ICT for peace foundation

POLICY BRIEF

SELF-DEFENCE AGAINST CYBERATTACKS?

DIGITAL AND KINETIC DEFENCE IN LIGHT OF ARTICLE 51 UN-CHARTER

Sara Pangrazzi (MLaw)

GENEVA 2021

ICT4Peace Foundation

ICT4Peace Publishing, Geneva. February 2021
Copies available from www.ict4peace.org

SELF-DEFENCE AGAINST CYBERATTACKS?

DIGITAL AND KINETIC DEFENCE IN LIGHT OF ARTICLE 51 UN-CHARTER

Sara Pangrazzi (MLaw)

ICT for peace foundation

ABSTRACT

The question on how international law applies to cyberattacks is one of the most pressing issues the international community of states faces as threats emerging from cyberattacks are growing. Basic governmental, economic, and public services as well as critical infrastructure increasingly depend on digital systems, which makes states vulnerable to such attacks. Moreover, there is a growing complexity of state and non-state actors behind cyberattacks and within hybrid constellations of conflicts. These developments pose a fundamental challenge to regulatory issues in the modern system of collective security.

This article elaborates the question of when a cyberattack constitutes an armed attack according to Article 51 UN-Charter and allows a state to enact kinetic as well as active cyber defence measures. The aim is to discuss the authors' understanding of the applicability of Article 51 UN-Charter in the cyber context and to offer recommendations with regard to active cyber and kinetic defence policy options for states from an international law perspective.

Suggested citation:

PANGRAZZI SARA, Self-Defence against Cyberattacks? Digital and Kinetic Defence in Light of Article 51 UN-Charter, Policy Brief, ICT for Peace Foundation, Geneva 2021

SELF-DEFENCE AGAINST CYBERATTACKS?

DIGITAL AND KINETIC DEFENCE IN LIGHT OF ARTICLE 51 UN-CHARTER

By Sara Pangrazzi[1]

I. INTRODUCTION

On 18 September 2020, a woman died after hackers encrypted the computers of the University Hospital of Düsseldorf. The incident is likely to be the first fatality from a ransomware attack. The hospital had to turn away emergency patients as a consequence to the ransomware attack, which froze its computer systems by invading thirty servers and thereby blocking the digital access to health data records. Consequently, a woman in a life-threatening condition had to be sent away to another hospital. She later died from treatment delays.[2] The Düsseldorf case was by far not the only cyberattack on a health care facility directly threatening the lives of people: In May 2017, the prominent "WannaCry" ransomware attack crashed the computer systems of British hospitals (among others) which forced them to cancel surgeries, and one month later, hospitals in Virginia and across Pennsylvania too had to turn away patients as a result of the "NotPetya" attack.[3] When people die from the cause of cyberattacks it is not only a matter of criminal law, it may also become a matter

1 Sara Pangrazzi (MLaw) is a Ph.D. Candidate in cybersecurity and international law at the University of Zurich. Her research focuses on the legal aspects regarding the law of self-defence as well as the regime of countermeasures with a particular focus on the principle of proportionality in both fields. Her research project is funded by the Forschungskredit Candoc of the University of Zurich. The author thanks her Ph.D. supervisor Prof. Dr. iur. Oliver Diggelmann, former Ambassadors Martin Dahinden and Daniel Stauffacher, PD Dr. sc. Markus Christen, and her collegue Salome Stevens for their review and inputs.

2 Eddy Melissa/Perlroth Nicole, Cyber Attack Suspected in German Woman's Death, The New York Times, 18 September 2020.

3 Ibid.

of national relevance and hence, of international law. How can a state react to these kinds of dangers when cyberattacks – as it often happens – are launched from or cross the territories of other states?

Today, the question on how international law applies to cyberattacks is one of the most pressing issues the international community of states faces as threats emerging from cyberattacks are growing. Basic governmental, economic, and public services as well as critical infrastructure increasingly depend on digital systems, which makes states and their civil society vulnerable to such attacks. Back in 2013[4] and 2015[5], the United Nations Group of Governmental Experts (UN GGE) confirmed that international law applies to cyberspace. Between 2016 and 2017 a further consensus on the topic failed, stopping UN deliberations in the field for almost two years.[6] Consequently, in 2019, the United Nations General Assembly established a new Group of Governmental Experts[7] and an Open-ended Working Group (OEWG)[8] with the mandate to study *how* international law applies to states' conduct in cyberspace. There still seems to be great interest in and a need to further clarify how international law applies in cyberspace.[9] One way of achieving this could be through the sharing of states'[10] as well as academic's points of view. It is hence important for scholars, and

4 UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, UN Doc. A/68/98 (hereinafter UN GGE Report 2013).

5 UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, UN Doc. A/70/174 (hereinafter UN GGE Report 2015).

6 Roguski Przemysław, Application of International Law to Cyber Operations: A Comparative Analysis of States' Views, The Hague Program For Cyber Norms Policy Brief, March 2020, p. 2.

7 UN General Assembly, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Resolution of 22 December 2018, UN Doc. A/RES/73/266.

