61] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 8. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

[62] See Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 120, para. 12.

[63] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 120–121, para. 13.

[64] Cf. UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 134 (Commentary to Article 51, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

countermeasures[65] – something the ILC Articles have left open to debate. France, to the contrary, notes that

> *"*[c]*ollective countermeasures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's rights."*[66]

The passage of the *Nicaragua* judgment cited above on the illegality of collective countermeasures involving the use of force may also point in a similar direction.[67] One could, however, interpret this statement as only relating to the question of use of force, while leaving the legality of collective countermeasures below the threshold of force unanswered. It also cannot be ruled out that states may agree on a new cyber-related rule which might allow collective countermeasures solely in the cyber context.

According to a statement made at the second substantive session of the OEWG in February 2020, Austria believes that the "severe cyber operation" targeting the country violated the rule of sovereignty and that a *"state may seek reparation under the law of state responsibility"* – if the act is attributable to a state.[68] Austria also noted that a

> *"target state may* […] *react through proportionate countermeasures"*.[69]

External sources revealed that a team of hackers managed to end the attacks within the IT system of the *Foreign Ministry* by putting the offending group in the "defensive".[70] Luckily, the hacking group only managed to get into the mail server and not into the intranet of the *Ministry*, making it easier

---

[65] Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020].

[66] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 7. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

[67] Cf. Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v. United States of America*) (Merits), ICJ Reports 14, para. 249.

[68] Government of Austria. (2020) *OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security: Statement by Austria on International Law*. New York, p. 1 (delivered on 11 February at the second substantive session of the OEWG).

[69] Ibid.

[70] Moechel, E. (2020) *Cyberhusarenstück Schlug Angreifer im Außenministerium.* [blog entry] 23 February. Radio FM4. Available from: https://fm4.orf.at/stories/2999042/ [Accessed 20 August 2020].

to kick the offenders out of the system.[71] Unfortunately, there is no further information as Austrian institutions declined to comment.[72] Based on the existing information, however, it can be assumed that the defence against the hacking group stayed below the use of force. It also seemed proportional and aimed at ceasing the initial wrongful conduct. There is, unfortunately, no information, whether the defenders had to intrude into the networks of another state or whether the defence stayed within the Austrian IT systems. If the latter case is true, the "hackback" by Austrian technicians could even have been a lawful retorsion and it could be assumed that Austria would have been capable to even go further than what it did.

To conclude, it is safe to say that there currently is an active debate about what states are allowed and not allowed to do when undertaking a "hackback" in the form of a countermeasure. But not only are there open questions with respect to countermeasures – also the traditional views on the right to self-defence raises new questions in the cyber context (even though the possibility to react in self-defence is very limited). Therefore, hackback as self-defence will be addressed in the next chapter.

4. HACKBACK AS SELF-DEFENCE

A "hackback" could also be a lawful exercise of the right of self-defence. The right of self-defence is enshrined in Article 51 UN Charter and states the following:

> *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security".*

This means that a lawful exercise of the right of self-defence must meet the following conditions:[73]

1. it must be a response to an armed attack;
2. the use of force, and the degree of force used, must be necessary and proportionate; and

[71] Ibid.

[72] Ibid.

[73] See Greenwood, C. (2011) Self-Defence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 8.

3. it must be reported to the *Security Council* and must cease when the *Security Council* has taken *"measures necessary to maintain international peace and security"*.

Another precondition that is, according to the present authors, implied is that of attribution to a state:[74] If a cyber operation reaches the threshold of an armed attack, the present authors argue that under current international law it would also be necessary to attribute the attack to a state in order to exercise the right to self-defence. While the ICJ has repeatedly found that only acts attributable to a state can constitute an armed attack, this view has been questioned by some scholars.[75] *Zemanek*, for example, argues that the ICJ would disregard resolutions adopted by the *Security Council* after the terrorist attacks of "9/11", especially resolutions *1368 (2001)* and *1373 (2001)*. According to *Zemanek*, these resolutions would implicitly recognize the terrorist attack as an "armed attack" in the sense of Article 51 UN Charter.[76]

However, the ICJ has since reiterated its position and stated that

> *"Article 51 of the Charter* […] *recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State"*.[77]

In addition, the notion to extend the right to self-defence against non-state actors has been criticized within the literature.[78]

---

[74] See section 2.

