EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

What is the measured response to a cyber attack on critical infrastructures?

Methodological, operational and legalistic approach for small states

by

Alexander Peychev*

April 2022

Supervised by Prof. Dr Plamen Pantev

Institute for Security and International Studies (ISIS), Sofia

Disclaimer: *This report has been prepared as part of a research internship at the Institute for Security and International Studies (ISIS), Sofia, funded by the European Union(EU) Non-Proliferation and Disarmament Consortium as part of a larger EU educational initiative aimed at building capacity in the next generation of scholars and practitioners in non-proliferation policy and programming. The views expressed in this paper are those of the author and do not necessarily reflect those of ISIS, the EU Non-Proliferation and Disarmament Consortium or other members of the network.*

*Alexander Peychev holds a Bachelor degree in International Relations from Sofia University "St. Kliment Ohridsky". He is interested in researching low-intensity conflicts in EU's Eastern Neighbourhood, North Africa and the Middle East. He speaks German, English and learns French.

ABSTRACT

Smaller European countries are limited by their scarce resources compared to larger countries. Therefore, their place and role in the international system are dubious and complicated. In most cases, they cannot exert influence and are subject to external one. In cyberspace, too, small states are faced with the problem of how best to prevent an adversary (e.g. a nation state) from conducting a cyber attack on their critical infrastructure. Since they are unable to initiate a "kinetic" response or impose economic sanctions on organizations and individual entities due to insufficient military and economic power, what are their available tools? In this paper, I will argue that small states are bound by necessity to strictly observe and promote international law, while they are bound to be active members in collective security organizations. Constructive efforts to apply international law to cyberspace and subject cyber weapons to arms control would allow states to develop cyber defense policies that can categorize responses to cyber attacks based on their impact. Solving the attribution problem and responding to cyber threats will be easier to accomplish when smaller states cooperate with their technologically advanced larger partners. The central question in this paper will be how a small state can effectively respond to a cyberattack on its critical infrastructure that is ultimately attributed to a larger and more powerful state. I begin by defining what small states are and what the most beneficial environment for their survival is. After that I define the concepts of critical infrastructure and cyber attack. Is international law applicable to the cyber domain? Are cyber weapons susceptible to arms control? I analyze first the operational capabilities of EU and NATO member states then I examine what international principles cyberattacks violate. I conclude by providing the best possible response to cyberattacks, recognizing the fact that defenders strive to mitigate the impact of the attack.

Keywords: cyberattacks, critical infrastructure, response, attribution

Acronyms

CBMs (Confidence Building Measures)

CERTs (Computer Emergency Response Teams)

CI (Critical Infrastructure)

CNA (Computer Network Attack)

CNE (Computer Network Exploitation)

CSIRT (Computer Security Incident Response Team)

ECI (European Critical Infrastructure)

ICJ (International Court of Justice

ICS (Industrial Control Systems)

ICT (Information and Communications Technology)

IHL (International Humanitarian Law)

IIL (International Law Commission)

IT (Information Technology)

LOAC (Law of Armed Conflict)

OCOs (Offensive Cyber Operations)

OT (Operational Technology)

SCADA (Supervisory Control and Data Acquisition)

UN GGE (UN Group of Governmental Experts)

1. Small states theory

Since the end of World War II, the number of states has been growing. Scholars point out that the change in the international system after 1945 increased the number of states due to "the rise of an international norm against conquest and the concomitant emergence of multilateral institutions that codify that norm".[1] As a result, more than half of the member states of the United Nations (UN) have fewer than 10 million citizens.

Previous research on the topic of small states has focused on population size as the key attribute of "smallness".[2] More citizens mean more taxpayers. Larger states can allocate more resources to social services, but more importantly, they can spend more on defense.[3] This goes hand in hand with the argument of neorealists that in an anarchic system of international relations the greatest asset needed for a state's survival is military power,[4] which can be converted to influence at any given time.[5] It follows that small states struggle to influence the international system.[6] From a neoliberal perspective, since small states cannot compete with larger states in terms of military power, they should focus on soft power that they can convert into diplomatic influence and achieve economic advantages.[7] Soft power is the ability to get others to want what you want through appeal and attraction rather than coercion.[8]

Recent research has focused on the analysis of small states at the state and individual levels. At the state level, small states tend to subordinate themselves under a hierarchy as a means to obtain order. They seek order in a hierarchical relationship to (i) enhance security and territorial integrity; (ii) clearly define and protect property rights at home and abroad; and (iii) set and enforce standards of behavior.[9] At the individual level, small states tend to have greater "normative power".[10]

For the purposes of this article, I will focus on European countries, members of EU and NATO classified as middle- and high-income countries with a population of approximately 10

---

[1] Fazal, T. M., & Griffiths, R. D., "Membership has its privileges: The changing benefits of statehood," *International Studies Review*, 16(1) (2014), p. 90.
[2] T. G. Masaryk, The *Problem of Small Nations in the European Crisis* (London: University of London, Athlone Press, 1966), p. 23.; J. A. R. Marriott, *Federalism and the Problem of the Small State* (London: Allen and Unwin, 1943), p. 62.; David Vital, *The Inequality of States: A Study of the Small Power in International Affairs* (Oxford: Clarendon Press, 1967), p. 8.
[3] Alesina, Alberto, and Enrico Spolaore, *The Size of Nations*, (The MIT Press, 2003), p. 17-18.
[4] Waltz, K. N., *Theory of international politics*, (Reading, Mass: Addison-Wesley Pub. Co., 1979), p. 88-97.
[5] Handel, M., *Weak states in the international system*, (Totowa, NJ: Frank Cass, 1981) p. 6.
[6] Keohane, Robert O, "Lilliputians' Dilemmas: Small States in International Politics," I*nternational Organization*, 23(2) (1969), p. 293.
[7] Andrew K. Rose, *Like Me, Buy Me: The Effect of Soft Power on Exports*, (NBER Working Papers 21537, National Bureau of Economic Research, Inc, 2015) p. 1-2.
[8] Nye, J. S. (1990), "Soft power," *Foreign Policy*, 80, p. 167.
[9] Lake, D.A., *Hierarchy in International Relations*, (Ithaca, NY: Cornell University Press, 2009), p. 9.
[10] Ingebritsen, C., "Norm entrepreneurs: Scandinavia's role in world politics," *Cooperation and Conflict*, 37(1) (2002), p. 13.

million people. I assume that small states gain more than their larger counterparts from highly institutionalized, cooperative, and peaceful international system,[11] from international institutions that provide them with an opportunity to gather, analyze, and disseminate data. These institutions are a forum for the exchange of views and decision-making. They define norms, monitor and enforce rules, settle disputes.[12]

2. Critical infrastructure, cyber attacks and the problem of attribution

Directive 2008/144/EC introduces the terms critical infrastructure (CI) and European critical infrastructure (ECI). Article 1 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". ECI, in turn, is a "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States". The definitions of critical infrastructure in the US[13] and Canada[14] are similar.

Critical infrastructure sectors such as water treatment, power generation and others rely on operational technology (OT) systems and more specifically industrial control systems (ICS), a subset of OT, that are used to supervise and control their key processes. Supervisory control and data acquisition (SCADA) systems are a subset of ICS and provide a graphical user interface for operators to easily observe the status of a system, receive alarms, and make adjustments to processes under control. These digital devices – sensors, controllers – are then connected to information technology (IT) networks such as data storage and business software, which in turn could be further connected to the internet. As a consequence of integrating technology in the management of critical systems, critical infrastructure has become reliable, automated and integrated both across sectors and geographically.[15] Considering the interdependencies between sectors, a disruptive cyberattack on the power grid for example can also affect the oil production sector by disrupting power to pumping stations, storage and control systems.

