Chapter 1: Current State of the International Legal Discourse on Cyber Harm

To assess the current state of the international legal discourse regarding cyber threats it is important to understand the nature of cyber threats. Hence, the following section first outlines popular categorical terms for cyber operations before the concept of cyber harm which this study uses is introduced. The study then gives an overview of the current state of the international legal discourse on cyber harm.

A. Popular categories of malicious cyber operations

Both in the international legal discourse, as well as in media reports, a variety of incidents are reported as 'cyber' incidents, making 'cyber' something of a modern buzzword for any operation that involves the use of a computer system or the internet. In particular, categorical terms based on the intention or the affiliation of the attacker are popular. As outlined in the following, such categories are frequently imprecise and hence need to be approached with caution from the legal perspective.

I. Cyber espionage

Various cyber operations have the purpose to access and exfiltrate confidential information via cyber means. Operations for this purpose are traditionally labelled cyber espionage.[1] Cyber espionage operations are typically

1 Russell Buchan, 'The International Legal Regulation of Cyber Espionage', in Anna Maria Osula/Henry Rõigas (eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016), 65–86, at 65: 'Espionage is a prevalent method of gathering intelligence and describes 'the consciously deceitful collection of information, ordered by a government or organisation hostile to or suspicious of those the information concerns, accomplished by humans unauthorised by the target to do the colleting.'; Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), commentary to rule 32, p. 168, para. 2: 'Cyber espionage involves, but is not limited

distinguished into two main categories. Espionage operations conducted by states for intelligence gathering – so-called 'political espionage' – and espionage operations by private actors for commercial reasons – so-called 'economic cyber espionage'. Noteworthy examples of political espionage include the *SolarWinds* operation, infiltrating inter alia the US Ministry for Nuclear Safety and the Defence Ministry in 2020[2], or the hack of the German parliament (Bundestag) in 2015 which compromised the servers of a significant number of parliamentarians.[3] Other espionage operations cannot always be neatly allocated to one of the two categories. For example, the allegedly state-sponsored vaccine espionage operations targeting vaccine research during the Coronavirus SARS-CoV-2 (COVID)-pandemic[4] was arguably conducted for both political as well as economic purposes.

Cyber espionage operations typically affect the confidentiality of information on information and communications technology (ICT) systems and networks but usually do not affect the integrity of data or cause disruption. It is often in an attacker's interest that the intrusion remains undetected so that exfiltration of information can continue as long as possible. On the technical level, cyber espionage is hence arguably the least intrusive mode of malicious cyber operations.[5] Nevertheless, it is important to note that it can have severe harmful effects: The exfiltration of classified information via cyber espionage can for example affect national security. Theft of intellectual property can cause great financial damage. Cyber espionage operations can also greatly interfere with the privacy of individuals.[6] Furthermore, once an attacker gains access to an ICT system

---

to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information.'.

2 David E. Sanger/Nicole Perlroth/Eric Schmitt, '*Scope* of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit', *New York Times,* 9 September 2021, available at: https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

3 'Data stolen during hack attack on German parliament, Berlin says', *DW News*, 29 May 2015, available at: https://www.dw.com/en/data-stolen-during-hack-attack-on-german-parliament-berlin-says/a-18486900.

4 Dan Sabbagh/Andrew Roth, 'Russian state-sponsored hackers target Covid-19 vaccine researchers', *Guardian* 16 July 2020, available at: https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers.

5 Luke Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law* 20 (2019), 349–377, 359, 360.

6 Anne Peters, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II', *EJIL:Talk!*, 4 November 2013, available at: https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/; UN General

during a cyber espionage operation it may only be the first step before the attacker wreaks further havoc, e.g. by altering or deleting data.[7] States are hence increasingly concerned about cyber espionage in international relations.[8]

II. Cyber terrorism

In the public and international legal discourse the term cyber terrorism is repeatedly used. Although a uniform definition does not exist cyber terrorist attacks are characterized by the intent of the attacker to spread fear and intimidation among the civilian population, through the cyber-induced occurrence of significant harm to physical objects or injury or death to individuals.[9] Both the UN Group of Governmental Experts (UN GGE) Reports 2021 as well as a 2017 UN Security Council Resolution acknowledged the threat of cyber terrorist attacks against critical infrastructure.[10] The risk

---

Assembly Resolution A/RES/68/167, 18 December 2013: 'Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights (…)'.

7 Przemysław Roguski, '*Violations of Territorial Sovereignty in Cyberspace – an Intrusion-Based Approach,*' in: Dennis Broeders/Bibi van den Berg (eds.), *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield 2020), 65–84, at 75, 76; see also below chapter I.C.I.

8 See in more detail chapter 3.C.IV.

9 Along these lines Irina Rizmal, 'Cyberterrorism: What are we (not) talking about?', *Diplo,* 3 August 2017, available at: https://www.diplomacy.edu/blog/cyberterrorism-what-are-we-not-talking-about :'For an attack to constitute an act of terrorism, it must also have a serious intended effect in terms of human and economic casualties or intense fear and anxiety – terror – among citizens'.

10 United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), para. 13: 'The Group reaffirms that the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security'; reiterating United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), A/70/174, 22 July 2015 (UN GGE Report 2015), para. 6; with regard to protection of critical infrastructure UN Security Council Res. 2341, 13 February 2017: 'Recognizing that protection efforts entail multiple streams of efforts, such as (…) cybersecurity'. See also generally

of cyber terrorist activities was also highlighted in a UN Office for Drugs and Crime (UN ODC) report.[11]

Yet, the label cyber terrorism is frequently overused. Terrorist groups have so far not shown great interest in malicious cyber operations.[12] No cyber terrorist attack has yet occurred that would fit the characteristic features of cyber terrorism – which is the causation of severe cyber-induced damage to spread fear and intimidation among the civilian population.[13] While e.g. the targeting of several Israeli websites, e.g. of the national airline and the disclosure of credit card details of Israeli citizens in 2012 were likened to cyber terrorism[14] the operation fell short of causing widespread fear, or severe casualties. Furthermore, activities like disseminating terrorist content, recruiting for and financing of terrorist organization, such as al-Qaida, via cyberspace are often misleadingly framed as cyber terrorism.[15] Even if such activities are eventually conducted for terrorist purposes they merely utilize cyberspace but do not attack it.[16] The label 'cyber' terrorism hence frequently does not fit. Due to this potential for misunderstanding this study uses the term cyber terrorism only cautiously.