[75] See Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 15; Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17, p. 241.

[76] Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 15; Judgment of 19 December 2005, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Separate Opinion Judge Simma), ICJ Reports 334, paragraph 11.

[77] Advisory Opinion of 9 July 2004, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ Reports 136, paragraph 139; see also Judgment of 19 December 2005, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Merits), ICJ Reports 168, paragraphs 146, 160.

[78] Gray, C. (2018) *International Law and the Use of Force*. 4th edition. Oxford: Oxford University Press, p. 210; Vidmar, J. (2017) The Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111, p. 302; see also Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 8. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020]; see, however, Murphy, S. D. (2005) Self-Defense and the Israeli Wall Advisory Opinion: An Ipse Dixit from the ICJ?. *American Journal of International Law*, 99 (1).

As *Gray*, for example, points out, even if self-defence against non-state actors was permissible, it would still not allow a state to infringe the host state's rights.[79]

An armed attack constitutes a "use of force" within the meaning of Article 2(4) UN Charter. The ICJ stated in the *Nicaragua* case that "armed attacks" have to be distinguished as

> *"the most grave forms of the use of force from other less grave forms"*.[80]

Self-defence is permissible only in response to such armed attacks. The ICJ's original emphasis on differentiating an armed attack from a "mere frontier incident" has also been criticized in the literature.[81] However, the ICJ has since clarified that a single attack can also constitute an armed attack.[82] Nevertheless, it is obvious that not every use of force automatically justifies actions of self-defence.[83] To determine whether a use of force amounts to an armed attack, the ICJ considers the "scale and effects" of an attack.[84] The type of weapon used to reach the threshold of an attack is irrelevant: "armed attack" in the sense of Article 51 includes both kinetic and "cyber"weapons.[85]

According to *Constantinou*,

> "[an] *armed attack implies an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (ie scale) which have as their consequence (ie effects) the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental*

---

[79] See Gray, C. (2018) *International Law and the Use of Force*. 4th edition. Oxford: Oxford University Press, p. 210, with further references.

[80] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America*) (Merits), ICJ Reports 14.

[81] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 341.

[82] Judgment of 6 November 2003, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*) (Merits), ICJ Reports 161, paragraphs 57, 61; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 342.

[83] Greenwood, C. (2011) Self-Defence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 12; Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 7.

[84] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America*) (Merits), ICJ Reports 14, para. 195.

[85] Woltag, J. (2015) Cyber Warfare. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraphs 8f.

> *authority, ie its political independence, as well as damage to or deprivation of its physical element namely, its territory".*[86]

While this definition (or other similar ones) could just as well be applied to cyber operations, the *Tallinn Group of Experts* could agree only to a very basic outline. According to them,

> *"a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement"*,

whereas

> *"acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks".*[87]

The *Tallinn Group of Experts* could, however, not agree on whether cyber operations can be considered "armed attacks" if they do not result in injury, death, damage, or destruction, but nonetheless have extensive negative effects.[88] It is generally difficult to determine the scale and effects of cyber operations, since cyber attacks do not always manifest in the "analogous" world and if they do, they only have an "indirect" impact.[89]

In view of the immense harm that a failure of "critical infrastructure" could potentially have, some focus on whether the target of the attack can be qualified as such, in order to assess whether an armed attack has occurred.[90] However, this is problematic for two reasons. First, there is no uniform definition of "critical infrastructure" and different understandings exist within each national legal framework. Second, the two concepts

---

[86] Constantinou, A. (2000) *The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter*. Ant. N. Sakkoulas, p. 64; Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law*. (online edition), paragraph 9.