---

[11] Thorhallsson, B., & Steinsson, S, "Small State Foreign Policy," *Oxford Research Encyclopedia of Politics* (2017), p. 11.
[12] Karns, M. P., Mingst, K. A., Stiles, K. W., *International organizations*, 3rd edn, (Boulder, CO: Lynne Rienner, 2015), p. 27.
[13] The White House, Office of the Press Secretary, *Executive Order -- Improving Critical Infrastructure Cybersecurity,* February 12, 2013 (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity).
[14] Government of Canada, *National Strategy for Critical Infrastructure*, 2009 (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx).
[15] ENISA, *Critical Infrastructures and Services*, Retrieved on 25.04.2022 (https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services).

An example of this was the attack on SolarWinds - a large software company that provides system management tools. Among their customers are operators of critical infrastructures. The Orion software was infected with malicious code that allowed the attackers to gain access to the systems of the software's customers.[16] Another sophisticated cyberattack such as Stuxnet, which disrupted Iran's nuclear facilities by destroying 984 uranium enrichment centrifuges in 2010, shows that a cyberattack targeting ICS can also result in physical damage.[17]

There is not a single agreed upon definition of cyber attack.[18] A typical definition is "unwelcome attempt to steal, expose, alter, disable or destroy information through unauthorized access to computer systems".[19] It encompasses a wide range of cyber attacks – from criminals seeking financial gains and hacktivists who seek attention for their causes and do no physical harm, to state-sponsored cyber attacks on critical infrastructure. The threat of nation states damaging the information systems that control their adversary's critical infrastructure, potentially causing physical harm, is highlighted in the Trump administration's 2017 National Security Strategy. This apparent disagreement on how to distinguish between kinds of cyber attacks based on their goal is leading experts to categorize cyber attacks based on their impact. The UK National Cyber Security Center distinguishes between two types of cyber attacks – untargeted (taking advantage of the openness of the internet): phishing, water-holing, ransomware, scanning; and targeted (specifically tailored attacks on systems, processes and personnel to): spear-phishing, deploying a botnet, subverting of supply chain. Botnets that deliver Distributed Denial of Service (DDoS) attacks, which despite being classified as "targeted" cyber attacks, can for example target private video game companies and are therefore irrelevant to a country's national security.[20]

The debate about what cyber attacks are is gradually shifting to military science, where cyberspace is seen as the fifth domain of military operations alongside land, sea, air and space.[21] This prompts cyber defense scholars to drop the concept of cyber attack as used in the civilian sector and introduce a new one - "offensive cyber operations" (OCOs). OCOs have two parts. The first one is computer network exploitation (CNE), the second – computer

[16] Oladimeji, Saheed, & Kerner, Sean Michael, „SolarWinds hack explained: Everything you need to know", TechTarget, June 16, 2021 (https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know).
[17] Zetter, Kim, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", Wired, November 3, 2014 (https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/).
[18] Grauman, Brigid. "Cyber-security: The Vexed Question of Global Rules," Security Defence Agenda and McAfee, February 2012, p.6, Available at (https://www.files.ethz.ch/isn/139895/SDA_Cyber_report_FINAL.pdf).
[19] IBM, "What is a cyber attack?" (https://www.ibm.com/topics/cyber-attack).
[20] Singer, P. W., & Friedman, A., *Cybersecurity and Cyberwar: What everyone needs to know*, (Oxford: Oxford University Press, 2014), p. 70.
[21] United States Department of Defense. "The Definition of Cyberspace." Deputy Secretary of Defense Memorandum (May 12, 2008), Retrieved on 25.04.2022 (https://www.gao.gov/assets/a321824.html).

network attack (CNA). CNE is about collecting information and "pre-attack reconnaissance", which in itself gives the attacker a second option – to destroy information, thus "progressing into a cyber attack", or CNA.[22] Martin Libicki argues that cyber espionage is "the unauthorized extraction of information from a computer system", hence CNE. According to him, penetrating the system can again provide the opportunity of conducting an attack - CNA, which he simply defines as cyber attack. However, he agrees that both cyber-espionage and cyber-attacks are usually conflated;[23] necessitating the distinction between the two introduced with the term OCOs.

OCOs or cyber attacks can be conceptualized further. The Lockheed Martin kill chain divides a cyber attack into four phases. The first stage is reconnaissance and preparation of resources that will exploit the identified vulnerability and access the system. Stage two focuses on gaining persistent access to the system by altering data. Stage three is further broken down into four sub-stages, which can be summarized as follows: 1. conducting internal reconnaissance; 2. moving through the system "laterally", setting the right conditions for further compromise; 3. continue establishing a foothold to mask activities and allow future re-compromise; 4. repeat. In the last stage four, the attacker will achieve their set goal - disrupt the system, steal information or something else.[24] The kill chain model can be explained as a gradual breach of the three security objectives of any information system - a breach of confidentiality (keeping data private), integrity (not allowing unauthorized alteration of system data and instructions) and availability (keeping the system functional and accessible).[25]

In summary, impact is important when defining cyberattacks. But it's also important to attribute them when they damage critical infrastructure. For example, if State A cannot identify who conducted a damaging cyberattack, it would have difficulty punishing the perpetrators and deterring anyone from future cyberattacks. The goal of attribution is to identify governments and organizations, not individuals.[26] The link between the party conducting the intrusion and the party who should bear responsibility, i.e. a foreign state, is at the core of the attribution problem. The victim state in particular wants to hold the latter to account.[27]

---

[22] Whyte, C., & Mazanec, B. M., *Understanding cyber warfare: Politics, policy and strategy*, (London; New York: Routledge, 2019), p. 80-82.
[23] Libicki, M. C., *Cyberspace in peace and war*, 2nd edn, (Annapolis, Maryland: Naval Institute Press, 2021), p. 72.
[24] Whyte, & Mazanec, *Understanding cyber warfare,* p. 92-93.
[25] Singer, & Friedman, *Cybersecurity and Cyberwar*, p. 35.
[26] Rid, Thomas, & Buchanan, Ben, "Attributing Cyber Attacks," *Journal of Strategic Studies*, 38 (1–2) (2015), p. 13.
[27] Lin, Herbert, „Attribution of Malicious Cyber Incidents: From Soup to Nuts", Journal of International Affairs, March 9, 2017 (https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents).

Rid & Buchanan propose a Q-model of attribution based on three levels of analysis, ending with "communication", i.e. releasing results to the public. The model also strives to ascertain responsibility with greater certainty to avoid bias. At the tactical level, a forensics team begins gathering technical evidence of the intrusion to identify both the nature of the malicious activity and the individuals responsible for the attack. This is followed by an operational analysis layer, where the conclusions drawn in the previous layer are mixed with information from different sources. It is based on the assumption that all-source information presents a broader picture of the intrusion, thus allowing the construction of competing hypotheses.