---

on the subject International Law Association, *Study Group on Cybersecurity, Terrorism, and International Law,* 31 July 2016.

11 United Nations Office on Drugs and Crime (UN ODC), *The use of the Internet for terrorist purposes* (United Nations 2012).

12 David P. Fidler, 'Cyberspace, Terrorism and International Law', *Journal of Conflict & Security Law* 21 (2016), 475–493, at 478.

13 Rizmal, 'Cyberterrorism' 2017 (n. 9).

14 UN ODC, 'The Use of the Internet' 2012 (n. 11), 12.

15 See already James Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', Center for Strategic and International Studies, 2002, p. 4; also critical on this expansive use of the term Rizmal, 'Cyberterrorism' 2017 (n. 9): '[T]he label 'cyberterrorist' in the political discourse has mainly been applied to actors and organisations already framed as terrorist, despite recognising that these actors have not yet carried out activities that could be labelled as cyberterrorism'.

16 On the distinction between operations attacking the confidentiality, integrity and availability of ICT and operations merely utilizing ICT for other malicious purposes see below chapter 1.B.III.

III. Cyber war

The threat of a looming cyberwar has dominated the international legal discourse for a significant amount of time.[17] Bolstering the cyberwar narrative both the NATO and the US have defined cyberspace as the fifth domain of warfare[18] – regardless of the fact that cyberspace is a fictitious notion as you cannot 'go into' cyberspace.[19] While operations in cyberspace have become an important operational field during armed conflict – as the war in Ukraine after the Russian invasion in February 2022 shows[20] – so far, a cyber war in the sense of an armed confrontation primarily conducted by cyber means has not yet occurred and it seems unlikely that this will change in the future.[21]

In order to amount to a forceful confrontation a cyber operation would need to amount to a prohibited use of force prohibited under Art. 2 (4) of the Charter of the United Nations (UN Charter) which would be the case if it is comparable in 'scale and effects' comparable to kinetic attacks.[22] Some operations have likely reached this threshold, such as the *Stuxnet* operation

17 See above Introduction; see the extensive amount of literature on cyberwar, e.g. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press 2013), Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Intersentia 2014); Julia Dornbusch, *Das Kampfführungsrecht im internationalen Cyberkrieg* (Baden-Baden: Nomos 2018); Sven-Hendrik Schulze, *Cyber-»War« – Testfall der Staatenverantwortlichkeit* (Tübingen: Mohr Siebeck 2015); Li Zhang, 'A Chinese Perspective on Cyber War', *International Review of the Red Cross* 94 (2012), 801–807.

18 On the character of cyberspace as a domain of warfare and the function of this 'foundational metaphor' serving particular interests within the US military, e.g. with regard to the establishment of the US Cyber Command, Jordan Branch, 'What's in a Name? Metaphors and Cybersecurity', *International Organization* 75 (2021), 39–70, at 48.

19 Also critical of the characterization of cyberspace as a domain of warfare François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 11.

20 During the Russian invasion of Ukraine cyber operations were primarily used to demoralize and spread disinformation, see Friedel Taube, 'Russia-Ukraine conflict: What role do cyberattacks play?', *Deutsche Welle*, 28 February 2022, available at: https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572.

21 Thomas Rid, *Cyber Will Not Take Place*, (London: Hurst 2017).

22 Harold Hongju Koh, 'International Law in Cyberspace', *Harvard International Law Journal* 54 (2012), 4.

against Iran in 2010 which disabled centrifuges in a nuclear enrichment facility in Natanz and arguably could have led to casualties, or the *Black Energy* operation against Ukraine which disabled part of a Ukrainian region's electricity grid.[23] Yet, such operations were singular cyber operations and did not lead to an ongoing armed confrontation primarily conducted via cyberspace.

Nevertheless, the term cyber war is invoked in an inflationary manner in situations which clearly fall short of an armed confrontation between states. The *SolarWinds* operation – an espionage operation lacking any destructive effect – has e.g. been likened to an act of cyber war.[24] Also the interference in the US presidential election in 2016 and potentially *any* form of state-sponsored cyber misconduct have been framed as an act of cyber war.[25] Such examples show that in the political discourse the term 'cyberwar' has become a placeholder for mere cyber confrontation or conflicts of states, conducted in cyberspace.[26] From a legal perspective the notion of cyber war hence needs to be approached with great caution as well.

IV. Cyber attack

Closely connected to the notion of cyber war is the notion of cyber attack. The Tallinn Manual defines the term as cyber operations that cause 'injury or death to persons or damage or destruction to objects'.[27] Such a definition of the term hence limits it to acts which likely amount to a use of force. Other definitions have a broader scope: *Brown* and *Tullos* for example

23 See in more detail on a violation of the prohibition of the use of force chapter 3.B.I.

24 Yevgeny Vindman, 'Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is', *JustSecurity*, 26 January 2021, available at: https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it.

25 Jordan Robertson/Laurence Arnold, 'Cyberwar: How Nations Attack Without Bullets or Bombs', *Washington Post*, 14 December 2020, available at: https://www.washingtonpost.com/business/energy/cyberwar-how-nations-attack-without-bullets-or-bombs/2020/12/14/878f2e88-3e43-11eb-b58b-1623f6267960_story.html.

