UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Applying Chapters VI and VII of the Charter of the United Nations in the Cyber Context

The Challenges and Opportunities of Information and Communications Technologies

TALITA DE SOUZA DIAS

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This project is part of the Security and Technology Programme Cyber Workstream, which is supported by the Governments of France, Germany, the Netherlands, Norway, and Switzerland and by Microsoft.

The author would like to thank Duncan Hollis, Henning Lahmann, Giacomo Persi Paoli, Vera Rusinova, Makane Moïse Mbengue, Nemanja Malisevic, Eneken Tikk, and Pedro Antonino for their comments to earlier drafts of this paper.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

CITATION

T. de Souza Dias. *Applying Chapters VI and VII of the Charter of the United Nations in the Cyber Context: the Challenges And Opportunities of Information and Communications Technologies*, Geneva, Switzerland: UNIDIR, 2021.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

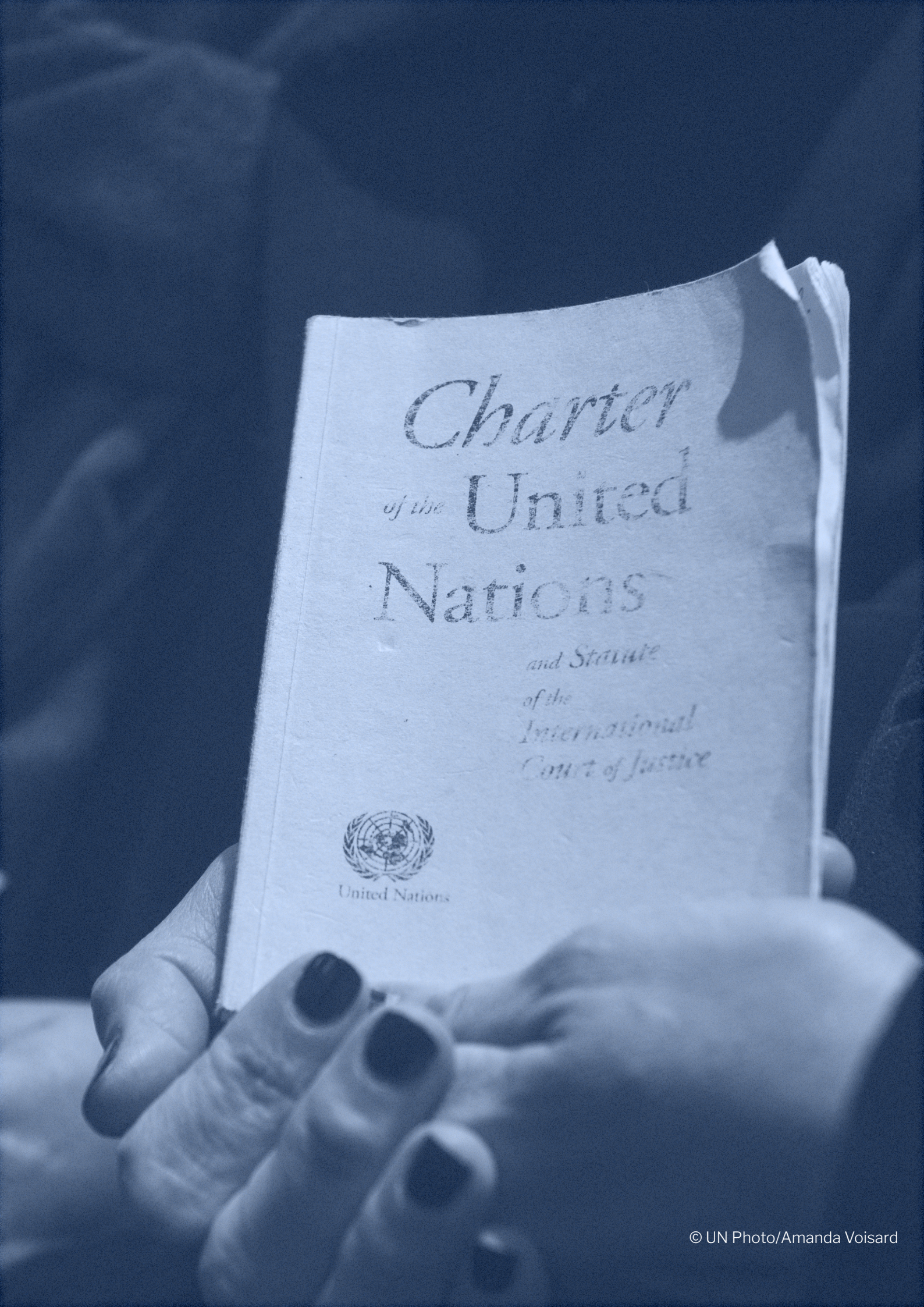
TABLE OF CONTENTS

ABOUT THE AUTHOR

TALITA DE SOUZA DIAS is the Shaw Foundation Junior Research Fellow in Law at Jesus College, University of Oxford. Her research focusses on the application of international law to new technologies, including the regulation of online hate speech and due diligence in cyberspace. Talita is also a lecturer in criminal law at St Catherine's College, University of Oxford. Prior to that, she was a Postdoctoral Research Fellow with the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government. She holds a DPhil in Law and a Magister Juris (MJur) degree from the University of Oxford as well as a Bachelor of Laws (LLB) from the Federal University of Pernambuco (UFPE). Talita has previously interned at the International Criminal Court, and she is a qualified lawyer in Brazil, where she clerked for a Criminal Appeals Chamber. Contact Dr. Talita de Souza Dias at: talita.desouzadias@jesus.ox.ac.uk.

LIST OF ACRONYMS AND ABBREVIATIONS

GGE	Group of Governmental Experts
ICJ	International Court of Justice
ICTs	information and communications technologies
KYC	Know-Your-Customer
KYT	Know-Your-Transaction
OEWG	Open-Ended Working Group
VPNs	virtual private networks



EXECUTIVE SUMMARY

International law as a whole and the Charter of the United Nations, in particular, apply to information and communications technologies (ICTs) and the digital environments that they enable, unless these are explicitly carved out.

With the increasing global dependence on ICTs and the expansion of vulnerabilities to malicious cyber operations, disputes, and situations triggering Chapter VI of the Charter have arisen and will continue to arise in respect of those technologies.

Not only has the Security Council formally and informally met to discuss international peace and security in the cyber context but several types of ICT-related incidents or situations could potentially amount to threats to the peace, breaches of the peace, and acts of aggression, triggering the Council's enforcement powers under Chapter VII of the Charter.

To address cyber events constituting disputes likely to endanger the maintenance of international peace and security or situations which might lead to international friction or give rise to a dispute, under Chapter VI, as well as threats to the peace, breaches of the peace, or acts of aggression, under Chapter VII, traditional dispute settlement and enforcement measures may be complemented or replaced with new, ICT-specific measures of an adjudicatory, legal, technical, capacity-building institutional, and/or cooperative nature.


.sf-sub-indicator
.cart-menu .cart-icon-wr
er-outer.transparent header#top
nav .sf-menu > li.current_page_
nav .sf-menu > li.current-menu-
nav > ul > li > a:hover > .sf-sub
nav ul #search-btn a:hover span,
nav .sf-menu > li.current-menu-
hover .icon-salient-cart,.ascend
:1!important;color:#ffffff!impo
rent header#top nav>ul>li.but
out-widget-area-toggle a i.
er-outer.transparent

1. INTRODUCTION

Chapters VI and VII of the Charter of the United Nations (hereafter, the Charter) are the bedrock of the United Nations collective security system, the purpose of which is to maintain and restore international peace and security.[1] Chapter VI, the system's first pillar, requires States to settle by peaceful means any disputes likely to endanger international peace and security.[2] To meet this obligation, Charter VI empowers the Security Council and the General Assembly to assist the parties to the dispute, such as by offering procedural or substantive recommendations for its resolution.[3] The obligation to settle disputes peacefully—rather than by armed force—finds its natural counterpart in Chapter VII and the collective security role vested in the Security Council. Under Chapter VII, the Council is empowered to take binding, coercive action of a military or non-military nature with respect to threats to the peace, breaches of the peace, and acts of aggression.[4] Chapters VI and VII have been used to tackle, inter alia, territorial disputes,[5] armed conflict,[6] terrorism,[7] the dissemination of weapons of mass destruction,[8] the illegal exploitation of natural resources,[9] refugee crises,[10] and atrocity crimes[11]—all of which have traditionally taken place in the physical domains of land, air, and sea. But with the ubiquity of ICTs employed across all domains of State activity, Chapters VI and VII may not only be triggered by cyber events but also used to ground measures of a new, even 'virtual' nature. In this way, ICTs may present both challenges and opportunities for the United Nations collective security system.

As noted in the Final Substantive Report of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, adopted by consensus in March 2021:

> States … are increasingly concerned about the implications of the malicious use of ICTs for the maintenance of international peace and security, and subsequently for human rights and development. In particular, concern was expressed regarding the development of ICT capabilities for purposes that undermine international peace and security. Harmful ICT incidents

1 See Article 1, Charter of the United Nations.

2 Article 33, Charter of the United Nations.

3 Articles 35 and 36, Charter of the United Nations.

4 Articles 39–42, Charter of the United Nations.

5 E.g., Security Council 242 (1967) (on the situation in the Middle East following the Six-Day War); Security Council 1177 (1998) (on the situation concerning Ethiopia and Eritrea).

6 E.g., Security Council 1986 (2011) (on the conflict in Cyprus); Security Council 1975 (2011) (on the situation in Côte d'Ivoire); Security Council 2501 (2019) (on Afghanistan).

7 E.g., Security Council 2462 (2019) (on countering terrorism and terrorism financing).

8 Security Council 1540 (2004) (requiring Member States to develop and enforce appropriate legal and regulatory measures against the proliferation of chemical, biological, radiological, and nuclear weapons and their means of delivery, in particular, to prevent the spread of weapons of mass destruction to non-State actors).

9 E.g., Security Council 2457 (2019) (relating to the ongoing cooperation with the African Union).

10 E.g., Security Council 1208 (1998) (on the treatment of refugees in the African continent); Security Council 2449 (2018) (on humanitarian aid in Syria).

11 Security Council 1970 (2011) (referring the situation in Libya to the International Criminal Court); Security Council 1953 (2005) (referring the situation in Darfur, Sudan to the International Criminal Court).

> are increasing in frequency and sophistication, and are constantly evolving and diversifying. Increasing connectivity and reliance on ICTs without accompanying measures to ensure ICT security can bring unintended risks, making societies more vulnerable to malicious ICT activities. Despite the invaluable benefits of ICTs for humanity, their malicious use can have significant and far-reaching negative impacts.[12]

Similarly, in its May 2021 report, the Group of Governmental Experts (GGE) on advancing responsible State behaviour in cyberspace in the context of international security recognized that "[m]alicious ICT activity by persistent threat actors, including States and other actors, can pose a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals",[13] and that "the use of ICTs in future conflicts between States is becoming more likely".[14]

The negative impacts of ICTs have been particularly felt during the COVID-19 pandemic, where new and existing vulnerabilities arising from our increased dependence on ICTs have been exploited for malicious ends.[15] From ransomware and other cyberattacks against the healthcare sector, to attempts to steal vaccine research and to spread 'viral' disinformation,[16] we have seen a worrying increase in harmful cyber operations that pose a real or imminent threat to international peace and security in the digital age.[17]

For their part, the Security Council and its various Member States have expressed growing concern over the current cyber threat landscape. Notably, the Council has held its first formal, open debate on cybersecurity in June 2021.[18] This followed two informal Arria-formula meetings on the topic in 2020.[19] The first, in May 2020, looked at cyber stability, conflict prevention, and capacity-building more generally,[20] while the second, held in August 2020, specifically discussed cyberattacks against critical infrastructure, including the healthcare sector.[21] Previous Arria-formula meetings have been held on

---

12 OEWG (2021, §15).

13 GGE (2021, §8).

14 GGE (2021, §7).

15 GGE (2021, §10); OEWG (2021, §4).

16 ENISA (2020, 'Cybersecurity in the Healthcare Sector during COVID-19 Pandemic'); Muthuppalaniappan and Stevenson (2021, 1–4); Milanovic and Schmitt (2020, 247).

17 See, e.g., GGE (2021, 6–11) Council of the EU (2020, 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic'); Herczyski (2020, 'Statement on behalf of the European Union); Juul (2020, 'Joint statement from Denmark, Finland, Iceland, Sweden and Norway'); Feakin (2020, 'Statement by Australian during UNSC Arria Formula Meeting on Cybersecurity'); Global Affairs Canada, (2020, 'Statement on Malicious Cyber Threats to the Health Sector'); UK (2020, 'UK Condemns Cyber Actors Seeking to Benefit from Global Coronavirus Pandemic').