An important note here is that operators and owners of critical infrastructure are mostly private legal entities who can identify what disrupted their network but cannot answer the question of why they were targeted in the first place. It requires cooperation between state and non-state actors, which is described as operational.[28] Rid & Buchanan take operational collaboration between state and non-state actors for granted, which according to Michael Daniel, former Cybersecurity Coordinator on the National Security Council Staff, is not the case. Operational collaboration remains a theoretical approach that has not been put into practice. Therefore, the operational level of analysis of the Q-model requires a national legal framework that legally compels private entities to cooperate with the state as a whole.[29]

At the strategic analysis level, policy makers and top analysts place the cyber attack in a geopolitical context. They summarize the information of the tactical and operational level. The main goal here is to understand the motive behind the attack. Here the hypotheses are tested. After the entire analysis process is completed, the result is shared with the public with three objectives: improved credibility, attribution and defenses.[30]

I will use Herbert Lin's paper on the three meanings of attribution to provide an additional insight to the Q-model. Attributing malicious cyber activity to a machine can be compared to the tactical or technical level of analysis in the Q-model. By this Lin means tracking the trail to the computer or computers from which the malicious actor operated. The work is laborious, especially in the case of a multi-stage cyber attack, and can cross national borders. This is done through a forensic analysis of the clues left by the intrusion. The attribution of malicious cyber activity to a specific perpetrator or organization is similar to the operational level. Linking the perpetrator to the machine requires extensive investigation and gathering information from multiple sources. Finally, the attribution of an intrusion to the responsible

[28] The Aspen Institute's Cybersecurity Group published elaborating on this concept: "An Operational Collaboration Framework." Aspen Cybersecurity Group, November 2018 (https://www.aspeninstitute.org/publications/an-operational-collaboration-framework/).
[29] Daniel, Michael, "Closing the Gap: Expanding Cyber Deterrence," in *New Conditions and Constellations in Cyber*, ed. Alexander Klimburg, (The Hague: The Hague Centre for Strategic Studies, 2021), p. 156.
[30] Rid, & Buchanan, "Attributing Cyber Attacks," p. 26.

adversary corresponds to the strategic level of the Q-model.[31] If the question at the operational level is who did it, the one at the strategic level is who is to blame, i.e. which state should be held responsible for the intrusion.[32]

In conclusion, attribution of a cyberattack is an integrated process consisting of numerous levels of analysis, each building on the previous with the aim of establishing a state's responsibility. It is also a resource-intensive process that can pose a challenge to small states. Allocation of resources should be done taking into account the damage dealt by the attack.

3. Cyber attacks and international law

The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) convened first in 2004 has agreed in 2013 that international law, state sovereignty and human rights apply to cyber space. In addition to that, states should not use proxies to commit cyber attacks on other states, nor should they tolerate non-state actors launching attacks from their territory, i.e. state responsibility was pointed out. [33] In its next report in 2015 the UN GGE noted that the principle of non-intervention in other states' internal affairs applies to cyberspace. It was also advised that states should not support or conduct cyberattacks on critical infrastructure and they should protect their own critical infrastructure from cyber threats.[34]

The 2013 UN GGE agreed on voluntary confidence-building measures (CBMs). The report vows states to promote a peaceful information and communications technology (ICT) environment. CBMs open the path to a future arms control regulation of the cyber space.[35] Arms control originally referred to the creation of rules to limit arms competition, mainly nuclear arms. Later the term became more abstract. Jozef Goldblat includes eight measures in the original definition of arms control. Among those more relevant to cyber attacks are: (i) preventing certain military activities (cyber activities); (ii) reducing the risk of an unintended war; (iii) building confidence between states through greater openness on military matters.[36] In 2013 the following CBMs were recommended: exchanging views and information on national policies; the creation of bilateral or multilateral frameworks for CBMs; sharing of information among states on cybersecurity incidents between countries computer emergency

[31] Lin, „Attribution of Malicious Cyber Incidents: From Soup to Nuts".
[32] Healy, Jason, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, (Washington, DC: Atlantic Council of the United States, 2012), p. 1.
[33] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 2013, *Summary*, A/68/98, 24 June 2013 (henceforth GGE 2013), p. 2.
[34] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 2015, *Summary*, A/70/174, 22 July 2015 (henceforth GGE 2015), p. 2.
[35] Wolter, Detlev, "The UN Takes a Big Step Forward on Cybersecurity", Arms Control Asssociation, (https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity).
[36] Goldblat, Jozef, *Arms Control: The New Guide to Negotiations and Agreements*, 2nd edn, (London: SAGE Publications Ltd, 2002), p. 3.

response teams (CERTs) on bilateral and multilateral level, through existing or newly created channels for crisis management and early warning and through channels at policy-making levels. It also advises states to cooperate on CI incidents and law enforcement mechanisms to reduce misunderstandings.

Goldblat also stipulates that arms control is often used interchangeably with several concepts; again the most relevant to cyber attacks may be "arms regulation", i.e. the creation of international norms to regulate states behavior in cyberspace by defining what cyber weapons are.[37] But traditional arms control regimes, it is argued, are difficult to apply to cyberspace. How can states limit weapons that cannot be assessed quantitatively? This is hindered by the facts that specific cyber weapons are created to target specific systems (Stuxnet) and that cyber weapons in general cannot be destroyed. The technical innovation creates additional challenges. By the time they are signed, arms control treaties will potentially be obsolete.[38] Considering all these obstacles, Joseph Nye proposes that cyber arms control should focus not on arms regulation but on "targets regulation".[39] But targets regulation falls not under the scope of arms control but of international humanitarian law (IHL). Jus in bello regulates what is a legitimate target of war. The 2015 GGE report adopted both the no first use pledge of cyber weapons against civilian infrastructure in peacetime and the restraint on cyber attacks on critical infrastructure, suggesting the applicability of IHL in cyberspace.[40]

The idea of regulating targets of cyber attacks is promoted by the US and its NATO allies in the Tallinn Manual. The Talinn Manual is an interpretation of the law of armed conflict (LOAC) in cyber space.[41] The impetus for The Tallinn Manual came after the 2007 DDoS attack on NATO member Estonia and the 2008 Russian cyber operations against Georgia. The aim was to examine the applicability of international law in cyberspace. It makes suggestions under which circumstances states can use force in connection with cyber operations (jus ad bellum) and how this force can be used in an armed conflict (jus in bello). The Tallinn Manual 2.0 was published in 2017.[42]

Alongside the Tallinn Manuals, NATO has affirmed since its 2014 Wales Summit that "cyber defence is part of the Alliance's core task of collective defense" and that international law applies in cyberspace. At the 2016 Warsaw Summit cyberspace was recognized as a domain

[37] Goldblat, *Arms Control*, p. 3.
[38] Council on Foreign Relations, "Why Are There No Cyber Arms Control Agreements?", January 16, 2018 (https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements).
[39] Nye, J. S., "Normative Constraints on Cyber Arms," in *Getting Beyond Norms: New Approaches to International Cyber Security Challenges*, ed. Fen Osler Hampson and Michael Sulmeyer, (Waterloo, ON, CA: Centre for International Governance Innovation, 2017), p. 20.
[40] GGE 2015, *supra* note 34, p. 2.
[41] Libicki, *Cyberspace in peace and war*, p. 636.
[42] Schmitt, Michael N., ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge, UK: Cambridge University Press, 2017) (hereinafter Tallinn Manual 2.0).

of operations. Emphasis was put on strengthening the national cyber defence capabilities. At the 2016 Brussels Summit a Comprehensive Cyber Defence Policy was endorsed. It focuses on collective defence, crisis management and cooperative security. NATO supports member states in improving their national cyber defenses by sharing information, exchanging best practices and conducting cyber defense exercises.[43]

Similar to NATO, the EU has adopted its own cyber security policy. The Directive on Security of Network and Information Systems EU 2016/1148 (the NIS Directive), which is part of the EU Cybersecurity Strategy, provides legal measures to achieve high common level of cybersecurity in the EU. It obliged Member States to create national cybersecurity capabilities, e.g. national CSIRT, to collaborate with other EU countries – operational EU CSIRT network, strategic NIS cooperation group and to supervise critical infrastructure sectors.[44]

The NIS Directive has proven effective in boosting cyber resilience of private and public entities but also showed weaknesses.[45] One major problem was that the scope of application was largely left to the discretion of Member States. It gave Member States leeway in implementing security, incident reporting, and supervision and enforcement obligations.[46] In order to respond to the growing number of cyberattacks and the inherent threats of the digitalization of critical infrastructure sectors, a new directive was drafted.[47] The new NIS 2 Directive has yet to come into force and be implemented. Its latest revised version envisions more stringent measures for supervision and enforcement.[48]

Concisely, the UN, EU and NATO come to the conclusion that international law applies in cyberspace. Moreover, member states are recommended (as in the case of the UN GGE reports) or obliged (NATO and EU policy) to develop their own cyber defense capacities, to cooperate with other states and to protect their critical infrastructure.