26 Leonhard Kreuzer, 'Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen', in Ines-Jacqueline Werkner/Niklas Schörnig (eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (Wiesbaden: Springer 2019), 63–86, at 69.

27 Schmitt, 'Tallinn Manual 2.0' 2017 (n.1), rule 92.

define cyber attacks as any cyber operation that causes physical damage[28], without indicating that a particular threshold of physical damage needs to be met. Even broader, France employs the term for any kind of hacking.[29] Other commentators have included the motivation of a malicious actor as a decisive element for a characterization as a cyber 'attack'.[30] Due to these largely divergent understandings using this term can likely lead to misunderstandings.[31] This study will hence also avoid it to the largest extent possible.

V. Cybercrime

Cybercrime operations are typically pursued by private actors for economic gain. The term is usually not used for state-sponsored cyber operations.[32] Examples of cybercrime operations are the ransomware attacks against the meat-processing company JBS in July 2021 by the cybercrime group REVil[33] or the theft of research data on COVID vaccines from an Oxford University research institute by a cybercrime group in February 2021.[34]

Cybercrime is a broad term that covers a variety of activities conducted against or via ICT for economic gain. The most popular means of cybercrime are operations which infiltrate or disrupt the orderly functioning of computer systems and networks via technical means – i.e. so-called 'hacking'.[35] But the cybercrime offences under cybercrime treaties also include

28 Gary D. Brown/Owen W. Tullos, 'On the Spectrum of Cyberspace Operations', *Small Wars Journal*, 11 December 2012, available at: https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.

29 France, Strategic Review of Cyber Defence, 2018, p. 4.

30 Oona Hathaway et al, 'The Law of Cyber Attack', *California Law Review* 100 (2012), 817–885, 836f.

31 Also arguing for caution with regard to the term Michael N. Schmitt, 'Terminological Precision and International Cyber Law', *Articles of War,* 29 July 2021, available at: https://lieber.westpoint.edu/terminological-precision-international-cyber-law/.

32 Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), 20.

33 On the operation against JBS see the list of significant cyber incidents and the entries for May 2021 available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

34 The group subsequently sold the acquired data internationally, see ibid. in the entries for February 2021.

35 In more detail on 'hacking' and the concept of cyber harm see below chapter 1.B.

content-related offences, such as propaganda, or copyright-related offences, or computer-related offences, e.g. electronic fraud.[36] The term cybercrime hence carries a certain ambiguity. On the one hand, it is very broad and even includes offences which are merely conducted via cyberspace. On the other hand, it excludes state-sponsored cyber operations. As cybercrime is an established legal term, in particular employed by cybercrime treaties, this study will refer to cybercrime when suitable, albeit mindful of its definitional complexity.

VI. Imprecision of categorical terms

The above-mentioned examples show that popular terms for categorizing cyber operations have to be approached with caution. In particular, the terms cyber terrorism, cyber war and cyber attack are not based on a precise legal distinction but cover a wide variety of activities which deviate if and how they target ICT systems and networks. Only the term cyber espionage grasps activities that largely resemble one another on the technical level. For all categories the main distinguishing criterion is an attacker's motivation or affiliation.[37] As the preventive approach requires diligence measures against 'all hazards'[38], regardless of motivation or affiliation of an attacker, it is consequent that this study will largely avoid such motivation-based terminology. It will only refer to cyber espionage and cybercrime operations when suitable and more frequently refer to the neutral term 'cyber operations' or 'cyber incidents'[39], as well as to the umbrella notion 'cyber harm'. This notion is introduced in the following.

---

36 The Budapest Convention on Cybercrime distinguishes between four categories of cybercrime: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; copyright-related offences; see in more detail chapter 4.D.I; see also ITU, *Understanding cybercrime: Phenomena, challenges and legal Response* (ITU 2012), 12.

37 Lahmann, 'Unilateral Remedies' 2020 (n.32), 19.

38 Eneken Tikk/Kadri Kaska/Liis Vihul, International Cyber Incidents – Legal Considerations (NATO CCDCOE 2010), p. 10; Stein Schjolberg/Solange Ghernaouti-Hélie, *A Global Treaty on Cybersecurity and Cybercrime* (2nd edition, Oslo: AiTOslo 2011), p. 32.

39 Nevertheless, with regard to some categories of cyber harm the motivation of the attacker is at least a relevant factor to be taken into account, e.g. with regard to the intent to coerce under acts amounting to a prohibited intervention, see chapter 3.B.II.

B. The concept of cyber harm

I. Cyber harm as exploitation of code vulnerability

From cyber war, to cybercrime, to cyber terrorism to cyber espionage – on the core technical level all such cyber operations largely look alike: They exploit vulnerabilities in the design of ICT. ICT hardware, software and networks, including the internet, operate via code. Such code – often a line of millions of 1's and 0's[40] – inevitably entails errors which attackers can use to gain entry to a computer system or control a computer or data stored on it. Errors in code hence open the door to the compromising of the so-called 'CIA triad'. The CIA triad protects the confidentiality (C), integrity (I) and the availiability (A) of ICT systems and networks: Confidentiality protects against unauthorized access of the data stored in ICT systems and networks.[41] Integrity means that the stored data is complete and not improperly modified.[42] Availability means that authorized users should be able to access data upon request.[43] The compromising of one or several aspects of the CIA triad[44] is typically called 'hacking'. It is what this study understands as 'cyber harm'. Cyber harm is hence a broad umbrella term that largely grasps the activities traditionally framed under the above-mentioned categorical terms.[45]

II. Means of causing cyber harm

The exploitation of code vulnerabilities typically occurs through various stages. Attackers often first identify targets and vulnerabilities (so-called

40 Ryan Dube, 'What Is Binary Code and How Does It Work?', Lifewire, 2 March 2022, available at: https://www.lifewire.com/what-is-binary-and-how-does-it-work-4692749.