18 Estonia (2021, 'UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace').

19 Security Council Report (2020, 'In Hindsight: The Security Council and Cyber Threats').

20 Security Council Report (2020, 'Arria-formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building').

21 Security Council Report (2020, 'Arria-formula Meeting on Cyber-Attacks Against Critical Infrastructure').

'Cybersecurity and International Peace and Security', in November 2016,[22] and 'Hybrid Wars as a Threat to International Peace and Security', in March 2017.[23]

The impact of ICTs on international peace and security has also featured in several Security Council resolutions on related matters. In particular, the Council has stressed the use of ICTs for terrorist purposes, including the financing, planning, and preparation of such activities, as well as the recruitment and incitement of others to commit terrorist acts, while listing suspected individuals and urging States to cooperate and prevent such acts.[24] More recently, the Council has unanimously adopted a resolution strongly condemning attacks by any means against civilians and civilian objectives, including critical civilian infrastructure, such as hospitals and schools, as well as urging parties to an armed conflict to protect those services.[25] While not explicitly referring to ICTs, several Council Members condemned cyber operations targeting critical infrastructure during the debates preceding the adoption of the resolution.[26]

Similarly, when addressing the Council in the 2017 annual 'Hitting the Ground Running Workshop', the Secretary-General warned that "cyber warfare had become a first-order threat to international peace and security" and that "[m]assive cyberattacks could well become the first step in the next major war".[27] He also called for more thought to be devoted to "how the Council should anticipate, prevent and, if necessary, respond to such an urgent threat to global security".[28] This has prompted the Secretary-General to declare, as one of his ten priorities for 2021, "[s]eiz[ing] the opportunities of digital technologies while protecting against their growing dangers".[29]

In short, there is no question that harmful cyber operations have already given rise to disputes between States, particularly regarding the attribution of conduct to States, and that they can endanger or disrupt international peace and security. Thus, it is only a matter of time before the Security Council is seized of the matter, whether to avert such threats or to address their disastrous consequences. Yet there is little guidance in the Charter itself, United Nations practice, or the literature as to how Chapters VI and VII can be used to tackle cyber incidents. Likewise, little has been written on how to leverage the power of ICTs to address these and other phenomena.

Against this background, the present paper seeks to assess how the United Nations mechanisms for the peaceful settlement of disputes (Chapter VI) and enforcement action (Chapter VII) can be transposed to the cyber context. First, it addresses two foundational questions: what is 'cyberspace', and to what extent international law—

22 Security Council Report (2016, 'Open Arria-formula Meeting on Cybersecurity').

23 Security Council Report (2017, 'Arria-Formula Meeting on Hybrid Wars'). See also Security Council Report (2020, 'In Hindsight: The Security Council and Cyber Threats').

24 See, e.g., Security Council 2214 (2015, 5); Security Council 2250 (2015, preamble); Security Council 2133 (2014, preamble); Security Council 2178 (2014, 7, 11, 17); Security Council 2129 (2013, 14).

25 Security Council 2573 (2021, 1, 6); Security Council 425 (2021, 3–4, 7, 12–13, 15, 19, 25). See also Kavanagh (2017).

26 Security Council SC/14506 (2021).

27 S/2018/404 (2018, Annex, 3).

28 S/2018/404 (2018, Annex, 3).

29 IISD (2021, 'UN Secretary-General Presents 10 Priorities for 2021').

and the Charter in particular—applies thereto, including in civilian and military contexts. Second, it assesses the extent to which harmful cyber operations can amount to disputes likely to endanger international peace and security, situations of international friction, threats to the peace, breaches of the peace, and acts of aggression, thus falling within the scope of Chapters VI and VII of the Charter. Third, it looks at the measures that might be needed from the Security Council, the General Assembly, or Member States to peacefully settle or avert 'cyber disputes', as well as to prevent or respond to cyber operations amounting to threats to the peace, breaches of the peace, and acts of aggression. In particular, the paper asks whether addressing cyber incidents requires the use of ICTs, or cyber-specific measures, and identifies what these measures may look like, providing a roadmap for action by States and relevant United Nations bodies. These findings may be of interest to international lawyers, diplomats and cybersecurity experts working for Member States, United Nations bodies, and non-governmental organizations, as well as academics.

As a framing paper, this piece does not purport to give definitive answers to the questions it addresses. Rather, its primary aim is to lay out the key legal issues that might arise when applying Chapters VI and VII of the Charter to ICT-related situations, while suggesting some possible avenues and laying the groundwork for further discussion. Accordingly, all views expressed here are tentative and do not exhaust alternative interpretations of the matter. In particular, all cyber events and measures discussed below can but need not necessarily come within the scope of Chapters VI and VII. The methodology used for interpreting the relevant legal provisions of the Charter and other applicable rules of international law follows articles 31–32 of the Vienna Convention on the Law of Treaties.[30] Given the paucity of materials on the topic to date, propositions were based on the practice developed by the Security Council and other United Nations bodies on analogous non-cyber events, as well as available State practice, and academic commentary on more general issues surrounding the application of international law to ICTs.

30 (1969, 1155 UNTS 331).

2. TRIGGERING CHAPTERS VI AND VII OF THE CHARTER IN THE ICT ENVIRONMENT

2.1. Imaginary Lines? The Charter along the Cyber–Physical and Military–Civilian Divides

The concept of 'cyberspace' is now fully ingrained in mainstream political and legal discourse. It is often used to single out online activities occurring in the man-made 'virtual' or 'cyber' domain and contrast them with those taking place in the 'real-world', that is, the traditional physical domains of land, air, sea, and outer space.[31] In the same vein, 'cyberspace' is often divided into military and civilian activities, following the traditional peace and war divide in international law.[32] There is widespread agreement among States that the Charter applies in its entirety to ICTs, along with States' obligation to settle disputes by peaceful means.[33] Yet such divisions between 'cyber' and 'physical' spaces, as well as civilian and military technologies, have led many to question the applicability of other rules of international law to ICTs. Most notably, fearing the further militarization of cyberspace and the escalation of armed conflict, some States have questioned the applicability of certain rules and concepts of international humanitarian law to the cyber context.[34] Other States have challenged the application of States' duties to respect and protect the sovereign rights of other States in cyberspace.[35] On this view, it is argued that cyber-specific State practice and *opinio juris*—the two elements of customary international law—must be sufficiently demonstrated from scratch for those rules to apply in the 'virtual' domain.[36]

Assessing the validity of those claims is important because the Charter does not apply in a vacuum. Quite the contrary: in resolving their disputes, whether in respect to cyber or other activities, States, the International Court of Justice (ICJ), and other judicial or arbitral institutions continue to be bound by existing international law. Similarly, despite the breadth of its powers, the presumption is that the Security Council will act

---

31 See, e.g., Schondorf (2020, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations').

32 See, e.g., Libicki (2016).

33 See GGE (2021, §§18, 25, 70, 71(a), (e)); OEWG (2021, §§7, 34, 35); GGE (2015, §§24, 26, 28(b)); GGE (2013, §20).

34 See People's Republic of China (2020, 'Statement by Minister-Counsellor Mr. Yao Shaojun at Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure'); People's Republic of China (2020, 'Statement during UNSC Arria Formula Meeting on Cybersecurity', 1:21:00), Russian Federation (2020, 'Commentary of the on the Initial "Pre-Draft" of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security', 2). But note that, in its May 2021 report, the GGE has agreed that "international humanitarian law applies only in situations of armed conflict" while recalling "the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction".

35 Wright, (2018, 'Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General', 5).

36 United Kingdom (2021, 'Application of International Law to States' Conduct in Cyberspace', §§10, 12); Schondorf (2020, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations'); New Zealand, (2020, 'The Application of International Law to State Activity in Cyberspace, 16–17). See also Schmitt (2020, 'New Zealand Pushes the Dialogue on International Cyber Law Forward').

consistently with international law,[37] especially when making general, quasi-legislative decisions, in line with the purposes and principles of the Charter.[38] Accordingly, even if States have not contested the Charter's application to ICTs, carving out other rules of international law from this context would have serious implications for the interpretation and implementation of ICT-related measures adopted under Chapters VI and VII.

Now, is 'cyberspace' really a 'space' or a separate 'domain' of State activity, such that it is not automatically subject to existing rules of international law? At least three reasons seem to indicate otherwise.

First, from a technical standpoint, the virtual environment that we often call 'cyberspace' is only made possible due to a combination of technologies that have physical, logical, content, and personal layers or dimensions.[39] In other words, what creates this virtual space that enables human beings to communicate with each other, process and store information, as well as control other machines or devices, is just a set of ICTs. And these ICTs themselves are made up of hardware, software, data, and, most importantly, the people who use, control, or are otherwise affected by them.[40] As such, the digital 'space' or 'environment' projected on our screens is itself an illusion or simulation of physical objects, persons, places, or activities—albeit one that is very much grounded in real technologies.[41] These are, in turn, spread across existing physical domains (e.g., the Internet's underground fibre-optic cables cross multiple lands and seas, Wi-Fi radio waves permeate the air, and satellites transmit their signals from outer space), and are powered by both physical devices (e.g., computers, smartphones, and transmission towers) and non-physical, human knowledge (mainly algorithms and the information they process).

Indeed, the word 'cyber' alludes to the field of cybernetics, defined as the study of remote control through devices[42] or "command and control and communications in … the mechanical world".[43] The term 'cyberspace' itself originated in art[44] and science fiction[45] to describe human experiences grounded both in physical and non-physical components. Thus, 'cyberspace' is best defined as a multidimensional human phenomenon that is, deep down, enabled by ICTs.[46] For the purposes of international law, it should not be conceived of as a separate space or domain, but a set of new, digital technologies created by and affecting human beings in all existing domains.

Second, and relatedly, international law is not limited to certain types of technology,

---

37 See ECtHR (2011, Al-Jedda v United Kingdom, §102); ECtHR (2016, Al-Dulimi and Montana Management Inc v Switzerland, §§ 139–140, 146); Wood (2017, 1, 19, 23–24).

38 See Articles 1–2 and 24(2), Charter of the United Nations.

39 Sullivan (2016, 454, fn 88). See also Tsagourias (2015, 13). See also Johnson and Post (1996, 1367).

40 Lessig (2006, 20); Lessig (1996, 1406).

41 Lessig (2006, 9, 83); Cohen (2007, 226–227).

42 Lessig (2006, 3).

43 Tabanski (2011, 76) citing Wiener (1955).

44 Lillemose and Kryger (2015, 'The (Re)invention of Cyberspace').

45 Gibson (1982); Gibson (1984, 69); Neale (2000).

46 See Lessig (2006, 84–85).

but applies to all of them, whether electronic or mechanical, digital or analogue, physical or virtual. As the ICJ held in its *Nuclear Weapons Advisory Opinion,* Articles 42 and 51 of the Charter "do not refer to specific weapons", but "apply to *any* use of force, *regardless of the weapons employed*".[47] The same applies, *mutatis mutandi*, to other provisions of the Charter and ICTs, whether these are used for civilian or military purposes. According to the OEWG Chair:

> States emphasized that measures to promote responsible State behaviour *should remain technology-neutral, underscoring that it is the misuse of technologies, not the technologies themselves, that is of concern.*[48]

Such a technology-neutral and dynamic approach to the interpretation and application of international law is an important "safeguard against [the] rapidly evolving nature of ICT technologies".[49]

Third, irrespective of whether 'cyberspace' is a space, a domain, or a set of technologies, certain rules of international law are of a general nature. This means that they apply across the board to all types and areas of State—and increasingly non-State[50]—activity, to the extent relevant.[51] The reason is simple and quite intuitive: by definition, rules of 'general international law' are general, such that their scope of application is sufficiently broad to encompass old and new phenomena fitting within their abstract definition.[52]

As seen earlier, there is no question that this is the case of the Charter as a whole and Chapters VI and VII in particular, which States have consistently recognized apply to ICTs.[53] But the same is also true of other general rules or principles of international law found in treaty or customary international law, such as sovereignty, non-intervention, and several rules requiring diligent behaviour, even if some States have questioned or opposed their applicability to ICTs.[54] Furthermore, even specific rules or regimes of international law, such as international human rights law and international humanitarian law, are not limited to a certain 'domain' or type of activity. The concept of a 'domain' arose in the field of international humanitarian law but was never meant to limit the applicability of its rules.[55] Rather, it serves as an "organizing idea, reflecting the way

---

47 ICJ (1996, Nuclear Weapons Advisory Opinion, §39) [emphasis added]. See also §§85–86 in relation to international humanitarian law.

48 See OEWG (2021, 'A/AC.290/2021/CRP.3*', §8) [emphasis added].

49 Czech Republic, (2020, 'Comments Submitted in Reaction to the Initial "Pre-Draft" Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security', 2).

50 Relevant rules of international law binding on non-State actors include international humanitarian law and international criminal law—see ICRC (2013, 'Cyberwarfare and International Humanitarian Law: The ICRC's Position', 2); Rodenhäuser and Mačák (2021). Other rules of international law such as positive human rights duties and other due diligence obligations require States to prevent and redress State and non-State acts—see Sullivan (2016, 454–455); Coco and de Souza Dias (2021, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law').

51 PCIJ (1927, The Case of the S.S. Lotus, §45); ILC (2006, A/CN.4/L.682, §120). See also Akande, Coco and de Souza Dias (2021, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond').