8 UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Resolution of 5 December 2018, UN Doc. A/RES/73/27.

9 See Roguski (above n 6), p. 2.

10 See Roguski (above n 6) referring to the mandate of the 2019 UN GGE, UN General Assembly, Advancing responsible State behaviour in cyberspace in the context of international security, Resolution of 22 December 2018, UN Doc. A/RES/73/266, p. 3 which includes the sharing of opinions open to all member states and to the OEWG, Chair's working paper in view of the Second substantive session (10–14 February, 2020), p. 2 [last consulted 13.12.2020]. The third (and final) substantive session was postponed to March 2021. Many states have already commented on the initial pre-draft of the OEWG report: See United Nations Open-ended Working Group: <https://www.un.org/disarmament/open-ended-working-group/> [last consulted 13.12.2020].

even more so for states to contribute to the clarification of the applicable norms on the international stage as it is the latter's responsibility that is at question and their conduct, which ultimately needs to be in line with international law.

Although the legal framework regulating states' behavior and states' responsibilities in cyberspace is still being debated and needs further discourse, national efforts expanding their (passive and also active) military cyber capabilities are undergoing. Certain states such as the USA or the UK invest considerable resources into addressing cybersecurity issues. As part of this strategy, they created their own military cyber commands to "react" to dangers arising from cyberattacks, thereby also increasingly using offensive cyber capabilities to "disrupt adversaries".[11] Recently, on 7 October 2020 Switzerland too decided to strengthen its cyber defence by pushing forward an own cyber command which in contrast is primarily aiming at *protecting* the digital military infrastructure.[12] While such developments are undisputedly important to address the emerging risks, it is also crucial that they correlate with the underlying rules that bind states' behavior, especially if defence measures are being launched offensively by interfering into another state's infrastructure. For military purposes especially, it is hence important to clarify when (and if) *active* (kinetic and/or digital) defence measures are legitimate in light of international law. Active military measures which intervene into another state may breach international norms such as the latter's sovereignty or the global ban on the use of force according to Article 2(4) UN-Charter if they are not justified under international law. The *only* justification, under which a state, according to international public law, may offensively defend itself and intervene in another states' territory by military means, is the exceptional situation of an armed attack according to Article 51 UN-Charter giving rise to the right of self-defence. However, Article 51 UN-Charter is strictly limited by legal requirements (even if drafted in vague legal terms as remains to be explained further down in this text).

11 See Ministry of Defence et al., National Cyber Force Transforms Country's Cyber Capabilities to Protect UK, 19 November 2020: <https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk> [last consulted 13.12.2020]. These developments are happening while little is known about the Force's activity see: Sabbagh Dan, UK unveils National Cyber Force of Hackers to Target foes Digitally, The Guardian, 19 November 2020. According to Sabbagh an estimated 60 countries have so far developed offensive hacking capabilities, among others the most advanced nations Iran and North Korea. Similarly, the US: See U.S. Cyber Command Public Affairs, The Cutting Edge of Defense: <https://www.cybercom.mil/Media/News/Article/2342894/the-cutting-edge-of-defense/> [last consulted 13.12.2020].

12 Der Bundesrat, Medienmitteilung, 07.10.2020: <https://www.admin.ch/gov/de/start/dokumentation/ medienmitteilungen.msg-id-80621.html> [last consulted 13.12.2020].

Active military self-defence measures, which are not justified under Article 51 UN-Charter and which reach a certain degree of severity, may consequently themselves constitute an unlawful (armed) attack. The right of self-defence is therefore an absolute exception to the global ban on the use of force among states and can only be used reluctantly. It is part of the so-called *ius ad bellum* which in other words means "the right to war". Historically, it is intended as a states' "emergency right" to defend itself in order to secure its existence when there is not enough time to inform the Security Council and there is an "*instant and overwhelming necessity of self-defence, leaving no choice of means, and no moment for deliberation*".[13] It seems quite clear however, that states explicitly hold on to that "nothing in the UN-Charter shall impair their – according to the wording of the Charter – *inherent right* of individual or collective self-defence".[14] Therefore, even while being an absolute exception, it constitutes a significant cornerstone within the modern system of collective security, which is embedded in the UN-Charter's Chapter VII on the regulation of actions with respect to threats to the peace, breaches of the peace, and acts of aggression.

This article elaborates the important question of when a cyberattack constitutes an armed attack according to Article 51 UN-Charter and hence allows a state to enact kinetic as well as active cyber defence measures. The aim is to discuss the authors' understanding of the applicability of Article 51 UN-Charter in the cyber context and to offer recommendations with regard to active cyber and kinetic defence policy options for states. The analysis proceeds in two parts. The first part will address the traditional concept of an armed attack and apply it to the cyber context. It does so by revealing the difficulties, challenges, and dangers at hand. More concretely, it will take a closer look as to the gravity and the type of consequences necessary to constitute an armed attack according to Article 51 UN-Charter as well as elaborate on the question of what the required degree of state involvement is in the context of self-defence. Finally, it concludes by answering the question of why the scope of

13 See Wood Michael, The Caroline Incident – 1837, in: T. Ruys/O. Corten/A. Hofer (eds), The Use of Force in International Law: A Case-Based Approach (Oxford: Oxford University Press 2018) citing the correspondence between US Secretary of State, Daniel Webster, and British Government's representatives in Washington, in which Webster repeatedly used the celebrated Caroline formula. The Caroline formula became a crucial reference in the legal discourse regarding self-defence.