41 Chad Perrin, 'The CIA Triad', *TechRepublic,* 30 June 2008, available at: https://www.techrepublic.com/article/the-cia-triad/.

42 Josh Frühliner, 'The CIA triad: Definition, components and examples', *CSO Online*, 10 February 2020, available at: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.

43 Ibid.

44 If e.g. an attacker erases data all three aspects of the CIA triad are compromised: The erased data was accessed without authorization, was improperly modified and as a consequence is not accessible upon request anymore.

45 See above chapter 1.A.I–VI.

reconnaissance phase[46]), such as through probing or mapping[47], before they move towards exploiting found vulnerabilities by infiltrating a server and potentially taking control of it.[48] The most common tool which is used to compromise the CIA of ICT is malware. Malware is a catch-all term for different kinds of software designed to harm or exploit a computer, server or computer network, whether it is a virus, a worm, a Trojan horse, or ransomware.[49]

While a comprehensive list of various types of malware is not feasible, suffice it to highlight several particularly prominent types of malware that are repeatedly mentioned in the legal and political discourse and in the course of this study: 'Trojan horses' and more generally 'spyware' are often used to gain access to and copy data. They are hence regularly used for espionage purposes. 'Ransomware' is an increasingly popular tool for cybercriminals to extort money from victims. This type of malware encrypts data on the victim's hard drive; in order to regain access to the data the attacker demands payment of a ransom. Ransomware operations are hence akin to digital extortion. Another popular attack mode is a Distributed Denial of Service attack (DDoS) by which an attacker gains control over a huge number of infiltrated servers. Using this 'botnet' of infiltrated 'zombie' servers the attacker sends so many mass requests to a targeted server that the latter collapses.[50] While such operations primarily exploit vulnerabili-

46 Roguski, 'Territorial Sovereignty' 2020 (n. 7), 75.

47 Woltag, 'Cyber Warfare' 2014 (n. 17), 28.

48 On the seven stages of so-called cyber kill chains see Eric Hutchins/Michael J. Cloppert/Rohan M. Amin, 'Reconnnaisance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Action on objective', in *Information Warfare & Security Research* 1 (2011), 1–14, at 5; see also Roguski, 'Territorial Sovereignty' 2020 (n. 7).

49 Microsoft, Robert Moir, *Defining Malware*, 2009; ITU Toolkit for Cybercrime Legislation, February 2010, section 1(n), p. 12, 13: 'malware may be defined as a program that is inserted into a computer program or system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the computer program, data or system.'; see the definition of malware by Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), glossary, 2.0, 566: 'Software' [that] may be stored and executed in other software, firmware, or hardware that is designed adversely to affect the performance of a computer system. Examples of malware include Trojan horses, 'rootkits', 'viruses' and 'worms'.'; Woltag, 'Cyber Warfare' 2014 (n. 17), 28.

50 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), glossary, 2.0, 565: '[DDoS is a] technique that employs multiple computing devices (e.g., computers or smartphones), such as the bots of a 'botnet' (...)), to cause a 'denial of service' [i.e. the non-availability of computer system resources to their users, addition by the author] to a single or multiple targets.'.

ties of the 'zombie' servers they simultaneously affect the availability of information on the targeted servers.[51]

Beyond these examples other forms of exploitation of vulnerabilities via malware are conceivable. For this reason the Convention on Cybercrime of the Council of Europe (CoE) – the so-called 'Budapest Convention' – deliberately entails broad offences which focus on the *effect* on the victim's ICT, instead of naming the use of specific forms of malware as offences.[52] Due to this effect-dependency the offences stipulated by various cybercrime treaties are adaptable to unknown, new types of malware.[53]

III. Exclusion: Human error, social engineering and content harm

The CIA triad is not only compromised through the exploitation of code via malware. Often, it is facilitated or enabled by human error. ICT users for example often use insecure passwords that can be guessed, or fall prey to so-called social engineering attacks. Social engineering can trick victims into entering passwords or other confidential information, e.g. by sending so-called phishing emails. With the acquired information attackers can subsequently gain access to a system or network in a subsequent step and hereby compromise the CIA triad. Many attackers consider social engineering attacks even more efficient than gaining access via purely technical means.[54] From the preventive perspective of this study the compromising of the CIA triad via social engineering is distinct as it involves active

51 Cybercrime Convention Committee (T-CY), T-CY Guidance Note, T-CY (2013)29, 8 October 2013, p.7.

52 The Council of Europe Convention on Cybercrime, 23 November 2001, ETS 2001, No. 185, stipulates the following broad offences: Illegal access (Art. 2), illegal interception (Art. 3), system interference (Art. 4), data interference (Art. 5); see in more detail chapter 4.D.I.

53 Cybercrime Convention Committee, T-CY (2013)29, 8 October 2013, p. 17: 'The numbers and variety of forms of malware are so vast that it would not be possible to describe even currently-known forms in a criminal statute. The Cybercrime Convention deliberately avoids terms such as worms, viruses, and trojans. Because fashions in malware change, using such terms in a Convention would quickly make it obsolete and be counterproductive.'

54 A cyber operation against a German steel mill was e.g. facilitated by social engineering, see on this e.g. Allianz Global Corporate & Specialty, *Cyber attacks against critical infrastructure*, available at: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

recklessness on the side of the victim. It is hence excluded from this study's notion of cyber harm.