52 Tassinis (2020, 242–243).

53 See note 29.

54 Akande, Coco and de Souza Dias (2021, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond').

55 McCosker (2020, 78).

we conceptualize the battlefield and categorize actions taking place during armed conflict".[56] Granted, certain rules of international law, such as the Convention on the Law of the Sea[57] and the Convention on International Civil Aviation,[58] are chiefly applicable to a single domain. However, these limitations cannot be read into otherwise general rules, meant to have general applicability.[59]

The interconnectedness and transboundary—even global—reach of the Internet and other ICTs also means that it is difficult if not impossible to separate between civilian and military uses of those technologies.[60] Even in the case of internal networks not connected to the Internet, the pervasiveness of connected devices, such as smartphones and watches, is such that vulnerabilities in the global network can eventually reach Intranets.[61] And with the help of human engineering techniques, such as deception and infiltration, it is not hard to imagine malicious software or hardware being used to create backdoors in isolated computers or devices.[62] Most importantly, the core of the Internet, comprising packet routing and forwarding (such as Internet routers and their protocols), naming and numbering systems (such as the Internet's Doman Name System), cryptographic mechanisms of security and identity (such as public and private keys), and physical transmission media (such as cables and signals),[63] is either owned or controlled by private entities operating for private, commercial ends.[64]

Thus, not only do militaries depend on private providers to access and operate ICTs but vulnerabilities in civilian information infrastructure can also affect military ICTs. In the same vein, harm to military hardware or software can easily spill over to civilian ICTs.[65] Accordingly, when considering the application of the Charter, and in particular Chapters VI and VII, to ICTs, their networked, interconnected nature, including between civilian and military applications, must be borne in mind. This further underscores the importance of upholding both international human rights law and international humanitarian law in the ICT environment, and of recalling that humanitarian principles do not seek to legitimize or encourage armed conflict.[66]

In sum, from both a technical and legal standpoint, the line between virtual and physical spaces is imaginary and often unhelpful. As affirmed by a growing number of States,

---

56 McCosker (2020, 97).

57 (1994, 1833 UNTS 397).

58 (1947, 15 UNTS 295).

59 Schmitt (2017, 31, §4); Khanna (2018, 141). See, generally, ICJ (1996, Nuclear Weapons Advisory Opinion, §39).

60 See Sommer and Brown (2011, 'Reducing Systemic Cybersecurity Risk', 9–12); ICRC (2019, 'Position Paper—International Humanitarian Law and Cyber Operations during Armed Conflicts', 4–5).

61 Telegraph (2015, 'Top Five Common Intranet Security Weaknesses').

62 Abbott (2019, 'Interlopers in Things? IoT Devices May be Used as Backdoors to your Network').

63 Global Commission on the Stability of Cyberspace (2018, 'Definition of the Public Core, to which the Norm Applies').

64 See ITU (2008, 8, §1.12). On the role of private companies in tackling malicious cyber operations, see, e.g. Burt, (2020, 'Cyberattacks Targeting Health Care Must Stop').

65 See Gisel and Rodenhäuser (2019, 'Cyber Operations and International Humanitarian Law: Five Key Points').

66 GGE (2021, §§36, 70, 71(f)).

the default position is that international law as a whole applies to ICTs, unless these are explicitly carved out from the scope of applicable rules. Likewise, it is unrealistic to draw lines between military and civilian ICTs, with international rules and measures often affecting both civilian and military applications.

2.2. Cyber Events Triggering Chapter VI of the Charter

Chapter VI of the Charter seeks to give effect to States' obligation to settle their disputes by peaceful means, laid down in Article 2(3). As such, it is chiefly addressed to Member States, with Article 33(1) providing that:

> The parties to any dispute, the continuance of which is *likely to endanger the maintenance of international peace and security,* shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.[67]

At the same time, to assist States in discharging this duty whenever disputes have the potential to endanger international peace and security, Articles 34, 35(1)–(2), 36, and 38 of the Charter grant the Security Council a number of ancillary functions, such as the power to investigate the situation, as well as to recommend a particular process for settling the dispute at any stage thereof.[68] Likewise, Article 35(2)–(3) envisions a secondary role for the General Assembly, in that it can be seized of a particular dispute insofar as it is not being considered by the Security Council, in line with Articles 11 and 12 of the Charter.[69] Under Article 37(2) of the Charter, the Council must also decide whether to recommend appropriate means and terms of settlement for the parties, if they fail to resolve the dispute peacefully on their own.[70]

However, several conditions must be met before these functions can be triggered. First, a dispute between two or more 'parties' must exist. Second, the dispute must be such that its continuance is likely to endanger the maintenance of international peace and security. Third, in the case of Security Council investigations, there must be a 'dispute' or a 'situation which might lead to international friction or give rise to a dispute', following which the Council will determine whether its continuance is likely to endanger international peace and security.

A dispute is not a mere disagreement, but a claim on a point of law or fact that is opposed by the other party, whether explicitly or implicitly.[71] The obligation to settle disputes peacefully has been extended beyond States to non-State groups that are both protected from the use of force and must refrain from using it under Article 2(4) of the Charter, such as de facto regimes or national liberation movements.[72] However,

---

67 Emphasis added.

68 Tomuschat (2012, 'Article 33', §§ 1, 3).

69 General Assembly 43/51 (1988, §§16-19).

70 Giegerich (2012, §2).

71 United Nations A/1388 (1950, 6–7); Schweisfurth (2012, §23); Tomuschat (2012, 'Article 2(3)', §27).

72 Tomuschat (2012, 'Article 33', §§9, 12).

purely domestic disputes fall outside the scope of this obligation.[73] Indeed, in contrast to Article 2(3), Article 33 of the Charter and Chapter VI as a whole are limited to those disputes "the continuance of which is *likely* to endanger the maintenance of *international* peace and security".[74] This means that, even if the dispute in question is geographically or thematically limited to a single State, it must still have the *potential* to threaten the maintenance of peace and security beyond the purely domestic level.

While some debate remains as to whether and to what extent this threshold differs from a 'threat to the peace' under Article 39 (which triggers Chapter VII and the Council's coercive powers),[75] it is now generally accepted that both types of threat encompass situations *not directly* involving the use of armed force or physical violence.[76] A recent example is the Council's qualification of the COVID-19 pandemic as "likely to endanger the maintenance of international peace and security".[77] Similarly, the climate crisis has been qualified as such a type of threat during Council meetings.[78] As others have noted, this reflects a broader shift in the Council's mandate from military to human security.[79]

In the cyber context, many disputes over different aspects of ICTs are likely to endanger the maintenance of international peace and security. As seen earlier, ICTs have a multifaceted, dual-use, and transboundary nature, spanning different physical and non-physical components and crossing multiple frontiers in a matter of seconds. The first implication is that 'cyber disputes' can easily fall outside a State's exclusive domestic jurisdiction and within the scope of Chapter VI. The second implication is that such disputes may not only refer to claims and counterclaims over the now-widespread use of malicious code or programmes to affect the confidentiality, integrity, or accessibility of the target's data and software, that is, disputes over 'virtual' objects or spaces, such as traditional malware[80] or 'disinformation'.[81] They may also involve hardware and ICT users, provided that their potential impact on international peace and security is sufficiently serious. Examples of operations carried out through or against hardware include the insertion of physical backdoors,[82] such as by using wiretaps or USB keys,[83] signal interference or jamming,[84] overheating, and power outages.[85] Likewise, numerous software, hardware or information-based operations, such as

73 Article 2(7), Charter of the United Nations. See also Tomuschat (2012, 'Article 33', §11).

74 Emphasis added.

75 See Pobjie (2020, 3).

76 Pobjie (2020, 2, 9, 11–12); Kirsch (2012, 'Article 39', §§13, 21, 26–27).

77 Security Council 2532 (2020, preamble).

78 S/2020/751 (July 2020, 14, 27, 48, 82); Pohl and Kurnoth (2020, 'Summary: UNSC Open Debate on Climate and Security'); Security Council SC/14445 (2021).

79 Pobjie (2020, 2); Kirsch (2012, 'Article 39', §15). See generally Nasu (2013).

80 Kaspersky (2018, 'What is Malicious Code').

81 See Pobjie (2020 4), on the possible qualification of 'cyberattacks' and 'disinformation' as 'threats to international peace and security'.

82 Paganini (2013, 'Hardware Attacks, Backdoors and Electronic Component Qualification').

83 Eclypsium (2019, 'Anatomy of a Firmware Attack').

84 Fang et al. (2016, 2).

85 ENISA, (2017, 'Hardware Threat Landscape and Good Practice Guide', 16–18, 23–24).

ransomware,[86] surveillance,[87] online hate speech,[88] electoral interference, and other covert information campaigns,[89] may give rise to disputes that threaten international peace and security because of their impact on the well-being of individuals around the world.[90]

Importantly, as a result of the Internet's decentralized infrastructure, anonymity, and the use of spoofing techniques, such as virtual private networks (VPNs),[91] it will be difficult if not impossible to factually attribute such cyber operations to States with sufficient certainty, even if the necessary technical or forensic analysis has been carried out.[92] Legal attribution of the acts of private entities to States will likewise be challenging, given the high threshold of attribution established under customary international law, that is, effective control over specific acts or operations.[93] Similarly, irrespective of factual or legal attribution, political attribution of a cyber operation to a State or non-State group[94] may significantly affect the relationship between States.[95] Thus, many inter-State cyber disputes have revolved and will continue to revolve around factual, technical, legal, and political attribution.[96] Other disputes have concerned the extent of the harm caused, the lawfulness of the relevant conduct, as well as the scope, and interpretation of international law as it applies to ICTs.[97]

A recent example of one such dispute relates to the so-called 'SolarWinds hack', dubbed the "largest and most sophisticated [cyber]attack" ever.[98] Not only did it lead to the exfiltration of data belonging to ICT companies in different states and governmental agencies in the United States,[99] but also the insertion of backdoors allowing the

---

86 Fruhlinger, (2020, 'Ransomware Explained: How it Works and How to Remove it').

87 GGE (2021, §37).

88 Article 19 (2015, 9–14); Cyber Law Toolkit (2021, 'Scenario 19: Hate speech'). See also ICTR (2007, Prosecutor v Nahimana et al., Appeal Judgement, 220–228, 306–309) (considering whether hate speech, broadcasted on the radio, can constitute incitement to genocide and the crime against humanity of persecution).

89 GGE (2021, §9).

90 GGE (2021, §§8–9).

91 Lessig (2006, 236); The Things Network (2021, 'Network Architecture').

92 Shamsi et al. (2016, 2886–2887); Skopik and Pahi (2020, 6–7, 14); Yannakogeorgos (2013, 9, 13–16).

93 ICJ (1986, 'Military and Paramilitary Activities in and against Nicaragua', §115). See also Mikanagi and Mačák (2020, 60–64).

94 See generally Egloff and Smeets (2021).

95 E.g., Soldatkin and Holland (2021, 'Far Apart at First Summit, Biden and Putin Agree to Steps on Cybersecurity, Arms Control'), on the geopolitical tensions between the United States and the Russian Federation following the United States' attribution of cyberoperations to Russian nationals.

96 E.g., Eichensehr (2017, 'Three Questions on the WannaCry Attribution to North Korea'); Goldsmith (2017, 'The Strange WannaCry Attribution'); AFP and AP (2017, 'North Korea denies US WannaCry Cyberattack Accusation'); Osborne (2018, 'North Korea Claims Hacker Responsible for WannaCry Outbreak Does not Exist'); BBC, (2018, 'UK and US Blame Russia for "Malicious" NotPetya Cyber-Attack'). See generally GGE (2021, §§ 22–26).

97 E.g., People's Republic of China (2017, 'International Strategy of Cooperation on Cyberspace') (claiming that cyberspace is a "new domain of state sovereignty" and that "every country has the right and responsibility to maintain its cyber security and protect the legitimate rights and interests of various parties in cyberspace through national laws and policies"); *versus* Wright, (2018, 'Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General' (arguing that "[o]nline as well as everywhere else, the principle of sovereignty should not be used by [S]tates to undermine fundamental rights and freedoms").

98 Reuters (2021, 'SolarWinds Hack was "Largest and Most Sophisticated Attack" Ever: Microsoft President').

99 Jibilian and Canales (2021, 'The US is Readying Sanctions against Russia over the SolarWinds Cyber Attack'); Borghard (2021, 'Was SolarWinds a Different Type of Cyber Espionage?').

perpetrators to remotely control a host of physical devices, including some found in US power grids and nuclear facilities.[100] This has led to suggestions that similar operations affecting operational technologies may be perceived as a threat to use force.[101] The United States formally attributed the operation to the Russian Federation and imposed economic sanctions on Russian nationals and assets in response.[102] For its part, the Russian Federation has not only denied any involvement in the operation but also challenged the legality of those sanctions.[103] Even assuming that the Russian Federation had no involvement in the hack itself, a dispute within the scope of Chapter VI could still arise between the United States and the Russian Federation over the latter's alleged failure to prevent its territory from being used to perpetrate the acts in question.[104]

In contrast, a situation which *might* lead to international friction or give rise to a dispute, the existence of which authorizes the Security Council to open an investigation, has a much wider scope of application. A 'situation' refers to the totality of events, circumstances, and relations that might precede an instance of international friction or a specific dispute.[105] This follows on naturally from the preventive function of Article 34, that is, to enable the Council to act independently from States and other entities and prevent a dispute from arising in the first place.[106] Yet, like a dispute, a situation must be specific enough to trigger a Security Council inquiry.[107] When it comes to ICTs, although general cybersecurity problems such as ransomware or online hate speech are unlikely to qualify as a 'situation' for the purposes of Article 34, a single or a series of such incidents would certainly fall within the scope of said provision.

2.3. Cyber Events Triggering Security Council Action under Chapter VII: Threats to the Peace, Breaches of the Peace, and Acts of Aggression Committed through ICTs

In contrast to Chapter VI, Chapter VII of the Charter is primarily addressed to the Security Council. Specifically, it empowers the Council to require or authorize States to adopt whichever measures it deems necessary to maintain or restore international peace and security.[108] In this way, Chapter VII gives effect to the Council's primary responsibility for the maintenance of international peace and security, recognized in Article 24(1) of the Charter. However, as with Chapter VI, only certain types of events or

---

100 Joe Weiss and Bob Hunter (2021, 'The SolarWinds Hack Can Directly Affect Control Systems'); Software Engineering Institute, CERT Coordination Center (2020, 'SolarWinds Orion API Authentication Bypass Allows Remote Command Execution: Vulnerability Note VU#843464'). See generally USENIX (2012, 2).