14 See Article 51 UN-Charter.

Article 51 UN-Charter shall be only reluctantly extended to comprise the claim for digital and kinetic self-defence in response to cyberattacks.

II. "ARMED" CYBERATTACK ACCORDING TO ARTICLE 51 UN-CHARTER?

In the traditional context of international law, the right to self-defence is subject to considerable disagreements among states and scholars.[15] Yet, all states agree that the right to self-defence according to Article 51 UN-Charter arises, if there is an armed attack. There are however controversies as to what constitutes an armed attack in the sense of the UN-Charter.[16] Traditionally, an armed attack requires a causal and considerable loss of life or extensive destruction of property, regardless of the means used.[17] Although the conventional case of an armed attack is the one of an invasion by regular armed forces of one state into the territory of another state,[18] recent developments show an increasingly hybrid or asymmetric character of war and conflicts.[19] Hybrid conflicts typically include a variety of state *and non-state* actors as well as different tactics.[20] From the perspective of international law,

15 Gray Christine, International Law and the Use of Force, 4th ed. (Oxford: Oxford University Press 2018), p. 120.

16 Ruys Tom, Armed Attack and Article 51 of the UN Charter (Cambridge: Cambridge University Press 2010); Gray (above n 15), p. 134.

17 Woltag Johann-Christoph, Cyber Warfare: Military Cross-Border Computer Network Operations under International Law (Cambridge: Intersentia 2014), p. 177; Zemanek Karl, Armed Attack, in: R. Wolfrum (ed) MPEPIL (Oxford: Oxford University Press Update 2013), §21.

18 Gray (above n 15), p. 134.

19 On the new phenomenon of asymmetric war among others: Münkler Herfried, Asymmetrie and the Process of Asymmetrization, in: J. Schröfl et al. (eds.), Winning the Asymmetric War – Political, Social and Military Responses (Frankfurt: Peter Lang 2009), p. 111 et seq.; Münkler Herfried, Der Wandel des Krieges: von der Symmetrie zur Assymetrie, 3rd ed. (Weilerswist: Velbrück Wissenschaft 2014).

20 On the increasing complexity of actor constellations and tactics of asymmetric and hybrid war and its core problem of being mainly political: Schroefl Josef/Kaufman Stuart, Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War, 37/10 Studies in Conflict and Terrorism 2014, pp. 862 et seq. with further references.

these developments (mainly related to the aftermath of the 9/11 attacks) brought up the fundamental debate about whether the requirements for self-defence can be met by attacks by non-state actors.[21] Some states tend to qualitatively widen the scope of self-defence in radical ways in this regard.[22] These developments acquire special weight in light of the new technical possibilities of cyberattacks as we are getting (dangerously) close to the scope of Article 51 UN-Charter, when the fallout of computer-controlled life-support through a cyberattack causes a significant amount of fatalities. The significance of the debate becomes even more pressing as due to the wide-reaching anonymity in cyberspace, dubious and elusive group structures within conflicts are very realistic and often used strategically. Consequently, the also explicitly in the *cyber context*[23] discussed question of whether the legal requirements for self-defence can be met by attacks by non-state actors may have far-reaching consequences. An expansion of the right to self-defence by including private actors' conduct could – in the cyber realm – lead to cyberattacks by individual hackers being responded to with military means and may allow for problematic leeway to legitimate war. It needs to be emphasized that this expansive interpretation of the right to self-defence is not in line with the authors' view. Furthermore, even a widely accepted state practice and political decisions of powerful states cannot circumvent a legal analysis of the measures taken.

These outlined developments demonstrate that not only the special characteristics of cyberattacks but also the division of opinions on the concrete scope of Article 51 UN-Charter give rise to important questions concerning the applicability of the concept of

21 Gray (above n 15), pp. 120 et seq.

22 Gray (above n 15), p. 120 and p. 200 et seq. analyzing the 9/11 attacks that have brought a fundamental reappraisal of the law on the use of force against terrorism. Even though the Security Council did not explicitly authorize the US-military operation "enduring freedom" in response to the attacks, the US-practice still had a far-reaching impact on the current debate. It was repeatedly claimed that the international state community (as well as the UN-Secretary General and the president of the General Assembly) implicitly acknowledged the operations, see the Press Release of 8 October 2001, UN. Doc. SG/SM/7985 and GA/SM/274. Further also often cited in this regard: UN Doc. SC/7167 of 8 October 2001; the NATO Press Release 2001, p. 138; SC-Res. 1373 of 28 September 2001. On these developments more in detail: Meiser Christian/von Buttlar Christian, Militärische Terrorismusbekämpfung unter dem Regime der UN-Charta, in: F. Wilfried et al. (eds), Saarbrücker Studien zum Internationalen Recht, Bd. 30 (Baden-Baden 2005), pp. 19 et seq. Exposing the relationship between power politics and international law in the context of 9/11: Anand Ruchi, Self-Defense in International Relations (New York: Palgrave Macmillan 2009), pp. 84 et seq.