The study's notion of cyber harm also excludes offences which are committed via the means of a computer but do not target the CIA of ICT itself. Such malicious activities committed via the help of the internet are e.g. terrorist propaganda, hate speech or child pornography, or dissemination of 'fake' news'. The dissemination of disinformation during the COVID-pandemic, the interference in the US presidential elections in 2016 and 2020, or online hate speech against the Rohingya in Myanmar were e.g. frequently discussed as 'cyber' attacks or cyber harm.[55]

Yet, in these constellations ICT is only the means by which harm is amplified and disseminated but it is *not* the actual target itself. Using cyberspace to disseminate information leaves the CIA of ICT fully intact. The target is rather the human perception. Such content-based security risks are hence of a fundamentally different character than the ICT-vulnerability based notion of cyber harm.[56] While there is broad consensus on the illegitimacy and illegality of hacking it is far more contested which content is considered harmful in the international order. Deeming information harmful (or socially or politically destabilizing) has the risk to be abused by authoritarian governments to curb political dissent.[57] Information that is considered harmful in one state may be entirely uncontroversial and legitimate

55 Tom Burt, 'New Cyberattacks Targeting U.S. Elections', *MicrosoftBlog,* 10 September 2020, available at: https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/; Talita Dias/Antonio Coco*, Cyber Due Diligence in International Law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021), 90, 91.

56 See Leonhard Kreuzer, 'Disentangling the Cyber Security Debate', *Völkerrechtsblog*, 20 June 2018, available at: https://voelkerrechtsblog.org/de/disentangling-the-cyber-security-debate/.

57 On risks of counter-disinformation measures for freedom of expression Carme Colomina/Héctor Sanchez Margalef/Richard Youngs, 'The Impact of Disinformation on Democratic Processes and Human Rights in the World', *Study Requested by the DROI subcommittee* (European Parliament), April 2021, p. 16. For an overly broad definition of harmful information see e.g. China, National Cyberspace Security Strategy, 27 December 2016: 'Harmful information on the Internet erodes cultural security. Various ideological and cultural networks on the Internet are in conflict and confrontation, and excellent traditional culture and mainstream values are facing impact. Internet rumors, decadent culture and obscenity, violence, superstition and other harmful information that violates the core values of socialism (…) endanger cultural security'.

use of the freedom of expression in another state.[58] It is hence important to distinguish cyber harm from content-based information harm. While some international legal studies have implemented such a distinction[59], it is also frequently neglected in the international legal discourse.[60]

C. Different degrees of cyber harm

It is important to distinguish different degrees of cyber harm. Regardless of whether one frames a cyber operation under categorical terms such as cyber espionage, cyber war or cyber terrorism, the following three categories serve as analytical yardsticks in this regard.

I. Intrusive access operations: Loss of confidentiality

Intrusive access operations lead to the loss of confidentiality of data and the information this data embodies. They infiltrate an ICT system or network and typically copy data saved on it. Classical access operations are hence espionage operations. Usually access operations leave the integrity of data intact. One may hence be inclined to assess access operations as cyber harm of a lower intensity. Yet, while such an assumption may be apt in some cases, assuming a general presumption in this vein would go too far. On the one hand, access operations are often only a preparatory step before more disruptive steps are taken.[61] On the other hand, improperly acquired information can subsequently be published and hereby aggravate the harmful effect of a loss of confidentiality, e.g. through so-called doxing

58 Under international human rights law restrictions on free speech in cyberspace must comply with the requirements of legality, legitimacy, proportionality and necessity, UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011, para. 22.

59 The study group of the ILA has for example also implemented such a distinction, ILA, 'Cybersecurity and Terrorism' 2016 (n. 10), p. 2, para. 5.

60 A rare example from state practice in which a state argued for a distinction between cyber harm and content-based information risks is the statement by the Netherlands in the UN OEWG where it argued for an exclusion of disinformation problems which were 'outside of the scope of th[e] working group', Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the UN OEWG, 2020, p. 2, para. 15.

61 Roguski, 'Territorial Sovereignty' 2020 (n. 7), at 75, 76; this risk is typically associated with cyber espionage operations, see already above chapter 1.A.I.

operations in which malicious actors publish acquired personal data. Also access operations can hence already lead to severe harmful effects.

II. Disruptive operations: Impairment or loss of functionality

Disruptive cyber operations affect the functionality of a computer system or network. Examples are e.g. cyber operations which slow down the operation of a single server or a computer system; or DDoS attacks which cause the crashing of a server hosting a website[62], or ransomware attacks which encrypt files and hereby disrupt the orderly functioning of the computer system. Loss of functionality may hence be caused by a variety of malware types. Like the previous category of loss of confidentiality also the category of loss of functionality is limited to ICT-*internal* effects.

III. Destructive operations: Physical harm

Although the vast majority of cyber operations are access or disruptive operations some cyber operations can also have impacts 'in the real world beyond the cyber system itself'.[63] With regard to such ICT-*external* harm persons, physical objects or infrastructure are attacked '*through* cyberspace'.[64] An example of physical harm was e.g. the *Stuxnet* operation. In this case, malware manipulated the operation of centrifuges in an Iranian uranium enrichment facility and hereby led to their physical impairment.[65] Another example of physical cyber harm is the cyber-enabled impairment of medical equipment, e.g. during the COVID-pandemic, or the cyber-enabled crash of a car. Also physical damage to the ICT hardware itself may be considered physical cyber harm. It seems justified to consider physical harm as cyber harm when the resulting physical harm is sufficiently causally connected to the compromising of the CIA triad. Physical harm can also

62 Eleonora Viganò/Michele Loi/Emad Yaghmaei, 'Cybersecurity of Critical Infrastructure', in Markus Christen Bert Gordijn Michele Loi (eds.) *The Ethics of Cybersecurity* (Berlin: Springer Nature 2020), 157–178, 165.