[87] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 341.

[88] Op. cit., p. 342.

[89] Woltag, J. (2015) Cyber Warfare. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 13.

[90] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberspace*. Paris. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

of "critical infrastructure" and "armed attack" do not entirely correlate. The former issue could be solved in the near future. There are efforts within the European Union, for example, to harmonize the concept of critical infrastructure and measures that have to be taken to ensure their security. In this regard *Council Directive 2008/114/EC*[91] and the *Directive on Security of Network and Information Systems (NIS Directive)*[92] should be mentioned.

Council Directive 2008/114/EC defines critical infrastructure as

> *"an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"*.[93]

This means that whether certain infrastructure can be considered "critical", depends on the individual circumstances of each Member State.

The NIS Directive especially concerns network security for "operators of essential services" and "digital service providers". Essential services are therein determined within specific economic sectors (e.g. energy, transport, health) as being essential for the maintenance of "critical societal and/or economic activities" and that an incident would have *"significant disruptive effects on the provision of that service"*.[94] In Austria, the NIS Directive has been implemented by the NIS Act.[95]

Regarding the latter issue (namely the fact that the two concepts of "armed attack" and "critical infrastructure" do not correlate): There are possible scenarios where a critical infrastructure is targeted, but where

---

[91] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union* (2008/L-345/75), 23 December.

[92] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. *Official Journal of the European Union* (2016/L-194/01) 19 July.

[93] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union* (2008/L-345/75), 23 December. Article 2(a).

[94] Article 5(2) Directive 2016/1148/EU also requires the service to depend on network and informations systems, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. *Official Journal of the European Union* (2016/L-194/01), 19 July.

[95] Federal Act on Ensuring a High Level of Security of Network and Information Systems 2018 (*Netz- und Informationssystemsicherheitsgesetz – NISG*) Austrian Federal Law Gazette I No. 111/2018.

the operation is not severe enough as to reach the scale and effects of an armed attack. On the other hand, a cyber attack that leads to the destruction of e.g. an apartment building (which does not constitute "critical infrastructure") could be considered to reach the threshold of an armed attack. This means that the use of the terms "critical infrastructure" or "essential service provider" could be more confusing than helpful in determining whether an armed attack has occurred.

Having said this, given the reportedly low scale and effect of the operation against the *Austrian Foreign Ministry* in January 2020, it can be ruled out that such a cyber operation amounted to an armed attack, even if the *Ministry* decided to classify such as a use of force and even though it falls within the scope of the NIS Act. It can, however, not be ruled out that a future attack could reach the threshold of an armed attack, especially if the cyber operation was aimed at destroying infrastructure or causing ("considerable") damage. In that case, it might be easier to argue for a right of self-defence if critical infrastructure, such as the *Austrian Foreign Ministry*, was the target.

We can therefore conclude that the cyber operation against the *Austrian Foreign Ministry* did not entitle Austria to "hackback" with a forceful strike in self-defence, as only "the most grave forms of the use of force"[96] are qualified as armed attacks. Even if – for some reason – it did, the attack would, in accordance with the ICJ case law, have to be attributed to a state in order to take measures of self-defence against the attacker without consent of the host state.

5. HACKBACK BASED ON THE PLEA OF NECESSITY

States may rely on the plea of necessity during a hackback, which is quite different from the other legal bases mentioned before (countermeasure, self--defence). The plea of necessity, as set forth in Article 25 of the ILC Articles, is not dependent on the prior conduct of the injured state.[97] In the authors' opinion, the most important difference to the two legal bases mentioned

[96] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America*) (Merits), ICJ Reports 14.

[97] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 80 (Commentary to Article 25, paragraph 2). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020]: the "injured state" being the state against which measures on the basis of necessity are taken.

above is that no attribution to a state is required.[98] It "merely" suffices that the danger emanates from that state's territory. This section will elaborate on the extent to which a plea of necessity allows a hackback.