23 See the reference to the Tallinn Manuals Group of Experts below n 52.

an armed attack to the cyber context. It is hence not surprising that the cyber context makes the already disputed subject matter more complex. Accordingly, the law of self-defence is one of the most discussed topics in the context of cyberattacks.[24] Overall, the applicability of the right to self-defence against cyberattacks was implicitly and explicitly confirmed several times.[25] Some states even explicitly hold on to their right to self-defence in the event of cyberattacks.[26] Although it is widely undisputed that cyberattacks have the potential to qualify as an armed attack according to the Charter[27] since they may have disastrous and damaging consequences in the real world as the introductory case at the University Hospital of Düsseldorf illustrates, there remains a fundamental dispute on *how* the law of self-defence is to be applied concretely. So far, no government has officially declared a cyberattack to qualify as an armed attack according to Article 51 UN-Charter[28] and states have not yet evolved detailed state practice or consensus on rules in this domain.[29] Though, states began establishing and sharing their views on the matter and the current platforms of the UN GGE and the OEWG enable a further discussion of these regulatory issues.

Given the ongoing international regulatory debate and the anonymous nature of cyberspace, it seems unavoidable to ask the questions as to what degree of state involvement, if any, should be necessary for the fulfillment of an armed attack and what the required gravity of its consequences needs to be.

---

24 Inter alia: Diggelmann Oliver/Hadorn Nina, Gewalt- und Interventionsverbot bei Cyberangriffen: Ausgewählte Schlüsselfragen, in: C. Schubel et al. (eds), Jahrbuch für Vergleichende Staats- und Rechtswissenschaften (Baden-Baden: Nomos 2017), pp. 260 et seq.; Gervais Michael, Cyber Attacks and the Laws of War, 30 Berkeley Journal of International Law (2013), p. 525 et seq., 541 et seq; Jensen Eric T., Computer Attacks on Critical National Infrastructure, 38 Stanford Journal of International Law (2002), p. 207 et seq., 223 ff; Roscini Marco, Cyber Operations and the Use of Force in International Law (Oxford: Oxford University Press 2014), p. 69 et seq.; Schmitt Michael N. (ed), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press 2013), pp. 54 et seq. (hereinafter Tallinn Manual 2013); Woltag (above n 17), p. 175 et seq.

25 UN GGE Report 2013; UN GGE Report 2015.

26 This is among others the case in all the analyzed states by Roguski (above n 6): Australia, Estonia, France, Germany, the Netherlands, the UK, and the US.

27 Randelzhofer Albrecht/Nolte Georg, Article 51, in: B. Simma et al. (eds), The Charter of the United Nations: Oxford Commentaries on International Law, Vol. II, 3rd ed. (Oxford: Oxford University Press 2012), pp. 1419–1420.

28 Tallinn Manual 2013, p. 57; Gray (above n 15), p. 136. This remains the position in January 2021.

29 See generally the diverging comments and opinions by states on the initial pre-draft of the OEWG report (as mentioned above n 10). In its conclusion also: Roguski (above n 6), p. 24.

a) Required Degree of Gravity and Type of Consequences

Most states[30] as well as scholars[31] stipulate that cyberattacks reach the threshold of an armed attack when its "scale and effects" are comparable to traditional kinetic attacks rising to the required level. Hence, whether a cyber operation constitutes an armed attack shall depend on the intensity of its *consequences*. But what does this mean? And what is the required level?

The scale and effects approach, which was historically established by the ICJ in the Nicaragua case back in 1986, focuses on the scale or in other words the intensity of the effects of an attack.[32] From the specific wording of "armed" attack in Article 51 UN-Charter it is clear that not all actions qualifying as "force" in the sense of Article 2(4) UN-Charter may constitute an armed attack.[33] The scope of Article 51 UN-Charter is much narrower compared to that of armed force according to Article 2(4) UN-Charter and requires *physical* damages or injuries of a more serious level.[34] Accordingly, a state is not automatically enabled to offensively react to (armed) force. In fact, there is a gap for defence measures open to states as *military* means are strictly limited to reacting to armed force amounting to an armed attack.[35] It has been criticized that due to this restraint there are not always effective remedies available against a state that uses cross-border armed force not amounting to an armed attack.[36] Nevertheless, this

30 Among others see Roguski (above n 6), p. 21 naming France and the Netherlands. See their positions: French Ministry of the Armies, International Law Applied to Operations in Cyberspace, September 2019, p. 8 (hereinafter France: Operations in Cyberspace); Netherland, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, p. 8 (both citing Nicaragua, §191 and 195, respectively).

31 Tallinn Manual 2013, Rule 13, p. 55; Accordingly: Tallinn-Manual 2.0 2017, Rule 69, p. 330.

32 ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Rep. 1986, 14, §195.

33 Woltag (above n 17), p. 176.

34 Among others: Heintschel von Heinegg Wolff, Informationskrieg und Völkerrecht, in: V. Epping/K. Ipsen (eds), Brücken bauen und begehen: Festschrift für Knut Ipsen zum 65. Geburtstag (München: Beck 2000), p.141; Randelzhofer/Nolte (above n 27), p. 1401; Schmitt Michael, Angriffe im Computernetz und das ius ad bellum, 41/5 Neue Zeitschrift für Wehrrecht (1999), pp.191 et seq.; Woltag (above n 17), p. 176.