3.1. The danger of normalizing malicious cyber activities for Small States

The consensus on the applicability of international law to the cyber domain and the need for the creation of specific norms that regulate state behavior in cyber space has contradicted with the de facto actions of states in the ICT environment.[49] This leads to what Martin Libicki calls

[43] NATO, *Cyber Defence*, March 23, 2022 (https://www.nato.int/cps/en/natohq/topics_78170.htm).
[44] ENISA, *NIS Directive*, Retrieved on 25.04.2022 (https://www.enisa.europa.eu/topics/nis-directive).
[45] Baldin, Anna, "EU: Towards the adoption of the NIS 2 Directive", DataGuidance, December 2021, (https://www.dataguidance.com/opinion/eu-towards-adoption-nis-2-directive).
[46] Ibid.
[47] European Parliament, "The NIS2 Directive: A high common level of cybersecurity in the EU", December 1, 2021 (https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333).
[48] ENISA, *ENISA CSIRT MATURITY FRAMEWORK*, 2022, p. 20, Available at https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework.
[49] Hathaway, Melissa, "When Violating the Agreement Becomes Customary Practice" in *Getting Beyond Norms,* p. 6.

“normalized behavior” or “normalization” - “an activity is normalized when carried out by at least one capable and serious country - especially if that country does not deny such activity or make excuses about it”.[50]

For example, Ukraine has suffered attacks on its critical infrastructure in 2015 and 2016. The first attack targeted three power distribution companies. The companies were attacked by spear phishing emails. When workers clicked on the Word document attached to the email, they were infected with a program called Blackenergy3. After the initial intrusion, the perpetrators continued reconnaissance, exploration and mapping of the networks. Eventually, they gained access to employee credentials, which allowed them to gain control of the SCADA network. Then they altered information before disrupting the system. This oversimplified explanation of the attack should not detract from its sophistication.[51] This was a deliberate attack to a state’s critical infrastructure in a peacetime. It is attributed to “Sandworm”, group associated with the Russian Federation - a member of GGE.[52] The cyber attack on Ukraine's power grid shows that small states in cyber space (I argue here that Ukraine in 2015 was in fact a small European state given its cyber defense capabilities), especially ones that are not members of a collective security organizations, find themselves in the natural state of Hobbes where a powerful country can violate the sovereignty of a not so powerful one with no consequences.

Larger states, even superpowers, could hardly benefit from this. By breaching SolarWind’s Orion the perpetrators put the reliability of and the trust in the ICS of critical infrastructures in the U.S. Still, this malicious cyber activity is CNE, which didn’t evolve into CNA.[53] But should cyberespionage on this scale, such as hacking into the power grid that leaves the door open for disruption later, be considered normal? A cyberspace where no one is safe, where actors do not abide by international law, is a return to the security dilemma. In such an environment, the rationale for Small State A, a victim of an infiltration into its critical infrastructure systems, would be to breach Larger State B's power grid ICS in response. This differs from a hack-back, which describes cyber activity against an adversary carried out by an NGO in response to a breach of its IT systems. The hypothetical case can play in the Mutually Assured Destruction (MAD) model only if, for example, Small State A and Large State B both know that each has access to the other's ICS. This proposition contains a notion of legality. It could build on the CBMs proposed by the GGE in 2013 - states should exchange

[50] Libicki, Martin C. "Norms and Normalization," *The Cyber Defense Review*, 5(1) (2020), p. 44.
[51] Zetter, Kim, „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid“, Wired, March 3, 2016 (https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/).
[52] Finkle, Jim, “U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage”, Reuters, January 8, 2016 (https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108).
[53] Goodin, Dan, “Microsoft president calls SolarWinds hack an “act of recklessness”, Ars Technica, December 18, 2020 (https://arstechnica.com/information-technology/2020/12/only-an-elite-few-solarwinds-hack-victims-received-follow-on-attacks/).

information at the political level,[54] i.e. head of A can tell head of B that cyber forces from A have breached B's power grid, which could lead to a greater incentive to codify international norms for state behavior in cyberspace.

The power advantage of larger states and superpowers could negate a possible cooperation between them and small states in cyberspace. The threshold for conducting OCOs is low, allowing small states to build their own cyber forces. That being said, it's not clear how a larger state would react to a small state conducting cyberespionage or worse, a cyberattack on the former's critical infrastructure. Schmitt argues that there is no legal or logical basis for distinguishing between a kinetic attack and a cyber attack when they have similar consequences and thus trigger an armed conflict.[55] Either way, small states should not play the security dilemma game because their normative power outweighs their military power. They should allow neither cyberespionage nor cyberattacks to become the norm. As mentioned, they benefit most from an open and peaceful system that protects their sovereignty and territorial integrity, and in which disputes are resolved in a legal manner.

3.2. Cyberattacks on critical infrastructure as internationally wrongful acts

Suppose a Small State A, suffers from a cyber attack on its power grid carried out by a cyber unit – XYZ, of an intelligence agency of a Larger State B. State A is member of a collective self-defence alliance WWW. It used to be part of the VVV alliance in which B was a major player. The countries have a cultural and historical connection. Do cyber attacks on critical infrastructure constitute an internationally wrongful act? An internationally wrongful act is a breach of an international obligation of a State and the conduct is attributable to the State under international law.[56] I examine possible violations of the principles of sovereignty, of non-intervention in a state's internal affairs and of prohibition of the threat or use of force.

3.2.1. Sovereignty

Article 2, paragraph 1 of the Charter of the UN states that: "1. The Organization is based on the principle of the sovereign equality of all its Members.", a provision further reiterated by the International Law Commission in its Draft Declaration on the Rights and Obligations of States: "Every State has the right to be legally equal to other State." States are equal and have an obligation, known as due diligence, which derives from the principle of sovereignty, to respect each other's sovereignty. Sic utere tuo ut alienum non laedas - use your own property in such a manner as not to injure that of another. By allowing OCO's to be conducted from its

[54] GGE 2013, supra note 33, p. 9.
[55] Schmitt, Michael N., "The Law of Cyber Warfare: Quo Vadis?," *Stanford Law & Policy Review*, 25 (2014), p. 290.
[56] ILC, "Draft articles on Responsibility of States for Internationally Wrongful Acts," *2001 Yearbook of the International Law Commission*, 2(2) (2001), Article 2

territory, a state violates this principle.[57] I hold the view, unanimously accepted by the experts who prepared the Tallinn Manual 2.0[58] that the prohibition on infringing sovereignty is a primary rule of international law. The violation of the sovereignty of other States constitutes an internationally wrongful act.

Suppose a cyber operation that causes physical damage resulting from manipulating a critical cooling system of a pipeline. The impact will be similar to a kinetic attack. Both are clear cases of sovereignty violation.[59] The more subtle case is when cyber operations lead to a temporary or permanent loss of functionality of cyber systems. The experts who contributed to The Tallinn Manual 2.0 agreed that permanent loss constitutes a breach of sovereignty with effects similar to armed attacks with physical damage. However, there is no consensus as to whether a temporary loss of functionality would violate the principle of sovereignty, much less whether attacks without damage or loss of functionality would violate it. A small state here should take a cautious approach to whether every cyberattack on its critical infrastructure is a breach of its sovereignty. The Czech Republic for example puts emphasis on whether the cyberattack causes: 1. death, injury or significant physical damage; 2. damage or disruption of an infrastructure with significant impact on national security; or its territory is used by a state A to attack state B.[60] For Romania, on the other hand, a violation of the principle of sovereignty means interfering with or preventing the State in any way from exercising its sovereign prerogatives.[61] It follows that the loss of functionality may not violate the Czech Republic's sovereignty, but a CNE would be enough for Romania to consider it an internationally wrongful act.

If they were to respond to the attack, they would have to adhere to the standard of reasonableness: "in order to attribute an act to the State, it is necessary to identify with reasonable certainty the actors and their association with the State".[62] This means that an attribution process must be initiated, ranging from a forensic analysis to analyzing all-source information to considering the political and legal circumstances surrounding the attack.[63] Even when applying the standard of reasonableness, the affected state can misattribute a cyberattack and its response to it can constitute an internationally wrongful act.[64] It is based

[57] Bannelier, K., & Christakis, T., *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, (Paris: Les Cahiers de la Revue Défense Nationale, 2017), p. 32.
[58] Tallinn Manual 2.0, *supra* note 41, commentary to rule 4, para 2 ('States shoulder an obligation to respect the sovereignty of other States as a matter of international law').
[59] Tallinn Manual 2.0, *supra* note 41, commentary to rule 4, para 11.
[60] Kadlčák, Richard, "Statement of the Special Envoy for Cyberspace and Director of Cybersecurity Department of the Czech Republic", 11 February 2020
[61] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021
[62] Kenneth P. Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R., 17 (1987) , p. 92, at pp. 101–102.
[63] Tallinn Manual 2.0, *supra* note 41, Chapter 4 Section 1, para 10.
[64] Tallinn Manual 2.0, *supra* note 41, Chapter 4 Section 1, para 12; see also ILC Articles on State Responsibility, Art 49 para 3 ("A State taking countermeasures acts at its peril, if its view of the question of wrongfulness turns out not to be well founded.")

on the assumption that states do not necessarily know everything that happens on their territory. Their response to a cyberattack launched from their territory should be that "of a Good government".[65] "States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory" is said in the 2015 GGE report.[66] Furthermore, states do not automatically bear responsibility and a link between a person or organization and the state should not be presumed.[67] Healy's proposed spectrum of responsibility presents a practical solution to the issue. Back to the scenario – Larger State B can fully cooperate with A and prosecute the perpetrators; it may be reluctant to cooperate; can hire non-state actors, carry out the attack with its cyber powers, or mix both. This would allow Small State A to better plan its response.[68]

As mentioned above, the impact of the cyber attack will determine the will to attribute it to the state ultimately responsible. It is therefore to be expected that attacks on CI that do not lead to any damage and loss of functionality or lead only to a temporary loss of functionality may not be attributed and there will be no response to them.

3.2.2. Non-intervention

The prohibition of intervention in the internal affairs of a state is a norm of customary international law. It was defined by the International Court of Justice (ICJ) in its judgment on the Nicaragua case. According to it: "A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."

In order for the Larger State B to be able to violate this non-intervention obligation, it must be proven in the attribution process that the cyber attack on the CI had the motive to change the foreign policy of the Small State A, namely to leave the WWW alliance. Or as suggested by Schmitt, the cyber operation should be so economically damaging that it would coerce A to vote in a certain way at the WWW meeting of heads of state.[69] This would constitute an

[65] ILC, "Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries", *2001 Yearbook of the International Law Commission*, 2(2) (2001), p. 155, §17.
[66] GGE 2015, *supra* note 34, p. 8.
[67] Corfu Channel, United Kingdom v Albania, Judgment, Merits, ICJ GL No 1, [1949] ICJ Rep 4, ICGJ 199 (ICJ 1949), 9th April 1949, United Nations [UN]; International Court of Justice [ICJ], p. 18.
[68] Healy, *Beyond Attribution,* p. 2-3.
[69] Schmitt, Michael, „Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attacks", Just Security, February 24, 2022 (https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks).

intervention in A's domaine resérvé - those "areas where States are free from international obligations and regulation",[70] which is foreign policy in this scenario.

However, an attack that would have severe impact on the economy and thus fit the loss of functionality hypothesis would certainly lead to a violation of the principle of sovereignty, which is enough to trigger a response.

It is difficult enough for A to prove that the cyberattack on its CI was carried out by ZYX, a cyber unit of one of B's intelligence agencies, let alone find evidence to suggest that B's motive was to change A's foreign policy thus violating the principle of non-intervention. The logical approach here for Small State A would be to turn to its allies on the WWW for assistance in: 1. mitigating the effects of the cyber attack; 2. attributing the attack to the responsible state. The WWW treaty would certainly make provision for such cases. This would correspond to the obligation in the GGE report of 2015: "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts taking into account due regard for sovereignty".[71]

3.2.3. Use of force

The cyberattack against CI of Small State A could qualify as unlawful use of force. Article 2, paragraph 4 of the UN Charter sets an obligation for states to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations" Scholars argue on whether the concept of force is limited to armed force only[72] or it can also apply to other use of force, e.g. cyber operations, when its impact is similar.[73] The ICJ states that generic terms are likely to evolve over time given that treaties are of continuing duration. As a result it is presumed that it was intended those terms to have an evolving meaning.[74] Cyber attacks resulting in physical damage of infrastructure, death or injury most certainly fit the definition of use of force. As with the principle of sovereignty, the question here is whether disruptive OCOs resulting in temporary loss of functionality are uses of force. It has been argued that cyberattacks whose disruption affects state security

[70] Ossoff, William, "Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace," *Harvard International Law Journal*, 62(1) (2021), p. 297.
[71] GGE 2015, *supra* note 34, p. 8.
[72] Dörr, Oliver, & Randelzhofer, Albrecht, "Article 2(4)," in *The Charter of the United Nations: A Commentary,* ed. Bruno Simma et al, (Oxford: Oxford University Press, 2012) 1, p. 208, para 16 ("The term ['force'] does not cover any possible kind of force, but is, according to the correct and prevailing view, limited to armed force.").
[73] Brownlie, Ian, *International Law and the Use of Force by States,* (Oxford: Oxford University Press, 1963), p. 362 ("[Art 2(4)] applies to force other than armed force"); Tallinn Manual 2.0, rule 69 ("A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.").
[74] Dispute Regarding Navigational and Related Rights, Costa Rica v Nicaragua, Judgment on the merits, ICGJ 421 (ICJ 2009), 13th July 2009, International Court of Justice [ICJ], p. 213, para 66.

significantly fall under the scope of use of force.[75] Such are attacks on critical infrastructure. Germany suggests a case-by-case approach when considering whether an OCO has violated the principle.[76] Norway's position is similar – a cyber operation may constitute use of force, even an armed attack, if its scale and effects are comparable.

Unlike the violation of the non-intervention principle, the violation of the prohibition on the use of force cannot be substituted by a violation of the principle of sovereignty. This is because the use of force is a prerequisite for invoking self-defence under Article 51 of the UN Charter. Even if the cyber attack in the scenario did not result in any damage, but only in disruption of the cyber infrastructure, and was nevertheless classified as use of force, the permitted response under self-defense is limited by the conditions of necessity and proportionality.[77] Again for an attack to constitute an internationally wrongful act it must be attributed to a state.

3.2.4. Conclusions

A cyber attack on CI that causes damage and costs lives violates all three principles of international law. The most important of them in connection with response is the principle of the prohibition on the use of force. An armed response to such an attack will be possible after invoking Article 51. An armed response to such an attack is possible by invoking Article 51. However, the prospects for this are unlikely since Small State A is member of the WWW alliance which has its collective defence norm. The most likely result of a cyber attack on the power grid is a disruption of the system, leading to a temporary loss of functionality. This scenario will only violate the sovereignty of the victim state. What will be the measured response?

4. Response

The response to a cyberattack depends on its impact. Mitigating the effects of a cyberattack on critical infrastructure is done by CERTs. As addressed earlier, EU and NATO member states are obliged to build their national capabilities to defend themselves against malicious cyber activities. The organizations have their own response teams. The NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU) signed a Technical Arrangement on Cyber Defense in 2016. The goals were to deepen cooperation between the organizations and enhance the cyber defences

[75] Roscini, Marco, *Cyber operations and the use of force in international law*, (New York: Oxford University Press, 2016), p. 55.
[76] Federal Government of Germany, 'On the Application of International Law in Cyberspace', Position Paper March 2021, p. 6.
[77] Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v United States, Merits, Judgment, (1986) ICJ Rep 14, ICGJ 112 (ICJ 1986), OXIO 88, 27th June 1986, United Nations [UN]; International Court of Justice [ICJ], para 194.

of both organisations by exchanging cyber defence-related data.[78] The European Union Agency for Cybersecurity (ENISA) assists national CSIRTs by its Maturity Framework. The Framework's goal is to enhance the capability to deal with cyberattacks. This includes "incident prevention, detection, resolution and quality management" not just "incident handling". In addition, ENISA's ICS-SCADA Maturity Framework focuses solely on enhancing ICS-SCADA security, which is vital for the management of critical infrastructures.[79]

The technical response to a cyber attack by CSIRTs is not examined in this paper. It is a matter of a future study. For the purpose of the research, I assume that in the event of a cyber attack on its critical infrastructure, a small state, member of the EU and NATO, will be supported by its allies in its incident response.

What are the legal options for Small State A, a member of NATO and the EU, which recently suffered from a cyber operation against its critical infrastructure? I analyze whether a state can resort to self-defense under Article 51 of the UN Charter or invoke Article 5 of the NATO treaty. What is the EU Cyber Diplomacy Toolbox?

4.1. Self-defense

According to Article 51 of the UN Charter, the minimum for a call for self-defense is an "armed attack". As already noted the prerequisite for resorting to self-defense is first, attributing the cyberattack to the attacker state so it can constitute an internationally wrongful act and second the OCO must have similar to armed use of force scale and effects. Under self-defense states may use force themselves which otherwise would constitute and internationally wrongful act.

LOAC does not specify what constitutes an act of war, but affirms that states have a right of self-defense. Two principles are taken into account when states resort to self-defense: necessity and proportionality. Necessity requires the existence of an armed attack, which can be ongoing or imminent. Lack of alternatives to an armed response is another core condition for the state of necessity (Gill & Ducheine, 2013). Next, the state of necessity, in accordance with article 25 of the International Law Commission (ILC) "Articles on the Responsibility of States for Internationally Wrongful Acts", must be invoked only to "safeguard an essential interest against a grave and imminent peril" and states should make sure that their self-defense act "does not seriously impair an essential interest of the other State concerned". The State wanting to resort to its right of self-defense "must not have contributed to the occurrence

[78] NATO, "NATO and the European Union enhance cyber defence cooperation", February 10, 2016 (https://www.nato.int/cps/en/natohq/news_127836.htm).
[79] ENISA, Analysis *of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*, 2015, Available at https://www.enisa.europa.eu/publications/maturity-levels.

of the state of necessity." Violating the sovereignty of a state, could be argued is an essential interest.

In this case the principle of proportionality addresses the force that can be used to respond and limits the scale, scope, duration and intensity of the defensive response (DeWeese, 2015).[80] Scholars argue that proportionality does not imply a "tit-for-tat" response, a response equivalent to the original attack. The reaction can be a mixture of cyber attack and kinetic attack .[81] It is not clear whether a small state can conduct a successful military operation in response to a damaging cyberattack on its CI. In this case proportionality should precisely mean "mathematical equivalency", i.e. responding to a cyberattack with a cyberattack. Interpreting the concept as Gil & Ducheine do fits powerful states that can punish the aggressor in ways that small states cannot, hence normalizing lethal responses to cyber activities.

Libicki suggests that cyberattacks should not be responded to with kinetic ones. This would be illegal. The rationale behind the Las Vegas Framework - what happens in cyberspace, stays in cyberspace - is that cyberattacks should not be carried out because they could provoke a kinetic reaction, which is more dangerous than the cyberattacks themselves. The uncertainty of attribution and the difficulty of proving the attacker's intentions are among the considerations supporting this argument. Furthermore, the notion that a state that is the victim of a cyberattack on its critical infrastructure will not respond with lethal use of force also influences the behavior of an attacker, who is considering between a cyberattack and a cyberattack, supported by a kinetic attack.[82]

The Las Vegas Framework can serve as a basis for normalizing state behavior in cyberspace. For example, the Larger State B will not respond with a kinetic attack on the Small State A hacking into B's power grid, a measure taken by A because B previously breached the ICS of A's critical infrastructure. But as mentioned earlier, states do not benefit from attacking each other's critical infrastructure. And the consequences of such actions are difficult to assess. The Las Vegas rule explicitly excludes kinetic response to a malicious cyber activity, deemed illegal. A cyber attack on critical infrastructure is also a violation of international law. If Small State A wants to comply with international law, the rule of Las Vegas and stay under the threshold of possible armed conflict, it would have to react disproportionately, e.g. by conducting a massive DDoS campaign against government sites of B, which should be

[80] DeWeese, Geoffrey S., "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence" in *7th International Conference on Cyber Conflict. Proceedings 2015*, ed. M.Maybaum, A.-M.Osula, L.Lindström, (NATO CCD COE Publications, April 2015), p. 86-87.
[81] Gill, Terry D., & Ducheine, Paul, A. L., „Anticipatory Self-Defense in the Cyber Context," *International Law Studies*, 30 (2013), p. 461.
[82] Libicki, *Cyberspace in peace and war*, pp. 641-643.

conducted in such a way that it would be difficult to attribute the attack to A. But then again is this kind of response proportional? If not, should it be accompanied by diplomatic measures?

4.2. NATO Article 5

Article 51 of the UN Charter gives states the right to an individual or a collective act of self defense. Article 5 of the NATO treaty prescribes that the use of force against an individual states constitutes an attack against all member, thus triggering the collective self-defense. Does Article 5 of the NATO Treaty apply in cyber space? "A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all."[83] What is a serious cyberattack? Jens Stoltenberg answers that "the level of cyberattack that would provoke a response must remain purposefully vague".[84] In accordance with this in the Brussels Summit Communiqué is stated in paragraphs 32 and 33 that a case-by-case approach will be applied when considering whether a cyberattack violated the prohibition of the use of force hence constituting an armed attack.[85] This position is reaffirmed by national positions of states such as Germany and Norway as cited above.

But why didn't the Czech Republic invoke Article 5 after attributing an explosion at an ammo depot that killed two people to a secret operation by a GRU unit? Instead, the Czech Republic responded by ordering 18 Russian diplomats to leave the country.[86] OCOs are somewhat similar to the ammo depot sabotage. In addition to the forensic analysis, an analysis of various intelligence sources is necessary in order to attribute the sabotage to the perpetrators and then connect them to the ultimately responsible state. Schmitt argues that the quantitative threshold, i.e. how high the number of victims or the damage caused, is unclear when describing an armed attack. But he points out that per the International Committee of the Red Cross (ICRC) "it makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces."[87] Thus, an armed conflict can ensue from deadly cyber operations (Schmitt 2015: 5). But the use of deadly force was not among the measures taken by the Czech Republic. The Czech Republic followed the example set by the United Kingdom, which expelled Russian diplomats in response to the poisoning of ex-spy Sergei Skripal in Salisbury. In both cases, the rest of NATO and the EU did the same in a

[83] NATO, "NATO will defend itself", August 27, 2019 (https://www.nato.int/cps/en/natohq/news_168435.htm).
[84] Atlantic Council, "Stoltenberg Provides Details of NATO's Cyber Policy", May 16, 2018 (https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy/)
[85] NATO, "Brussels Summit Communiqué", June 14, 2021 (https://www.nato.int/cps/en/natohq/news_185000.htm).
[86] RFE/RL, „A Look Back At The Deadly 2014 Czech Depot Blast That Prague Is Now Blaming On Russian Agents", April 18, 2021 (https://www.rferl.org/a/czech-republic-russia-depot-blast-gallery-expulsions/31209726.html).
[87] Pictet, Jean (ed), *Commentary: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces the Field*, (Geneva: ICRC, 1952), p. 20.

show of solidarity.[88] This is an example for classifying an act of violence, which essentially constitutes an armed attack against a sovereign nation, as a mere violation of sovereignty. It further raises suspicion about the possibility that a small state, even a NATO member, could use force in the event of a damaging cyberattack. Which leads to the question, what if the cyber attack is just disruptive but not damaging?

NATO member states can still act as one and response proportionally without having to invoke Article 5 by coordinating economic and diplomatic measures, shown by the above example. Response in the cyber domain is not to be excluded, too. This was stated in paragraph 31 of the Brussels Summit Communiqué and by the Secretary-General himself during Cyber Defence Pledge Conference in 2018.

4.3. EU Cyber Diplomacy Toolbox

In October 2017 the Council of the EU adopted a framework, known as Cyber Diplomacy Toolbox.[89] Its goal is to form a joint diplomatic response to malicious cyber activities in the ICT environment, deterring future attacks. The measures are organized in five different categories.

The first group is preventive measures. It can be roughly described as an attempt by the EU to extract its soft power in the cyber space – promoting OSCE CBMs, enhancing transparency, predictability and stability; conducting dialogues with other states and thus reducing risks of misperceptions and misunderstanding; capacity building in third countries by prosecuting cyber criminals and increasing response capacities.

The second group of measures is cooperative. The emphasis here is put on a diplomatic response to an ongoing cyber incident. EU-led political and thematic dialogues and EU-led diplomatic démarches may address the state from which the attack is stemming. This corresponds to the suggestion of the GGE 2015 report that states should respond to requests to mitigate malicious cyber activity aimed at the critical infrastructure. It is noted that this can be beneficial when there are no established bilateral channels between the victim state and the attacker state.

Stability measures are declarations made by various representatives of the EU. They address what state behavior in cyberspace the EU does not tolerate and what the consequences of malicious cyber activities would be. Statements intended to deter.

---

[88] Borger, Julian, Wintour, Patrick, & Stewart, Heather "Western allies expel scores of Russian diplomats over Skripal attack", The Guardian, March 27, 2018 (https://www.theguardian.com/uk-news/2018/mar/26/four-eu-states-set-to-expel-russian-diplomats-over-skripal-attack).

[89] General Secretariat of the Council, "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities", Brussels, October 9, 2017.

The substantial response is in groups four and five. Restrictive measures, i.e. economic sanctions, under Article 215 TFEU are acts of retorsion. They are unfriendly acts and do not violate international law.[90] The restrictive measures are implemented with the goal of changing a policy or activity of the attacker. Category five relates to a mutual support obligation between Member States in the event of a cyber attack. Countermeasures can be taken in addition to the diplomatic support outlined in groups two and three. However, they require that the cyberattack be attributed to a state because they are illegal per se. The possibility of a cyberattack triggering collective self-defense under Article 42(7), in accordance with Article 51 of the UN Charter, is also noted. Again, the cyberattack's scale and effects should be equivalent to that of an "armed aggression".

In 2019 the Council of the European Union adopted Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796. These legal documents specify the restrictive measures proposed in the Toolbox in response to a cyber attack. For example, if a cyber unit of a Larger State B's intelligence service conducts a cyberattack against Small State A's, member of the EU, critical infrastructure, the result of which is disruptive, not damaging (there is a temporary loss of functionality), all Member States will freeze "all funds and economic resources belonging to, owned, held or controlled by" natural or legal persons responsible for the attack. A travel ban will be issued, too.

The goal of the attribution process is to find the state which is ultimately responsible for a cyberattack. The state responsibility in this sanction regime seems irrelevant. The regulation focuses on who did the attack. This however doesn't mean that states cannot be sanctioned. Natural or legal persons, entities or bodies are object of the sanctions. These can be state officials, state banks, and state institutions. It is therefore to be expected that a severe cyberattack on a critical infrastructure would lead to them being sanctioned and thus to the attribution of the attack to the state.

4.4. Conclusions

Small states, members of NATO and EU, can rely on their allies when faced with the problem of attribution. Even if a cyberattack on their CI does not meet the threshold of an armed attack, thus triggering collective defense provisions, the organizations have their instruments to respond – countermeasures (expelling diplomats, conducting cyber operations in retaliation) and retorsion (economic sanctions). The possibility of a counterattack against the perpetrator in cyberspace cannot be ruled out. However, if a response is to be measured, small states should not resort to kinetic reactions. As they benefit the most from peaceful cyber space without malicious cyber activities, small states can use their membership in EU and NATO to focus on promoting preventative measures – CBMs, creating customary

[90] Tallinn Manual 2.0, *supra* note 41, rule 20, commentary 4.

international norms that regulate cyber space, diplomatic settlement of cyber incidents. In the meantime, they must improve their defense capabilities to increase the cost to perpetrators and deter them from attacking.

Bibliography

Alesina, Alberto, and Enrico Spolaore, *The Size of Nations*, (The MIT Press, 2003).

Andrew K. Rose, *Like Me, Buy Me: The Effect of Soft Power on Exports*, (NBER Working Papers 21537, National Bureau of Economic Research, Inc, 2015).

Bannelier, K., & Christakis, T., *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, (Paris: Les Cahiers de la Revue Défense Nationale, 2017).

Brownlie, Ian, *International Law and the Use of Force by States*, (Oxford: Oxford University Press, 1963).

Corfu Channel, United Kingdom v Albania, Judgment, Merits, ICJ GL No 1, [1949] ICJ Rep 4, ICGJ 199 (ICJ 1949), 9th April 1949, United Nations [UN]; International Court of Justice [ICJ].

Daniel, Michael, "Closing the Gap: Expanding Cyber Deterrence," in *New Conditions and Constellations in Cyber*, ed. Alexander Klimburg, (The Hague: The Hague Centre for Strategic Studies, 2021), pp. 152-162.

David Vital, *The Inequality of States: A Study of the Small Power in International Affairs* (Oxford: Clarendon Press, 1967).

DeWeese, Geoffrey S., "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence" in *7th International Conference on Cyber Conflict. Proceedings 2015*, ed. M. Maybaum, A.-M. Osula, L. Lindström, (NATO CCD COE Publications, April 2015), pp. 81-92.

Dispute Regarding Navigational and Related Rights, Costa Rica v Nicaragua, Judgment on the merits, ICGJ 421 (ICJ 2009), 13th July 2009, International Court of Justice [ICJ].

Dörr, Oliver, & Randelzhofer, Albrecht, "Article 2(4)," in *The Charter of the United Nations: A Commentary*, ed. Bruno Simma et al, (Oxford: Oxford University Press, 2012) 1.

Fazal, T. M., & Griffiths, R. D., "Membership has its privileges: The changing benefits of statehood," *International Studies Review*, 16(1) (2014), pp. 79-106.

Federal Government of Germany, 'On the Application of International Law in Cyberspace', Position Paper, March 2021.

General Secretariat of the Council, "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities", Brussels, October 9, 2017.

Gill, Terry D., & Ducheine, Paul, A. L., „Anticipatory Self-Defense in the Cyber Context," *International Law Studies*, 30 (2013), pp. 438-471.

Goldblat, Jozef, *Arms Control: The New Guide to Negotiations and Agreements*, 2nd edn, (London: SAGE Publications Ltd, 2002).

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 2013, A/68/98, 24 June 2013.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 2015, A/70/174, 22 July 2015.

Handel, M., *Weak states in the international system*, (Totowa, NJ: Frank Cass, 1981).

Hathaway, Melissa, "When Violating the Agreement Becomes Customary Practice" in *Getting Beyond Norms: New Approaches to International Cyber Security Challenges*, ed. Fen Osler Hampson and Michael Sulmeyer, (Waterloo, ON, CA: Centre for International Governance Innovation, 2017), pp. 5-13.