101 Hollis and van Benthem (2021, 'What Would Happen If States Started Looking at Cyber Operations as a "Threat" to Use Force?').

102 Brandom (2021, 'US Institutes New Russia Sanctions in Response to SolarWinds Hack').

103 Brennas (2020, 'Russia Denies "Baseless" SolarWinds Claims as Trump Administration Divided on Hack'); Graziosi (2020, 'Russia Denies Claims it was Responsible for Massive Hacking Campaign Targeting US Government and Private Companies').

104 See ICJ (1949, Corfu Channel Case, 22).

105 Schweisfurth (2012, 'Article 34', §24).

106 Schweisfurth (2012, 'Article 34', §6–7.

107 Schweisfurth (2012, 'Article 34', §26.

108 See Articles 39, 41 and 42 Charter of the United Nations.

situations trigger Chapter VII. According to Article 39 of the Charter, such a gateway to enforcement action under Chapter VII is the Council's determination of a threat to the peace, a breach of the peace, or an act of aggression.

There is general agreement that the Council enjoys a wide margin of discretion in determining whether a particular set of facts can be qualified as one of those triggers.[109] However, the practice of the Council indicates that at least the text of Article 39 itself, along with other provisions of the Charter, limit the scope of the Council's discretion in making such determinations.[110] As the wording of Article 39 suggests, what primarily separates those three categories of triggers to Chapter VII is the severity of the situation, including its scale, victims, and proximity to actual violence.

Though not without contestation, the Council has understood a threat to the peace in the widest possible sense.[111] In particular, it has given the label to a variety of situations, specific or general, that may directly or indirectly undermine the state of peace between at least two States, whether by leading to armed conflict or violence, or affecting the overall conditions in society which are necessary to keep the peace, in line with the concept of 'positive peace'.[112] Accordingly, internal situations that may threaten the peace in other States, in a region or globally, even if indirectly, may be qualified as threats to the peace. Examples have included terrorism,[113] piracy,[114] the proliferation of weapons of mass destruction,[115] small arms and light weapons trafficking,[116] food crises,[117] the HIV epidemic,[118] the Ebola outbreak in Africa,[119] and drug trafficking.[120]

As seen earlier, the Security Council has already met formally to discuss cybersecurity issues, including, in particular, present and emerging cyber threats to international peace and security, the impact of malicious uses of ICTs in future conflicts, compliance with international law, and the possible options to respond and to seek a peaceful solution to cyber conflicts or disputes.[121] Likewise, informal Council meetings have addressed the impact of cyberattacks against critical infrastructure, such as hospitals and vaccine research facilities, as well as the threat of hybrid conflicts and cyberwarfare.[122]

---

109 Kirsch (2012, 'Article 39', §§4–5).

110 Kirsch (2012, 'Article 39', §§6, 35); ICTY (1995, Tadić Case, §28).

111 Kirsch (2012, 'Article 39', §13).

112 Kirsch (2012, 'Article 39', §§13–15; de Wet (2009, §§6–15).

113 See note 7 and Security Council 1373 (2001) ("reaffirming that the 9/11 attacks, like any act of terrorism, constitute a threat to international peace and security").

114 E.g., Security Council 2500 (2019) (renewing the counter-piracy measures off the coast of Somalia for 12 months), Security Council 2383 (2017) (renewing the authorization for international naval forces to fight piracy off the coast of Somalia).

115 See note 8.

116 Security Council 2220 (2015); Security Council 2117 (2013); Security Council 1467 (2003).

117 Security Council 2417 (2018) (on conflict-induced food insecurity and the threat of famine).

118 Security Council 1308 (2000) (holding that the HIV epidemic "may pose a risk to stability and security"); Security Council 1983 (2011) (affirming the Security Council's primary responsibility to maintain international peace and security and finding that "the spread of HIV can have a uniquely devastating impact on all sectors and levels of society").

119 E.g., Security Council 2177 (2014).

120 E.g., Security Council S/PRST/2010/4 (2010).

121 Estonia (2021, 'UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace', 3).

122 Notes 20–23.

In earlier resolutions determining the existence of a threat to the peace, particularly those regarding terrorism, the Council has highlighted the role of ICTs in amplifying or spurring violence.[123]

There is little doubt that cyber operations targeting the healthcare sector and other vital services, especially during a pandemic, could, at least in theory, qualify as threats to the peace,[124] given their impact on the life and health of individuals worldwide.[125] Similarly, the use of ICTs in the context of armed conflict, such as for intelligence-gathering or monitoring purposes, or to directly cause physical harm to civilian or military targets, may not only threaten but also significantly undermine the peace in different States, given the interconnectedness of the Internet and other ICTs.[126]

Other good candidates for a 'threat to the peace' qualification include ransomware and certain types of ICT supply chain attacks.[127] Ransomware has already caused significant harm worldwide.[128] It has been used by criminal and terrorist groups, as well as States, to finance unlawful activities, including by circumventing Security Council sanctions.[129] Ransomware attacks have also caused significant economic losses in hundreds of public and private entities around the world[130] and disrupted the delivery of critical services, such as food distribution[131] and healthcare.[132] For their part, ICT supply chain attacks are characterized by the use of malicious software or hardware to exploit vulnerabilities in ubiquitous software or hardware products, such as email providers or messaging applications.[133] While these types of cyber operations have already led to massive economic losses around the world, the risk of serious physical harm to States, private entities, and individuals is latent when 'operational technology'—software or hardware used to monitor or control physical devices—is targeted.[134] Examples of such devices include sensors, thermostats and control valves in water treatment and energy distribution systems, including nuclear power plants, as well as medical equipment.[135]

A possible cyber threat to the peace combining elements of ransomware and ICT supply chain attacks was the 2017 NotPetya attack: not only did it affect businesses and public service providers, such as Ukraine's main airport and State banks, but also the Chernobyl nuclear power plant, whose automatic Windows-based sensors were

123 Note 17.

124 See GGE (2021, §§8–10); Estonia (2021, 'UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace', 2).

125 See GGE (2021, §45).

126 See GGE (2021, §§7, 11).

127 See GGE (2021, §56).

128 Firch (2021, '10 Cyber Security Trends You Can't Ignore in 2021').

129 Huffman et al. (2018, 'Is Paying a Ransom to Stop a Ransomware Attack Illegal?'). See also US Department of the Treasury (2020, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments') (on US sanctions).

130 ENISA (2020, 'Threat Landscape 2020—Ransomware', 3).

131 Morrison (2021, 'Ransomware Attack Hits Another Massive, Crucial Industry: Meat').

132 ENISA (2020, 'Threat Landscape 2020—Ransomware', 3); Mathews (2021, 'Ransomware Attacks on the Healthcare Sector are Skyrocketing').

133 See Smith (2020, 'A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response'). See also GGE (2021, §§56–58); GGE (2013, §24); GGE (2015, §13(g)).

134 GGE (2021, §11).

135 See Courtney (2019, 'Digital Doomsday').

shut down, forcing the site to monitor radiation levels manually.[136] More recently, on 7 May 2021, hackers from Russian-based cybercriminal group DarkSide broke into the system of a major oil pipeline on the east coast of the United States, encrypting the victim's confidential data and demanding a ransom of US$ 5 million in cryptocurrency—paid following significant disruption in oil distribution.[137] Earlier this year, cyber criminals attempted to poison the water supply in Florida by increasing the amount of sodium hydroxide released by remotely controlled valves.[138] And back in 2016, Ukraine fell victim to a winter power blackout thanks to a computer worm infecting its remote operational technology monitoring system.[139] With the urge to work remotely prompted by the COVID-19 pandemic, these and other similar types of operations remotely targeting physical devices in critical infrastructure are bound to grow in number and sophistication.[140]

Aside from cyber operations causing or threatening to cause physical or material harm to persons, objects, or the environment, it is unclear whether purely non-physical harms to data or software that carry no prospect of material repercussions could qualify as a threat to the peace. The Council's practice so far seems to indicate that even in the case of generalized, non-conventional threats to the peace, there should be at least an indirect link to a potential armed conflict, violent confrontation, or some form of material harm to persons, objects, or the environment.[141] However, with the growing importance of data, information, and software for public and private entities, cyber operations targeting these non-physical components can cause serious economic losses, as well as reputational, and other types of moral harm. It is not hard to imagine that, at least in the future, these may significantly undermine peaceful relations between States and therefore be qualified by the Security Council as threats to the peace, even if the prospect of physical harm is remote. This interpretation is a part of a more general tendency to weaken the physical versus non-physical divide when it comes to both goods and harms.

In contrast to threats to the peace, the Security Council has not frequently determined the existence of breaches of the peace. So far, all examples of such a determination have corresponded to armed confrontations between States or non-State groups, such as the Malvinas/Falkland Islands conflict and Iraqi's invasion of Kuwait.[142] Nevertheless, a textual and purposive interpretation of the term, in the context of other Charter provisions, suggests that it covers not only armed force, but *at least* other forms of physical violence or harm to persons, objects, or the environment. The key difference between a 'threat to' and a 'breach of' the peace seems to relate to timing: whereas a threat implies imminence, a breach corresponds to the actualization of whatever is

136 Greenberg (2018, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History').

137 Tidy, (2021, 'Colonial Hack: How did Cyber-Attackers Shut off Pipeline?'); Nakashima et al. (2021, 'Ransomware Attack Leads to Shutdown of Major U.S. Pipeline System'). For a very similar attack that occurred last year, see Seals, (2020, 'U.S. Pipeline Disrupted by Ransomware Attack').

138 Tidy (2021, 'Hacker Tries to Poison Water Supply of Florida City').

139 Zetter (2016, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid').

140 Russon (2021, 'US Fuel Pipeline Hackers "Didn't Mean to Create Problems"').

141 Kirsch (2012, 'Article 39', §30).

142 Kirsch (2012, 'Article 39', §41).

threatened, *in casu*, a rupture of peaceful relations between States and other global actors.

In any event, given the discretionary nature of the determination of a breach of the peace, the Security Council need not follow such precedents when deciding to attach the label to new factual situations. Therefore, nothing stops the Council from finding that a breach of the peace exists whenever a cyber operation has occurred and resulted in the breakdown of peaceful relations. Such a cyber operation may directly cause physical harm, prompting or amplifying violence or armed conflict, or affect non-physical goods which are deemed essential to maintaining the peace in an international setting, such as widespread disinformation campaigns targeting electoral results or health advice, or online incitement to violence, hatred or discrimination, especially in politically unstable regions or in times of global distress. Violations of democratic principles have already featured in a number of binding Council resolutions, though they have been qualified as threats to the peace and linked to dangerous overall conditions, such as humanitarian catastrophes or civil strife.[143] A possible breach of the peace already on the Security Council's radar[144] is the situation in Myanmar, where widespread violence against the Rohingya and the ensuing cross-boundary refugee flows were spurred in large part due to online hate speech.[145]

Lastly, an act of aggression is the most serious of Chapter VII triggers. As General Assembly resolution 3314 indicates, aggression is usually defined as a serious use of military force by a State against another State.[146] Examples include the military occupation or annexation of another State's territory, bombardment or the use of weapons in the territory of another State, or the sending by or on behalf of a State of non-State groups that carry out serious acts of armed force against another State.[147] However, like the other two triggers, the determination of an act of aggression is a political, discretionary act, which means that in doing so the Security Council is not limited by any existing instrument except the Charter itself.[148] Thus, the Council may well determine the existence of an act of aggression in situations that do not neatly fit within the list of acts in resolution 3314 or previous determinations of acts of aggression.

In particular, given the growing military and economic power of non-State groups, especially in the ICT environment, the Council might well consider that an act of aggression has been directly committed by one such group, irrespective of attribution to or support of a State. Such a finding has been made by the Council in at least one

143 See, e.g., Security Council 1542 (2004) (on the situation in Haiti).

144 E.g., Security Council SC/13055 (2017); Security Council SC/14430 (2021).

145 HRC A/HRC/39/64 (2018, §74). Stecklow (2018, 'Why Facebook is losing the war on hate speech in Myanmar'). On the role of online hate speech in armed conflict generally, see Mercy Corps (2019, 'The Weaponization of Social Media: How Social Media can Spark Violence and What can be Done about it'); ICRC (2021, 'Misinformation, Disinformation and Hate Speech in Armed Conflict and Other Situations of Violence: A Practical Guide for Field Teams').

146 General Assembly 3314 (XXIX) (1974, Article 1).

147 General Assembly 3314 (XXIX) (1974, Article 3).

148 Kirsch (2012, 'Article 39', §§43–44); Martenczuk (1999, 540–542).

resolution.[149] It would sit alongside what some States and scholars see as a expansion in the concept of 'armed attack' within the meaning of Article 51 of the Charter, which would include acts committed by a non-State groups irrespective of attribution to a State.[150]

In the same vein, at least cyber operations having the scale and physical, kinetic effects akin to military weapons, such as the destruction or shutting down of a power plant, may well be qualified as armed attacks or acts of aggression.[151] Questions remain as to whether cyber operations affecting the delivery of public or private services in a non-physical but functional way, such as distributed denial of service attacks against critical systems, or causing purely economic harm could qualify as an *armed* attack, given the military connotation of the term.[152] But fewer objections are likely to arise if such an operation is qualified as an act of *aggression*, given the political nature of its determination.[153] It is an altogether different question whether the Council would, in fact, make such a determination—or similar findings of threats to or breaches of the peace for that matter—bearing in mind that the most serious cyber operations yet have implicated at least one permanent member of the Security Council. Likewise, it is questionable whether the Council should be making those determinations in circumstances where they would lead to further politicization or militarization of ICT-related events.

149 Security Council 419 (1977). See also Dinstein (2015, §31).

150 See Chachko and Deeks (2016, 'Which States Support the "Unwilling and Unable" Test?'); Trapp (2015); Bethlehem (2012); Wilmshurst (2005, §6). *Contra* ICJ (2004, 'Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory', §139); ICJ (2005, 'Armed Activities on the Territory of the Congo', §146); Haque (2021, 'Self-Defense Against Non-State Actors: All Over the Map').

151 Schmitt (2017, 340–342, esp. §§6–8).

152 Schmitt (2017, 339–343, esp. §§2, 12–13).

153 See Dinstein (2015, §1) (noting that "[i]t has never been settled whether aggression of itself must consist of use of force, or whether it could manifest itself through lesser acts, such as the threat of force, or even acts unrelated to the use of force").


MACRO
VERIFYING DATA v.401
· ALPHA 1048
ROT. SPEED = 1204.3
POSITIVE ANALYSIS
POSITIVE DATA 201-45
>> BETA v.7
STRUCTURE ANALYS
> POS. // ROT.
VERIFYING DATA v. 50
· ALPHA 3913
CONTINUE...
GATE DIAGNOSTICS
SUBSPACE PI
00.23453.34
00.9945345
NC 00.52
NC 00.22
NC
F5
F6
F7
LR6
LR6
JF

3. IMPLEMENTING CHAPTERS VI AND VII OF THE CHARTER IN THE ICT ENVIRONMENT

Having established that specific or general situations involving the use of ICTs may trigger the application of Chapters VI and VII of the Charter, the question arises as to whether these situations call for cyber-specific measures. While there is no single, general answer to this question, traditional mechanisms of dispute settlement, investigation, and military or non-military enforcement action remain available and can be useful in the face of new types of situations affecting hardware, software, data, or individuals. However, it is possible to conceive of several non-conventional measures directed at any of those ICT components that could substitute for or complement the adoption of traditional measures under Chapters VI and VII of the Charter.

For the sake of simplicity, these various 'cyber measures', whether virtual or physical, can be divided into five broad categories: i) dispute settlement and fact-finding mechanisms, ii) quasi-legislative measures, iii) technical and capacity-building measures, iv) institutional arrangements, and v) cooperation. These are not water-tight categories but reflect the overarching aspects of each type of measure.

In the same vein, *triggers* to Chapter VI—situations which might lead to international friction or a dispute, and disputes likely to endanger international peace and security—and Chapter VII—threats to the peace, breaches of the peace, and acts of aggression—overlap to some extent. This means that measures taken or recommended under Chapter VI may be adopted by the Security Council under Chapter VII, and vice versa. Accordingly, some categories of measures described below may fall within the scope of Chapters VI and/or VII, depending on their triggers, nature, and purpose. It is also worth noting that such ICT measures may well be useful in tackling traditional, non-ICT triggers.

3.1. Dispute Settlement and Fact-Finding Mechanisms for ICT-Related Situations

Article 33(1) of the Charter provides States and other parties to a dispute likely to endanger international peace and security with a catalogue of mechanisms to resolve any such disputes. Without any preference, parties may resort to negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, regional agencies or arrangements, or other peaceful means of their choice. Likewise, before assisting the parties in the resolution of such disputes, the Security Council may carry out an investigation into the facts of a situation likely causing international friction or giving rise to a dispute. For its part, Article 41 of the Charter empowers the Council to create judicial or quasi-judicial bodies to settle disputes between States, non-State entities, and individuals.[154] The Security Council has used those powers to establish the

154 Kirsch (2012, 'Article 41', §26).

International Criminal Tribunals for the Former Yugoslavia[155] and Rwanda,[156] as well as the Special Tribunal for Lebanon.[157]

Faced with the growing digitalization of goods and services, it has become increasingly common for individuals and corporations to conclude agreements and register commercial or public transactions using different ICTs.[158] The most common of such technologies is blockchain, that is, a software-based system serving as a digital ledger for automated transactions which are validated by different users in a decentralized manner and subsequently made public and immutable.[159] The technology has been used in numerous applications, such as cryptocurrency, smart contracts, digital identity, voting mechanisms, and other digital transactions.[160]

Given the ease with which financial and notarial operations can be automated using computer programmes, it is only natural that disputes involving such transactions are being resolved by digital means too. For instance, the UK Jurisdiction Taskforce has recently issued detailed rules on digital dispute resolution in the United Kingdom, applicable to different digital technologies, such as cryptocurrency, smart contracts, distributed ledger technology, and fintech applications.[161] In disputes subscribing to the rules, all written claims, counterclaims, responses, and evidence are submitted electronically to the competent tribunal, whose decision is directly and automatically implemented 'on-chain', that is, on the relevant blockchain platform, using a private key.[162] By the same token, in disputes involving virtual transactions, such as the use of cryptocurrency to evade economic sanctions and finance terrorism,[163] the effective use of certain software applications and expert knowledge, such as chain analysis, will be essential.

To be sure, many ICT-related disputes or situations falling within the scope of Chapters VI and VII do not lend themselves to fully automated dispute resolution mechanisms, such as complex questions surrounding legal, political, or factual attribution of cyber operations. Yet several aspects of online dispute resolution and fact-finding mechanisms, such as remote hearings, electronic submissions, secure party identification, and digital evidence can help address several types of situations involving the use of ICTs. The same goes for traditional, non-ICT situations—a development accelerated by the COVID-19 pandemic.[164] Moreover, although the ICJ is the preferred forum for

155 Security Council 827 (1993).

156 Security Council 955 (1994).

157 Security Council 1757 (2007).

158 See OECD (2021, 'Digital Trade'); Elding and Morris (2018).

159 Conway (2020, 'Blockchain Explained'); IBM (2021, 'What is Blockchain Technology?').

160 Daley (2021, '30 Blockchain Applications and Real-World Use Cases Disrupting the Status Quo'); Business Insider (2020, 'The Growing List of Applications and Use Cases of Blockchain Technology in Business and Life').

161 Lawtech UK (2021, 'Digital Dispute Resolution Rules', 4).

162 Lawtech UK (2021, 'Digital Dispute Resolution Rules', 6–8).

163 See Myers et al. (2020, 'Crypto-Controls: Harnessing Cryptocurrency to Strengthen Sanctions'); US Department of Justice (2020, 'Cryptocurrency Enforcement Framework: Report of the Attorney General's Cyber Digital Task Force', 45–48, 51).

164 Susskind (2020).

legal disputes between States,[165] it may not be the most appropriate venue for cyber disputes involving heavily technical fact-finding. In particular, key factual questions will ultimately depend on appointed experts whose transparency and legitimacy are far from established. The ICJ's advisory function, triggered by the Security Council, the General Assembly, or other authorized United Nations organs and specialized agencies,[166] could nonetheless be useful to clarify how the Charter and international law more generally apply to the use of ICTs. And one must not forget the key role of the Secretary-General in making "available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace".[167]

3.2. Quasi-Legislative Measures in the Cyber Context

Article 41 does not explicitly list the adoption of resolutions condemning, demanding, or endorsing certain conduct as one of the non-military measures available to the Security Council under Chapter VII. Yet these have become increasingly common in the Council's practice, particularly in the context of terrorism, weapons of mass destruction, armed conflict, and international criminal justice.[168] Notably, some of these resolutions have been addressed not only to States but also to non-State groups and individuals,[169] meaning that, at least under one view,[170] the Council can directly bind those entities. In the ICT context, these so-called quasi-legislative measures, whether general or specific, may not be strictly necessary for States, since, as argued earlier, existing international law applies as a whole to ICTs. However, at least two types of quasi-legislative measures under Chapters VI or VII focusing specifically on ICTs could be a helpful complement to the interpretation and application of international law in the cyber context.

First, the Security Council could make specific recommendations as to how States could implement their existing international obligations in the ICT environment. Although the GGE and OEWG are currently addressing the topic, their findings and recommendations remain predominantly general. As such, they could benefit from more concrete guidance from the Council or the General Assembly. Second, given the significance of non-State actors in the use, design, sale, and control of ICTs, the Council could directly address such entities, whether criminal groups or technology companies, to settle disputes or respond to threats to the peace, breaches of the peace, or acts of aggression occurring in the ICT environment. For instance, when seeking to counter the circumvention of its sanctions by States and non-State actors, the Council could require virtual asset providers and exchanges, such as Bitcoin and Ethereum, to ensure that their transactions follow the necessary checks to comply with current sanctions

165 Article 36(3), Charter of the United Nations.

166 Article 96, Charter of the United Nations.

167 Secretary-General (2018, Agenda for Disarmament: Implementation Plan, Action 30).

168 Kirsch (2012, 'Article 41', §§30–33). See generally Talmon (2005).

169 E.g., Security Council 1333 (2000, §§9, 16(b)); Security Council 2178 (2014, §1); Security Council 1203 (1998, §4).

170 See Peters (2014, 'Security Council Resolution 2178 (2014): The "Foreign Terrorist Fighter" as an International Legal Person, Part I').

lists.[171] This would be in line with recommendations made during the 2015 High Level Review of United Nations Sanctions, which called upon Member States to

> address transnational threats and new technologies, including the use of the Internet for illicit activities, within existing frameworks, including under Security Council resolutions 2161 and 2178. Other stakeholders including Internet users and the IT industry should be engaged to address such threats in the implementation of sanctions.[172]

Similarly, in any future resolution addressing the situation in Myanmar, the Council should require social media companies to moderate violent content in line with international human rights law.[173] By piercing the State veil and directly addressing non-State actors, these measures could fill an important responsibility gap in international law.

3.3. Technical and Capacity-Building Measures to Address ICT Incidents

Given the technical complexity of ICTs, disputes, situations, threats to the peace, breaches of the peace, or acts of aggression occurring in the cyber context may call for technical and capacity-building measures. States and corporations around the world have consistently adopted cybersecurity measures and other technical solutions to prevent, mitigate, and remedy a range of malicious cyber operations, while building the necessary capacity and resilience to address such threats domestically and internationally. Key examples of technical measures include the monitoring of suspicious cyber activity;[174] the use of encryption to protect the integrity and confidentiality of online communications; the issuance of technical standards for ICT products and data use,[175] along with the necessary mechanisms to verify that they are safe by design; risk assessments;[176] vulnerability disclosure programmes;[177] emergency shutdown systems; and human-in-the-loop safeguards. Particularly pressing is the need to curb the use of cryptocurrency for terrorism financing and sanctions evasion. To this end, the Council should consider requiring or recommending States and private entities to adopt technical measures such as Know-Your-Customer (KYC) or Know-Your-Transaction (KYT) checks, which enable financial institutions to verify the identity of users and trace their digital transactions. For their part, capacity-building measures ought to go beyond the acquisition of technical, cybersecurity expertise. They should also involve educational strategies, such as digital literacy and cyber awareness-raising

171 See note 148 and Jurva (2020, 'Using Blockchain to Avoid Global Sanctions & how Financial Institutions can Prevent it'); Fanusie and Robinson (2018, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services').

172 General Assembly and Security Council A/69/941-S/2015/432 (2005, 72, Rec. 146).

173 See HRC A/HRC/38/35 (2018); HRC A/74/486 (2019).

174 E.g., UK National Cyber Security Centre (2021, '10 Steps to Cyber Security: Monitoring').

175 GGE (2021, §§57(d), 63); ITU (2008, 8, §2.7, 2.10); G7 (2019).

176 GGE (2021, §57(a)).

177 GGE (2021, §§60-–64); OEWG (2021, §28).

campaigns, as well as legal, diplomatic, policy, legislative, regulatory, and dispute-settlement skills,[178] all of which are most needed among developing countries.[179]

3.4. Institutional Arrangements for the ICT Environment

As seen earlier, the Security Council has already established judicial and quasi-judicial institutions to maintain or restore international peace and security under Chapter VII. It has also used its Chapter VII powers to authorize Member States to contribute troops to either keep or enforce the peace in other States or regions,[180] as well as to set up temporary territorial administration structures.[181] Similarly, Chapter VI has been used to recommend institutional arrangements in the peaceful settlement of disputes.[182]

To assist the parties in resolving ICT-related disputes or situations within the meaning of Chapter VI, it is likely that either traditional or automated dispute settlement mechanisms would not suffice on their own. Given the abovementioned difficulties in factually attributing cyber operations, specific institutional arrangements benefitting from the necessary technical expertise could be put in place to deal with attribution investigations and disputes.[183] Reforms within the Council's existing bodies, such as its Sanctions Committee, may also be necessary to enable them to effectively deal with ICT-related challenges falling within their mandate.

Cyber-specific institutional arrangements may also be necessary when the Council decides to take military measures under Chapter VII. In particular, private control over the core of the Internet and other ICTs may require partnerships between States and technology companies to enforce the necessary military measures, whether software, hardware, or data-based. The same is true of State action in self-defence through ICTs: States are unlikely to mount an effective defence to repel or prevent cyber operations amounting to an 'armed attack' without the technical expertise of the industry. Thus, collective security in the digital age might become increasingly privatized,[184] and it is up to States and the Council to adopt all necessary safeguards, including corporate accountability.

178 OEWG (2021, §§59–61).

179 GGE (2021, §89); OEWG (2021, §58).

180 Article 42 and Chapter VIII, Charter of the United Nations. See also Bothe (2012, §§21–22, 33); Kirsch (2012, 'Article 42', §§8–10, 24).

181 Kirsch (2012, 'Introduction to Chapter VII: The General Framework', §§20–21).

182 Kirsch (2012, 'Introduction to Chapter VII: The General Framework', §§19, 35–37).

183 See GGE (2021, §§26–28); Shany and Schmitt (2020).

184 See Eichensehr (2017).

3.5. Cooperation

Lastly, different forms of international cooperation have been both recommended under Chapter VI and required under Chapter VII. Cooperation is an essential measure to address any international issue, but it becomes all the more important in the cyber context, given the global, interconnected nature of the Internet and other ICTs.[185] Without cooperation among States and technology companies, a cyber vulnerability in one location can quickly become a global problem,[186] as was the case with the SolarWinds hack. Key cooperative measures in the ICT environment include the notification of cyber incidents, as well as the sharing of incident-specific information and technical expertise.[187]

185 See GGE (2021, §11); GGE (2015, §19).

186 GGE (2021, §12).

187 E.g., People's Republic of China (2020, 'Statement by Minister-Counsellor Mr. Yao Shaojun at Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure'); Sullivan (2019, 'Remarks at the Second Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace'); CISA (2020, 'Alert (AA20-245A), Technical Approaches to Uncovering and Remediating Malicious Activity').

4. CONCLUSION

There is no question that international law as a whole and the Charter in particular apply to ICTs, as they do to other technologies. From a technical perspective, cyberspace is not a space or a domain proper, but a combination of digital technologies comprising physical, logical, data, and personal layers, spread across existing domains. Given the pervasiveness and interconnectedness of ICTs, different types of cyber operations, whether in isolation or taken together, might fall well within the scope of Chapters VI and VII of the Charter. They range from disputes about legal, political, or factual attribution of specific cyber operations to systematic ICT phenomena which can endanger or undermine international peace and security, such as ransomware, ICT supply chain attacks, disinformation, online hate speech, sanctions evasion, or cyber-enabled terrorism financing.

These operations do not take place in a completely virtual environment but go beyond software and data to cause serious harm to physical devices and persons, including States, companies, and, most importantly, individuals. As such, measures to address them under Chapters VI and VII of the Charter may take a variety of forms. They include traditional but also cyber-specific dispute settlement, fact-finding, quasi-legislative action, technical and capacity-building measures, institutional arrangements, and cooperation. For many of these measures, it will be necessary to involve technology companies, given their expertise and dominance in the ICT environment. While the adoption and implementation of those measures may raise new and old challenges, such as existing Global North–South and East–West political tensions, they offer States, the Security Council, and other United Nations bodies a unique opportunity to fill important gaps in international law and practice.

REFERENCES

Abbott, Cameron. 2019. 'Interlopers in Things? IoT Devices May be used as Backdoors to your Network.' *The National Law Review*, 27 August 2019. As of 21 May 2021: https://www.natlawreview.com/article/interlopers-things-iot-devices-may-be-used-backdoors-to-your-network.

Agence France-Presse (AFP) & Associated Press (AP). 2017. "North Korea denies US WannaCry cyberattack accusation.' *Deutsche Welle (DW)*, 21 December 2017. As of 21 May 2021: https://www.dw.com/en/north-korea-denies-us-wannacry-cyberattack-accusation/a-41886938.

Akande, Dapo; Coco, Antonio Coco & de Souza Dias, Talita. 2021. 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', *EJIL: Talk!*, 5 January 2021. As of 21 May 2021: https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

Al-Dulimi and Montana Management Inc. v Switzerland. 2016. ECtHR.

Al-Jedda v. United Kingdom. 2011. European Court of Human Rights (ECtHR).

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Merits). 2005. International Court of Justice.

Article 19. 2015. '"Hate Speech" Explained: A Toolkit'. As of 21 May 2021: https://www.article19.org/resources/hate-speech-explained-a-toolkit.

Australia. 2020. 'Statement by H.E. Dr. Tobias Feakin, Ambassador for Cyber Affairs.' 22 May 2020. As of 21 May 2021: https://vm.ee/sites/default/files/Estonia_for_UN/unsc_-_cyber_arria_22_may_2020_-_australian_statement_002.pdf.

BBC. 2018. 'UK and US Blame Russia for "Malicious" NotPetya Cyber-attack.' *BBC News*, 15 February 2018. As of 21 May 2021: https://www.bbc.co.uk/news/uk-politics-43062113.

Bethlehem, Daniel. 2012. 'Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors.' *The American Journal of International Law* 106(4): 770-777.

Borghard, Erica D. 2021. 'Was SolarWinds a Different Type of Cyber Espionage?' *Lawfare*, 9 March 2021. As of 21 May 2021: https://www.lawfareblog.com/was-solarwinds-different-type-cyber-espionage.

Bothe, Michael. 2012. 'Peacekeeping.' In *The Charter of the United Nations: A Commentary, Volume I*, edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1171. Oxford: Oxford University Press.

Brandom, Russell. 2021. 'US institutes new Russia sanctions in response to SolarWinds hack.' *The Verge*, 15 April 2021. As of 21 May 2021: https://www.theverge.com/2021/4/15/22385371/russia-sanctions-solarwinds-biden-white-house-putin-hack.

Brennas, David. 2020. 'Russia Denies "Baseless" SolarWinds Claims as Trump Administration Divided on Hack.' *Newsweek*, 21 December 2020. As of 21 May 2021: https://www.newsweek.com/russia-denies-baseless-solarwinds-claims-trump-admin-divided-hack-1556316.

Burt, Tom. 2020. 'Cyberattacks Targeting Health Care Must Stop.' *Microsoft On the Issues*, 13 November 2020. As of 21 May 2021: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/.

Carnegie Mellon University, Software Engineering Institute, CERT Coordination Center. 2020. 'SolarWinds Orion API Authentication Bypass Allows Remote Command Execution: Vulnerability Note VU#843464.' 26 December 2020. As of 21 May 2021: https://kb.cert.org/vuls/id/843464.

Chachko, Elena & Deeks, Ashley. 2016. 'Which States Support the "Unwilling and Unable" Test?' Lawfare, 10 October 2016. As of 5 July 2021: https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test.

Coco, Antonio & de Souza Dias, Talita. 2021. '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law.' *European Journal of International Law*, 2021 (forthcoming).

Cohen, Julie E. 2007. 'Cyberspace as/and Space.' *Columbia Law Review* 107: 210-256.

Conway, Luke. 2020. 'Blockchain Explained.' *Investopedia*, 17 November 2020. As of 21 May 2021: https://www.investopedia.com/terms/b/blockchain.asp.

Corfu Channel Case (United Kingdom v Albania) (Merits). 1949. International Court of Justice.

Council of the European Union (EU). 2020. 'Press Release: 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic.' 30 April 2020. As of 21 May 2021: https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

Courtney, Martin. 2019. 'Digital Doomsday.' *Engineering & Technology Magazine*, 8 October 2019. As of 21 May 2021: https://eandt.theiet.org/content/articles/2019/10/digital-doomsday.

Cybersecurity & Infrastructure Security Agency (CISA), 2020. 'Alert (AA20-245A): Technical Approaches to Uncovering and Remediating Malicious Activity.' 24 September 2020. As of 21 May 2021: https://us-cert.cisa.gov/ncas/alerts/aa20-245a.

Czech Republic. 2020. 'Comments submitted by the Czech Republic in Reaction to the Initial "Pre-draft" Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.' 11 March 2020. As of 21 May 2021: https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf.

Daley, Sam. 2021. '30 Blockchain Applications and Real-World Use Cases Disrupting the Status Quo.' *Built In*, 31 March 2021. As of 21 May 2021: https://builtin.com/blockchain/blockchain-applications.

de Wet, Erika. 2009. 'Peace, Threat to', *Max Planck Encyclopedia of Public International Law*, June 2009. As of 21 May 2021: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e374.

Dinstein, Yoram. 2015. 'Aggression', *Max Planck Encyclopedia of Public International Law*. September 2015. As of 21 May 2021: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e236.

Eclypsium. 2019. 'Anatomy of a Firmware Attack.' *Security Boulevard*, 19 December 2019. As of 21 May 2021: https://securityboulevard.com/2019/12/anatomy-of-a-firmware-attack/.

Egloff, Florian J. & Smeets, Max. 2021. 'Publicly Attributing Cyber Attacks: A Framework.' *Journal of Strategic Studies*. 10 March 2021. As of 5 July 2021: https://doi.org/10.1080/01402390.2021.1895117.

Eichensehr, Kristen. 2017. 'Public-Private Cybersecurity.' *Texas Law Review* 95: 467-538.

———. 2017. 'Three Questions on the WannaCry Attribution to North Korea.' *Just Security*, 20 December 2017. As of 21 May 2021: https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/.

Elding, Catherine & Morris, Richard. 2018. 'Digitalisation and its Impact on the Economy: Insights from a Survey of Large Companies.' *European Central Bank Economic Bulletin* 7. As of 21 May 2021: https://www.ecb.europa.eu/pub/economic-bulletin/focus/2018/html/ecb.ebbox201807_04.en.html.

Estonia. 2021. 'UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace.' 29 June 2021. As of 5 July 2021: https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Concept-note-UNSC-open-debate-on-cybersecurity-29.06.2021.pdf.

European Union (EU). 2020. Statement on Behalf of the European Union by Mr. Pawel Herczyski, Managing Director for CSDP and Crisis Response, European External Action Service, 22 May 2020. As of 21 May 2021: https://vm.ee/sites/default/files/Estonia_for_UN/20_05_22_arria_cyber_eu_statement_as_delivered_unread_paras.pdf.

European Union Agency for Network and Information Security (ENISA). 2017. 'Hardware Threat Landscape and Good Practice Guide.' 8 February 2017. As of 21 May 2021: https://www.enisa.europa.eu/publications/hardware-threat-landscape.

———. 2020. 'Cybersecurity in the Healthcare Sector during COVID-19 Pandemic.' 11 May 2020. As of 21 May 2021: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic.

———. 2020. 'Threat Landscape 2020—Ransomware.' 20 October 2020. As of 21 May 2021: https://www.enisa.europa.eu/publications/ransomware.

Fang, Weidong; Li, Fengrong; Sun, Yanzan; Shan, Lianhai; Chen, Shanji; Chen, Chao & Li Meiju. 2016. 'Information Security of PHY Layer in Wireless Networks.' *Journal of Sensors* 2016: 1-10. As of 21 May 2021: https://doi.org/10.1155/2016/1230387.

Fanusie, Yaya J. & Robinson Tom. 2018. 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services.' *Center on Sanctions & Illicit Finance*, 12 January 2018. As of 21 May 2021: https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO_Bitcoin_Laundering.pdf.

Firch, Jason. 2021. '10 Cyber Security Trends You Can't Ignore in 2021.' *Purplesec*, 31 December 2020. As of 21 May 2021: https://purplesec.us/cyber-security-trends-2021/#Ransomware.

Fruhlinger, Josh. 2020. 'Ransomware Explained: How it Works and How to Remove it.' *CSO*, 19 June 2020. As of 21 May 2021: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

G7, 2019. 'Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices.' 26 August 2019. As of 21 May 2021: https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf.

Gibson, William. 1982. *Burning Chrome*. New York: Omni.

———. 1984. *Neuromancer*. New York: Ace.

Giegerich, Thomas. 2012. 'Article 36.' In *The Charter of the United Nations: A Commentary, Volume I,* edited by Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1119. Oxford: Oxford University Press.

———. 2012. 'Article 37.' In *The Charter of the United Nations: A Commentary, Volume I,* edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1146. Oxford: Oxford University Press.

Gisel, Laurent & Rodenhäuser, Tilman. 2019. 'Cyber Operations and International Humanitarian Law: Five Key Points', *Humanitarian Law & Policy*, 28 November 2019. As of 21 May 2021: https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.

Global Affairs Canada. 2020. 'Statement on Malicious Cyber Threats to the Health Sector.' 30 April 2020. As of 21 May 2021: https://www.canada.ca/en/global-affairs/news/2020/04/statement-on-malicious-cyber-threats-to-the-health-sector.html.

Global Commission on the Stability of Cyberspace. 2018. 'Definition of the Public Core, to which the Norm applies.' May 2018. As of 21 May 2021: https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf.

Goldsmith, Jack. 2017. 'The Strange WannaCry Attribution.', *Lawfare*, 21 December 2017. As of 21 May 2021: https://www.lawfareblog.com/strange-wannacry-attribution.

Graziosi, Graig. 2020. 'Russia Denies Claims it was Responsible for Massive Hacking Campaign Targeting US Government and Private Companies.' *The Independent*. As of 21 May 2021: https://www.independent.co.uk/news/world/russia-hack-us-government-b1773987.html.

Greenberg, Andy. 2018. 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History.' *WIRED Magazine*, 22 August 2018. As of 21 May 2021: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

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

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

———. 2021. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,* advance copy, 28 May 2021. As of 4 June 2021: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

Haque, Adil Ahmad. 2021. 'Self-Defense against Non-State Actors: All Over the Map.' *Just Security*, 24 March 2021. As of 21 May 2021: https://www.justsecurity.org/75487/self-defense-against-non-state-actors-all-over-the-map/.

Hewlett-Packard (HP). 2015. 'Top Five Common Intranet Security Weaknesses.' *The Telegraph*, 19 November 2015. As of 21 May 2021: https://www.telegraph.co.uk/business/sme-home/five-common-intranet-security-weaknesses/.

Hollis, Duncan B. & van Benthem, Tsvetelina. 2021. 'What Would Happen if States Started Looking at Cyber Operations as a "Threat" to Use Force?.' *Lawfare*, 30 March 2021. As of 21 May 2021: https://www.lawfareblog.com/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force.

Huffman, Bart W.; Lowell, Michael J.; Bartnick, Wendell J. & Nowicki, Julianne K. 2018. 'Is Paying a Ransom to Stop a Ransomware Attack Illegal?.' *ReedSmith*, 19 January 2018. As of 21 May 2021: https://www.sxsw.com/wp-content/uploads/2018/03/Legality-of-Paying-Ransom-FINAL-2018.1.19.pdf.

Human Rights Committee, 2018. Report of the Independent International Fact-finding Mission on Myanmar: Advance Edited Version, UN document A/HRC/39/64, 12 September 2018.

Human Rights Council. 2018. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN document A/HRC/38/35, 6 April 2018.

———. 2019. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN document A/74/486, 9 October 2019.

IBM, 2021. 'What is Blockchain Technology?.' As of 21 May 2021: https://www.ibm.com/topics/what-is-blockchain.

Insider Intelligence. 2020. 'The Growing List of Applications and Use Cases of Blockchain Technology in Business and Life.' *Business Insider*, 2 March 2020. As of 21 May 2021: https://www.businessinsider.com/blockchain-technology-applications-use-cases?r=US&IR=T.

International Civil Aviation Organization (ICAO). 1944. *Convention on International Civil Aviation*. 15 UNTS 295.

International Committee of the Red Cross (ICRC). 2013. 'Cyberwarfare and International Humanitarian Law: The ICRC's position.' June 2013. As of 5 July 2021: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf.

———. 2019. 'Position Paper—International Humanitarian Law and Cyber Operations during Armed Conflicts.' 28 November 2019. As of 21 May 2021: https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.

———. 2021. 'Misinformation, Disinformation and Hate Speech in Armed Conflict and Other Situations of Violence: A Practical Guide for Field Teams'. As of 21 May 2021: https://shop.icrc.org/download/ebook?sku=4526/002-ebook.

International cyber law: interactive toolkit contributors. 2020. 'Scenario 19: Hate speech.', *International Cyber Law: Interactive Toolkit*, 1 October 2020. As of 21 May 2021: https://cyberlaw.ccdcoe.org/w/index.php?title=Scenario_19:_Hate_speech&oldid=2231.

International Institute for Sustainable Development (IISD). 2021. 'UN Secretary-General Presents 10 Priorities for 2021.' *SDG Knowledge Hub*, 3 February 2021. As of 21 May 2021: https://sdg.iisd.org/news/un-secretary-general-presents-10-priorities-for-2021/.

International Law Commission (ILC). 2006. Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, Report of the Study Group of the International Law Commission Finalized by Martti Koskenniemi, UN document A/CN.4/L.682, 13 April 2006.

International Telecommunications Union (ITU). 2008. 'Global Cybersecurity Agenda, High-Level Experts Group: Report of the Chairman of the HLEG. As of 21 May 2021: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf.

Jibilian, Isabella & Canales, Katie. 2021. 'The US is Readying Sanctions against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why it's Such a Big Deal.' *Business Insider*, 15 April 2021. As of 21 May 2021: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T.

Johnson, David & Post, David. 1996. 'Law and Borders: The Rise of Law in Cyberspace.' *Stanford Law Review* 48(5): 1367-1402.

Jurva, Gina. 2020. 'Using Blockchain to avoid Global Sanctions & How Financial Institutions can Prevent it.' *Thomson Reuters: Legal Executive Institute*, 9 June 2020. As of 21 May 2021: https://www.legalexecutiveinstitute.com/blockchain-global-sanctions/.

Juul, Mona. 2020. 'Joint Statement from Denmark, Finland, Iceland, Sweden and Norway by Ambassador Mona Juul at the Arria-meeting on Cyber Stability and Conflict Prevention.' 22 May 2020. As of 21 May 2021: https://www.norway.no/en/missions/UN/statements/security-council/2020/arria-cyber-stability-and-conflict-prevention.

Kaspersky. 2018. 'What is Malicious Code.' 2 February 2018. As of 21 May 2021: https://www.kaspersky.co.uk/resource-center/definitions/malicious-code.

Kavanagh, Camino. 2017. 'The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century.' *UNIDIR Resources*, December 2017. As of 21 May 2021: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/UNIDIR_UN_Cyber_Peace_Sec.pdf.

Khanna, Pallavi. 2018. 'State Sovereignty and Self-Defence in Cyberspace.' *BRICS Law Journal* 5(4): 139-154.

Kirsch, Nico. 2012. 'Article 39.' In *The Charter of the United Nations: A Commentary, Volume II*, edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1272. Oxford: Oxford University Press.

———. 2012. 'Article 41.' In *The Charter of the United Nations: A Commentary, Volume II*, edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1305. Oxford: Oxford University Press.

———. 2012. 'Article 42.' In *The Charter of the United Nations: A Commentary, Volume II*, edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1330. Oxford: Oxford University Press.

———. 2012. 'Introduction to Chapter VII: The General Framework.' In *The Charter of the United Nations: A Commentary, Volume II*, edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1240. Oxford: Oxford University Press.

Lawtech UK. 2021. 'UK Jurisdiction Taskforce: Digital Dispute Resolution Rules.' 22 April 2021. As of 21 May 2021: https://technation.io/lawtech-uk-resources/#rules.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion. 2004. International Court of Justice.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion. 1996. International Court of Justice.

Lessig, Laurence. 1996. 'The Zones of Cyberspace.' *Stanford Law Review* 48: 1403–1411.

———. 2006. *Code: Version 2.0*. New York: Basic Books.

Lawrence, Nigel & Traynor, Patrick. 2012. "Under New Management: Practical Attacks on SNMPv3", paper, *WOOT'12: Proceedings of the 6th USENIX conference on Offensive Technologies*, Berkeley, United States, August 2012, available at https://dl.acm.org/doi/10.5555/2372399.2372416, p. 1.

Libicki, Martin C. 2016. *Cyberspace in Peace and War.* Annapolis: Naval Institute Press.

Lillemose, Jacob & Kryger, Mathias. 2015. 'The (Re)invention of Cyberspace.' *Kunstkritikk,* 24 August 2015. As of 21 May 2021: https://web.archive.org/web/20150826204717/http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/.

Martenczuk, Bernd. 1999. 'The Security Council, the International Court and Judicial Review: What Lessons from Lockerbie?.' *European Journal of International Law* 10(3): 517–547.

Mathews, Lee. 2021. 'Ransomware Attacks on the Healthcare Sector are Skyrocketing', *Forbes*, 8 January 2021. As of 21 May 2021: https://www.forbes.com/sites/leemathews/2021/01/08/ransomware-attacks-on-the-healthcare-sector-are-skyrocketing/.

McCosker, Sarah. 2020. 'Domains of Warfare.' In *Oxford Guide to International Humanitarian Law,* edited by Ben Saul and Dapo Akande, 77. Oxford: Oxford University Press.

Mercy Corps. 2019. 'The Weaponization of Social Media: How Social Media can Spark Violence and What Can be Done about it.' November 2019. As of 21 May 2021: https://www.mercycorps.org/research-resources/weaponization-social-media.

Mikanagi, Tomohiro & Mačák, Kubo. 2020. 'Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok case.' *Cambridge International Law Journal* 9(1): 51–75.

Milanovic, Marko & Schmitt, Michael. 2020. 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic.' *Journal of National Security Law & Policy* 11: 247–284.

Military and Paramilitary Activities in and against Nicaragua (Merits) (Nicaragua v United States of America), Judgment of 27 June 1986. International Court of Justice.

Morrison, Sara. 2021. 'Ransomware Attack Hits another Massive, Crucial Industry: Meat.' *Vox*, 10 June 2021. As of 5 July 2021: https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers.

Muthuppalaniappan, Menaka & Stevenson, Kerrie. 2021. 'Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health.' *International Journal for Quality in Health Care* 33(1): 1–4.

Myers, Adam, Szymanski, William, Jackson, Daniel, Wynkoop, Ellen, Heine, Pete, Hoffman, Tyler & Mostoller, Bri. 2020. 'Crypto-Controls: Harnessing Cryptocurrency To Strengthen Sanctions.' *War on the Rocks*, 9 December 2020. As of 21 May 2021: https://warontherocks.com/2020/12/crypto-controls-harnessing-cryptocurrency-to-strengthen-sanctions/.

Nakashima, Ellen, Torbati, Yeganeh & Englund, Will. 2021. 'Ransomware Attack Leads to Shutdown of Major U.S. Pipeline System', *The Washington Post*, 8 May 2021. As of 21 May 2021: https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/.

Nasu, Hitoshi. 2013. 'The Place of Human Security in Collective Security.' *Journal of Conflict and Security Law* 18: 95–129.

Neale, Mark. 2000. 'No Maps for These Territories.' *Docurama*.

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). 2021. *Chair's Summary*, UN document A/AC.290/2021/CRP.3*, 10 March 2021.

———. 2021. *Final Substantive Report*, UN document A/AC.290/2021/CRP.2, 10 March 2021.

Organization for Economic Co-operation and Development (OECD). 2021. 'Digital Trade.' (n.d.) As of 21 May 2021: https://www.oecd.org/trade/topics/digital-trade/.

Osborne, Charlie. 2018. 'North Korea Claims Hacker Responsible for WannaCry Outbreak Does not Exist.' *ZDNet*, 14 September 2018. As of 21 May 2021: https://www.zdnet.com/article/north-korea-claims-hacker-responsible-for-sony-breach-does-not-exist/.

Paganini, Pierluigi. 2013. 'Hardware Attacks, Backdoors and Electronic Component Qualification.' *INFOSEC*, 11 October 2013. As of 21 May 2021: https://resources.infosecinstitute.com/topic/hardware-attacks-backdoors-and-electronic-component-qualification/.

People's Republic of China. 2017. 'International Strategy of Cooperation on Cyberspace.' 1 March 2017. As of 21 May 2021: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

———. 2020. 'Statement by Minister-Counsellor Mr. Yao Shaojun at Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure.' 26 August 2020. As of 21 May 2021: https://www.fmprc.gov.cn/ce/ceun/eng/hyyfy/t1809700.htm.

Peters, Anne. 2014. 'Security Council Resolution 2178 (2014): The "Foreign Terrorist Fighter" as an International Legal Person, Part I.' *EJIL: Talk!*, 20 November 2014. As of 21 May 2021: https://www.ejiltalk.org/security-council-resolution-2178-2014-the-foreign-terrorist-fighter-as-an-international-legal-person-part-i/.

Pobjie, Erin. 2020. 'COVID-19 and the Scope of the UN Security Council's Mandate to Address Non-Traditional Threats to International Peace and Security.' *Max Planck Institute for Comparative Public Law and International Law Research Paper Series* 41: 1–24. As of 21 May 2021: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725850.

Pohl, Benjamin & Kurnoth Hannah Elisabet. 2020. 'Summary: UNSC Open Debate on Climate and Security.' *Climate Diplomacy*, 24 July 2020. As of 21 May 2021: https://climate-diplomacy.org/sites/default/files/2020-10/UNSC%20Summary_final.pdf.

Prosecutor v Nahimana et. al. (Appeal Judgement). 2007. ICTR-99-52. International Criminal Tribunal for Rwanda (ICTR).

Reuters Staff. 2021. 'SolarWinds Hack was "Largest and Most Sophisticated Attack" Ever: Microsoft President.' *Reuters*, 15 February 2021. As of 21 May 2021: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R.

Rodenhäuser, Tilman & Mačák, Kubo. 2021. 'Even 'Cyber Wars' have Limits. But What if They Didn't?' *Humanitarian Law and Policy*, 9 March 2021. As of 5 July 2021: https://blogs.icrc.org/law-and-policy/2021/03/09/even-cyber-wars-have-limits/.

Schmitt, Michael, ed. 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

———. 2020. 'New Zealand Pushes the Dialogue on International Cyber Law Forward.' *Just Security*, 8 December 2020. As of 21 May 2021: https://www.justsecurity.org/73742/new-zealand-pushes-the-dialogue-on-international-cyber-law-forward/.

New Zealand. (2020) 'The Application of International Law to State Activity in Cyberspace.' 1 December 2020 (on file with author).

Russian Federation. 2020. 'Commentary of the Russian Federation on the Initial "Pre-Draft" of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.' 22 May 2020. As of 21 May 2021: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

Russon, Mary-Ann. 'US Fuel Pipeline Hackers "Didn't Mean to Create Problems".' *BBC News*, 11 May 2021. As of 21 May 2021: https://www.bbc.co.uk/news/business-57050690.

Schondorf, Roy. 2020. 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations.' *EJIL: Talk!*, 9 December 2020. As of 21 May 2021: https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

Schweisfurth, Theodor. 2012. 'Article 34.' In *The Charter of the United Nations: A Commentary, Volume I,* edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1086. Oxford: Oxford University Press.

Seals, Tara. 'U.S. Pipeline Disrupted by Ransomware Attack.' *Threat Post*, 19 February 2020. As of 21 May 2021: https://threatpost.com/pipeline-disrupted-ransomware-attack/153049/.

Security Council Report. 2016. 'Open Arria-formula Meeting on Cybersecurity.' *What's In Blue,* 23 November 2016. As of 21 May 2021: https://www.securitycouncilreport.org/whatsinblue/2016/11/open-arria-formula-meeting-on-cybersecurity.php.

Shany, Yuval & Schmitt, Michael N. 2020. 'An International Attribution Mechanism for Hostile Cyber Operations.' *International Law Studies* 96: 196–222.

Soldatkin, Vladimir & Holland, Steve. 2021. 'Far Apart at First Summit, Biden and Putin Agree to Steps on Cybersecurity, Arms Control.' *Reuters*, 17 June 2021. As of 5 July 2021: https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/.

Sommer, Peter & Brown, Ian. 2011. 'Reducing Systemic Cybersecurity Risk.' *OECD/IFP Project on 'Future Global Shocks"*, 14 January 2011. As of 21 May 2021: https://www.oecd.org/gov/risk/46889922.pdf.

———. 2017. 'Arria-Formula Meeting on Hybrid Wars.' *What's In Blue*, 30 March 2017. As of 21 May 2021: https://www.securitycouncilreport.org/whatsinblue/2017/03/arria-formula-meeting-on-hybrid-wars.php.

———. 2019. 'In Hindsight: The Security Council and Cyber Threats.' *January 2020 Monthly Forecast*, 23 December 2019. As of 21 May 2021: https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php.

———. 2020. 'Arria-formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building.' *What's In Blue*, 21 May 2020. As of 21 May 2021: https://www.securitycouncilreport.org/whatsinblue/2020/05/arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building.php.

———. 2020. 'Arria-formula Meeting on Cyber-Attacks Against Critical Infrastructure.' *What's In Blue*, 25 August 2020. As of 21 May 2021: https://www.securitycouncilreport.org/whatsinblue/2020/08/arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure.php.

S.S. "Lotus", France v Turkey, Judgment. 1927. Permanent Court of International Justice (PCIJ).

Shamsi, Jawwad A.; Zeadally, Sherali; Sheikh, Fareha & Flowers, Angelyn. 2016. 'Attribution in Cyberspace: Techniques and Legal Implications.' *Security and Communications Networks* 9: 2886–2900.

Skopik, Florian & Pahi, Timea. 2020. 'Under False Flag: Using Technical Artifacts for Cyber Attack Attribution.' *Cybersecurity* 3(8): 1–20. As of 21 May 2021: https://doi.org/10.1186/s42400-020-00048-4 at 6–7, 14.

Smith, Brad. 2020. 'A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response.' *Microsoft on the Issues*, 17 December 2020. As of 21 May 2021: https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

Stecklow, Steve. 2018. 'Why Facebook is Losing the War on Hate Speech in Myanmar.' *Reuters*, 15 August 2018. As of 21 May 2021: https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

Sullivan, Clare. 2016. 'The 2014 Sony Hack and the Role of International Law.' *Journal of National Security Law and Policy* 8: 437–468.

Sullivan, John. 2019. 'Remarks at the Second Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace.' *United States Department of State*, 23 November 2019. As of 21 May 2021: https://www.state.gov/remarks-at-the-second-ministerial-meeting-on-advancing-responsible-state-behavior-in-cyberspace/.

Susskind, Richard. 2020. 'The Future of Courts.' *Remote Courts* 6(5). As of 21 May 2021: https://thepractice.law.harvard.edu/article/the-future-of-courts/.

Tabanski, Lior. 2011. 'Basic Concepts in Cyber Warfare.' *Military and Strategic Affairs* 3(1): 75–92.

Tadić Case, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction. 1995. International Criminal Tribunal for the former Yugoslavia (ICTY).

Talmon, Stefan. 2005. 'The Security Council as World Legislature.' *The American Journal of International Law* 99(1): 175–193.

Tassinis, Orfeas Chasapis. 2020. 'Customary International Law: Interpretation from Beginning to End.' *European Journal of International Law* 31(1): 235-267.

The Things Network. 2021. 'Network Architecture.' (n.d.) As of 21 May 2021: https://www.thethingsnetwork.org/docs/network/architecture.html.

Tidy, Joe. 2021. 'Hacker Tries to Poison Water Supply of Florida City.' *BBC News*, 8 February 2021. As of 21 May 2021: https://www.bbc.co.uk/news/world-us-canada-55989843.

———. 2021. 'Colonial Hack: How did Cyber-attackers Shut off Pipeline?.' *BBC News*, 11 May 2021. As of 21 May 2021: https://www.bbc.co.uk/news/technology-57063636.

Tomuschat, Christian. 2012. 'Article 2(3).' In *The Charter of the United Nations: A Commentary, Volume I,* edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 181. Oxford: Oxford University Press.

———. 2012. 'Article 33.' In *The Charter of the United Nations: A Commentary, Volume I,* edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf, 1071. Oxford: Oxford University Press.

Trapp, Kimberly. 2015. 'Can Non-State Actors Mount an Armed Attack?.' In *The Oxford Handbook of the Use of Force in International Law,* edited by Marc Weller, 680. Oxford: Oxford University Press.

Tsagourias, Nicholas. 2015. 'The Legal Status of Cyberspace.' In *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russel Buchan, 13. Cheltenham: Edward Elgar Publishing.

UK Mission to the United Nations. 2021. 'United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Application of International Law To States' Conduct In Cyberspace—United Kingdom Statement.' 3 June 2020. As of 4 May 2021: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

UK National Cyber Security Centre (NCSC). 2021. '10 Steps to Cyber Security: Monitoring.' (n.d.) As of 21 May 2021: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring.

United Kingdom (UK) Government. 2020. 'Press Release: UK Condemns Cyber Actors Seeking to Benefit from Global Coronavirus Pandemic.' 5 May 2020. As of 21 May 2021: https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic.

United Nations. 1945. *Charter of the United Nations*. 1 UNTS XVI.

———. 1969. *Vienna Convention on the Law of Treaties*. 1155 UNTS 331.

United Nations General Assembly. 1950. *Report of the Interim Committee of the General Assembly*. UN document A/1388 (1950), 16 January–18 September 1950.

———. 1974. *Definition of Aggression.* UN document A/RES/3314 (XXIX) (1974), 14 December 1974.

———. 1982. *Convention on the Law of the Sea*. 1833 UNTS 397.

———. 1988. *Declaration on the Prevention and Removal of Disputes and Situations Which May Threaten International Peace and Security and on the Role of the United Nations in this Field*. UN document A/RES/43/51 (1988), 12 May 1988.

United Nations General Assembly & Security Council. 2015. *Annex to the Letter Dated 12 June 2015 from the Permanent Representatives of Australia, Finland, Germany, Greece and Sweden to the United Nations Addressed to the President of the Security Council: Compendium of the High Level Review of United Nations Sanctions*, UN document A/69/941-S/2015/432, 12 June 2015.

United Nations Secretary-General. 2018. *Agenda for Disarmament: Implementation Plan*. (n.d.) As of 21 May 2021: https://www.un.org/disarmament/sg-agenda/en/#actions.

United Nations Security Council. 1967. UN document S/RES/242 (1967), 22 November 1967.

———. 1977. UN document S/RES/419 (1977), 24 November 1977.

———. 1993. UN document S/RES/827 (1993), 25 May 1993.

———. 1994. UN document S/RES/955 (1994), 8 November 1994.

———. 1998. UN document S/RES/1177 (1998), 26 June 1998.

———. 1998. UN document S/RES/1203 (1998), 24 October 1998.

———. 1998. UN document S/RES/1208 (1998), 19 November 1998.

———. 2000. UN document S/RES/1308 (2000), 17 July 2000.

———. 2000. UN document S/RES/1333 (2000), 19 December 2000.

———. 2001. UN document S/RES/1373 (2001), 28 September 2001.

———. 2003. UN document S/RES/1467 (2003), 18 Mar 2003.

———. 2004. UN document S/RES/1540 (2004), 28 April 2004.

———. 2004. UN document S/RES/1542 (2004), 30 April 2004.

———. 2005. UN document S/RES/1953 (2005), 31 March 2005.

———. 2007. UN document S/RES/1757 (2007), 30 May 2007.

———. *Presidential Statement*. UN document S/PRST/2010/4, 24 February 2010.

———. 2011. UN document S/RES/1970 (2011), 26 February 2011.

———. 2011. UN document S/RES/1975 (2011), 30 March 2011.

———. 2011. UN document S/RES/1983 (2011), 7 June 2011.

———. 2011. UN document S/RES/1986 (2011), 13 June 2011.

———. 2013. UN document S/RES/2117 (2013), 26 September 2013.

———. 2013. UN document S/RES/2129 (2013), 17 December 2013.

———. 2014. UN document S/RES/2133 (2014), 27 January 2014.

———. 2014. UN document S/RES/2177 (2014), 18 September 2014.

———. 2014. UN document S/RES/2178 (2014), 24 September 2014.

———. 2015. UN document S/RES/2214 (2015), 27 March 2015.

———. 2015. UN document S/RES/2220 (2015), 22 May 2015.

———. 2015. UN document S/RES/2250 (2015), 9 December 2015.

———. 2017. *Security Council Presidential Statement Calls on Myanmar to End Excessive Military Force, Intercommunal Violence in Rakhine State*. UN document SC/13055, 6 November 2017. As of 21 May 2021: https://www.un.org/press/en/2017/sc13055.doc.htm.

———. 2017. UN document S/RES/2383 (2017), 7 November 2017.

———. 2018. *Letter Dated 30 April 2018 from the Permanent Representative of Finland to the United Nations Addressed to the President of the Security Council, Annex, 'Hitting the Ground Running": Fifteenth Annual Workshop for Newly Elected Members of the Security Council,* UN document, S/2018/404, 3 May 2018.

———. 2018. UN document S/RES/2417 (2018), 24 May 2018.

———. 2018. UN document S/RES/2449 (2018), 13 December 2018.

———. 2019. UN document S/RES/2457 (2019), 27 February 2019.

———. 2019. UN document S/RES/2462 (2019), 13 June 2019.

———. 2019. UN document S/RES/2500 (2019), 4 December 2019.

———. 2019. UN document S/RES/2501 (2019), 20 December 2019.

———. 2020. UN document S/RES/2532 (2020), 1 July 2020.

———. 2020. *Letter Dated 28 July 2020 from the President of the Security Council Addressed to the Secretary-General and the Permanent Representatives of the Members of the Security Council*. UN document S/2020/751, 30 July 2020.

———. 2021. *Letter Dated 29 April 2021 from the President of the Security Council Addressed to the Secretary-General and the Permanent Representatives of the Members of the Security Council*. UN document S/2021/415, 30 April 2021.

———. 2021. *Security Council Press Statement on Situation in Myanmar*, UN document SC/14430, 4 February 2021. As of 21 May 2021: https://www.un.org/press/en/2021/sc14430.doc.htm.

———. 2021. *Press Release: Climate Change 'Biggest Threat Modern Humans Have Ever Faced', World-Renowned Naturalist Tells Security Council, Calls for Greater Global Cooperation*, UN document SC/14445, 23 February 2021. As of 21 May 2021: https://www.un.org/press/en/2021/sc14445.doc.htm.

———. 2021. *Security Council Strongly Condemns Attacks against Critical Civilian Infrastructure, Unanimously Adopting Resolution 2573 (2021)*. UN document SC/14506, 7 April 2021. As of 21 May 2021: https://www.un.org/press/en/2021/sc14506.doc.htm.

———. 2021. UN document S/RES/2573 (2021), 27 April 2021.

United States of America (US) Department of Justice. 2020. 'Cryptocurrency Enforcement Framework: Report of the Attorney General's Cyber Digital Task Force.' October 2020. As of 21 May 2021: https://www.justice.gov/cryptoreport.

US Department of the Treasury. 2020. 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.' 1 October 2020. As of 21 May 2021: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

Weiss, Joe & Hunter, Bob. 2021. 'The SolarWinds Hack Can Directly Affect Control Systems.' *Lawfare*, 22 January 2021. As of 21 May 2021: https://www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems.

Wiener, Norbert. 1955. *Cybernetics or Control and Communication in the Animal and the Machine*. Cambridge: The MIT Press & John Wiley and Sons.

Wilmshurst, Elizabeth. 2005. 'Principles of International Law on the Use of Force by States in Self-Defence.' *Chatham House*, October 2005. As of 5 July 2021: https://www.chathamhouse.org/sites/default/files/publications/research/2005-10-01-use-force-states-self-defence-wilmshurst.pdf.

Wood, Michael. 2017. 'The Interpretation of Security Council Resolutions, Revisited.' *Max Planck Yearbook of United Nations Law Online* 20: 1-35. As of 21 May 2021: https://doi.org/10.1163/13894633_02001002.

Wright, Jeremy. 2018. 'Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General Jeremy Wright QC MP.' 23 May 2018. As of 21 May 2021: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Yannakogeorgos, Panayotis A. 2012. 'Strategies for Resolving the Cyber Attribution Challenge.' *Air Force Research Institute Perspectives on Cyber Power*, December 2013. As of 21 May 2021: https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF.

Zetter, Kim. 2016. 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.' *WIRED Magazine*, 3 March 2016. As of 21 May 2021: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

International law as a whole and the Charter of the United Nations, in particular, apply to information and communications technologies (ICTs) and the digital environments that they enable. To address cyber events constituting disputes likely to endanger the maintenance of international peace and security or situations which might lead to international friction or give rise to a dispute, under Chapter VI, as well as threats to the peace, breaches of the peace, or acts of aggression, under Chapter VII, traditional dispute settlement and enforcement measures may be complemented or replaced with new, ICT-specific measures.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

@unidirgeneva @UNIDIR un_disarmresearch