For a state to be able to invoke necessity, the conditions – narrowly defined in Article 25[99] – must be met. These are (1) the grave danger either to the essential interests of the state or of the international community as a whole and (2) that the conduct in question does not seriously impair an essential interest of the state or states towards which the obligation exists, or of the international community as a whole.[100]

Even if these conditions are met, necessity may not be invoked by a state as a ground for precluding wrongfulness if (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the State has contributed to the situation of necessity.[101]

In the Commentary to the ILC Articles, the ILC cited various decisions and cases in which the plea of necessity was put forward (or its existence at least not denied) as justification for the fact that the plea of necessity is part of the applicable customary international law (*lex lata*).[102] Even though critical voices in the literature have argued that Article 25 of the ILC Articles should have been seen to be merely an aid to orientation and should not have been adopted verbatim,[103] it cannot be denied that the concept of necessity exists in customary international law. On the other hand, it is

---

[98] Ibid. See also Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 25, paragraph 10; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1621; note, as already highlighted above, that some scholars argue that attribution is also not required for the exercise of self-defence.

[99] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 80 (Commentary to Article 25, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[100] Op. cit., Article 25(1); on necessity and its applicability in a cyber context see also: Vidmar, J. (2017) The Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111, p. 302; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1619; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26.

[101] Op. cit., Article 25(2).

[102] Op. cit. pp. 80ff (Commentary to Article 25, paragraphs 3ff).

[103] Sloane, R. D. (2012) On the Use and Abuse of Necessity in the Law of State Responsibility. *American Journal of International Law*, 106 (3), p. 447; see also Schaller, C. (2017) Beyond Self--Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1630 [questioning state practice regarding the requirement *"that the action must not seriously impair the essential interests of other States"*].

also apparent that the precise nature and scope of the plea of necessity remain controversial.[104]

What amounts to an "essential interest" is not unilaterally defined and therefore vague.[105] According to the ILC, the extent to which a given interest is "essential" depends on all the circumstances and therefore cannot be prejudged. It extends to particular interests of the state and its people, as well as of the international community as a whole.[106]

As has been elaborated in the context of self-defence (see above), the designation of certain parts of a state's infrastructure as "critical infrastructure" might be suggestive of their characterisation of an interest as essential, but not determinative.[107] *Schaller* argues that an essential interest within the meaning of Article 25 and Rule 26 of the *Tallinn Manual* should not be narrowed down solely to the concept of critical infrastructure.[108] As the *Tallinn Group of Experts* agreed, an essential interest

> *"is most clearly implicated when critical infrastructure is targeted in a manner that may have a severe negative impact on a state's security, economy, public health, safety, or environment"*.[109]

Similar to the determination whether a cyber operation reaches the threshold of an armed attack, the involvement of critical infrastructure can be an indicative but not a decisive factor in determining if essential interests are in danger.

---

[104] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 13). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020]; Schaller, C. (2017) Beyond Self--Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1636 [who promotes a necessity regime for cyber incidents, because the *"contours of the concept of necessity as applied in the cyber context are not yet sufficiently clear to dispel concerns* [of their abuse]*"*].

[105] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 2.

[106] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 15). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[107] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 2.

[108] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1632.

[109] Schmitt, M. and Vihul, L. (eds.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 5.

Similar to self-defence, however, focusing on the term "critical infrastructure" could lead to some confusion (see above). Particularly with regard to necessity, one has to be aware of circular reasoning. Since critical infrastructure is defined as concerning vital or essential interests of the state and/or the public and that damage of this infrastructure could seriously harm these interests, one cannot argue that there is a state of necessity just on the basis that a cyber operation is targeting critical infrastructure.