63 Brown/Tullos, 'Cyberspace Operations' 2012 (n. 28).

64 Marco Roscini, 'Military Objectives in Cyber Warfare', in Mariarosaria Taddeo/Ludovica Glorioso (ed.), *Ethics and Policies for Cyber Operations* (NATO CCDCO 2017), 99–114, at 103.

65 On the operation see also Delerue, 'Cyber Operations' 2020 (n. 19), 2020, 407.

affect the functionality of cyber operations and hereby simultaneously have disruptive effects.[66] The increasing popularity of 'smart' objects connected to the internet and the use of artificial intelligence will likely heighten vulnerabilities for ICT-external harm in the future.[67]

IV. Other categorization of cyber harm effects

Other commentaators have developed more finely grained scale charts of different effects, distinguishing e.g. seven different degrees of effects[68], or between 'secondary' harm manifesting on the infrastructure controlled by ICT and 'tertiary' physical harm to individuals and objects as a consequence of the failure of the ICT infrastructure[69], or between harm to software, hardware, data and persons.[70] Again others merely distinguish between two categories of effects – 'functional' and 'physical' cyber harm[71], or 'physical and non-physical' effects.[72]

Yet, the three different categories of harmful effects outlined by this study on the one hand allow for a nuanced approach regarding ICT-internal harm by distinguishing between loss of confidentiality and loss of functionality. On the other hand, they also allow to compactly grasp various degrees of cyber harm, regardless of the specific malware used. This nuanced but compact categories of various degrees of cyber harm are best suited to assess the significance of cyber harm under the harm prevention rule.

D. Current state of the international legal discourse

To contextualize the current discussions on the harm prevention rule in cyberspace and cyber harm more generally it is important to be aware

66 Viganò/Loi/Yaghmaei have framed this as 'physical-functional' harm, 'Cybersecurity' 2020 (n. 62), 166.

67 On the risk of disabling cars via cyber means Bruce Schneier, 'Class Breaks', *Schneier on Security*, 3 January 2017, available at: https://www.schneier.com/blog/archives/2017/01/class_breaks.html; see also Viganò/Loi/Yaghmaei, 'Cybersecurity' (n. 62), 166.

68 Chircop, 'Territorial Sovereignty' 2019 (n. 5), 359, 360.

69 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press 2014), 52.

70 Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 55), 72f.

71 Viganò/Loi/Yaghmaei, 'Cybersecurity' (n. 62), 166.

72 Delerue, 'Cyber Operations' 2020 (n. 19), 36.

of the inherent structural challenges for international law in cyberspace. These challenges are partially the reason for the underdeveloped status quo of international law in cyberspace and have partially caused the above-mentioned problems of reactive approaches.[73] Yet, they also play a role regarding the application and implementation of the harm prevention rule and hence need to be highlighted.

I. Gradual recognition of the applicability of international law in cyberspace

Already the technical design of cyberspace is a challenge for international law. Cyberspace is a decentralized network. A large number of private actors manage and operate most of the physical ICT infrastructure. The Internet Engineering Task Force e.g. develops core internet standards and protocols.[74] The seamless flow of data is enabled by settlement-free peering of private actors and packet-switched private networks.[75]

This seamless flow of data creates an ubiquity of cyberspace that is largely based on the technical community[76] and bypasses the state as a regulatory actor.[77] Due to its borderless technical character cyberspace has even been likened to a global commons.[78] Furthermore, non-state actors not only have a vital role in cyberspace as technical architects and operators but also as threat actors. Due to the interconnectedness of cyberspace even single attackers can wreak tremendous havoc. For example, a young attacker with limited hacking skills exposed the private addresses of a

73 See Introduction.

74 Internet Engineering Task Force, *DIG Watch,* available at: https://dig.watch/actors/internet-engineering-task-force.

75 Policy Brief: Internet Interconnection, *Internet Society*, 30 October 2015, available at: https://www.internetsociety.org/policybriefs/internetinterconnection/; Center for Democrary & Technology, 'ETNO Proposal Threatens Access to Open, Global Internet', 21 June 2012, available at: https://cdt.org/insights/etno-proposal-threatens-access-to-open-global-internet/, p. 3: 'The flow of communications between networks is (…) achieved through unregulated commercial agreements (…)'.

76 Dennis Broeders, *The Public Core of the Internet* (Amsterdam: Amsterdam University Press 2015), 11.

77 Milton L. Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22 (2020), 779–801, at 790.

78 Ibid., 794; Woltag has however convincingly pointed out that cyberspace should not be framed as a global commons as it is not an area outside of national jurisdiction, Woltag, 'Cyber Warfare' 2014 (n. 17), 56.

number of German parliamentarians following a cyber operation.[79] These aspects challenge the concept of 'supreme authority and territory'[80] under the concept of sovereignty, as well as of the state as a main threat vector on which international law is based.[81]

Hence, it was initially debated whether international law, or even domestic law, should apply in cyberspace.[82] Inter alia due to the work of the UN Group of Governmental Experts (UN GGE) – a group of selected governmental experts established by the UN General Assembly[83] – this debate is largely over. Cyberspace is based on physical components, e.g. on fibre-optic cables, routers, servers, as well as individuals acting in cyberspace. This 'physical layer'[84] of cyberspace is widely seen as the connecting link to the jurisdiction of the territorial state and consequently its regulation under international law. The UN GGE recognized in several consensual reports that the principle of territorial jurisdiction over the physical ICT infrastructure located on a state's territory, as well as international law more generally,

79 Grace Dobush, '20-year-old German Hacker Confesses in Doxxing Case', *Handelsblatt*, 1 August 2019, available at: https://www.handelsblatt.com/english/politics/data-leak-20-year-old-german-hacker-confesses-in-doxxing-case/23841212.html?ticket=ST-5094425-QxFvHBqs49OdjSVXp2nm-cas01.example.org. Acknowledging the cyber threat from non-state actors UN GGE Report 2021, para. 14: 'The Group also reaffirms that the diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk.'