Healy, Jason, Beyond Attribution: Seeking National Responsibility for Cyber Attacks, (Washington, DC: Atlantic Council of the United States, 2012).

ILC, "Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries," *2001 Yearbook of the International Law Commission*, 2(2) (2001).

ILC, "Draft articles on Responsibility of States for Internationally Wrongful Acts," *2001 Yearbook of the International Law Commission*, 2(2) (2001).

Ingebritsen, C., "Norm entrepreneurs: Scandinavia's role in world politics," *Cooperation and Conflict*, 37(1) (2002), pp. 11-23.

J. A. R. Marriott, *Federalism and the Problem of the Small State* (London: Allen and Unwin, 1943).

Kadlčák, Richard, "Statement of the Special Envoy for Cyberspace and Director of Cybersecurity Department of the Czech Republic", 11 February 2020.

Karns, M. P., Mingst, K. A., Stiles, K. W., *International organizations*, 3rd edn, (Boulder, CO: Lynne Rienner, 2015).

Kenneth P. Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R., 17 (1987).

Keohane, Robert O, "Lilliputians' Dilemmas: Small States in International Politics," I*nternational Organization*, 23(2) (1969), pp. 291-310.

Lake, D.A., *Hierarchy in International Relations*, (Ithaca, NY: Cornell University Press, 2009).

Libicki, M. C., *Cyberspace in peace and war*, 2nd edn, (Annapolis, Maryland: Naval Institute Press, 2021).

Libicki, Martin C. "Norms and Normalization," *The Cyber Defense Review*, 5(1) (2020), pp. 41-54.

Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v United States, Merits, Judgment, (1986) ICJ Rep 14, ICGJ 112 (ICJ 1986), OXIO 88, 27th June 1986, United Nations [UN]; International Court of Justice [ICJ].

Nye, J. S. (1990), "Soft power," *Foreign Policy*, 80, pp. 153-171.

Nye, J. S., "Normative Constraints on Cyber Arms," in *Getting Beyond Norms: New Approaches to International Cyber Security Challenges*, ed. Fen Osler Hampson and Michael Sulmeyer, (Waterloo, ON, CA: Centre for International Governance Innovation, 2017), pp. 19-23.

Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021.

Ossoff, William, "Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace," Harvard *International Law Journal*, 62(1) (2021), pp. 295-322.

Pictet, Jean (ed), *Commentary: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces the Field*, (Geneva: ICRC, 1952).

Rid, Thomas, & Buchanan, Ben, "Attributing Cyber Attacks," *Journal of Strategic Studies*, 38 (1–2) (2015), pp. 4-37.

Roscini, Marco, *Cyber operations and the use of force in international law*, (New York: Oxford University Press, 2016).

Schmitt, Michael N., "The Law of Cyber Warfare: Quo Vadis?," *Stanford Law & Policy Review*, 25 (2014), pp. 269-300.

Schmitt, Michael N., ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge, UK: Cambridge University Press, 2017) (hereinafter Tallinn Manual 2.0).

Singer, P. W., & Friedman, A., *Cybersecurity and Cyberwar: What everyone needs to know*, (Oxford: Oxford University Press, 2014).

T. G. Masaryk, The *Problem of Small Nations in the European Crisis* (London: University of London, Athlone Press, 1966).

Thorhallsson, B., & Steinsson, S, "Small State Foreign Policy," *Oxford Research Encyclopedia of Politics* (2017).

Waltz, K. N., *Theory of international politics*, (Reading, Mass: Addison-Wesley Pub. Co., 1979).

Whyte, C., & Mazanec, B. M., *Understanding cyber warfare: Politics, policy and strategy*, (London; New York: Routledge, 2019).

Links

Atlantic Council, “Stoltenberg Provides Details of NATO’s Cyber Policy”, May 16, 2018 (https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy/)

Baldin, Anna, “EU: Towards the adoption of the NIS 2 Directive”, DataGuidance, December 2021, (https://www.dataguidance.com/opinion/eu-towards-adoption-nis-2-directive).

Borger, Julian, & Wintour, Patrick, & Stewart, Heather “Western allies expel scores of Russian diplomats over Skripal attack”, The Guardian, March 27, 2018 (https://www.theguardian.com/uk-news/2018/mar/26/four-eu-states-set-to-expel-russian-diplomats-over-skripal-attack).

Council on Foreign Relations, “Why Are There No Cyber Arms Control Agreements?”, January 16, 2018 (https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements).

ENISA, *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*, 2015, Available at https://www.enisa.europa.eu/publications/maturity-levels.

ENISA, *Critical Infrastructures and Services*, Retrieved on 25.04.2022 from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.

ENISA, *ENISA CSIRT MATURITY FRAMEWORK*, 2022, Available at https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework.

ENISA, NIS Directive, Retrieved on 25.04.2022 from https://www.enisa.europa.eu/topics/nis-directive.

European Parliament, “The NIS2 Directive: A high common level of cybersecurity in the EU”, December 1, 2021 (https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333).

Finkle, Jim, “U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage”, Reuters, January 8, 2016 (https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108).

Goodin, Dan “Microsoft president calls SolarWinds hack an “act of recklessness”, Ars Technica, December 18, 2020 (https://arstechnica.com/information-technology/2020/12/only-an-elite-few-solarwinds-hack-victims-received-follow-on-attacks/).

Government of Canada, *National Strategy for Critical Infrastructure*, 2009 (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx).

Grauman, Brigid. “Cyber-security: The Vexed Question of Global Rules,” Security Defence Agenda and McAfee, February 2012, Available at (https://www.files.ethz.ch/isn/139895/SDA_Cyber_report_FINAL.pdf).

IBM, “What is a cyber attack?” (https://www.ibm.com/topics/cyber-attack).

Lin, Herbert, „Attribution of Malicious Cyber Incidents: From Soup to Nuts“, Journal of International Affairs, March 9, 2017 (https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents).

NATO, “Brussels Summit Communiqué”, June 14, 2021 (https://www.nato.int/cps/en/natohq/news_185000.htm).

NATO, “NATO and the European Union enhance cyber defence cooperation”, February 10, 2016 (https://www.nato.int/cps/en/natohq/news_127836.htm).

NATO, “NATO will defend itself”, August 27, 2019 (https://www.nato.int/cps/en/natohq/news_168435.htm).

NATO, Cyber Defence, March 23, 2022 (https://www.nato.int/cps/en/natohq/topics_78170.htm).

Oladimeji, Saheed, & Kerner, Sean Michael, „SolarWinds hack explained: Everything you need to know“, TechTarget, June 16, 2021 (https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know).

RFE/RL, „A Look Back At The Deadly 2014 Czech Depot Blast That Prague Is Now Blaming On Russian Agents“, April 18, 2021 (https://www.rferl.org/a/czech-republic-russia-depot-blast-gallery-expulsions/31209726.html).

Schmitt, Michael, „Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attacks“, Just Security, February 24, 2022 (https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks).

The Aspen Institute’s Cybersecurity Group published elaborating on this concept: “An Operational Collaboration Framework.” Aspen Cybersecurity Group, November 2018 (https://www.aspeninstitute.org/publications/an-operational-collaboration-framework/).

The White House, Office of the Press Secretary, *Executive Order -- Improving Critical Infrastructure Cybersecurity,* February 12, 2013 (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity).

United States Department of Defense. “The Definition of Cyberspace.” Deputy Secretary of Defense Memorandum (May 12, 2008), Retrieved on 25.04.2022 from https://www.gao.gov/assets/a321824.html.

Wolter, Detlev, “The UN Takes a Big Step Forward on Cybersecurity”, Arms Control Asssociation, (https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity).

Zetter, Kim, “An Unprecedented Look at Stuxnet, the World's First Digital Weapon”, Wired, November 3, 2014 (https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/).

Zetter, Kim, „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid“, Wired, March 3, 2016 (https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/).