The examples given in the *Tallinn Manual* illustrate (according to most of the experts) situations in which essential interests are gravely and imminently threatened. Such situations would include

> *"a cyber-operation that would debilitate the State's banking system, cause a dramatic loss of confidence in its stock market, ground flights nation-wide, halt all rail traffic, stop national pension and other social benefits, alter national health records in a manner endangering the health of the population, cause a major environmental disaster, shut down a large electrical grid, seriously disrupt the national food distribution network, or shut down the integrated air defence system would provide the basis for the application of this rule"*.[110]

To invoke the plea of necessity, such essential interests of a State must face a grave and imminent peril. A peril can, in accordance with the expert group of the *Tallinn Manual*, be seen as "grave", when the threat is especially severe, if the interest is interfered with in a fundamental way, like destroying the interest or rendering it largely dysfunctional.[111]

With regard to the "imminence" of such peril, the Commentary to the ILC Articles states that such imminence must be

> *"objectively established and not merely apprehended as possible"*,[112]

and the decision that measures must be taken must be

---

[110] Ibid.

[111] Op. cit., Article 25, paragraph 4.

[112] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 15). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

> *"clearly established on the basis of the evidence reasonably available at the time".*[113]

It should not be understood solely as a temporal issue.

The *Tallinn Group of Experts* agreed that peril should always be imminent when the "last window of opportunity" to take action to prevent it is about to close.[114] The last window of opportunity is familiar from the debate surrounding the right to anticipatory self-defence.[115] There, it is argued that

> *"restrictive approaches to imminency run counter to the purposes animating the right of self-defence"*[116]

and that

> *"the correct standard for evaluating a preemptive operation must be whether or not it occurred during the last possible window of opportunity in the face of an attack that was almost certainly going to occur".*[117]

One has to keep in mind that this last window of opportunity standard would generally provide States with considerable leeway for action whether invoking the right to self-defence or the plea of necessity.[118] From its meaning, the "last window of opportunity" standard should rather be applied to test whether a certain measure is "the only way" to protect essential interests from a grave and imminent peril, than to test if that peril is "imminent".

In conclusion, reacting based on necessity remains an exceptional measure.[119] Therefore, the wrongfulness of measures can only be precluded on the basis of necessity, if they are – based on reasonable certainty[120] – the only way for a state to safeguard essential interests from a grave and imminent danger. When determining essential interests, states will most

---

[113] Op. cit., p. 83 (Commentary to Article 25, paragraph 16).

[114] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 139.

[115] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1635.

[116] Schmitt, M. N. (2003) Preemptive Strategies in International Law. *Michigan Journal of International Law*, 24 (2), p. 534; see also references in Schaller, C. (2017) Beyond Self--Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, pp. 1619, 1635 (fn. 115).

[117] Schmitt, M. N. (2003) Preemptive Strategies in International Law. *Michigan Journal of International Law*, 24 (2), p. 535.

[118] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1635.

likely resort to their definition of critical infrastructure, although it should be kept in mind that necessity is not restricted to critical infrastructure. In addition, the main focus should be to determine 1) if it is a "grave peril" that threatens essential interests and 2) if other measures (e.g. [cyber] diplomacy) that do not affect the rights of other states could be taken (arg. "the only way"). The present authors argue, however, that if a peril to an essential interest is imminent, there might be a lower standard with regard to what is reasonable to expect on the "gravity" of the attack if the window of opportunity is about to close (e.g. in the moment before a malware is inserted to or data is extracted from a critical system).

So even though the recent cyber operation was directed against the *Austrian Foreign Ministry* (and therefore, arguably, against a critical infrastructure) it would not allow Austria to react out of necessity. Only if essential interests (like water supply, power supply or general matters of internal security) are threatened in a way that would render them largely dysfunctional would it be permissible to invoke necessity. Therefore, not every cyber operation against networks of critical infrastructure allows for measures taken in necessity, but only those attacks that also threaten the essential interest that such infrastructure is "critical" to maintain. In other words: This exceptional rule should rather apply in cases like an imminent power outage ("black-out") or other events with grave consequences that similarly effect essential interests of the state and/or the population.