35 Dinstein Yoram, War Aggression and Self-Defence, 6th ed. (Cambridge: Cambridge University Press 2017), p. 206; Randelzhofer/Nolte (above n 27), pp. 1401–1403; Woltag (above n 17), p. 176.

36 Woltag (above n 17), p. 176 with reference to Greenwood Christopher, Self-Defence, in: R. Wolfrum (ed), MPEPIL (Oxford: Oxford University Press Update 2011), §12 and Randelzhofer/Nolte (above n 27), p. 1402.

limitation in the use of military defence measures is not an unforeseen gap in the UN-Charter, but intent.[37] Self-defence is – as already mentioned above – an extraordinary measure to protect a states' existence and must be seen as a narrow exception to the general ban of the use of force. The gap is intended to ensure that not every use of force automatically escalates into a full-scale war but would be primarily mitigated through non-military means.[38] In any case, states that are the target of armed force according to Article 2(4) UN-Charter not amounting to an armed attack do not find themselves in a legal vacuum: They rather have the option to enact non-military, non-forceful countermeasures and bring the matter to the attention of the UN Security Council, which may qualify the act to be a threat to or a breach of the peace or an act of aggression according to Article 39 UN-Charter, which enables the Council to apply collective security measures such as economic embargos.[39]

Nevertheless, it was repeatedly admitted that the precise threshold needed to reach the level of an armed attack according to Article 51 UN-Charter in and out of cyberspace remains somehow vague.[40] The UN-Charters Article's traditional focus on physical destruction and fatalities at least means – in the authors' opinion – that cyberattacks not leading to physical consequences or more concretely, to serious physical destruction or death cannot be considered to fulfill the requirements of an armed attack. Hence, mere disruptions or destructions of the information infrastructure not leading to serious physical damage would not be sufficient, neither would be cyber espionage activities.[41] Scholars have provided for several hypothetical scenarios where cyberattacks could possibly amount to an armed attack: Dinstein for instance names – and this is interesting in light of the introductory case – fatalities caused by loss of computer-controlled life-support, an extensive electricity blackout

37 Randelzhofer/Nolte (above n 27), p. 1402; Stein Torsten/Buttlar Christian, von Völkerrecht (Köln: Heymann 2009), p. 279. See Woltag (above n 17), p. 176 stating that this is disputed by Kranz Jerzy, Die völkerrechtliche Verantwortlichkeit für die Anwendung militärischer Gewalt, 48 Archiv des Völkerrechts (2010), pp. 281–337, p. 302 with further references.

38 Randelzhofer/Nolte (above n 27), p. 1402; Woltag (above n 17), p. 176.

39 Diggelmann/Hadorn (above n 24), p. 261. Non-military measures are subject to the legal regime of unilateral and/or Security Council countermeasures. While the technical attribution remains equally challenging in this field, the legal preconditions allow for a more cooperative approach in these regimes. These aspects are being discussed in more detail in the authors' Ph.D. project.

40 Tallinn Manual 2013, Rule 13, p. 55.

41 Stein Torsten/Marauhn Thilo, Völkerrechtliche Aspekte von Informationsoperationen, 60/1 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (2000), p. 8; Woltag (above n 17), p. 179.

creating considerable harmful corollaries, the flooding of inhabited areas caused by the shutting-down of digital control systems of waterworks and dams, or deadly aircraft crashes caused by a manipulation of the aircraft software.[42]

Some scholars[43] as well as states[44] however claim that cyberattacks impairing the national interest of a state could be seen as an armed attack regardless of whether the consequences are physical. According to these (expansive) views this could for instance be the case for the stealing of data vital to national security – like for instance the location of nuclear weapons launch instruments.[45] Some go even as far as to consider cyberattacks that cause considerable economic damage as by crashing a state's major stock exchange to qualify as an armed attack.[46] It has also been argued that cyberattacks targeting critical national infrastructure should generally give rise to the right of self-defence even if – traditionally – the consequences would not fulfill the scope of an armed attack according to Article 51 UN-Charter.[47] It must be clearly emphasized that these latter views are all inconsistent with current international law.[48] Although such attacks could indeed have far-reaching consequences for a states' interests, espionage and the mere "stealing" of sensitive data are not generally qualified as armed attacks under international law, irrespectively of the

42 Dinstein Yoram, Computer Network Attacks and Self-Defense, 76 International Law Studies (2002), p. 105; as cited by Woltag (above n 17), p. 179.

43 Tallinn Manual 2013, Rule 13, p. 56–57.

44 E.g. France: Operations in Cyberspace, p. 8; Roguski (above n 6), p. 21. Noteworthy is also the statement by the Dutch Minister of Defense, Ank Bijleveld, in June 2018, according to which a cyberattack would qualify as an armed attack *"if it targets the entire Dutch financial system or if it prevents the government from carrying out essential tasks such as policing or taxation and it would thus trigger a state's right to defend itself, even by force*." Minister Bijleved was quite explicit that the right to self-defense is, in the view of the Netherlands, not limited to cyberattacks that lead to physical destruction, see <https://puc.overheid.nl/mrt/doc/PUC_248137_11/1/> [last consulted 13.12.2020]. Hereto also: Schmitt Michael, Estonia Speaks Out on Key Rules for Cyberspace, Just Security, 10 June 2019: <https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/> [last consulted 04.01.2021].