80 Jens Bartelson, 'Dating Sovereignty', *International Studies Review* 20 (2018), 509–513, at 510.

81 On the challenge of such structural developments for the application of existing international legal rules see Heike Krieger/Georg Nolte, 'The International Rule of Law – Rise or Decline? Points of Departure', in Heike Krieger/Georg Nolte/Andreas Zimmermann (eds), *The International Rule of Law – Rise or Decline? – Approaching Current Foundational Challenges* (Oxford University Press 2019) 3–30, 15.

82 An infamous declaration assessed cyberspace outside the grasp of international law, John Perry Barlow, A Declaration of Independence for Cyberspace (1996), available at: http://w2.eff.org/Misc/Publications/ John_Perry_Barlow/barlow_0296.declaration.txt.

83 The group was first established in 2004 following UN General Assembly Resolution A/RES/58/32, 8 December 2003, para. 4.

84 Antal Berkes, 'Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control', *Israel Law Review* 52 (2019), 197–231, 201; Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 1, para. 4; Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019, para. 42.

applies.[85] No state hence seriously questions the general applicability of international law and the UN Charter in cyberspace anymore. While some states still argue for the development for new rules for cyberspace[86] the understanding prevails that such new rules would evolve as additional rules to the existing rules.[87]

Yet, a lack of certainty remains as to *how* existing rules of international law apply, including with regard to the harm prevention rule. Furthermore, the problem of non-state actors as important threat vectors lingers on with regard to the enforcement of international law. Due to the problem of attribution and technical evidence it is notoriously difficult to trace the source of a malicious cyber operation, at least in a timely manner.[88] Even if the server from which an attack presumably was conducted is identified the evidence may have been manipulated. While states have attributed cyber operations to states, as in the case of the attribution of the *WannaCry* attack to North Korea, such attribution constituted political attribution which did not meet the required standards of legal attribution.[89] The attribution

85 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013 (UN GGE Report 2013), para. 20: 'State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.' This assertion was reiterated in the UN GGE Report 2015 and the UN GGE Report 2021, para. 71 lit. b.

86 China's Positions on International Rules-making in Cyberspace, October 2021: 'The international community should *develop* (emphasis added) universally accepted norms, rules and principles within the framework of the UN, to jointly address the risks and challenges, and uphold peace, security and prosperity in cyberspace.'

87 UN GGE Report 2021, para. 16: 'The Group also underscores the inter-relationship between norms, confidence-building measures, international cooperation and capacity-building. Given the unique attributes of ICTs, the Group reaffirms the observation of the 2015 report that additional norms could be developed over time, and, separately, notes the possibility of future elaboration of additional binding obligations, if appropriate.'; UN OEWG, Final Report 2021, para. 29: 'Given the unique attributes of ICTs, States reaffirmed that, taking into account the proposals on norms made at the UN OEWG, additional norms could continue to be developed over time. States also concluded that the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel.'

88 See already above in the Introduction.

89 Kristen Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *JustSecurity,* 20 December 2017, available at: https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/; states themselves distinguish between political and legal attribution see Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the internation-

problem leads to an accountability gap that presents a persisting problem for the enforcement of international law in cyberspace.

II. States' preference for strategic ambiguity

A further structural problem for international legal progress was states' reluctance to commit to legally binding rules. While a significant number of states has in recent years published their opinio iuris on the applicability of international law in cyberspace[90] and has contributed to the inclusive UN Open-Ended Working Group (OEWG), established by the UN General Assembly in 2018, ambiguity remains. In statements on international law in cyberspace states frequently walk a fine line between asserting the applicability of international law, inter alia for deterrent purposes, but avoiding to commit to norms that may limit their ability to conduct offensive cyber operations themselves. A variety of states has asserted sovereignty as a prohibitive primary rule of international law but omitted to specify criteria for a violation of such a rule.[91]

States' strategic avoidance of accountability mechanisms also explains their preference for informal and non-binding norms. Instead of asserting binding legal rules, the UN GGE Reports for example assert '*non-binding*, *voluntary* norms of *responsible* state behaviour'.[92] As these norms largely reiterate existing binding rules of international law their categorization as non-binding creates an ambiguity that may undermine the legal force of international law in cyberspace on the mid-term.[93] While the recent inten-

al legal order in cyberspace, Appendix, International Law in Cyberspace, p. 6; for an overview of political attribution in state practice see Christina Rupp/Alexandra Paulus, *Official Public Political Attribution of Cyber Operations – State of Play and Policy Options* (Stiftung Neue Verantwortung 2023), 60.

90 See e.g. Finland, International law and cyberspace, Finland's national positions, October 2020; Iran, Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, July 2020; New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020; France, International Law Applies to Operations in Cyberspace, September 2019; Germany, On the Application of International Law in Cyberspace, March 2021.

91 See in more detail chapter 3.B.III.

92 UN GGE Report 2015 stipulates norms, rules and principles (Part III, paras. 15–68), as opposed to international law (Part IV, paras. 69–73).

93 On the risk of diluting the binding character of existing legal obligations in cyberspace through the extensive use of hortatory language see below chapter 2.F.II.1.

sification of the international legal discourse is to be welcomed – the UN OEWG mandate was extended until 2025[94] and the UN GGE agreed on a consensual report[95] – it remains to be seen to what extent these processes can lead to norm acknowledgment, stabilization and internalization. With regard to the noteworthy but reluctant final results of both the UN GGE Report 2021[96] and the UN OEWG[97] it seems unlikely that states' appetite for specific and binding rules in cyberspace will grow significantly in the near future.

III. Filling the void: Non-state actor proposals

Due to the slow progress on the inter-state level non-state actors have advanced norm assessments and proposals and hereby partially filled the void of international law in cyberspace. Microsoft proposed a digital Geneva Convention and has put forward proposals on cyber norms.[98] The Global Commission on the Stability of Cyberspace (GCSC) proposed norms on advancing cyber stability.[99] Under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) a group of international law experts convened and produced two detailed manuals on the applicability of international law in cyberspace.[100] In December

94 UN General Assembly Resolution A/RES/75/240, 31 December 2020, paras. 1–4.

95 After the failure of the UN GGE Report 2017 the consensual report of 2021 is a significant step. See highlighting the positive aspects of the UN Report Michael N. Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace', *JustSecurity,* 10 June 2021, available at: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

96 The UN GGE Report 2021 e.g. reiterated the unfortunate distinction between norms and rules, paras. 15–68, and international law, paras. 69–73.

97 The UN OEWG Final Report dedicates only four out of 80 paragraphs to the application international law in cyberspace and even these paragraphs remain very general, paras. 34–37.

98 Microsoft, Five Principles for Shaping Cybersecurity Norms, 2013; Microsoft, International Cybersecurity Norms – Reducing conflict in an Internet-dependent world, 2014; Microsoft, From Articulation to Implementation: Enabling progress on cybersecurity norms, 2016.

99 Global Commission on the Stability of Cyberspace, 'Advancing Cyberstability', Final Report, November 2019, Annex B.

100 Schmitt, 'Tallinn Manual on Cyber Warfare' 2013 (n. 17); Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1).

2020 it was announced that a third Tallinn Manual would follow.[101] Such proposals as expert or stakeholder manuals evidently lack legal authority[102] but in particular the Tallinn Manual has been remarkably successful in influencing the international legal discourse and is cited by various states in their statements on international law in cyberspace.[103] Due to this influence in particular the Tallinn Manual plays an important role for this study and is cited at various points. Yet, it is important to be mindful of its lack of legal authority.

IV. Turn to preventive approaches against cyber security risks

As a way forward states have increasingly turned to preventive approaches which bypass the notorious challenges of reactive approaches in cyberspace and focus on cyber resilience to better identify, protect against, respond to

101 NATO CCDCOE, 'CCDCOE To Host the Tallinn Manual 3.0 process', 14 December 2020, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/; the CCDCOE has furthermore published the Cyber Law Toolkit 2024, an interactive resource on international law and cyber operations, available at: https://cyberlaw.ccdcoe.org/wiki/Main_Page.

102 Cautioning against expert manuals as authoritative documents in international law Anton Petrov, *Expert Laws of War Restating and Making Law in Expert Processes* (Cheltenham et al.: Edward Elgar 2020); see also critically of the methodology of the Tallinn Manual 1 anticipating crises and narratives and potential repercussions for other areas of international law, Heike Krieger, 'Conceptualizing Cyberwar, Changing the Law by Imagining Extreme Conditions?', in Thomas Eger/Stefan Oeter/Stefan Voigt (eds), *International Law and the Rule of Law under Extreme Conditions: An Economic Perspective* (Tübingen: Mohr Siebeck 2017), 195–212, at 201; on the risk of undermining the legal legitimacy of the proposed rules see Heike Krieger/Jonas Püschmann, 'Law-making and legitimacy in international humanitarian law', in Heike Krieger (ed.), *Law-Making and Legitimacy in International Humanitarian Law* (Cheltenham et al.: Edward Elgar 2021), 1–14, at 8. The Tallinn Manual itself acknowledges its lack of legal authority Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 2: 'It is essential to understand that Tallinn Manual 2.0 is not an official document, but rather the product of two separate endeavours undertaken by groups of independent experts (…) The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. Nor does it reflect the position of any other organisation or State represented by observers or of any of the States involved in the 'Hague Process' (…) Ultimately, Tallinn Manual 2.0 must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law'.

103 See e.g Netherlands, 'International Law in Cyberspace' 2019 (n. 89) p. 3; Germany, 'Application of International Law' 2021 (n. 90), p. 2.

and recover from cyber threats.[104] E.g. France has alluded to the advantages of preventive approaches in light of notorious attribution problems.[105] The European Union (EU) has made prevention and resilience one of the central aspects of its cyber strategy.[106] The need for cooperative prevention of cyber harm is also mentioned in a Memorandum of Understanding (MoU) between the EU and the Association of Southeast Asian Nations (ASEAN)[107], as well as by the Non-Aligned Movement (NAM).[108] States increasingly acknowledge that often the most effective risk mitigation is prevention and resilience instead of retaliation.[109] For implementing preventive approaches in cyberspace the harm prevention rule takes centre stage.

104 *Microfocus,* 'What is Cyber Resilience', available at: https://www.microfocus.com/en-us/what-is/cyber-resilience; Underlining the importance of resilience also ILA, 'Cybersecurity and Terrorism' 2016 (n. 10), p. 70, para. 245.

105 France, 'Strategic Review' 2018 (n. 29), p. 9: 'The uncertainty intrinsically linked to the attribution of an attack should encourage states to focus their efforts on preventive measures.'

106 EU, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, 16 December 2020, p. 4f.

107 ASEAN-EU Statement on Cybersecurity Cooperation, 1 August 2019, para.4.

108 NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), para. 19: 'States should focus on cooperating to prevent conflicts in cyberspace from erupting in the first place.'

109 The Tallinn Manual has also recognized that in cyberspace an act of mitigation is often less effective than its prevention, see Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 7, p. 46, para. 11: '[I]n light of the nature of cyber activities, preventive measures are arguably prudent. For instance, the speed of cyber operations often makes an act of mitigation less effective than the successful prevention thereof'; on the inferiority of reaction to prevention in the environmental context Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020) 77–240, at 158: '[I]t is plain that prevention is what is needed, since "reaction" is generally inferior, and sometimes impossible.'