6. CONCLUSION

This contribution has demonstrated that international law allows certain ways to react to malicious cyber operations. States can either react through

[119] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 17; UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 80 (Commentary to Article 25, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[120] Schmitt, M. and Vihul, L. (eds.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 14; UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 16). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

countermeasures, self-defence or out of necessity. The purpose of this contribution was to elaborate on these three ways in more detail.

Austrian news reports and press releases suggest that the cyber operation against the *Austrian Foreign Ministry* did not cause major damage. Thus, it most likely cannot be classified as a use of force according to Article 2(4) UN Charter, but it might be severe enough to constitute a violation of Austria's sovereignty. Austria has remained silent as to the territorial origins of the operation. However, in case the whereabouts are known, it could also be argued that the host state, from which the operation originated – acted in violation of the due diligence principle. In these cases, Austria would be permitted to take countermeasures against the state to which the wrongful conduct (in the former instance) or the negligence (in the latter instance) could be attributed. Such countermeasures could be any type of activity aimed at ceasing the wrongful conduct, as long as it does not amount to force and is necessary and proportionate.

Given the low-level nature of the cyber operation, the possibility to act in self-defence or out of necessity seems out of question. However, it cannot be ruled out that Austria (or any other state) may be able to rely on these measures in case it will be the target of a more severe cyber operation in the future.

To conclude, even when applying a more "traditional" approach by applying existing customary international law as expressed in the ILC Articles and by ICJ case law, many questions as to what the concrete response options are, remain. These questions will likely only be solved if more states come forward with their national views about how international law applies to cyber operations. With its press releases and statements at UN level, Austria finally entered this discussion. There is no doubt that the cyber operation against the *Foreign Ministry* has acted as a stimulus for this debate.

LIST OF REFERENCES

[1] Advisory Opinion of 9 July 2004. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory.* ICJ Reports 2004, 136.

[2] Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Nicholas Tsagourias and Russell Buchan (eds.). *Research Handbook on International Law and Cyberspace.* Cheltenham and Northampton: Edward Elgar Publishing.

[3] Austrian Federal Ministry for European and International Affairs. (2020) *Cyber Attack on the Foreign Ministry is Over.* [press release] 13 February. Available from: www.bmeia.gv.at/en/the-ministry/press/announcements/2020/02/cyber-attack-on-the-foreign-ministry-is-over/ [Accessed 19 August 2020].

[4] Austrian Press Agency. (2020) *Schwerwiegender Angriff auf IT-Systeme des Außenministeriums.* [press release] 4 January. Available from: https://www.ots.at/presseaussendung/OTS_20200104_OTS0020/schwerwiegender-angriff-auf-it-systeme-des-aussenministeriums [Accessed 19 August 2020].

[5] Award of 4 April 1928. *Island of Palmas Case (Netherlands v. United States of America).* Reports of International Arbitral Awards, United Nations, Vol. II.

[6] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14.

[7] Brunner, I., Dobric, M. and Pirker, V. (2019) Proving a State's Involvement in a Cyber--Attack: Evidentiary Standards Before the ICJ. *Finnish Yearbook of International Law*, 25.

[8] Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945 (1 UNTS XVI).

[9] Clark, D. D. and Landau, S. (2011) Untangling Attribution. *Harvard National Security Journal*, 2.

[10] Constantinou, A. (2000) *The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter*. Ant. N. Sakkoulas.

[11] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union* (2008/L-345/75), 23 December.

[12] Dinniss, H. (2014) *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press.

[13] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. *Official Journal of the European Union* (2016/L-194/01) 19 July.

[14] Federal Act on Ensuring a High Level of Security of Network and Information Systems 2018 *(Netz- und Informationssystemsicherheitsgesetz – NISG)* Austrian Federal Law Gazette I No. 111/2018.