45 Woltag (above n 17), p.179 with reference to Joyner Christopher C./Lotrionte Catherine, Information Warfare as International Coercion: Elements of a Legal Framework, 12/5 European Journal of International Law (2001), pp. 855–56.

46 Some of the Experts of the Tallinn Manual took this view: Tallinn Manual 2013, Rule 13, p. 56; Sharp Walter Gary, Cyberspace and the Use of Force (Falls Church: Aegis Research Corp. 1999), p. 117.

47 Tallinn Manual 2013, Rule 13, p. 56; Jensen (above n 24), p. 209.

48 This reflects the authors' as well as other scholars' view: Among others Woltag (above n 17), p. 179.

quality of the acquired information.[49] Similarly, the manipulation of a stock exchange system does not cause direct physical destruction or human casualties whereas it would be rather qualified as economic (or political) coercion, concepts intentionally excluded from the scope of the law of self-defence.[50] Likewise, the targeting of critical infrastructure in itself does not violate Article 51 UN-Charter if the manipulation does not lead to physical consequences that fulfill the requirements of an armed attack. These scenarios would – depending on their respective qualification – at most allow non-military countermeasures and do (deliberately) not legitimate a forceful military measure of self-defence which legally ultimately means a right to wage war. While an armed attack will in most cases also violate other fundamental principles of international law such as the principle of non-intervention or the ban on the use of force there needs to be a much higher degree of destruction or considerable fatalities in order for a cyberattack to qualify as an armed attack.[51] Cyberattacks will therefore only constitute an armed attack according to the UN-Charter if their effects meet the scale and degree of gravity necessary in another state's territory.[52] A mere impairment of network systems of critical national and/or private infrastructure with no physical consequences of a more serious degree cannot be qualified as sufficient in light of traditional international law. This will regularly not be the case where system functioning of the affected infrastructure can be restored by switching the control functions on to parallel systems or by removing the malware.[53] Also, as long as cyberattacks affecting hospitals do not lead to a considerable loss of life, states should be reluctant to declare war. The decision to wage war, in the opinion of the author, is of too fundamental and far-reaching relevance, bears too many risks regarding international security, and is also questionable in light of proportionality.

b) State Involvement: Legal and Technical Attribution

Although scenarios like the one of cyberattacks targeting critical infrastructure leading to devastating consequences in the physical world or to a considerable number of deaths are hypothetically indeed possible, further requirements of an armed attack that are often given less attention – such as the required degree of state involvement

49 See Woltag (above n 17), pp. 124 et seq., p. 179.

50 See Woltag (above n 17), pp. 135 et seq., p. 180.

51 Woltag (above n 17), p. 180.

52 Woltag (above n 17), p.181.

53 Ibid.

– need to also be taken into account. In the authors' opinion, this also needs to be strictly the case in any concrete situation before considering an armed attack as given. Various states[54] as well as scholars[55] however affirm the possibility that private conduct may constitute an armed attack in the cyber context. As abovementioned, this is already highly debated in the non-cyber context and obviously is even more questionable in the cyber context.[56]

Traditionally, an armed attack according to Article 51 UN-Charter is to be launched from one state onto the territory of another state. This comes from international law primarily regulating the relations between states as territorially defined subjects of international law. In its core, the right to self-defence is hence meant for a state to defend itself against unlawful military conduct of another state. Nonetheless, the above-mentioned changing face of conflicts, in which actor constellations are increasingly hybrid, forced states and scholars to pay renewed attention to the underlying legal norms such as right of self-defence.[57] However, if cyberattacks by private individuals, groups or further non-state actors shall be responded by military means, the attacks need to be not only technically but also legally attributed to a state. If an attack by non-state actors shall be attributed to a state in light of Article 51 UN-Charta, if at all, from a legal perspective it would follow the logic of the more recently developed – but highly controversial – "safe-haven" doctrine.[58] According to this doctrine a state may become responsible for non-state actors launching transborder attacks from its territory if it is unwilling or unable to prevent the concerning actors

54 Germany accepts that self-defence measures may also be applicable in case of attributable conduct of non-State actors: Deutscher Bundestag, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. A. S. Neu, A. Hunko, W. Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE, BT-Drs. 18/6989, Krieg im „Cyber-Raum" – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung, 10 December 2015, p. 11. Similarly, France acknowledges that general state practice may shift towards accepting the right to self-defence against non-State actors: France: Operations in Cyberspace, pp. 8–9. See Roguski (above n 6), p. 22.

55 The majority of the Tallinn Manuals' Group of Experts was ready to extend the right of self-defence against non-state actors although they recognized its controversy in the traditional context. The minority of experts did not accept the premise, however. See Tallinn Manual 2013, p. 58–59.

56 Critical among others: Boulos Sonia, The Tallinn Manual and Jus ad bellum: Some Critical Notes, in: J.M. Ramírez/L.A. García-Segura (eds), Cyberspace: Risks and Benefits for Society, Security and Development (Cham: Springer 2017), p. 231 et seq., p. 238 et seq.

57 As indicated above n 22.

58 Diggelmann/Hadorn (above n 24), p. 266 with further references.

from carrying these out against the victim state.[59] The doctrine however remains very complex and is highly debated.[60] In its core, the doctrine would – and this in one of the main critics – fundamentally transform the *ius contra bellum* regime which seeks to limit the resort to force between states to the absolute necessary and the transformation of which a large number of states is probably not ready to accept.[61]

Notwithstanding the doctrinal ambiguity, in order to legally assume state involvement, there needs to be technical or other relevant evidence to start with. Consequently, military defence means will regularly not be lawful, if there are evidentiary issues of state involvement. With regards to cyberspace, this will *de facto* mostly – if not always – be the case. Cyberattacks are very difficult – if not impossible – to technically attribute to a state, and even if cyberattacks can be located to emerge from a certain territory, it is not clear whether there is actually a state behind the attacks, and if so, whether the respective state is indeed the "right" state. Cyberattacks often affect and emerge from several state territories simultaneously. In cyberspace, the attacker typically uses the infrastructure of an uninvolved or many uninvolved third parties as steppingstones by hacking himself into other IP-addresses, where the attack can be launched from.[62] He thus often remains anonymous. And obviously, if "the right" person or nationality of a person will be detected behind cyberattacks, the burden

59 Tibori-Szabó Kinga, The "Unwilling or Unable" Test and the Law of Self-Defence, in: C. Paulussen et al. (eds), Fundamental Rights in International and European Law (The Hague: T.M.C. Asser Press 2016), pp. 73 et seq.

60 On the debate among others: Christakis Theodore, Challenging the "Unwilling or Unable" Test, 77 ZaöRV (2017), pp. 19–22; Corten Oliver, The "Unwilling or Unable" Test: Has it Been, and Could it be, Accepted?, 29/3 Leiden Journal of International Law (2016), pp. 777–799; Tams Christian J., Self-Defence against Non-State Actors: Making Sense of the "Armed Attack" Requirement, in: M. O'Connell/C. Tams/D. Tladi (Authors), Self-Defence against Non-State Actors, Max Planck Trialogues (Cambridge: Cambridge University Press 2019), pp. 90–173; Tibori-Szabó (above n 59), pp. 73–97.

61 See Corten (above n 60), p. 798; Corten Oliver, The Law Against War (Oxford: Hart Publishing 2010), pp. 739–53; Starski Paulina, Right of Self-Defense, Attribution and the Non-State Actor – Birth of the "Unable or Unwilling" Standard?, Heidelberg Journal of International Law (2015), pp. 405 et seq.

62 See Singer P.W./Friedman Allan, Cybersecurity and Cyberwar, What Everyone Needs to Know, (Oxford: Oxford University Press 2014), p. 33 stating that a sophisticated user can easily hide or disguise his IP address by routing his activities through another point on the Internet, making it appear that the latter node was responsible for the harmful traffic. Similarly: Dunn Cavelty Myriam, Why Cyberattacks don't Work as Weapons, ETH Zukunftsblog, 18 January 2018.

to additionally prove state involvement[63] or its "safe haven" to the hacker(s) in this concrete case is even more difficult. Hence, it will typically not be clear against which state the self-defence measure is to be launched.[64] Furthermore, as malware may not only infect the target system itself but may also spread to other computers worldwide, collateral damage is very realistic in cyberspace.[65] It is therefore often not only unclear who the attacker is but also who exactly was meant to be the addressee of the attack. In the authors' opinion, for a military decision to launch an offensive (digital or kinetic) measure in self-defence it must therefore at least be taken into account that a counterattack may hit the wrong state and thereby harm an uninvolved third party. Or that the concerned state might enter into an undesired conflict. Such a (misdirected) forceful self-defence measure against a peaceful or uninvolved state – as of therefore not being lawful – could consequently itself constitute an (armed) attack against the latter. This would ultimately make this initially uninvolved state a new conflict party and thus potentially start a spiral of escalation. A state must hence be aware of the possible consequences of his authorized measures and consider that – even if allegedly out of self-defence – it might be starting war with a peaceful state which would ultimately lead to much more collateral damage.

Finally, since the subject matter of self-defence against private as well as state actors is already legally controversial in the traditional non-cyber context, it certainly remains too ambiguous with regards to cyberattacks. The technical difficulties to trace back attacks to the real source are – at least to date – still too fundamental and will hence render a legal attribution mostly impossible. Overall, an attribution of a cyberattack to a state and thereby assuming an armed attack as given will mostly be affirmed too roughly. Especially, if a victim state solely evaluates a cyberattack as an armed attack without considering its real-world context and an additional use of any conventional armed force.[66] A too frivolous attribution could, due to the mostly little to no technical evidence at hand, lead to the possibility of cyberattacks by criminals or emerging from uninvolved third states being answered with war. Hence, due to the fundamental legal and technical attribution problems, "armed" cyberattacks in

63 Schulze Sven-Hendrik, Cyber-„War" – Testfall der Staatenverantwortlichkeit (Tübingen: Mohr Siebeck 2015), pp. 141–142.