[15] Government of Austria. (2020) *Austrian Statement on Rules, Norms and Principles for Responsible State Behaviour* (delivered on 17 June at the Informal OEWG June Consultations).

[16] Government of Austria. (2020) *OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security: Statement by Austria on International Law*. New York (delivered on 11 February at the second substantive session of the OEWG).

[17] Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020].

[18] Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020].

[19] Gray, C. (2018) *International Law and the Use of Force*. 4th ed. Oxford: Oxford University Press.

[20] Greenwood, C. (2011) Self-Defence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.

[21] Guitton, C. (2017) *Inside the Enemy's Computer: Identifying Cyber-Attackers.* London: Hurst & Company.

[22] Henriksen, A. (2015) Lawful State Responses to Low-Level Cyber-Attacks. *Nordic Journal of International Law*, 84 (2).

[23] Judgment of 9 April 1949. *Corfu Channel (United Kingdom v. Albania).* ICJ Reports 1949, 4.

[24] Judgment of 27 June 1986. *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*. ICJ Reports 1989, 14.

[25] Judgment of 6 November 2003. *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America).* ICJ Reports 2003, 161.

[26] Judgment of 19 December 2005. *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda).* ICJ Reports 2005, 334.

[27] Koivurova, T. (2010) Due Diligence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.

[28] Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58.

[29] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-

engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

[30] Moechel, E. (2020) *Cyberhusarenstück Schlug Angreifer im Außenministerium*. [blog entry] 23 February. Radio FM4. Available from: https://fm4.orf.at/stories/2999042/ [Accessed 20 August 2020].

[31] Moechel. E. (2020) *Vorläufige Bilanz des Cyberangriffs auf das Außenministerium.* [blog entry] 16 February. Radio FM4. Available from: https://fm4.orf.at/stories/2998771/ [Accessed 20 August 2020].

[32] Murphy, S. D. (2005) Self-Defense and the Israeli Wall Advisory Opinion: An Ipse Dixit from the ICJ?. *American Journal of International Law*, 99 (1).

[33] Roscini, M. (2014) *Cyber Operations and the Use of Force.* Oxford: Oxford University Press.

[34] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95.

[35] Schmitt, M. (2003) Preemptive Strategies in International Law. *Michigan Journal of International Law*, 24 (2).

[36] Schmitt, M. (2014) "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law,* 54.

[37] Schmitt, M. (ed.). (2013) *The Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

[38] Schmitt, M. (2015) In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum*, 125.

[39] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

[40] Schmitt, M. (2020) *Cyber Operations Against Vaccine R & D: Key International Law Prohibitions and Obligations*. [blog entry] 10 August. EJIL:Talk!. Available from: www.ejiltalk.org/cyber-operations-against-vaccine-r-d-key-international-law-prohibitions-and-obligations/ [Accessed 20 August 2020].

[41] Shackelford, S. J., and Andres, R. B. (2011) State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, 42.

[42] Sloane, R. D. (2012) On the Use and Abuse of Necessity in the Law of State Responsibility. *American Journal of International Law,* 106 (3).

[43] Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17.

[44] United Nations General Assembly. (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN Doc A/68/98. New York: United Nations. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement [Accessed 20 August 2020].

[45] United Nations General Assembly. (2014) *Developments in the Field of Information and Telecommunications in the Context of International Security.* UN Doc A/RES/68/243. New York: United Nations. Available from: https://undocs.org/A/RES/68/243 [Accessed 20 August 2020].

[46] United Nations General Assembly. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN GAOR 70th Session, Item 93, UN Doc A/70/174. New York: United Nations. Available from: https://undocs.org/A/70/174 [Accessed 20 August 2020].

[47] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[48] Vidmar, J. (2017) The Use of Force as a Plea of Necessity. *AJIL Unbound*, 111.

[49] Woltag, J. (2015) Cyber Warfare. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.

[50] Wright, J. (2018) *Cyber and International Law in the 21st Century.* London. [online] Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 20 August 2020].

[51] Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.