64 Similarly: Diggelmann/Hadorn (above n 24), p. 263.

65 Reinhard Fabian, Der digitale Gegenangriff ist keine brauchbare Strategie für die Cyber-Verteidigung, NZZ, 1 August 2020.

66 Woltag (above n 17), p. 181.

fact only rarely, if at all, meet *all* the required conditions according to Article 51 UN-Charter.

III. WHY ONLY RELUCTANTLY, IF AT ALL, OPEN UP THE SCOPE TO DIGITAL AND KINETIC SELF-DEFENCE

The above-mentioned challenges are all reasons to only restrictively make use of forceful self-defence according to Article 51 UN-Charter. This reluctance in doing so is generally not only recommendable for Switzerland as a neutral state, but also for the entire international community of states. All the aspects of an armed attack need to be given, ultimately also the certainty as to the responsible state behind the attack. There is an inherent danger that armed attacks will be affirmed too impulsively – a condition which does not at all align with the time needed to technically trace back a source of a cyberattack, and if tracing back is possible timely, the remaining of uncertainty.[67] All in all, in the authors' opinion, the developments regarding the application and extension of Article 51 UN-Charter are not unproblematic in light of international law: On the one hand, they tend to expand the scope of self-defence to non-physical (e.g. economic) damage and on the other hand, by the tendency of opening up self-defence against non-state actors in cyberspace, they increase the circle of possible "war situations" and "war actors" probably too radically. Put simply, the entering into war would "more easily" be legally justified. This could even encompass cases like for example, private hackers launching economically motivated ransomware attacks against a hospital, which traditionally would need to be considered under (international) criminal law rather than being considered as

67 Similarly, among others: Randelzhofer/Nolte (above n 27), p. 1420; Stein/Marauhn (above n 41), p. 10; Roscini Marco, World Wide Warfare – Jus ad Bellum and the Use of Cyber Force, 14 Max Planck YB UN L 85 (2010), p. 96 et seq. Further also: Mäder Lukas/Häsler Sansano Georg, Interview with Alain Vuitel and Thomas Süssli, Ein Cyberangriff der Armee würde Monate dauern, NZZ, 6 January 2020 where Süssli refers to the remaining of too much uncertainty in the context of hackbacks. Stating that even at 60–70% there remains too much uncertainty as to be sure to actively launch a counterattack.

military state conduct according to the UN-Charter. These issues become especially relevant since cyberattacks with considerable economic consequences are on the rise, which – notwithstanding the importance of taking them seriously – should in the authors' opinion rigorously not be equated with "acts of war".

The doctrinal ambiguities in the interpretation of international law and (the thereby possible contribution to) the changing character of war should be taken into account before and while states make their active kinetic *and* cyber self-defence a military strategy. Ultimately, in any concrete situation of an attack there remains an inherent need for an individual assessment of the respective (cyber and real-world) circumstances at hand. However, a military decision to enact a measure in self-defence should in the authors' opinion not only be a strategic, but in its core also a legally compliant one. Hence, – from an international legal point of view – the main focus of military cyber defence strategies should primarily be on de-escalation by protecting cyber infrastructure and networks, building up resilience as well as a focus on *damage limitation* and *termination*. This would in other words imply to primarily foster more passive defence measures while reserving digital or kinetic counterattacks only to the cases where there is not only an "instant and overwhelming necessity of self-defence, leaving no choice of means, and no moment for deliberation" but also the certainty as to the attacker behind the attack. Such a legal assessment would in its result ensure to be in line with the core legal meaning and purpose of Article 51 UN-Charta and still enable a state to exceptionally defend itself against an aggressor by repelling an unlawful armed attack. Additionally, due to the remaining uncertainties and ambiguities as to the attribution of cyberattacks to a state, states should also more intensively engage in clarifying the international standard of proof necessary for acts of self-defence.

In conclusion, *expanding* the right to war by widening the scope of Article 51 UN-Charter would run against the actual aim of the UN-Charter, which is to promote peace among nations. In fact, these developments could lead to fundamental alterations of the landscape of future conflicts.[68] Therefore, from the perspective of international law, instead of launching forceful military counterattacks, states should rather enhance and engage in a dialogue about international forms and processes of cooperation and dispute settlement in the field of cybersecurity and remember that besides using military means, there are also possibilities of informing the Security Council or of

68 Boulos (above n 56), p. 241.

enacting non-forceful countermeasures (sanctions). Finally, if in a particular case the scope of an armed attack according to Article 51 UN-Charter would still be considered as given, the enacted measure itself needs to meet the essential legal requirement of proportionality. Therefore, whether the concrete digital and/or kinetic defence measure is proportional and hence itself compliant with international law needs an additional (legal) consideration. This however is subject to a further discussion.

Author

Sara Pangrazzi

Sara Pangrazzi (MLaw) is a Ph.D. Candidate in cybersecurity and international law at the University of Zurich. She focuses on the legal aspects regarding the law of self-defence as well as the regime of countermeasures with a particular focus on the principle of proportionality in both fields. Her research project is funded by the Forschungskredit Candoc of the University of Zurich.

About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organisations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with the publication of a book by the UN ICT Task Force on the practice and theory of ICT in the conflict cycle and peace building in 2005 and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation