The International Law Protections against Cyber Operations Targeting the Healthcare Sector

Priya Urs, Talita Dias, Antonio Coco, Dapo Akande

The International Law Protections against Cyber Operations

Targeting the Healthcare Sector

Priya Urs, Talita Dias, Antonio Coco, Dapo Akande

February 2023

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD
OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

Acknowledgments

We are incredibly grateful to the Government of Japan for generously funding the research presented in this report. In particular, we would like to thank Tomohiro Mikanagi, Akihiro Tsuji and Yusuke Hatakeyama for their constant support throughout the project.

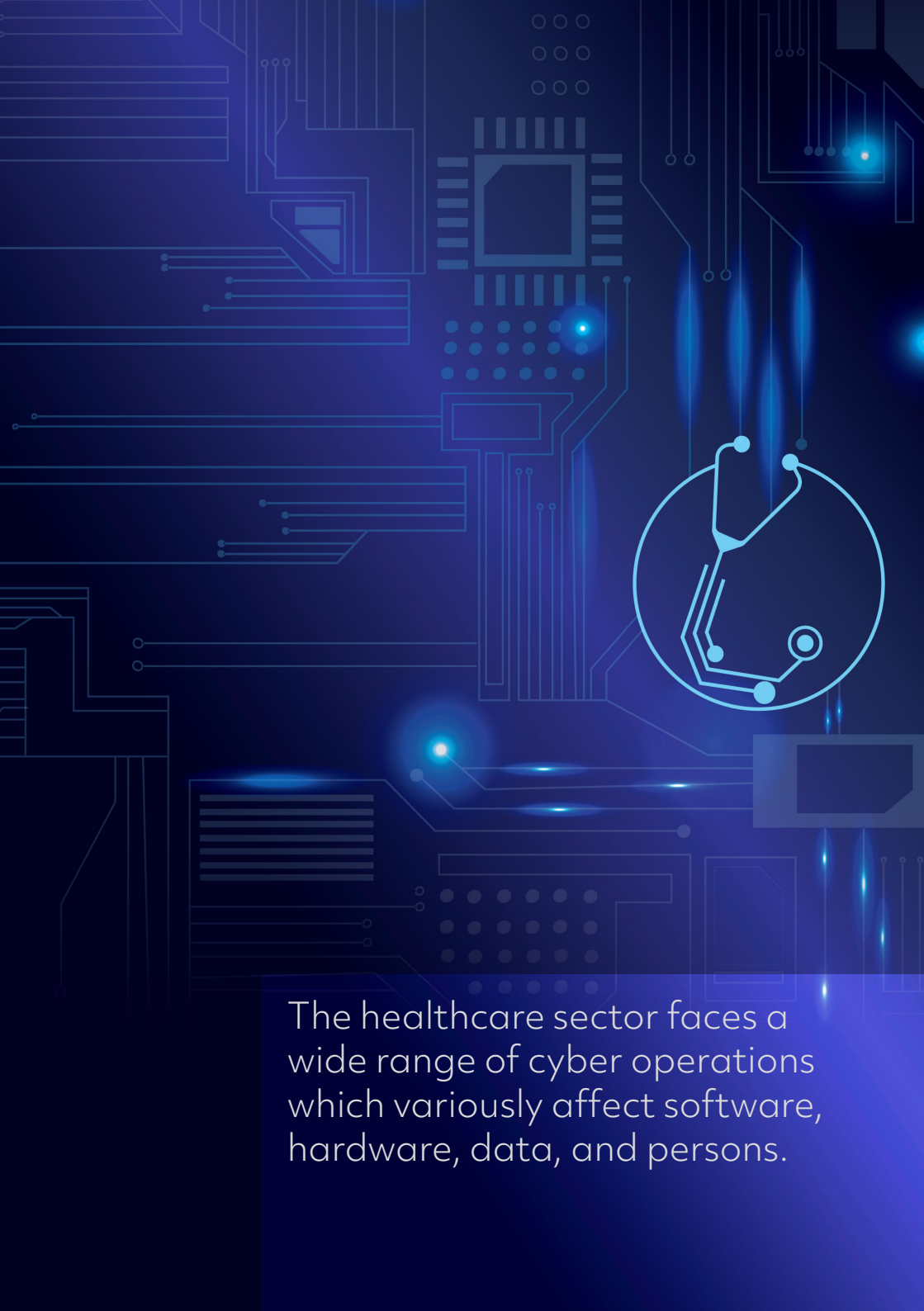
This work would not have been possible but for the enthusiasm and guidance of our principal investigator, Dapo Akande, who encouraged us to push the boundaries of our thinking in international law in the context of cyber operations and engaged with us in detail on the various chapters of this report.

Thanks to Tsvetelina van Benthem, an invaluable colleague and friend, for always being ready to debate with us the various topics discussed in the report. Duncan Hollis and Harold Hongju Koh have also been immensely supportive of this work.

We would like to thank Pinar Özcan for her meticulous and dedicated assistance in finalising the various chapters and preparing the report for publication.

Finally, we are grateful to all the academics and practitioners who took the time to engage with the ideas presented in this report, whether by providing comments on our work, engaging in discussions with us, or attending our workshops. We are especially grateful for the constructive comments by the participants of the internal seminar on 13 May 2022 and the conference of the Oxford Process on International Law Protections in Cyberspace on 12–13 October 2022, both held at the Blavatnik School of Government, University of Oxford. Parts of this research were also presented at the 80th biennial conference of the International Law Association in Lisbon in June 2022 and the annual conference of the Society of Legal Scholars in London in September 2022, where we received further feedback on the work.

Table of Contents



The healthcare sector faces a wide range of cyber operations which variously affect software, hardware, data, and persons.

Chapter 1 Introduction

I. The Landscape of Cyber Operations against the Healthcare Sector

Since the start of the COVID-19 pandemic, there has been a marked global increase in cross-border malicious cyber operations against the healthcare sector. The targets of these operations include hospitals and other healthcare providers, research institutes and pharmaceutical companies, including those responsible for the development of COVID-19 vaccines, medical suppliers and distributors, health ministries and regulators, the World Health Organization (WHO), and even the public. These operations have disrupted the provision of healthcare, compromised sensitive digital information, such as patient records, clinical trial data, or the intellectual property associated with vaccine research, and have brought about the spread of false health-related information—all hindering states' management of the pandemic and, ultimately, public health. It is a common refrain in the context of malicious cyber operations that '[a]ttacks on healthcare are attacks on people'.[1]

Although cyber operations against the healthcare sector are not new, the COVID-19 pandemic exposed the particular vulnerability of the sector to these operations. To begin with, the information and communications technologies (ICTs) employed by the healthcare sector are 'complex, vulnerable and sometimes outdated', and the sector 'suffers from a systemic lack of resources to secure its infrastructure, train its personnel, and hire and retain cybersecurity staff'.[2] At the same time, the increased use by healthcare providers of internet-connected

1 Czech Republic, CyberPeace Institute, Microsoft, 'Compendium of Multistakeholder Perspectives: Protecting the Healthcare Sector from Cyber Harm' (Report, 2022) (hereafter 'Czech Compendium') 4 <https://www.mzv.cz/un.newyork/en/news_events/the_ministry_of_foreign_affairs_together.html> accessed 5 January 2023.

2 CyberPeace Institute, 'Playing with Lives: Cyberattacks on Healthcare are Attacks on People' (Report, 2021) 16 <https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf> accessed 5 January 2023.

medical devices – many of which function on outdated operating systems vulnerable to attack[3] – increases their exposure to remote cyber operations.[4] The CyberPeace Institute has articulated three key reasons why the healthcare sector is increasingly the target of malicious cyber operations:

> *Healthcare services are critical to maintain as patient health depends on them. This has made hospitals a target of choice for digital extortion.*
>
> *Healthcare is the custodian of valuable and sensitive information, such as medical records and vaccine research, making it an attractive target for data theft and cyberespionage.*
>
> *Healthcare has found itself at the center of strategic inter-state rivalries due to the pandemic, which have spilled into malicious activities such as disinformation campaigns against the sector.*[5]

With significant demands being placed on an already strained sector, healthcare's vulnerability to cyber operations has also increased with the pandemic. In the two-year period between 2020 and 2022, the CyberPeace Institute reported as many as 447 cyber operations against the healthcare sectors of 40 countries.[6] The effects of such operations have been significant and varied. In many cases, cyber operations against the ICTs on which hospitals and other healthcare providers depend interrupted the provision of healthcare to individuals. The indiscriminate

3 ibid 32–33.
4 Examples of connected medical devices include infusion pumps, x-ray machines and MRI scanners. See Czech Compendium (n 1) 9.
5 CyberPeace Institute, 'Playing with Lives' (n 2) 16, 29, 62.
6 The statistics reported by the Institute's 'Cyber Incident Tracer' are impressive in their detail and are searchable by incident type, sub-sector and country, among other criteria. The statistics cited here may have changed since the time of writing. See 'Cyber Incident Tracer #Health' (CyberPeace Institute) <https://cit.cyberpeaceinstitute.org/explore> accessed 29 August 2022.

'WannaCry' ransomware operation of 2017, for example, significantly disrupted, amongst others, the functioning of the United Kingdom's (UK) National Health Service (NHS) so as to cause the cancellation of over 19,000 medical appointments and procedures across one third of NHS trusts and 8% of General Practitioners.[7] The overall cost of the WannaCry ransomware to the NHS has been estimated at £92 million.[8] More recently, in 2021, a series of cyber operations targeting the Republic of Ireland's Health Service Executive and Department of Health resulted in the shutting down, amongst others, of radiology services across the state.[9] In such cases, cyber operations have seriously risked patient health. In Brno, the Czech Republic and Düsseldorf, Germany, individuals requiring urgent treatment had to be transferred to other hospitals, in the latter case culminating in their death.[10] At least one lawsuit has been filed against a private healthcare provider in the US on the basis that complications that arose during the delivery of a baby, which later died, went undetected as a direct result of the disruption of the hospital's use of its ICTs by ransomware.[11]

7 UK Department of Health and Social Care, 'Securing Cyber Resilience in Health and Care: Progress Update October 2018' (Cyber Security Policy Implementation Update, 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf> accessed 29 August 2022. See also CyberPeace Institute, 'Playing with Lives' (n 2) 34.

8 UK Department of Health and Social Care (n 7).

9 C Lally, J Horgan-Jones and A Beesley, 'Department of Health Hit by Cyberattack Similar to that on HSE', The Irish Times (17 May 2021) <https://www.irishtimes.com/news/health/department-of-health-hit-by-cyberattack-similar-to-that-on-hse-1.4566541> accessed 5 January 2023.

10 S Porter, 'Cyberattack on Czech Hospital Forces Tech Shutdown During Coronavirus Outbreak', Healthcare IT News (19 March 2020) <https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak> accessed 5 January 2023; W Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', Wired (11 November 2020) <https://www.wired.co.uk/article/ransomware-hospital-death-germany> accessed 5 January 2023. One anonymised account of the effects of the Ryuk ransomware against Universal Health Services in the US suggests that it resulted in patient deaths. See CyberPeace Institute, 'Playing with Lives' (n 2) 65.

11 M Miliard, 'Hospital Ransomware Attack Led to Infant's Death, Lawsuit Alleges', Healthcare IT News (1 October 2021) <https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges> accessed 5 January 2023.

In addition to various forms of disruption to the provision of healthcare, cyber operations in the healthcare context also increasingly involve the compromise, theft or online publication of sensitive or confidential medical data.[12] The EU Agency for Cybersecurity explains that it is the 'shift towards the online provisioning of healthcare services, remote eHealth and telemedicine approaches' which has increased 'the opportunities for adversaries to exfiltrate medical data'.[13] This may be sold on the dark web or used to make false welfare or insurance claims. In Singapore, for example, over the period 2017–2018, the private healthcare company 'SingHealth' was the victim of a targeted cyber operation involving the theft of the personal details of close to 1.5 million patients and, in some cases, outpatient dispensed medication records, including those of the Prime Minister, whose data was 'specifically targeted and repeatedly accessed'.[14] Similarly, in 2020, the personal data of 1.4 million people who had undergone COVID-19 tests in Paris was stolen.[15] The same is possible in respect of data shared on the COVID-19 contact tracing mobile applications or other platforms deployed by some states.[16]

Where stolen medical records are published online – for example, pending the payment of a ransom – the compromise of such sensitive data can have significant psychological effects on individuals, in particular for those with diagnoses they fear may ostracize them

12 Data breaches are on the rise. CyberPeace Institute, 'Playing with Lives' (n 2) 58; European Union Agency for Cybersecurity (ENISA), Threat Landscape 2021 (Report, 2021) 62 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> accessed 5 January 2023.

13 ENISA, Threat Landscape 2021 (n 12) 62.

14 Singaporean Ministry of Communications and Information Committee of Inquiry, 'Public Report on The Cyber Attack On Singapore Health Services Private Limited's Patient Database on or around 27 June 2018' (Report, 10 January 2019) i <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/public-report-of-the-coi> accessed 5 January 2023.

15 S Elzas, 'Hackers Steal Covid Test Data of 1.4 Million People from Paris Hospital System', RFI (16 September 2021) <https://www.rfi.fr/en/france/20210916-hackers-steal-covid-test-data-of-1-4-million-people-from-paris-hospital-system> accessed 5 January 2023.

16 ENISA, Threat Landscape 2021 (n 12) 24.

from their communities, such as substance abuse or HIV/AIDS.[17] The compromise or theft of patient data may also lead to the erosion of trust in healthcare providers, discouraging individuals from seeking medical care or from sharing critical information with medical professionals.[18]

During the COVID-19 pandemic, state-sponsored actors have also 'pursue[d] information related to recovery and vaccine development efforts' and 'related to infection rates, country-level responses, and treatments'.[19] These cyber operations compromise the confidentiality and thus the reliability of clinical trials, such as the operation which targeted the trial by the Indian pharmaceutical company, Dr Reddy's Laboratory, of the Sputnik V vaccine, leading to the closure of vaccine production facilities across several states.[20] This hinders regulatory approval of vaccines or other medicines or medical technology on the basis of compromised clinical trials, affecting in turn the ability of a

17 CyberPeace Institute, 'Playing with Lives' (n 2) 45.

18 ibid; R Shandler and MA Gomez, 'The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government' (2022) Journal of Information Technology and Politics <https://doi.org/10.1080/19331681.2022.2112796> accessed 5 January 2023.

19 ENISA, Threat Landscape 2021 (n 12) 16. See also CrowdStrike, 'Global Threat Report' (Report, 2021) 11 <https://www.crowdstrike.co.uk/resources/reports/global-threat-report/> accessed 5 January 2023. For example, the 'Cozy Bear' cyber operations of 2020 targeted research facilities across the UK, US and Canada. ibid 13. UK National Cyber Security Centre, 'Advisory: APT29 targets COVID-19 vaccine development' (16 July 2020) <https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf> accessed 5 January 2023; D Sabbagh, 'Hackers "try to steal Covid vaccine secrets in intellectual property war"', The Guardian (22 November 2020) <https://www.theguardian.com/world/2020/nov/22/hackers-try-to-steal-covid-vaccine-secrets-in-intellectual-property-war> accessed 5 January 2023; A Walker 'UK "95% sure" Russian hackers tried to steal coronavirus vaccine research', The Guardian (17 July 2020) <https://www.theguardian.com/world/2020/jul/17/russian-hackers-steal-coronavirus-vaccine-uk-minister-cyber-attack> accessed 5 January 2023; BioNTech, 'Statement Regarding Cyber Attack on European Medicines Agency' (9 December 2020) <https://investors.biontech.de/news-releases/news-release-details/statement-regarding-cyber-attack-european-medicines-agency> accessed 5 January 2023; 'Pfizer/BioNTech vaccine docs hacked from European Medicines Agency', BBC News (9 December 2020) <https://www.bbc.co.uk/news/technology-55249353> accessed 5 January 2023.

20 A Millar, 'Five Pharma Cybersecurity Breaches to Know and Learn From' (Pharmaceutical Technology, 17 September 2021) <https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/> accessed 5 January 2023.

state to address a pandemic or other public health crises. In short, '[i]n the case of sensitive or confidential data, the mere fact that data has been exposed to non-authorised users may signify a permanent loss of its value'.[21]

As the COVID-19 pandemic illustrates, the dissemination of false health-related information in the form of misinformation or disinformation – the inadvertent or intentional dissemination of false information – can likewise affect public health by exposing individuals to false health-related information and making access to accurate information more difficult. Such was the case with the 2020 cyber operation against the Georgian Ministry of Health, Labour and Social Affairs, which involved the theft of pandemic-related data, including from the National Center for Disease Control and the Richard Lugar Centre for Public Health Research, a part of which was then published online alongside false information.[22] The WHO has gone so far as to declare the existence of a widespread 'infodemic' accompanying the COVID-19 pandemic, which it found has led to 'poor observance of public health measures'.[23] As one report notes, individuals and businesses have been targeted with false information relating to the 'green pass, mandatory vaccination, health passports, mass immunity testing, and lockdowns'.[24]

21 T Dias and A Coco, 'Cyber Due Diligence in International Law' (Oxford Institute for Ethics, Law and Armed Conflict (ELAC) Report, 2021) 72 <https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallaw pdf.pdf> accessed 5 January 2023.

22 Institute for Development of Freedom of Information, 'Cyberattack on the Ministry of Health and Russian Trace' (IDFI, 3 September 2020) <https://idfi.ge/en/strategy_of_russian_cyber_operations> accessed 5 January 2023. See also E Tucker, 'US Officials: Russia Behind Spread of Virus Disinformation', AP News (28 July 2020) <https://apnews.com/article/virus-outbreak-ap-top-news-health-moscow-ap-fact-check-3acb089e6a333e051dbc4a465cb68ee1> accessed 5 January 2023.

23 WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFCR, 'Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation – Joint Statement' (23 September 2020) <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation> accessed 5 January 2023. See also ENISA, Threat Landscape 2021 (n 12) 78, 109–110.

24 ENISA, Threat Landscape 2021 (n 12) 78.

In recent years, states have emphasised the need to protect the healthcare sector from malicious cyber operations. The UN 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', which published its first report in 2021 following three successive reports of the UN 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (UN GGE),[25] expressed concern about the effects of cyber operations against the healthcare sector:

> *Of specific concern is malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public … and health sector entities. The COVID-19 pandemic has demonstrated the risks and consequences of malicious ICT activity that seeks to exploit vulnerabilities in times when our societies are under enormous strain.* [26]

Additionally, the report noted that '[t]he COVID-19 pandemic [has] heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities'.[27] The UN 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (UN OEWG) noted in its own report of 2021 that 'the COVID-19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities'.[28] A handful of states have

25 The UN 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', comprising, until 2013, members from 15 states and subsequently 20 states, published successive reports in 2010 (UN Doc A/65/201), 2013 (UN Doc A/68/98) and 2015 (UN Doc A/70/174).

26 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135 (hereafter 'UN GGE Report 2021') para 10. The Group was composed of representatives of 25 states.

27 UN GGE Report 2021 (n 26) para 45.

28 'Final Substantive Report of the Open-Ended Working Group on Developments in the field of Information and Telecommunications in the context of international security,

in individual statements also advanced the view that the healthcare sector is a part of their critical infrastructure, which they propose should be protected from malicious cyber operations.[29] It is now widely acknowledged that malicious cyber operations against the healthcare sector constitute a critical threat to the provision of healthcare, with widespread and devastating effects on the provision by public and private institutions of healthcare, the development of medicines and medical technologies, public trust in healthcare providers and other relevant institutions, and individuals' ability to access accurate health-related information online.

II. A Taxonomy of Cyber Operations against the Healthcare Sector

The healthcare sector faces a wide range of cyber operations which variously affect software, hardware, data, and persons.[30] As seen in Section I, whether a cyber operation against healthcare ICTs targets software, hardware or data, it almost always has further 'real-world' effects, that is, effects on people. For the purpose of the analysis of their lawfulness in subsequent chapters, these operations may be helpfully divided into three categories which represent the most common cyber operations in the context of healthcare.[31] These are: (1) disruptive cyber

Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2 (hereafter 'UN OEWG Report 2021') para 26. The report was adopted by consensus.

29 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136. See e.g. ibid 8 (Australia), 31(Czech Republic), 46 (Ireland), 57 (Netherlands), 79 (Thailand).

30 For this fourfold categorisation of the 'layers' of ICTs, see Dias and Coco (n 21) 59–78. The effects of a cyber operation which initially perpetrates one such layer need not be limited to that layer; in reality, the effects of a cyber operation typically extend beyond the layer originally targeted.

31 The CyberPeace Institute refers to the respective categories of 'disruptive attacks', 'data breaches' and 'disinformation operations'. CyberPeace Institute, 'Playing with Lives' (n 2) 51.

operations, (2) cyber operations involving the compromise, theft or publication of online data (or 'data breaches'), and (3) misinformation and disinformation operations.

A. Disruptive Cyber Operations

Disruptive cyber operations like ransomware operations (or 'ransomware attacks'), 'denial of service' operations (or 'DoS attacks'), viruses and worms usually target software or hardware with a view to compromising their integrity, availability, or both.[32] In essence, the software or hardware targeted stops functioning as it should or can no longer be used.[33] Such operations typically have effects on different ICT layers, as in the case of the insertion of a 'virus or parasitic code' into software which then 'destroys or distorts the internal workings of the hardware which it attacks'.[34] This is the case with cyber operations which target software linked to the functioning of internet-connected medical devices.[35]

Of the various kinds of disruptive cyber operations in the context of healthcare, ransomware is the most common.[36] This was true even in the years prior to the COVID-19 pandemic, with the European Union (EU) Agency for Cybersecurity describing healthcare providers as 'the favourite target' of ransomware.[37] Ransomware operations use malware to encrypt operating systems or data pending the payment of a ransom to restore access through a decryption key.[38] The malware is executed in various ways, such as email attachments or other downloads, through pop-up windows, or by exploiting technical vulnerabilities in

32 ENISA, Threat Landscape 2021 (n 12) 8.
33 See Dias and Coco (n 21) 80–82.
34 ibid 65.
35 ibid 64.
36 CyberPeace Institute, 'Playing with Lives' (n 2) 52.
37 ENISA, 'Threat Landscape – Ransomware' (Report, 2020) 13 <https://www.enisa.europa.eu/publications/ransomware> accessed 5 January 2023.
38 ENISA, Threat Landscape 2021 (n 12) 8; J Fruhlinger, 'Ransomware Explained: How it Works and How to Remove It', (CSO, 19 June 2020) <https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html> accessed 5 January 2023.

cybersecurity.[39] These operations are particularly successful when they target hospitals and other healthcare providers because they have 'a significant impact on healthcare professionals' capacity to deliver vital services', making the payment of a ransom the easiest route to restoring access and thereby medical services.[40]

'Denial of service' operations, or 'DoS attacks', while equally disruptive, operate by overloading and thereby restricting the functioning of 'information systems, devices, or other network resources', such as 'email, websites, online accounts … or other services that rely on the affected computer or network'.[41] These operations 'flood' the target host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users'.[42] Increasingly, 'denial of service' operations take the form of 'distributed denial of service' operations, or 'DDoS attacks', which cause larger-scale disruption through 'botnets'—multiple computers or other devices infected with malware and remotely controlled by the operator.[43] These operations are increasingly successful because of the ease with which vulnerable internet-connected or 'Internet of Things' devices, along with the use of 5G or other networks, can be used to create botnets.[44] For all these reasons, 'distributed denial of service' operations pose 'one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreases in performance, loss of data, and service outages'.[45] In addition to the disruption caused by such operations to their targets, the insertion of malware into the remotely-controlled devices also has significant effects on the devices themselves, which

39 Fruhlinger (n 38).
40 CyberPeace Institute, 'Playing with Lives' (n 2) 51.
41 CISA, 'Security Tip (ST04-015): Understanding Denial-of-Service Attacks' (20 November 2019), <https://www.cisa.gov/uscert/ncas/tips/ST04-015> accessed 5 January 2023.
42 ibid.
43 ibid.
44 ENISA, Threat Landscape 2021 (n 12) 69.
45 ibid 8.

may break down or need to be shut down.[46]

B. Compromise, Theft or Publication of Online Data

Given the significant value associated with medical data, such as patients' medical records, clinical trial data and the intellectual property associated with the development of new medicines and medical technology, cyber operations increasingly target the data layer of ICTs associated with healthcare. The kinds of cyber operations of concern in this context vary. To begin with, ransomware operations may, in cases where the ransom is not paid, lead to the permanent deletion of encrypted data. This can have devastating effects on the provision of healthcare. In at least two cases in the United States (US), the failure by private healthcare providers to pay the ransom resulted in the destruction of their electronic medical records and eventually in the closure of their operations.[47] In some cases of ransomware, sensitive data may not only be encrypted but may also be exfiltrated and later 'dumped' on publicly accessible websites. This use of ransomware is described as 'double extortion'.[48] Since 2019, 'double-extorsion' ransomware has been used not only to encrypt medical records but also to steal it and publish it online with a view to securing an additional ransom from the individuals whose records are made public.[49] The additional advantage of exfiltrating sensitive patient data, in addition to encrypting it, is that the potential reputational cost to the targeted healthcare provider incentivises them to pay the ransom even in cases in which the encrypted data has been securely backed up.[50]

Beyond ransomware, other kinds of cyber operations target data through other means and for reasons other than financial gain. Such operations include the installation of Remote Access Trojans (RATs)

46 ibid 69.
47 ENISA, 'Threat Landscape – Ransomware' (n 37) 13.
48 CyberPeace Institute, 'Playing with Lives' (n 2) 53.
49 ibid.
50 ibid.

or 'backdoors', as well as spyware and other surveillance operations, which secure access to data through malware that targets software or hardware.[51] In the context of the COVID-19 pandemic, the UK, the US and Australia identified such operations against organisations involved in the development of COVID-19 vaccines, the intention of which was, in their view, to 'steal' information and intellectual property relating to the development and testing of COVID-19 vaccines'.[52] Similarly, the European Medicines Agency was also subjected to the theft and online publication of data relating to the Pfizer/BioNTech vaccine, which was at the time pending regulatory approval, and which the Agency considered as potentially 'undermin[ing] trust in vaccines'.[53] In some cases, stolen data is published online in selective or amended form, or alongside false information, perhaps with a view to giving a veneer of authenticity to disinformation or to damage the reputation of the targeted institution. This was the case with the European Medicines Agency's data breach.[54]

C. Misinformation and Disinformation Operations

Misinformation and disinformation are two prime examples of so-called 'information' or 'influence' operations, that is, 'the deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviors of the targeted audience in ways that align with the authors' interests.'[55] Other examples include propaganda (the selective and

51 See Dias and Coco (n 21) 88–91.
52 UK National Cyber Security Centre (n 19).
53 European Medicines Agency (EMA), 'Cyberattack on EMA – Update 5 (15 January 2021) <https://www.ema.europa.eu/en/news/cyberattack-ema-update-5> accessed 5 January 2023; EMA 'Cyberattack on EMA – Update 6' (25 January 2021) <https://www.ema.europa.eu/en/news/cyberattack-ema-update-6> accessed 5 January 2023; 'Pfizer/BioNTech Vaccine Docs Hacked from European Medicines Agency' (n 19); BioNTech (n 19).
54 EMA, Update 5 (n 53); EMA, Update 6 (n 53); 'Pfizer/BioNTech Vaccine Docs Hacked from European Medicines Agency' (n 19).
55 T van Benthem, T Dias and DB Hollis, 'Information Operations under International Law' (2022) 55 Vanderbilt Journal of Transnational Law 1217, 1217-1218. See also DB Hollis, 'The Influence of War, The War for Influence' (2018) 32 Temple International and Comparative Law Journal 30, 35–36; ELAC, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' (2021) preambular para 3 <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-

carefully orchestrated presentation of information, facts or views to emotionally influence and/or manipulate audiences) and hate speech (that is, the use of rhetoric to attack, denigrate or dehumanise individuals or groups on the basis of protected characteristics, such as race, ethnicity, nationality, religion, gender, sexual orientation or disability).[56] These have been part and parcel of domestic and international life for centuries; consider political propaganda and commercial advertising, for example. Yet the unprecedented directness, speed and scale at which information operations are disseminated online have brought about a range of new challenges.[57]

To begin with, it is difficult to contain the virality of false and extreme content once it is published online, especially due to engagement-based ranking and recommendation algorithms for online content as well as inaccurate content moderation systems.[58] The result is an increased risk of online information operations unfolding into offline harms.[59] This has been put into sharp relief during the COVID-19 pandemic. Our dependence on online platforms as sources of information has turned them into sweet spots for health-related disinformation and

overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/> accessed 5 January 2023.

56 See T Dias, 'Information Operations in a Russia-Ukraine Peace Settlement' (Ukraine Peace Settlement Project Option Paper, July 2022) <https://www.lcil.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.lcil.cam.ac.uk/ukraine/dias_information_operations.pdf> accessed 5 January 2023.

57 UN Human Rights Committee (HRC), 'Disinformation and freedom of opinion and expression Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan' (13 April 2021) UN Doc A/HRC/47/25 para 2.

58 ibid para 16; UNGA, 'Promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (28 August 2018) UN Doc A/73/348 para 12; Amnesty International, 'Silenced and Misinformed: Freedom of Expression in Danger During Covid-19' (Report, 19 October 2021) 27–29 <https://www.amnesty.org/en/documents/pol30/4751/2021/en/> accessed 5 January 2023.

59 The Royal Society, The online information environment: Understanding how the internet shapes people's engagement with scientific information (Report, January 2022) 30–31 <https://royalsociety.org/-/media/policy/projects/online-information-environment/the-online-information-environment.pdf?la=en-GB&hash=691F34A269075C0001A0E647C503DB8F> accessed 5 January 2023.

misinformation, with serious consequences for human life and health.[60]

Early on during the 'infodemic', there were reports of individuals dying or becoming critically ill as a result of alcohol or bleach ingestion in different parts of the world.[61] These and other unsafe or untested home cures had been widely advertised by both private users and public figures on various online channels.[62] In an environment where the science around the disease was constantly evolving and individuals were desperate to find a cure, it is easy to see how disinformation and misinformation about COVID-19 treatments led to or at least contributed to extreme and harmful behaviour. Similarly, the spread of false or misleading information about COVID-19 vaccines, such as unverified stories about microchips inserted during vaccination, led to vaccine hesitancy and low-intake across developed and developing countries.[63] Disinformation and misinformation about virus containment measures, such as social distancing and mask wearing, also hindered government efforts to control the spread of the virus in different parts of the world.[64] Other COVID-19-related information operations had similarly devastating consequences, such as an increase in anti-Asian hate crime[65] and violence against healthcare providers,[66]

60 CyberPeace Institute, 'Playing with Lives' (n 2) 59–60.

61 See S Islam et al, 'COVID-19–Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis', (2020) 103(4) The American Journal of Tropical Medicine and Hygiene 1621; MMF Caceres et al, 'The impact of misinformation on the COVID-19 pandemic' (2022) 9(2) AIMS Public Health 262.

62 The Royal Society (n 59) 29; Amnesty International (n 58) 29–30.

63 The Royal Society, (n 59) 31–37; S Loomba et al, 'Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA', (2021) 5(3) Nature Human Behaviour 337.

64 R Hornik et al, 'Association of COVID-19 Misinformation with Face Mask Wearing and Social Distancing in a Nationally Representative US Sample', (2021) 36(1) Health Communication 6.

65 Human Rights Watch, 'Covid-19 Fueling Anti-Asian Racism and Xenophobia Worldwide' (Report, 12 May 2020) <https://www.hrw.org/news/2020/05/12/covid-19-fueling-anti-asian-racism-and-xenophobia-worldwide> accessed 5 January 2023; S Han et al, 'Anti-Asian American Hate Crimes Spike During the Early Stages of the COVID-19 Pandemic' (2022) Journal of Interpersonal Violence <https://doi.org/10.1177/08862605221107056> accessed 5 January 2023.

66 KP Iyengar, VK Jain, R Vaishya, 'Current situation with doctors and healthcare workers during COVID-19 pandemic in India', (2020) 98(2) Postgraduate Medical Journal 121; OA Bhatti et al, 'Violence against Healthcare Workers during the COVID-19 Pandemic:

both fuelled by online abuse or incitement.

Aside from their virality, these types of information operations have become even harder to trace in the digital environment, given internet anonymity and the use of spoofing techniques, such as virtual private networks and botnets. For instance, it is well-documented that several orchestrated disinformation campaigns revolving around the COVID-19 vaccine originated from Russia.[67] Yet, because botnets were used to launch such operations, it remains unclear precisely which individuals or public institutions were behind them.[68] Furthermore, one must not neglect the impact of information operations disseminated in private online fora, where privacy-enhancing tools, such as end-to-end-encryption, protect the content of messages from the public eye. WhatsApp messaging, for instance, was a prolific means for the dissemination of false information about various COVID-19 treatments.[69]

At the same time, the fight against online disinformation, misinformation and other information operations must not undermine internationally recognised human rights, such as privacy and freedom of expression.[70] It may be tempting for governments and online platforms to adopt drastic, stringent measures restricting the dissemination of online content during

A Review of Incidents from a Lower-Middle-Income Country' (2021) 87(1) Annals of Global Health 41; 'COVID-19: Health workers face online abuse for encouraging vaccination', Sky News (4 August 2021) <https://news.sky.com/story/covid-19-health-workers-face-online-abuse-for-encouraging-vaccination-12372107> accessed 5 January 2023.

67 JE Barnes, 'Russian Disinformation Targets Vaccines and the Biden Administration', The New York Times (5 August 2021) <https://www.nytimes.com/2021/08/05/us/politics/covid-vaccines-russian-disinformation.html> accessed 5 January 2023.

68 See K Hignett, 'From Russia with hate: How pro-Kremlin bots are fuelling chaos and lies about the pandemic', Metro News (10 July 2021) <https://metro.co.uk/2021/07/10/how-pro-kremlin-bots-are-fuelling-covid-19-conspiracy-theories-14867186/> accessed 5 January 2023; JW Ayers et al, 'Spread of Misinformation About Face Masks and COVID-19 by Automated Software on Facebook' (2021) 181(9) JAMA Internal Medicine 1251.

69 S Vijaykumar et al, 'Dynamics of social corrections to peers sharing COVID-19 misinformation on WhatsApp in Brazil', (2022) 29(1) Journal of the American Medical Informatics Association 33; D Khandelwal, 'Covid lies are tearing through India's family WhatsApp groups', Wired (14 April 2021) <https://www.wired.co.uk/article/india-covid-conspiracies-whatsapp> accessed 5 January 2023.

70 See UN Doc A/HRC/47/25 (n 57) esp. para 2.

a public health emergency such as the COVID-19 pandemic. However, insofar as information operations constitute speech acts and/or private data, any measures adopted to curb their spread must carefully balance between the need to protect health and other public interests, on the one hand, and individual rights affected thereby, on the other.

III. The International Legal Regulation in Peacetime of Cyber Operations against the Healthcare Sector

A. The Need for Clarification as to the Application of International Law

One part of the task of tackling cyber operations against the healthcare sector is preventative; increasing the robustness of cybersecurity to quickly identify malicious threats and mitigate their effects.[71] Another part of the task is bringing about accountability for malicious cyber operations through law, in particular where such operations are carried out by states or are otherwise attributable to them. A recent report considers a lack of accountability to be the biggest hurdle in addressing cyber operations against the healthcare sector:

> *[m]ost importantly, the sector suffers from a growing accountability gap, seemingly making attacking healthcare a risk-free crime, with impunity for criminal groups and state-sponsored actors alike.* [72]

Addressing the question of accountability for the carrying out of malicious cyber operations requires clarity as to whether such operations breach existing rules of international law. Since 2013, states have affirmed in principle in the consensus-based reports of the UN GGE and the UN OEWG that international law applies to cyber operations.[73] The

71 Various initiatives are helpfully compiled by the CyberPeace Institute. See CyberPeace Institute, 'Playing with Lives' (n 2) 92–99. See also Czech Compendium (n 1) 5–6.
72 CyberPeace Institute, 'Playing with Lives' (n 2) 9.
73 Mention was first made of the applicability of international law in the UN GGE's

2021 report of the UN OEWG concluded that:

> *States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.*[74]

Relevant rules of international law identified by the UN GGE include:

> *sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.*[75]

States nevertheless recognise that further clarification is required as to the manner of the application of these and other relevant rules of international law.[76] In the UN OEWG, states made particular note of the 'need for additional neutral and objective efforts to build capacity in the areas of international law'.[77] This report responds to their call for clarity.

report of 2013. See UN GGE Report 2013 (n 25) paras 19–20; UN GGE Report 2015 (n 25) paras 25–27; UN GGE Report 2021 (n 26) para 70; UN OEWG Report 2021 (n 28) para 34. See also 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan' (13 January 2015), UN Doc A/69/723 para 2(1).

74 UN OEWG Report 2021 (n 28) para 34.

75 UN GGE Report 2021 (n 26) para 70. See also ibid para 71; UN GGE Report 2015 (n 25) para 26. Although the UN OEWG did not ultimately name the applicable rules, it did confirm that the various 'norms' listed 'do not replace or alter States' obligations or rights under international law, which are binding'. UN OEWG Report 2021 (n 28) para 25.

76 UN GGE Report 2013 (n 25) para 16; UN OEWG Report 2021 (n 28) paras 34, 37.

77 UN OEWG Report 2021 (n 28) para 37.

B. Scope and Limitations of the Report

Against this backdrop, it is the aim of this report to clarify the applicability of existing rules of international law to cyber operation against the healthcare sector. To the extent that rules of international law are in fact applicable in this context, the report scrutinises the ways in which they apply to the various kinds of cyber operations targeting the healthcare sector. The focus of the report is the international legal rules applicable to the conduct of states in peacetime. The rules under consideration, noted by the UN GGE, are (1) the prohibition of the threat or use of force under Article 2(4) of the Charter of the United Nations ('UN Charter') and under customary international law, (2) the customary prohibition of intervention in the internal or external affairs of a state, (3) the prohibition of other relevant conduct as a consequence of the sovereignty of a state over its territory,[78] and (4) relevant obligations under international human rights law, namely obligations relating to the right to life, the right to health, the right to privacy, and the rights to freedom of expression and information. Owing to capacity constraints and given the considerable work already done by the International Committee of the Red Cross and others on the question of the applicability of the law of armed conflict or international humanitarian law to cyber operations, situations of armed conflict are excluded from the scope of this report.[79]

Given that the rules under consideration bind states, the report is also limited to addressing whether conduct by or attributable to a state may constitute a breach of the rules under consideration. Attribution may

78 UN GGE Report 2013 (n 25) para 20; UN GGE Report 2015 (n 25) para 27.

79 On this subject, see T Rodenhäuser, L Gisel, L Maybee, H Johnston and F Lauper, 'Signaling Legal Protection in a Digitalizing World: A New Era for the Distinctive Emblems?' (ICRC Humanitarian Law and Policy, 16 September 2021) < https://blogs.icrc.org/law-and-policy/2021/09/16/legal-protection-digital-emblem/ > accessed 5 January 2023; E Lawson and K Mačák, 'Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts', (ICRC Expert Report, 26 May 2021) < https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations > accessed 5 January 2023; ICRC 'International Humanitarian Law and Cyber Operations during Armed Conflicts', (Position Paper, November 2019) < https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf > accessed 5 January 2023.

be satisfied in a variety of ways, notably where the conduct in question is carried out by the organ of a state,[80] where an individual or entity is 'empowered' to exercise 'governmental authority' and is 'acting in that capacity',[81] or a person or group 'is in fact acting on the instructions of, or under the direction and control of' a state.[82] That said, the question of attribution of conduct to a state, which will need to be determined in accordance with the law of state responsibility, is not addressed in this report. For the purpose of the analysis of relevant rules, attribution of conduct to a state will be assumed.

The report is intended to supplement existing initiatives aimed at clarifying the application of international law to cyber operations. In addition to the multilateral dialogues amongst states at the UN GGE and the UN OEWG, several academic and civil society initiatives have undertaken this task. Chief amongst them is the Tallinn Manual 2.0, published at the initiative of North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in 2017.[83] The 'Interactive Toolkit' of the NATO CCD COE also includes the legal assessment of fictional scenarios involving cyber operations against medical facilities and vaccine research and testing.[84] The Oxford Process on International Law Protections in Cyberspace, an initiative of the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) supported by the Government of Japan and Microsoft, is also aimed at the clarification of the application of existing rules of

80 International Law Commission ('ILC'), 'Responsibility of States for Internationally Wrongful Acts' annexed to UNGA Resolution 56/83 (12 December 2001) UN Doc A/Res/56/83 (hereafter 'ARSIWA') art 4.
81 ARSIWA art 5.
82 ARSIWA art 8.
83 MN Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017).
84 'Scenario 20: Cyber Operations against Medical Facilities' (NATO CCDCOE, Cyber Law Toolkit) <https://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities> accessed 5 January 2023; 'Scenario 23: Vaccine Research and Testing' (NATO CCDCOE, Cyber Law Toolkit) <https://cyberlaw.ccdcoe.org/wiki/Scenario_23:_Vaccine_research_and_testing> accessed 5 January 2023.

international law to cyber operations.[85] The healthcare sector has been a major focus of the Oxford Process, with two statements as to the application of international law in this context – endorsed by over a hundred academics each – published in 2020.[86] In 2021, against the backdrop of the COVID-19 pandemic, ELAC also published the report 'Cyber Due Diligence in International Law', which considers the application of states' due diligence obligations in cyberspace.[87] More recently, the Czech Republic, the CyberPeace Institute and Microsoft convened a series of multi-stakeholder workshops on a wide range of issues surrounding cyber operations against the healthcare sector, culminating in the publication of the 'Compendium of Multistakeholder Perspectives: Protecting the Healthcare Sector from Cyber Harm'.[88] The CyberPeace Institute has also independently published a comprehensive assessment of the cyber threat landscape in the context of healthcare, including an overview of the various initiatives aimed at prevention and accountability in this context.[89]

IV. Structure of the Report

The remainder of the report is divided into four substantive chapters. Priya Urs is the main author of Chapters 2, 3 and 4 while Talita Dias and Antonio Coco are the main authors of Chapter 5.

Chapter 2 asks whether a cyber operation against the healthcare

85 ELAC, 'The Oxford Process on International Law Protections in Cyberspace' (2020) <https://www.elac.ox.ac.uk/the-oxford-process/> accessed 5 January 2023.

86 See ELAC, 'The Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector' (May 2020) <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/he-oxford-statement-on-cyber-operations-targeting-the-health-care-sector/> accessed 5 January 2023; ELAC, 'The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research' (August 2020) <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-second-oxford-statement/> accessed 5 January 2023.

87 Dias and Coco (n 21).

88 Czech Compendium (n 1).

89 CyberPeace Institute, 'Playing with Lives' (n 2) 53.

sector may constitute a 'threat or use of force' under Article 2(4) and an 'armed attack' under Article 51 of the UN Charter. Although there is wide agreement as to the application in principle of both provisions to cyber operations, on the basis at least of the effects of death, injury or destruction resulting from such operations, there is as yet insufficient clarity as to the manner in which such an assessment is made in practice. A particular problem is whether any ensuing effects of death, injury or destruction – which are of greatest concern in the healthcare context – are in causal terms too indirect or remote or not sufficiently proximate as to qualify a cyber operation as a use of force or an armed attack. After scrutinising the various standards of causation used in international law, the chapter concludes that reasonable foreseeability is the most suitable standard in relation to both Article 2(4) and Article 51. The use of this standard suggests that a disruptive cyber operation against the healthcare sector, such as ransomware or a 'denial of service' operation, may constitute a use of force, since death, injury and destruction are reasonably foreseeable effects of disruptive cyber operations in the context of healthcare. On this basis, and subject to the criterion of gravity, a disruptive cyber operation may even constitute an armed attack. Conversely, death, injury and destruction are unlikely to be reasonably foreseeable effects of the theft, compromise or publication of online data or of disinformation and misinformation operations so as to constitute a use of force or, conditional on the satisfaction of the requirement of gravity, an armed attack. The reasonable foreseeability of intervening causes or, alternatively, the use alongside the standard of reasonable foreseeability of a requirement of directness will make the characterisation of these operations as a use of force or an armed attack difficult.

Chapter 3 examines whether a cyber operation against the healthcare sector may constitute a violation of the customary prohibition of intervention in the internal or external affairs of another state. It does so by fleshing out the requirements for unlawful intervention articulated by the International Court of Justice in the *Case Concerning Military*

and Paramilitary Activities in and Against Nicaragua.[90] These are the requirements of intervention in 'the internal or external affairs' of a state and 'coercion'. First, the chapter finds that 'the internal or external affairs' of a state, or its domestic jurisdiction, is better described in the context of the prohibition of intervention as referring to the sum of a state's choices and policies rather than the frequently invoked '*domaine réservé*', which would exclude from the scope of the prohibition all matters on which a state has undertaken international obligations. Where the implementation of a state's choice or policy as to healthcare is at issue, the matter clearly falls within the scope of the prohibition. Secondly, in the absence of sufficient clarity in practice, the chapter suggests that the requirement of coercion refers to conduct that deprives the state of choice or control over a matter within its domestic jurisdiction. Accordingly, disruptive cyber operations that deprive the targeted state of choice or control over its health-related choices or policies or their implementation are coercive, as are those that may reasonably foreseeably cause such effects. Conversely, the compromise, theft or publication of online data does not generally have coercive effects, though exceptions may exist. When it comes to misinformation and disinformation operations, intervening causes may make it difficult to causally link such operations to any loss of control by the targeted state over its healthcare choices or policies, although exceptions may exist.

Having considered the law on the use of force and the prohibition of intervention, **Chapter 4** identifies the remaining corollaries of the sovereignty of a state over its territory and considers whether cyber operations against the healthcare sector – in particular those that do not constitute a use of force, an armed attack, or an unlawful intervention – violate these rules. International law prohibits states from engaging in certain forms of conduct as a consequence of the sovereignty of a state over its territory. An analogy with non-consensual aerial, maritime and land-based incursions by one state into the territory of another suggests

90 Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US) (Merits) [1986] ICJ Rep 14.

that cyber operations carried out through a physical presence of the agent of one state in the territory of another may constitute a violation of the latter's territorial sovereignty. Since, however, most cyber operations are conducted remotely, the question of their lawfulness must be assessed on other bases. First, a cyber operation may be prohibited on the basis that it usurps the exercise of a governmental function by the territorial state even where it is carried out remotely. Secondly, remote cyber operations with effects in the territory of another state may be said to violate the territorial sovereignty of that state. Beyond physical damage, there is no clear agreement, however, as to the relevance of other effects to the assessment, such as the loss of functionality of ICTs. Given that most cyber operations against the healthcare sector are carried out remotely, their physical effects provide the clearest basis on which to characterise them as violations of territorial sovereignty. Disruptive cyber operations, like ransomware and 'denial of service' operations, target the functionality of ICTs and in turn cause physical damage by disrupting the provision of healthcare services. Subject to the satisfaction of causal requirements, such operations are likely prohibited as violations of territorial sovereignty. The compromise, theft and publication of confidential medical data cause neither physical damage nor the loss of functionality of ICTs. Nor do they interrupt the provision of healthcare, except where compromised data can no longer be relied on in the provision of medical care to individuals. Using a standard of reasonable foreseeability of effects, such exceptional cases may be construed as violations of territorial sovereignty. Disinformation and misinformation do not target ICTs in the same way as disruptive cyber operations and data breaches but, through the dissemination of false information, affect healthcare widely. In many cases, the causal chain or link between such operations and any eventual physical damage is tenuous, even when using the standard of reasonable foreseeability.

Chapter 5 looks at certain human rights, recognised under international human rights treaties and customary international law, which are most pertinent in the context of cyber operations against the healthcare sector.

These are the rights to life, health, privacy, and freedom of expression and information. It focuses on the various ways in which disruptive cyber operations, data breaches and information operations may engage or interfere with said rights. The chapter first notes that the application of human rights under certain treaties, such as the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the American Convention on Human Rights, is subject to a state's jurisdiction. Beyond a state's own territory, jurisdiction, in this sense, means effective control over a geographical space, a person, a company whose activities foreseeably impact an individual's human rights and, arguably, over the enjoyment of those rights, irrespective of any physical control. It then goes on to assess each human right – life, health, privacy, and freedom of expression and information – individually, noting that they entail both negative obligations to respect and positive duties to protect human rights online and offline.

First, when it comes to the right to life, the chapter finds that a violation takes place if a state engages in or fails to reasonably protect individuals from any foreseeable threat to life. This includes general conditions in society that may directly prevent individuals from enjoying their right to life with dignity, such as cyber operations targeting the healthcare sector. Though such threats or risks to life must be foreseeable and, thus, real, they need not be imminent unless they target a specific victim or emanate from an identifiable source. The chapter demonstrates how all three types of cyber operations discussed above may foreseeably risk the lives of patients or members of the public. Secondly, on the right to health, the chapter notes that states must not only refrain from limiting access to health facilities, but also exercise their best efforts to provide individuals with the conditions to achieve the highest attainable standard of health. Different cyber operations may affect essential qualities of healthcare, namely availability, accessibility, acceptability, and quality. Thirdly, when it comes to privacy, the chapter finds that health data, particularly patient information, is a special category of data deserving heightened protection under international human rights

law. States must not only refrain from interfering with such data by cyber or other means, but must also adopt positive measures to protect them from interference by third parties, including online. Finally, the chapter finds that, when adopting measures to protect the rights to life, health, and privacy from cyber operations targeting the healthcare sector, states must respect the right of individuals to receive, seek, and impart information and ideas of all kinds, online and offline. This means that, even if legitimately grounded in the protection of health or other rights, any limitation on freedom of expression or information must be grounded in law and must be necessary and proportionate to uphold the particular aim sought. Moreover, states themselves must not engage in health misinformation or disinformation or other harmful information operations. Likewise, the duty to protect the freedoms of expression and information requires states to exercise their best efforts to ensure a free flow of accurate, verifiable health-information online and offline, as well as a diverse, plural and robust media environment, including during health crises.

It is at least agreed that a cyber operation which causes effects comparable to conventional operations, namely death, physical injury or destruction, may qualify as a use of force.

Chapter 2

The Application of the Law on the Use of Force to Cyber Operations against the Healthcare Sector

I. Introduction

This chapter considers whether and under which conditions a cross-border cyber operation against a state's healthcare sector, where attributed to another state, may be said to constitute a 'threat or use of force' under Article 2(4) and an 'armed attack' under Article 51 of the Charter of the United Nations (hereafter 'UN Charter', 'the Charter').[1] Although there is wide agreement amongst states and commentators as to the application in principle of both provisions to cyber operations, on the basis at least of the causing of the effects of death, physical injury or destruction, there is as yet insufficient clarity as to the manner in which such an assessment might be made in practice. A particular problem that arises in the context of both Article 2(4) and Article 51 of the Charter, which is especially relevant in the context of cyber operations against the healthcare sector, is whether any ensuing effects of death, physical injury or destruction are in causal terms too indirect or remote or not sufficiently proximate as to qualify such operations as a use of force and an armed attack respectively. The question is addressed in this chapter by reference to suitable standards of causation in relation to Article 2(4) and Article 51. Conversely, given the focus of the chapter on cyber operations against the healthcare sector, in which context death, physical injury and destruction are chiefly the effects of concern, the chapter does not address the distinct question whether other kinds

1 The question has been posed whether, in the absence of attribution to a state, an armed attack by a non-state actor may give rise to a right of self-defence under Article 51 of the UN Charter. The chapter takes the view that such a right does not presently exist. See Section III below. Also recall the discussion of attribution in Chapter 1.

of effects might qualify a cyber operation as a use of force.[2]

Against this backdrop, Section II first identifies the criteria used to determine whether conduct constitutes a use of force under Article 2(4) of the UN Charter, namely the causing of effects of death, physical injury or destruction, and the qualified consideration of the means used and the target of the conduct in question, which may assist with the assessment of the effects. The emphasis on the effects of the conduct in the assessment under this provision suggests a particular need for a suitable standard of causation under international law with which to delimit relevant effects. Accordingly, the second part of Section II evaluates various standards of causation which might be used in relation to Article 2(4). Preferring the standard of reasonable foreseeability to the requirement of 'a sufficiently direct and certain causal nexus'[3] and the standard of proximity, it considers whether, by reference to the standard of reasonable foreseeability, various kinds of cyber operations against the healthcare sector may be said to constitute a use of force. These operations include disruptive cyber operations, such as ransomware operations (or 'ransomware attacks') and 'denial of service' operations (or 'DoS attacks'),[4] the compromise, theft or publication of data (or 'data breaches'), and disinformation and misinformation operations.

Section III considers the requirements for an armed attack under Article 51 of the UN Charter. In addition to the criteria of effects, means and

2 A question of particular interest in relation to cyber operations is whether psychological injury to individuals qualifies such operations as a threat or use of force or an armed attack. That psychological injury results from cyber operations is beyond doubt, but the existing practice does not suggest that this is a sufficient basis for the characterisation of conduct as a threat or use of force or an armed attack. Psychological injury being analogous in many respects to physical injury, the law may yet develop to consider it relevant in this context.

3 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Merits) [2007] ICJ Rep 43 (hereafter 'Bosnian Genocide'), 234.

4 Although the term 'denial of service attack' is preferred in the cyber context, the chapter uses the term 'denial of service operation' with a view to avoiding any confusion as to the characterisation or not of such operations as an 'armed attack' for the purpose of Article 51 of the UN Charter.

target used under Article 2(4), which are equally relevant under Article 51, it notes the additional requirement of gravity, comprising the scale of the conduct and its effects, articulated by the International Court of Justice (ICJ) in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (hereafter '*Nicaragua*').[5] Determining which effects are relevant to the assessment of gravity and the characterisation of conduct as an armed attack again requires the articulation of a suitable standard of causation under Article 51. As under Article 2(4), it is argued that the standard of reasonable foreseeability is the most suitable standard of causation in relation to Article 51. This standard is applied to the three categories of cyber operations facing the healthcare sector, namely disruptive cyber operations, the compromise, theft or publication of data, and disinformation and misinformation operations, to assist with the determination as to whether each of them may constitute an armed attack.

II. The Prohibition of the Threat or Use of Force

A. The Characterisation of Conduct as a Threat or Use of Force

The first question to be addressed is whether, and under which conditions, a cyber operation attributable to a state may be said to constitute a 'threat or use of force' for the purpose of the prohibition in Article 2(4) of the UN Charter. Subsection 1 suggests how to characterise conduct as use of force under Article 2(4) of the Charter generally, while Subsection 2 considers how such a characterisation might apply to cyber operations against the healthcare sector.

1. The Characterisation of Conduct as a Threat or Use of Force: In General

There is wide agreement that Article 2(4) of the UN Charter addresses

5 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits) [1986] ICJ Reports 14, 93.

armed force[6] and the threat of armed force,[7] while excluding the use or threat of economic or political coercion.[8] While the characterisation of military or other armed operations as a use of force under Article 2(4) is relatively straightforward, commentators offer several grounds on which to determine whether other kinds of conduct may constitute a use of force, namely the effects of the conduct in question, the means employed, and its target.[9] Of the three criteria, the effects of the conduct are indispensable to the analysis under Article 2(4), including in respect of cyber operations.[10] It is the causing of effects comparable to the effects of conventional weapons that characterises other means, such as cyber operations, as a use of force.[11] Conversely, the consideration of the means used and the target will not determine whether conduct constitutes a use of force. This subsection suggests that the consideration

6 I Brownlie, International Law and the Use of Force by States (OUP 1963) 361–362; O Dörr and A Randelzhofer, 'Article 2(4)', in B Simma, D-E Khan, G Nolte, A Paulus and N Wessendorf (eds), The Charter of the United Nations: A Commentary I (3rd edn, OUP 2012) 208; O Corten, The Law against War: The Prohibition on the Use of Force in Contemporary International Law (Bloomsbury 2021) 63; T Ruys, 'The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?' (2014) 108 American Journal of International Law 159, 163.

7 According to the ICJ in the Nuclear Weapons advisory opinion, 'if the use of force itself in a given case is illegal … the threat to use such force will likewise be illegal'. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226 (hereafter 'Nuclear Weapons'), 246. See also JA Green and F Grimal, 'The Threat of Force as an Action in Self-Defence under International Law' (2011) 44 Vanderbilt Journal of International Law 1, 10. The Tallinn Manual 2.0 takes the same approach in the cyber context. MN Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) 338.

8 The suggestion that the prohibition in Article 2(4) include economic and political coercion was explicitly rejected during the drafting of the UN Charter. Dörr and Randelzhofer (n 6) 209. See also ibid 208–209; Brownlie (n 6) 362.

9 In relation to cyber operations, see DB Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 Lewis and Clark Law Review 1023, 1041; M Roscini, Cyber Operations and the Use of Force in International Law (OUP 2014) 46–48; F Delerue, Cyber Operations and International Law (CUP 2020) 288–290.

10 The question may be posed whether relevant effects must actually manifest for conduct to constitute a use of force. Where the conduct does not in fact cause relevant effects, the better characterisation of the conduct is as an attempt at the use of force or perhaps, in some circumstances, as the threat of force.

11 As Corten suggests, the relevant question is 'whether or not damage is done'. Corten (n 6) 82.

of the effects of relevant conduct is the most suitable basis on which to determine whether a state has breached the prohibition on the use of force.

i. Effects

The consideration of the effects of the conduct in question is the most straightforward way to determine whether the conduct constitutes a use of force. Indeed, there is little disagreement that causing death, physical injury and destruction will qualify conduct as a use of force.[12] These effects are ordinarily associated with the use of conventional weapons. An effects-based approach also implies that 'physical force', the use of which has effects comparable to those resulting from the use of conventional weapons, falls within the scope of the prohibition in Article 2(4) of the Charter. Examples include 'the diversion of a river by an up-stream State, the release of large quantities of water down a valley, and the spreading of fire across a frontier'.[13] The logic applies equally to cyber operations,[14] and an effects-based approach has already been proposed by a number of states in the cyber context.[15] The

12 Y Dinstein, War, Aggression and Self-Defence (6th edn, CUP 2017) para 246; CC Joyner and C Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 European Journal of International Law 825, 849; Hollis, 'Why States Need an International Law for Information Operations' (n 9) 1041.

13 Dörr and Randelzhofer (n 6) 210. See also MN Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law 885, 908; DB Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' (2002) 76 International Law Studies 73, 82–83.

14 According to the Tallinn Manual 2.0, '[a]cts that injure or kill persons or physically damage or destroy objects are uses of force'. Tallinn Manual 2.0 (n 7) 333. This is not to endorse the suggestion in the Tallinn Manual 2.0 that the question whether conduct constitutes a violation of Article 2(4) must be assessed by reference to its scale and effects. ibid 330. See further Section II.A.2. On the effects-based characterisation of cyber operations as a use of force, see also Silver (n 13) 91; GP Corn and R Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207, 208; Corten (n 6) 104; R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Intervention?' (2012) 17 Journal of Conflict and Security Law 211, 219–221; Delerue (n 9) 296–297; HS Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 Journal of National Security Law and Policy 63, 73.

15 See e.g. Australian Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy' (Position Paper, October 2017) (hereafter

US Department of Defense, for example, suggested as much in a 2020 statement asserting that the relevant question when deciding whether a cyber operation constitutes a use of force is 'whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine'.[16]

'Australia Position Paper 2017') 90 <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf> accessed 6 January 2023; Finnish Ministry of Foreign Affairs, 'International Law and Cyberspace – Finland's National Positions' (Position Paper, October 2020) (hereafter 'Finland Position Paper 2020') 6 <https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859> accessed 6 January 2023; French Ministry of the Armies, 'Droit International Appliqué aux Opérations dans le Cyberespace' [International Law Applied to Operations in the Cyberspace]' (Position Paper, 2019) (hereafter 'France Position Paper 2019') 7 <https://prod-site-internet-minarm-admin.cnmosis.dirisi.defense.gouv.fr/sites/default/files/ema/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf> accessed 6 January 2023; Italian Government, 'Italian Position Paper on "International Law and Cyberspace"' (Position Paper, September 2021) (hereafter 'Italy Position Paper 2021') 8 <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf> accessed 6 January 2023; New Zealand Ministry of Foreign Affairs and Trade 'The Application of International Law to State Activity in Cyberspace' (Position Paper, December 2020) (hereafter 'New Zealand Position Paper 2020') para 7 <https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf> accessed 6 January 2023; 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136 (hereafter 'UN GGE Contributions Compendium') 19 (Brazil), 26 (Estonia), 35 (Germany), 58 (Netherlands), 70 (Norway), 84 (Singapore), 88 (Switzerland), 116 (UK), 137 (US); R Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 International Law Studies 395, 398–399.

16 PC Ney Jr, Former General Counsel of the US Department of Defense, 'DoD General Counsel Remarks' (US Cyber Command Legal Conference, 2 March 2020) <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/> accessed 6 January 2023. Even earlier, a 1999 memo suggested that 'the international community will be more interested in the consequences of a computer network attack than in its mechanism'. US Department of Defense Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (1999) 76 International Law Studies 460, 483. France took the same view in the UN OEWG, while suggesting also that it 'does not rule out the possibility that a cyberoperation [sic] without physical effects may also be characterised as a use of force'. See France, 'International Law Applied to Operations in Cyberspace - Paper shared by France with the Open-ended Working Group established by Resolution 75/240' (OEWG Submission, 2021) <https://documents.unoda.org/wp-content/uploads/2021/12/French-

Accordingly, the use of a cyber operation which produces 'destructive consequences analogous to a kinetic military attack' may constitute a breach of Article 2(4).[17] Such an approach is consistent with the purposes of Article 2(4), in particular the desire to ensure respect for the territorial integrity and political independence of states and the maintenance of international peace and security.[18]

Conversely, it is less clear that conduct which causes effects other than death, physical injury or destruction would be characterised as a use of force.[19] For instance, cyber operations may cause psychological, as opposed to physical, injury to individuals.[20] As the law stands, psychological injury is insufficient to characterise conduct as a use of force, but it is not impossible that psychological injury will be considered relevant to the characterisation of conduct as a threat or use of force in the future. Other examples of non-physical effects include the 'shutting down' by cyber operations of banking systems, the stock market or power grids, causing 'massive economic disruption' but not death, physical

position-on-international-law-applied-to-cyberspace.pdf> accessed 6 January 2023.

17 MC Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale Journal of International Law 421, 434–435. By the same logic, '[c]omputer-based espionage' and 'intelligence collection' are not included in the scope of Article 2(4). ibid. See also Y Dinstein, 'Computer Network Attacks and Self-Defence' (2002) 76 International Law Studies 99, 102; Dörr and Randelzhofer (n 6) 210; Silver (n 13) 87.

18 See UN Charter arts 1(1) and 2(4). In Ruys's words, 'the whole object of the Charter was precisely to limit the scope for unilateral use of force as much as possible'. T Ruys, 'Armed Attack' and Article 51 of the UN Charter (CUP 2011) 59–60. Other agree. See Dinstein, War, Aggression and Self-Defence (n 12) paras 256–258; C Gray, International Law and the Use of Force (4th edn, OUP 2018) 37–40.

19 See e.g. Italy Position Paper 2021 (n 15) 8; France Position Paper 2019 (n 15) 7. It is important to note that although the emphasis is on conduct which causes death, physical injury or destruction, there are circumstances where it will be regarded that a state has used force where such effects have not actually been caused. For example, there is no doubt that the occupation of territory by the armed forces of a state will constitute a use of force even where it has not been resisted, and thus no death, physical injury or destruction was caused. In such cases, what is determinative is that the state has used means that would cause such physical effects had there been resistance.

20 R Shandler and MA Gomez, 'The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government' (2022) Journal of Information Technology and Politics <https://doi.org/10.1080/19331681.2022.2112796> accessed 6 January 2023.

injury or destruction.[21] The assessment of the relevance of such effects is beyond the scope of this chapter, which is concerned with the death, physical injury and destruction being witnessed in the context of cyber operations against the healthcare sector.

ii. Means

The consideration of the means employed might, in some cases, assist with the characterisation of conduct as a use of force, as with the deployment of conventional weapons or weapons of mass destruction, which are specifically designed to cause the effects of death, physical injury and destruction. This is not always the case, and nor is the scope of Article 2(4) of the Charter limited to specific weapons.[22] There are some means which might be put to different uses, some of which will call for the characterisation of their use as force, while others will not.[23] This is particularly true of cyber operations.[24] As one commentator notes, the use of such means is not characterised as a use of force 'because of its inherent lethality but because of the potential destructiveness of the way it is being used'.[25] Put differently, the deployment of means in a manner that makes them capable of having the effects of death, physical injury or destruction will, where such effects actually manifest, lead to the characterisation of their use as force under Article 2(4).

21 Waxman (n 17) 436. See also J Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24 European Journal of International Law 129, 133–134; Silver (n 13) 85, 87. Waxman and Roscini criticise the existing distinction, suggesting that 'non-violent' or 'indirect' effects such as these should equally justify the characterisation of conduct as a use of force. Waxman (n 17) 436; M Roscini, 'World Wide Warfare – Jus ad Bellum and the Use of Cyber Force' (2010) 14 Max Planck Yearbook of United Nations Law 85, 107–108.

22 Nuclear Weapons (n 7) 244.

23 Corten refers to the use of such means 'for military purposes and with military effects'. Corten (n 6) 101. Roscini argues that the application of Article 2(4) requires the use of a 'weapon', which he defines as having the capacity to produce violent effects. Roscini, Cyber Operations and the Use of Force in International Law (n 9) 50.

24 Hollis, 'Why States Need an International Law for Information Operations' (n 9) 1042; Delerue (n 9) 289; Silver (n 13) 88.

25 Silver (n 13) 88. Some, like Corten and Ruys, impose a requirement as to intent which may be additionally relevant here. Corten (n 6) 86; Ruys, 'The Meaning of "Force"' (n 6) 160, 189.

The question may be asked whether the deployment of relevant means in a manner capable of producing the effects of death, physical injury or destruction is sufficient to characterise the conduct as a use of force even where such effects do not manifest. One view is that there has been a use of force even if the deployment of the means in question is ultimately unsuccessful, whether due to a deficiency on the part of the state deploying such means, the conduct of the targeted state, or any other intervening event. According to this logic, the launching of a missile into the territory of another state which in fact causes no death, physical injury or destruction could constitute a use of force because of its potential for causing such effects. In the words of Judge Robinson in the *Certain Activities* case, '[n]o shots need be fired, no heavy armaments need be used and certainly no one need be killed before a State can be said to have violated the prohibition'.[26] The same logic would apply too to the use of other means, such as cyber operations. The justification for such an approach is presumably the consideration of the risk of or intent to cause death, physical injury or destruction. Views are divided as to whether the characterisation of conduct as a use of force on this basis is an acceptable reading of the prohibition. In the absence of clarity on the point, and for the purpose of the analysis in this chapter, it is assumed that the conduct in question must have actually caused the effects of death, physical injury or destruction to be characterised as a use of force.[27] In the absence of such effects, the conduct may nevertheless be described as an attempted use of force or even a threat of the use of force.

On a different view entirely of the means deployed as a criterion for the characterisation of conduct as a use of force, the use of means that are 'external', in a physical sense, to a state – such as trade sanctions or an

26 Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica) (Separate Opinion of Judge Robinson) [2015] ICJ Rep 665, 820.

27 In support in the cyber context, see H Lahmann, 'Infecting the Mind: Establishing Responsibility for Transboundary Disinformation' (2022) 33(2) European Journal of International Law 411, 425.

economic embargo – will not constitute a use of force against it, while conduct that is 'internal' – such as the launching of a missile – will.[28] The utility of this distinction is limited; in any event, it does not assist in the assessment of cyber operations which are often neither fully 'external' nor fully 'internal'.[29]

iii. Target

Setting aside the consideration of the effects of the conduct and the means used, the target of the conduct in question might assist, as no more than a persuasive consideration, in the characterisation of the conduct as a use of force. The fact of the targeting of critical infrastructure, whether state owned or privately owned, may contribute to the assessment of the effects of the conduct as being more than just *de minimis* effects.[30] Conversely, a determination that conduct amounts to a use of force solely on the basis that the target of the conduct constitutes part of the 'critical infrastructure'[31] of the targeted state, such as its

28 Schmitt describes this as the criterion of 'invasiveness'. Schmitt, 'Computer Network Attack and the Use of Force in International Law' (n 13) 914.

29 Silver (n 13) 82.

30 Corten (n 6) 90; Delerue (n 9) 288–289, 298–304. In the context of an armed attack under Article 51, discussed below, one commentator suggests that 'the immediate disabling of vital infrastructure with inhibitive … effects on the ability of the State to act or on the elementary living conditions of the population can, in principle, produce the necessary destructive effect'. G Nolte and A Randelzhofer, 'Article 51', in B Simma, D-E Khan, G Nolte, A Paulus and N Wessendorf (eds), The Charter of the United Nations: A Commentary I (3rd edn, OUP 2012) 1419–1420. In the cyber context, see Tallinn Manual 2.0 (n 7) 343. The logic extends equally to the context of the use of force under Article 2(4). See Roscini, Cyber Operations and the Use of Force in International Law (n 9) 59.

31 The term 'critical infrastructure' has been used by states in their discussions in the UN GGE and the UN OEWG to include 'critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities'. 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135 (hereafter 'UN GGE Report 2021') para 10. See also 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2 (hereafter 'UN OEWG Report 2021') para 18. Examples include 'health care and medical infrastructure and facilities, energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes'. UN GGE Report 2021 (n 31) para 45; UN OEWG Report 2021 (n 31) para 18. At

healthcare sector, is too loose a construction—one which would 'suffer from over-inclusion'.[32] Such an approach might include the targeting of critical infrastructure by means of economic or political coercion, which are explicitly excluded from the scope of Article 2(4).[33]

2. The Characterisation of Conduct as a Threat or Use of Force: In the Context of Cyber Operations against Healthcare

A number of states have affirmed in their positions in the UN 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (UN GGE), the UN 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (UN OEWG) and national position papers that a cyber operation may constitute a use of force.[34] Some have qualified this view by proposing that a cyber operation will only constitute a use of force if its 'scale and effects' are 'comparable to traditional kinetic operations'.[35]

the same time, states consider that each of them is to 'determine' which infrastructures or sectors it deems critical within its jurisdiction'. ibid para 43.

32 Hollis, 'Why States Need an International Law for Information Operations' (n 9) 1042.

33 Waxman (n 17) 436. Note, however, that the targeting of critical infrastructure may be relevant for the analysis as to whether other rules of international law have been breached. See Chapters 3 and 4 on the prohibition of intervention and the obligation to respect the territorial sovereignty of states, respectively.

34 Australia Position Paper 2017 (n 15) 90; China, 'Contribution to the Initial Pre-Draft of OEWG Report' (OEWG Submission, 2020) 4 <https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf> accessed 6 January 2023; Finland Position Paper 2020 (n 15) 6; France Position Paper 2019 (n 15) 7; Government of Canada, 'International Law Applicable in Cyberspace' (Position Statement, 2022) (hereafter 'Canada Position Paper') para 44 <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng> accessed 6 January 2023; Italy Position Paper 2021 (n 15) 8; Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (Position Paper, 2021) (hereafter 'Japan Position Paper 2021') 6 <https://www.mofa.go.jp/files/100200935.pdf> accessed 6 January 2023; New Zealand Position Paper 2020 (n 15) para 7; UN GGE Contributions Compendium (n 15) 19 (Brazil), 25–26 (Estonia), 35 (Germany), 58 (Netherlands), 69 (Norway), 77 (Romania), 79 (Russia), 83 (Singapore), 88 (Switzerland), 116 (UK), 137 (US); Schöndorf (n 15) 398.

35 Australia Position Paper 2017 (n 15) 90. See also Canada Position Paper (n 34) para 44; UN GGE Contributions Compendium (n 15) 25, 30 (Estonia), 35 (Germany), 55

This language is presumably taken from the decision of the ICJ in *Nicaragua*, which in fact imposed the requirements as to 'scale and effects' in respect of an armed attack, as a means of distinguishing an armed attack from other uses of force.[36] There is no clear justification for imposing a requirement of scale specifically in relation to whether cyber operations constitute a use of force under Article 2(4). The effects of a cyber operation may be comparable to the effects of kinetic operations even without any additional requirement as to scale.[37] At most, it may be that, for any conduct – cyber or otherwise – to constitute a use of force under Article 2(4) of the Charter, a *de minimis* threshold as to the gravity of the effects must be satisfied.[38] Although there are no clear lines, causing even a limited number of deaths or physical injury to individuals will likely satisfy the *de minimis* threshold, while not all forms of destruction will.

The means most frequently deployed in the context of healthcare include the use of disruptive cyber operations, notably the use of ransomware and 'denial of service' operations, the compromise, theft or publication of online data, and disinformation and misinformation operations. The use of these means specifically in the context of healthcare may,

(Netherlands), 69 (Norway), 77 (Romania). The US refers to the 'nature and extent of injury or death to persons and the destruction of, or damage to, property'. ibid 137 (US). The view expressed by these states reflects that of the Tallinn Manual 2.0: '[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force'. Tallinn Manual 2.0 (n 7) 330.

36 Nicaragua (n 5) 103.

37 On 'scale and effects' in the context of Article 51 of the UN Charter, see Section III.A.1 below.

38 According to Corten, who supports such an approach, this would tend to exclude police or other enforcement operations. He persuasively argues that states have not, in their practice, considered such operations, where they are of insufficient gravity, as constituting a use of force within the meaning of Article 2(4) of the UN Charter and, as such, that they are excluded from the scope of the provision. See Corten (n 6) 62–90. He proposes the application of the requirement of gravity equally, but not exclusively, to cyber operations. Corten (n 6) 103–104. For Corten, the requirement as to coercive intent is 'generally reflected by military action of a certain degree of gravity'. ibid 86. In contrast, Ruys emphasises the requirement of intent, which could qualify even insufficiently grave conduct as a use of force. See Ruys, 'The Meaning of "Force"' (n 6) 160, 189. For Ruys, gravity is a relevant but not overriding consideration. ibid 207.

depending on the circumstances, lead to the effects of death, physical injury and destruction. That said, the critical nature of a target within the healthcare sector, such as a hospital or other healthcare provider, is insufficient itself to characterise relevant conduct as a use of force.[39]

When undertaking the assessment of effects under Article 2(4) of the Charter in the context of healthcare, the relevant effects are the physical destruction of a state's healthcare infrastructure, including the software, hardware and data layers comprising its information and communications technologies (ICTs), as well as death and physical injury which may result from the destruction of or even the disruption of the use of ICTs. All three – death, physical injury and destruction, or some combination of them – may be evidenced in the context of cyber operations against the healthcare sector. Disruptive cyber operations, such as ransomware and 'denial of service' operations, encrypt or otherwise disable the ICTs on which the provision of healthcare, medical research and related activities rely. The disruption may in turn cause the suspension of emergency and acute healthcare services[40] and the use of ICTs in the provision of healthcare more generally,[41] including the use of medical devices.[42] In at least two cases, the death of an individual has been linked to a disruptive cyber operation against a

39 On the designation of healthcare as part of the 'critical infrastructure' of a state, see (n 31) above.

40 See e.g. R Winton, 'Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating', Los Angeles Times (18 February 2016) <https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html> accessed 6 January 2023; W Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', Wired (11 November 2020) <https://www.wired.co.uk/article/ransomware-hospital-death-germany> accessed 6 January 2023.

41 See e.g. 'New Orangeworm Attack Group Targets the Healthcare Sector in the US, Europe and Asia' (Symantec Enterprise Blogs, 23 April 2018) <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia> accessed 6 January 2023; 'South Africa's Life Healthcare Hit by Cyber Attack', Reuters (9 June 2020) <https://www.reuters.com/article/us-life-healthcare-cyber-idUSKBN23G0MY> accessed 6 January 2023.

42 See e.g. T Brewster, 'Medical Devices Hit by Ransomware for the First Time in US Hospitals', Forbes (17 May 2017) <https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4c89894b425c> accessed 6 January 2023.

hospital.[43] In one case, a ransomware operation was said to cause the death of a patient who, as a result of the disruption, needed to be transferred from the affected hospital to another to continue life-saving treatment.[44] In another case, the death of a baby delivered with undetected complications was alleged to be the result of a cyber operation disrupting the hospital's use of its ICTs in the weeks leading up to the delivery.[45] Cyber operations involving the compromise, theft or publication of online medical data, such as patient medical history and confidential datasets pertaining to clinical trials, may also cause relevant effects. These operations do not typically disrupt the provision of healthcare, but they may, in some contexts, be the suggested cause of death or physical injury.[46] The compromise of clinical trial data, for example, which results in the failure to authorise the use of a life-saving medicine, could be said to cause subsequent death or physical injury. Finally, the spread of health-related misinformation and disinformation could also be said to result in relevant effects. Preventing individuals from accessing accurate health-related information, or disseminating false information which causes them to refuse vaccination, as in the context of the COVID-19 pandemic, may be linked to subsequent death or physical injury due to the exposed individuals having contracted COVID-19.

The characterisation of each of these categories of cyber operations in the healthcare context as a use of force requires the consideration,

43 Additionally, one anonymised account of the effects of the Ryuk ransomware against Universal Health Services suggests that it resulted in patient deaths in the US. See CyberPeace Institute, 'Playing with Lives: Cyberattacks on Healthcare are Attacks on People' (Report, 2021) 65 <https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf> accessed 6 January 2023.

44 See Ralston (n 40); J Tidy, 'Police Launch Homicide Inquiry after German Hospital Hack', BBC News (18 September 2020) <https://www.bbc.co.uk/news/technology-54204356> accessed 6 January 2023.

45 See M Miliard, 'Hospital Ransomware Attack Led to Infant's Death, Lawsuit Alleges', Healthcare IT News (1 October 2021) <https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges> accessed 6 January 2023.

46 See Subsection II.B.3.ii.

for legal purposes, of the causal chain or link between them and any ensuing effects of death, physical injury or destruction.

B. The Causal Connection between the Use of Force and Death, Physical Injury or Destruction

As part of the assessment of whether a cyber operation constitutes a use of force, the question arises whether there is a sufficient causal connection between the cyber operation in question and the ensuing effects of death, physical injury or destruction.[47] The question of causation is often raised in relation to the effects of cyber operations other than death, physical injury and destruction, but in fact its relevance is not so limited. As one commentator notes:

> *Physical damage to property, loss of life and injury to persons … are never the primary effects of a cyber operation: damage to physical property can only be a secondary effect, while death or injury of persons can be a tertiary effect of a cyber operation.*[48]

The primary effects are 'those on the attacked computer, computer system or network'.[49] Cyber operations against the healthcare sector illustrate the point well. Two commentators ask whether a cyber operation that 'incapacitates a hospital's computer network or an emergency 911 computer system', which may lead to death or physical injury, can be characterised as a use of force.[50] Another considers the example of a cyber operation that 'shut[s] down power to a hospital with no back-up generators', causing not just a power outage but affecting 'economic,

47 Causation is 'the process of connecting an act (or omission) with an outcome as cause and effect'. I Plakokefalos, 'Causation in the Law of State Responsibility and the Problem of Overdetermination: In Search of Clarity' (2015) 26 European Journal of International Law 471, 472.
48 Roscini, Cyber Operations and the Use of Force in International Law (n 9) 53.
49 ibid 52. See further Lin (n 14) 68.
50 Joyner and Lotrionte (n 12) 850.

social, mental and physical well-being, either directly or indirectly'.[51] A third example is that of a ransomware operation against a hospital which 'indirectly' results in the deaths of patients who need to transferred to other hospitals.[52] The question whether a state carrying out such operations is responsible under Article 2(4) for the ensuing effects of death, physical injury or destruction is yet to be conclusively answered.[53]

Against this backdrop, Subsection 1 outlines the treatment in international law of standards of causation. Subsection 2 suggests the need for a standard of causation in the application specifically of Article 2(4) of the UN Charter and scrutinises relevant standards in this context. It concludes that, where relevant effects manifest in fact, a standard of reasonable foreseeability is the most appropriate in relation to Article 2(4). Subsection 3 considers what the application of the standard of reasonable foreseeability means for the application of Article 2(4) to a range of cyber operations targeting the healthcare sector.

1. The Causal Connection: In General

There is a considerable lack of clarity in the practice of international law as to relevant standards of causation, both in the context of primary rules –such as Article 2(4) of the UN Charter, which does not itself articulate any

51 Schmitt, 'Computer Network Attack and the Use of Force in International Law' (n 13) 912.

52 'Scenario 20: Cyber Operations against Medical Facilities' (NATO CCDCOE, Cyber Law Toolkit) para L8 <https://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities> accessed 6 January 2023.

53 The existing literature has not addressed the issue in much detail. Using the terminology of proximity, Schmitt in fact refers to a 'but for' standard in the context of a cyber operation that indirectly causes death by interfering with relevant infrastructure (in his example, an air traffic control system leading to death from a plane crash). Schmitt, 'Computer Network Attack and the Use of Force in International Law' (n 13) 916. Corten hints that, for a cyber operation to constitute a use of force, 'the harmful effects [must] result directly from violence, even if that violence is caused by computerised means'. Corten (n 6) 104. Conversely, Lin considers both direct and indirect effects to be relevant to the assessment. Lin (n 14) 73–75. None of these positions is sufficiently elaborated. Lahmann specifically addresses the question of causation but his assessment is not limited to the use of force. Lahmann (n 27).

standard of causation – and in the law of state responsibility.[54] In addition to distinct requirements of causation that might be utilised across the primary and secondary rules of international law, international courts draw a further distinction between what they consider to be sequenced assessments of 'factual' and 'legal' causation.[55]

i. Factual Causation

Factual causation requires the articulation of a causal chain or link to determine that the effects are, in factual terms, 'the result of an internationally wrongful act'.[56] It is established in two parts. First, there must be agreement in the form of general or scientific knowledge as to the effects of certain kinds of conduct. Secondly, the causing of such effects by the conduct in question – the causal chain or link – must be established in fact in the circumstances under consideration.[57] Various standards of factual causation have been proposed in law and philosophy. These include, in the first place, the consideration of whether the effects would not have manifested 'but for' the conduct (also referred to as a *conditio sine qua non* or the condition of strong necessity).[58] Secondly, there is the requirement that the conduct was 'a "substantial factor" in producing the result'.[59] Finally, there is the question whether the relevant conduct was a

54 See generally Plakokefalos (n 47); V Lanovoy, 'Causation in the Law of State Responsibility' (2023) British Yearbook of International Law (forthcoming, advance copy available at <https://doi.org/10.1093/bybil/brab008>).

55 Plakokefalos (n 47) 475. In the criminal law context, see MJ Allen, Criminal Law (14th edn, OUP 2017) 49.

56 Lanovoy (n 54) 14.

57 Whichever standard of factual causation is preferred, it is at least agreed that proof of 'a singular instance of causation requires proof of (1) a scientifically valid causal law or generalization (the abstract "general causation" or causal capacity issue), and (2) complete instantiation of the allegedly relevant causal generalization and its underlying causal laws in the specific situation (the concrete "specific causation" issue)'. R Wright and I Puppe, 'Causation: Linguistic, Philosophical, Legal and Economic' (2016) 91(2) Chicago-Kent Law Review 461, 489.

58 On the reference in the wider literature to the requirement of 'strong necessity', see ibid 473.

59 AM Honoré, 'Necessary and Sufficient Conditions in Tort Law', in DG Owen (ed), The Philosophical Foundations of Tort Law (OUP 1997) 363.

'necessary element of a sufficient set' of events that led to the effects.[60] To be sure, these standards of factual causation are not exhaustive. Resolving the debate as to how to actually establish a causal chain or link is beyond the scope of this chapter.

ii. Legal Causation

Whichever standard of factual causation is preferred, the requirement of a factual chain or link may be more or less relevant to any eventual determination as to legal responsibility.[61] What is referred to as legal causation is an additional standard, motivated by policy, pragmatic or normative considerations,[62] to 'determine' whether the causal chain or link should be severed at any intermediate point, because beyond that point the wrongdoer could not have foreseen the result of his acts, or the results were too remote and not proximate'.[63] Legal causation is, in other words, a standard to delimit the scope of legal responsibility in situations in which the effects of the conduct may be 'too remote, inconsequential, or indirect for legal causation to be attributed'.[64] In some cases, factual causation may even be substituted for a standard of legal causation, such as where the task of establishing the causal chain or link proves too difficult or where responsibility is attributed in terms of strict liability.[65] In such cases, the causal chain or link is not ultimately the basis for

60 Plakokefalos (n 47) 476–478; AW Rovine and G Hanessian, 'Towards a Foreseeability Approach to Causation Questions at the United Nations Compensation Commission', in RB Lilich (ed), The United Nations Compensation Commission (Martinus Nijhoff 1995) 240–241. For a wider overview, see Wright and Puppe (n 57); Honoré, 'Necessary and Sufficient Conditions in Tort Law' (n 59).

61 AM Honoré, 'Theories of Causation and Remoteness of Damage', in A Tunc (ed) International Encyclopedia of Comparative Law, Vol. XI (Mohr 1971) Chapter 7 para 45; HLA Hart and AM Honoré, Causation in the Law (2nd edn, OUP 1985) 89, 105–106. The comparison to tort law is apposite given the chiefly reparative function of state responsibility. In support, see Plakokefalos (n 47) 476–477; Lanovoy (n 54) 10.

62 Plakokefalos (n 47) 478.

63 Lanovoy (n 54) 14. Plakokefalos refers to the requirement of 'legal causation' as a 'scope of responsibility' inquiry. Plakokefalos (n 47) 478.

64 D Shelton, 'Righting Wrongs: Reparations in the Articles on State Responsibility' (2002) 96(2) American Journal of International Law 833, 846.

65 Wright and Puppe (n 57).

imposing legal responsibility.[66]

In short, while factual causation refers to the exercise of establishing a causal chain or link between the conduct and its alleged effects, legal causation introduces policy, pragmatic or normative considerations to finally address the question of legal responsibility. For the purpose of identifying a suitable standard of causation in relation to Article 2(4) of the UN Charter, it suffices to say that the reliance on a causal chain or link, for the purpose of factual causation, may be qualified by or even substituted for a standard derived from considerations of policy or pragmatism, or normative considerations, including the desired scope of responsibility in relation to the provision.

2. The Causal Connection: In the Context of Article 2(4) of the UN Charter

Article 2(4) of the UN Charter does not specify any standard of causation with which to identify the legally relevant effects of an alleged use of force. That is, the provision is silent as to which effects may be too indirect or remote or not sufficiently proximate as to be said to result, in legal terms, from the use of force. This silence is largely unproblematic in the context of the use of force through conventional weapons, in which context the task of establishing a causal chain or link between the use of such a weapon and death, physical injury or destruction is straightforward. When it comes to other forms of conduct that might amount to a use of force, however, such as the use of cyber operations, a suitable standard of causation is needed in the application of Article 2(4).[67] That a standard of causation is necessary

66 The point is made well in the context of criminal law. For examples, see Allen (n 55) 49.

67 The practice of international courts and tribunals suggests that the standard of causation applied when determining whether there has been a breach by a state of an international obligation must be articulated in relation to the primary rule. See Plakokefalos (n 47) 481; Lanovoy (n 54) 20–21. See also International Law Commission ('ILC'), 'Articles on the Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc A/RES/56/10, reproduced in (2001) II(Part 2) Yearbook of the ILC (hereafter 'ARSIWA') 93 ('the requirement of a causal link is not necessarily the same in relation to every breach of an international obligation').

in this context is supported by the relevance of the effects of the conduct in its characterisation or not as a use of force. Put differently, a state's responsibility for having engaged in an unlawful use of force depends on the causing of death, physical injury or destruction rather than simply on the state having engaged in a certain kind of conduct. Determining whether death, physical injury and destruction are in fact the result of an alleged use of force is not straightforward in cases other than those involving the use of conventional weapons. As seen above, this is particularly so in the context of cyber operations, in which 'the indirect effects … are often more important than the direct effects'.[68] Clarification as to the appropriate standard of causation will also bring greater predictability as to the scope and applicability of Article 2(4) beyond the use of conventional weapons, which is important given the 'far reaching' implications that follow from the characterisation of conduct as a use of force.[69]

Three standards of causation are proposed by international courts which may be used in the context of the prohibition of the use of force in Article 2(4) of the UN Charter, each of which strikes a distinct balance between the requirements as to factual and legal causation respectively. These are: the requirement of a 'sufficiently direct and certain causal nexus' between the conduct and the effects (roughly equivalent to the 'but for' test, the *conditio sine qua non* or the requirement of strong necessity),

68 Roscini, 'World Wide Warfare' (n 21) 107.

69 See D Akande, 'The Use of Nerve Agents in Salisbury: Why Does it Matter Whether it Amounts to a Use of Force in International Law?' (EJIL Talk!, 17 March 2018) < <https://www.ejiltalk.org/the-use-of-nerve-agents-in-salisbury-why-does-it-matter-whether-itamounts-to-a-use-of-force-in-international-law/> accessed 6 January 2023. To briefly recall, the use of force cannot be justified as a countermeasure under the law of state responsibility. ARSIWA art 50(1). To the extent that the use of force may be said to constitute the breach of a jus cogens norm, the reliance on circumstances precluding wrongfulness is likewise excluded. ARSIWA art 26. Conversely, the targeted state – and perhaps also other states to which the obligation erga omnes in Article 2(4) is owed – is permitted the resort to countermeasures. ARSIWA art 22. Where the use of force constitutes an armed attack, the targeted state enjoys a right of self-defence under Article 51 of the UN Charter and either or both uses of force might lead to an escalation of events, triggering the applicability of the law of armed conflict and of international criminal law. Akande also identifies relevant implications for the law of armed conflict and international criminal law. ibid. See also Dinstein, War, Aggression and Self-Defence (n 12) paras 297–335. Lanovoy additionally notes the need for consistency in determinations as to reparations. Lanovoy (n 54) 62.

which requires a causal chain or link;[70] sufficient 'proximity' in space and time of the conduct and the effects, which uses considerations of proximity to limit the causal chain or link; and the 'reasonable foreseeability' of relevant effects, which, through the use of an objective standard of foreseeability, does away with the need for a causal chain or link.[71]

The appropriate standard of legal causation under Article 2(4) of the UN Charter must be tailored to account for the purposes underlying the provision, including respect for the territorial integrity and political independence of states and the maintenance of international peace and security.[72] This includes the consideration of the desirability of providing reparation for causing death, physical injury and destruction—the effects with which Article 2(4) is concerned and which are particularly relevant in the context of healthcare.[73] It may also include the potential deterrent effect associated with the ease of proving causation in the context of Article 2(4). Finally, the choice of the standard of causation may depend on the consideration of the various consequences of the invocation of state responsibility for an alleged use of force.[74] With all this in mind, the focus of the following discussion is the articulation of a suitable standard of causation which may be used in the context of Article 2(4). Each of the three standards is addressed with cyber operations against the healthcare sector in mind.

70 This is the standard preferred by the ICJ. See Bosnian Genocide (n 3) 234.

71 Lanovoy (n 54) 45. The distinction historically drawn in international law between 'direct' and 'indirect' causes is of limited value and is no longer utilised. See Rovine and Hanessian (n 60) 241–243, 247. Lahmann additionally explores the requirement of a 'substantial contribution' for individual criminal responsibility in international criminal law. Lahmann (n 27) 427–429.

72 See UN Charter arts 1(1) and 2(4). In Ruys's words, 'the whole object of the Charter was precisely to limit the scope for unilateral use of force as much as possible'. Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 59–60. See also Gray (n 18) 37–40; Dinstein, War, Aggression and Self-Defence (n 12) paras 256–258.

73 In support of the view that a standard of causation may be determined by reference to the underlying purpose of the law and the 'interests it was designed to protect', see Hart and Honoré (n 61) 102. Honoré additionally supports the consideration of 'the scope of the risk'. Honoré, 'Theories of Causation and Remoteness of Damage' (n 61) Chapter 7 para 59.

74 See (n 69) above.

i. A 'Sufficiently Direct and Certain' Causal Nexus

The requirement of a 'sufficiently direct and certain causal nexus', articulated by the International Court of Justice as the suitable standard of legal causation in the context of a claim for reparation pertaining to the breach of the obligation to prevent genocide, requires the establishment of a direct rather than an indirect causal chain or link between the conduct and its effects for the purpose of establishing responsibility. While referring to the requirement of a 'sufficiently direct and certain causal nexus' as the determinative standard of legal causation, the Court seemed to use the 'but for' test or the *conditio sine qua non* as the appropriate standard for undertaking the prior assessment of factual causation.[75]

The application of the requirement of a 'sufficiently direct and certain causal nexus' in the practice of international courts is summed up by one commentator as imposing a relatively strict requirement of directness, in effect requiring that the effects have been brought about 'in one causal step or moment'.[76] The advantage of using such a standard is that it is, in conceptual terms, relatively clear.[77] It imposes no requirements beyond the articulation of a causal chain or link on this basis. At the same time, actually establishing the factual causal chain or link – before imposing the requirement of directness – using the 'but for' test or *conditio sine qua non* can be difficult, since this method of establishing factual causation is typically understood as requiring the decision-maker to undertake the hypothetical counterfactual assessment of whether the effects in question would have resulted even without the conduct in question.[78] Such an exercise inevitably leads to unpredictable outcomes, since 'asking what hypothetically would have occurred if the condition at issue had not taken place leaves the way open for indeterminate

75 The Court asked 'whether the genocide at Srebrenica would have taken place even if the Respondent had attempted to prevent it by employing all means in its possession'. Bosnian Genocide (n 3) 234. Its approach to causation is not especially clear. See further Lanovoy (n 54) 49.
76 Lanovoy (n 54) 53.
77 I Plakokefalos (n 47) 490.
78 Hart and Honoré (n 61) 104. See also Plakokefalos (n 47) 476–477.

speculation'.[79] It is also limited in its ability to resolve cases involving more than one potential cause (cases of 'overdetermination'), in which each may be equally said to result in the effect in question.[80]

In the context of international law, commentators have found that the requirement of a 'sufficiently direct and certain causal nexus', with the strict construction given to the requirement of directness, is unlikely to ever capture the 'pervasive effects' of certain breaches of international obligations.[81] One case in point is a military blockade which might lead to malnutrition and starvation within a population, although not 'directly'.[82] Such conduct would not be unlawful based on the standard of a 'sufficiently direct and certain causal nexus'.[83] The same is true of cyber operations, in particular those targeting the healthcare sector, which do not 'directly' cause death, physical injury or destruction, but which could certainly do so 'indirectly'.[84] The requirement of a 'sufficiently direct and certain causal nexus'[85] is thus ill-suited to address death, physical injury or destruction as the less 'direct' effects of a state's conduct, including through the use of cyber operations. In light of the underlying objectives of remedying harm in the form of death, physical injury and destruction and deterring states from causing such effects, such a standard is too strict a requirement to apply in relation to conduct other than the use

79 Wright and Puppe (n 57) 472. See also ibid 473.

80 As Honoré explains, 'in some cases of "over-determination"—cases where each of two or more independent wrongful acts alone would have sufficed to bring about the harm—the but-for test leads to the dubious conclusion that neither act caused the harm'. Honoré, 'Necessary and Sufficient Conditions in Tort Law' (n 59) 363. Wright and Puppe illustrate the point using the example of two independent fires which may each be said to cause a house to burn down. The 'but for' test, conditio sine qua non, or, in philosophy, condition of 'strong necessity', does not resolve the question of causation in such cases. Wright and Puppe (n 57) 473–481.

81 Lanovoy (n 54) 53. The 'but for' or conditio sine qua non test has also been rejected in other areas of international law as being 'too demanding'. See e.g. V Stoyanova, 'Causation between State Omission and Harm within the Framework of Positive Obligations under the European Convention on Human Rights' (2018) 18 Human Rights Law Review 309, 316.

82 Silver (n 13) 90.

83 Bosnian Genocide (n 3) 234.

84 Roscini, Cyber Operations and the Use of Force in International Law (n 9) 48.

85 Bosnian Genocide (n 3) 234.

of conventional weapons. Determining state responsibility on this basis would limit the scope of the rule so as to exclude means other than conventional weapons in a manner inconsistent with the object and purpose of Article 2(4), in particular the desire to ensure respect for the territorial integrity and political independence of states and the maintenance of international peace and security.

ii. Proximity

A somewhat less restrictive alternative to the requirement of a 'sufficiently direct and certain causal nexus'[86] is the requirement of proximity, which would permit the consideration of relevant effects – death, physical injury and destruction – that are proximate in space and time although not necessarily direct.[87] Put differently, considerations of proximity determine where the causal chain or link should be severed for the purpose of establishing responsibility. One commentator seems to refer to such a standard in the cyber context by proposing that 'a cyber operation that immediately interferes with an ongoing operation of critical infrastructure is more likely to be deemed a use of force than one that only achieves the same effect over an extended period'.[88] The difficulty with using the standard of proximity is that it admits of varied application, permitting decision-makers to draw what are ultimately arbitrary distinctions between proximate and remote causes in any given factual context.[89] Accordingly, this 'rough and ready'[90] standard leaves decision-makers wide discretion as to the assessment of legal causation and thereby of

86 ibid 234.

87 Lanovoy (n 54) 57. A similar standard proposed in criminal law, which is 'far from scientific', requires that the conduct be more than a 'minimal cause' of the effects. Allen (n 55) 52. Conversely, it need not be the 'sole nor the main cause of the prohibited consequence'. ibid 53.

88 MN Schmitt, 'The Use of Cyber Force and International Law', in M Weller (ed), The Oxford Handbook of the Use of Force in International Law (OUP 2015) 1110, 1114.

89 For Hart and Honoré, the reference to 'proximity in space or time' is 'misleading'. Hart and Honoré (n 61) 87. In the context of international law, Plakokefalos exclaims that in judicial practice 'the definition of proximate cause includes anything ranging from factual causal analysis to criteria such as foreseeability and the proper examination of the scope of responsibility'. Plakokefalos (n 47) 488.

90 Honoré, 'Theories of Causation and Remoteness of Damage' (n 61) Chapter 7 para 76.

responsibility.[91] Discretion per se is unobjectionable and is unavoidable in any assessment of legal causation. Still, in the context of Article 2(4) of the UN Charter, predictability as to the application of the provision is paramount.[92] States require sufficiently clear guidance as to when their conduct might constitute a use of force against another state, thereby triggering the range of consequences arising under the law of state responsibility and perhaps also the law of armed conflict and international criminal law.[93] Such clarity is not lent by the standard of proximity.

iii. Reasonable Foreseeability

A third standard of causation asks whether the effects under consideration were reasonably foreseeable in the ordinary course of events so as to attribute them to the impugned state. In other words, is the 'foresight of harm such that in all the circumstances a reasonable man would adopt or refrain from a particular course of action'?[94] Unlike the standards of causation already discussed, the standard of reasonable foreseeability places 'emphasis on the circumstances in which the wrongful act took place, and the position of the responsible state in those circumstances', rather than on the articulation of a causal chain or link between the conduct and its alleged effects.[95] This is not to say that the standard of reasonable foreseeability is a requirement as to intent.[96] Nor does it call

91 For Honoré, the standard of proximity is no more than a useful 'rule of thumb' where it is necessary to choose between causes rather than to allocate responsibility. Honoré, 'Theories of Causation and Remoteness of Damage' (n 61) Chapter 7 para 76. Elsewhere, Hart and Honoré note that the standard of proximity, although often presented in 'factual, policy-neutral terms', leaves wide discretion as to the application of varied considerations of policy. Hart and Honoré (n 61) 97.

92 As Akande and Liefländer note in the context of the proposed right of pre-emptive self-defence, discussed below in Section III, '[a]ccepting vague general principles, rather than precise standards, weakens the law's power to impose meaningful restraints'. D Akande and T Liefländer, 'Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defence' (2013) 107 American Journal of International Law 563, 563. The point is equally relevant here.

93 See (n 70) above.

94 Hart and Honoré (n 61) 263.

95 Lanovoy (n 54) 63. This is not to say that a state cannot be held responsible, at the stage of reparation, for effects other than those that were reasonably foreseeable.

96 In contrast, some construe reasonable foreseeability as a presumption as to intent. R Pizzillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International

for the subjective consideration of what was actually foreseen.[97] Rather, it requires an objective assessment of whether the effects in question could have been reasonably foreseen in the circumstances.[98] According to this standard, a state will not be in breach of Article 2(4) of the Charter if the death, physical injury or destruction that manifested were not the reasonably foreseeable effects of the conduct in the circumstances under consideration. This excludes unforeseeable accidents having relevant effects.[99] Some commentators have hinted at the use of this standard of causation in the context of cyber operations.[100] One does so by imposing a requirement as to directness, suggesting that a cyber operation will constitute a use of force if its 'direct and foreseeable effects are physical injury or property damage'.[101] Another, using the example of a cyber operation that shuts down a hospital's power system, suggests that the knowledge that such an operation can 'cause destruction and serious injury' would qualify it as a use of force.[102] The only two states to have addressed the issue in the cyber context, Australia and New Zealand, support the use of a standard of reasonable foreseeability when assessing the relevance of the various effects of cyber operations.[103]

Responsibility of States', in R Provost (ed), State Responsibility in International Law (Routledge 1992) 12. When it comes to the use of force, Schmitt specifically supports a requirement of intent 'to directly cause physical damage to tangible property or injury or death'. Schmitt, 'Computer Network Attack and the Use of Force in International Law' (n 13) 913.

97 B Cheng, General Principles of Law as Applied by International Courts and Tribunals (CUP 1953) 250–251.

98 Honoré, 'Theories of Causation and Remoteness of Damage' (n 61) Chapter 7 para 91; Lanovoy (n 54) 63.

99 This approach precludes the need for a subjective assessment of 'hostile intent' underlying the conduct of the state, which some commentators propose as an alternative means of excluding accidents from the scope of Article 2(4). See e.g. Ruys, 'The Meaning of "Force"' (n 6) 172.

100 Lahmann uses the term 'presumed causation' to encompass standards ranging from 'strict liability' to 'reasonable likelihood'. Lahmann (n 27) 430–431. While noting that distinct standards could be applied in relation to specific primary rules, Lahmann ultimately prefers this standard to others. ibid 439.

101 Silver (n 13) 85. See also Roscini, Cyber Operations and the Use of Force in International Law (n 9) 47.

102 Schmitt, 'Computer Network Attack and the Use of Force in International Law' (n 13) 913. Note, however, that Schmitt combines this with a requirement of intent, which is not proposed here. ibid.

103 Australia suggested the consideration of 'whether the cyber activity could

On balance, reasonable foreseeability is the standard of causation best suited to Article 2(4) of the UN Charter in the context of cyber operations. It is not as restrictive as the requirement of a 'sufficiently direct and certain causal nexus', which does not capture the 'indirect' but significant effects of such operations.[104] With a view to attributing responsibility for the 'indirect' effects of death, physical injury and destruction resulting from cyber operations, this may be desirable as a matter of policy. At the same time, the standard of reasonable foreseeability is not as imprecise and arbitrary as the standard of proximity, giving states a clearer basis on which to carry out *ex ante* assessments of the lawfulness of proposed conduct and bringing greater consistency to *ex post* causal assessments under Article 2(4).[105] In addition, unlike both the standard of a 'sufficiently direct and certain causal nexus'[106] and the standard of proximity, both of which rely to varying extents on the articulation of a causal chain or link, establishing responsibility on the basis of the standard of reasonable foreseeability does not depend on establishing factual causation. Rather, it relies on the objective assessment of what is reasonably foreseeable in the circumstances. This is not necessary in respect of the use of conventional weapons, in which context the task of establishing a causal chain or link between the use of such a weapon and death, physical injury or destruction is straightforward. When it comes to the use of means other than conventional weapons, however, establishing a causal chain or link between the conduct and any eventual death, injury or destruction is a difficult and thus avoidable exercise. Indeed, commentators warn that '[c]ourts today increasingly have to deal with situations in which specific causation cannot be proven or disproven, due to insufficient knowledge of the relevant causal laws

reasonably be expected to cause serious or extensive … damage or destruction … to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning'. Australia Position Paper 2017 (n 15) 90. New Zealand proposed that states 'may take into account both the immediate impacts and the intended or reasonably expected consequential impacts'. New Zealand Position Paper 2020 (n 15) para 7.

104 Bosnian Genocide (n 3) 234.

105 On the latter, see Lanovoy (n 54) 63.

106 Bosnian Genocide (n 3) 234.

and/or the actual conditions in the specific situation or to probabilistic elements in the relevant processes'.[107] In this light, the better approach is one which is independent of a causal chain or link. According to the standard of reasonable foreseeability proposed here, as long as death, physical injury or destruction manifested in the circumstances and were the reasonably foreseeable effects of the conduct in question, no causal chain or link between the conduct and the effects must be established.

The objection might nevertheless be raised that foreseeability is itself arbitrary: 'in one sense everything is foreseeable, in another sense nothing'.[108] How likely, not unlikely, probable or possible does an effect have to be to be reasonably foreseeable? On the one hand, reasonable foreseeability does not imply 'infinite liability';[109] 'there is the obvious need to limit liability at some point'.[110] This is particularly so in the context of Article 2(4), a key provision of the UN Charter which would be in constant breach and rendered entirely ineffective if reasonable foreseeability were so widely construed. This is clearly undesirable in the context of Article 2(4). What is the 'reasonable and probable'[111] result of the conduct must thus be limited by the consideration of the circumstances, in particular the foreseeability of one or more intervening causes. The consideration of other reasonably foreseeable causes, in addition to the cause at issue, in effect limits what is the reasonably foreseeable effect of the conduct in question. Put differently, the standard of reasonable foreseeability cannot require one to imagine, as the reasonably foreseeable consequence of the conduct, the coinciding of all the conditions sufficient to cause the relevant effects. Alternatively, the standard of reasonable foreseeability may be combined with a requirement, more or less strictly construed, of directness of foreseeable effects.

107 Wright and Puppe (n 57) 493.
108 Hart and Honoré (n 61) 256–257.
109 Rovine and Hanessian (n 60) 244.
110 ibid 238. Rovine and Hanessian make the point in relation to the standard of proximity. It is equally relevant in relation to the standard of reasonable foreseeability.
111 Hart and Honoré (n 61) 257.

On the other hand, the question may be asked whether the effects that actually manifest can ever be foreseeable with any precision.[112] Is it necessary that the exact nature and extent of the effects that actually manifested were reasonably foreseeable, or is it sufficient that the kinds of effects that resulted from the relevant conduct – the class of death, physical injury or destruction – were reasonably foreseeable? Subject to the satisfaction of any gravity requirement,[113] it is sufficient that the state in question have reasonably foreseen that its conduct would result in the class of harms comprising death, physical injury or destruction so as to constitute a use of force.[114] Conversely, the reasonable foreseeability of the actual effects that resulted adds little to the assessment of whether there has been an unlawful use of force, although it may be relevant when determining any reparations due to the targeted state.

In the end, the standard of reasonable foreseeability is neither so strict

112 A related concern which is raised in the context of armed conflict is that the effects of relevant conduct may, 'almost by definition, [be] impossible to foresee'. Plakokefalos (n 47) 488. Although a valid practical consideration in the assessment of causation in respect of armed conflict generally, the point is not limited to the application of the standard of reasonable foreseeability. Indeed, the causal chain or link between the impugned conduct and the actual effects, required by the respective standards of a 'sufficiently direct and certain' causal nexus and proximity, may be equally if not more difficult to ascertain in the context of armed conflict. Rovine and Hanessian in fact suggest that in the context of the 'breakdown of civil order … and other cases presenting difficult causation questions, foreseeability will be a helpful concept'. Rovine and Hanessian (n 60) 235, 249. It is also worth noting that foreseeability is routinely used when making proportionality assessments in the law of armed conflict. See E-C Gillard, 'Proportionality in the Conduct of Hostilities: The Incidental Harm Side of the Assessment', (Chatham House Research Paper, 2018) 15–18 <https://www.chathamhouse.org/sites/default/files/publications/research/2018-12-10-proportionality-conduct-hostilities-incidental-harm-gillard-final.pdf> accessed 6 January 2023.

113 To the extent that there is a minimal gravity requirement under Article 2(4), the standard of reasonable foreseeability requires the foreseeability of effects that satisfy such a requirement. Conversely, for those who argue that no such requirement exists, it will be sufficient that conduct which might lead to death, physical injury or destruction of any gravity have been reasonably foreseeable. On the gravity requirement, see (n 38) above.

114 As Hart and Honoré note, 'it is sufficient if the accident is of a class that might well be anticipated as one of the reasonable and probable results of the wrongful act'. Hart and Honoré (n 61) 257. See also ibid 269. 'Class' refers in the context of Article 2(4) to death, physical injury and destruction. The same approach has been proposed in the context of positive obligations under international human rights law. See Stoyanova (n 81) 314–315.

as to exclude cyber operations and other means that do not 'directly' result in death, physical injury or destruction, nor so vague as to obscure the application of Article 2(4) of the Charter.

3. The Causal Connection: In the Context of Cyber Operations against Healthcare

In the context of cyber operations, what is reasonably foreseeable may in practice be limited by the fact that the assessment is necessarily carried out by reference to existing scientific or technical knowledge as to the use and effects of different kinds of cyber operations.[115] Existing knowledge suggests that the launching of a missile is more or less likely to result in death, physical injury and destruction. Existing knowledge as to the effects of cyber operations, which are constantly evolving, may be comparatively limited, resulting in a more limited set of foreseeable effects. The difficulty is compounded by the clandestine nature of conduct in cyberspace. That said, in the specific context of the healthcare sector, the case that death, physical injury and destruction are reasonably foreseeable effects of cyber operations is more easily made.[116] As one commentator notes, a cyber operation that disrupts a state's critical infrastructure, such as healthcare, is likely to result in 'some physical damage to property or persons'.[117] Others go further in suggesting that, at least in the context of a pandemic, the question of foreseeability

115 Discussing Mill's work on causation, Wright and Puppe agree with him that 'our knowledge of the laws of nature, being inductively derived from actual experience, can never be assumed to be complete'. Wright and Puppe (n 57) 469.

116 Lahmann, discussing disinformation operations, points to 'social science research [which] strongly suggests that exposure to false or misleading narratives … decreases trust in science and negatively affects social behaviour, including the willingness to get vaccinated'. Lahmann (n 27) 437.

117 Roscini, Cyber Operations and the Use of Force in International Law (n 9) 59.

> *has little relevance to operations involving health facilities and capabilities, and public health activities … for the scope and scale of a pandemic is such that almost any interference with the provision of medical care and public health activities would foreseeably impact the health of individuals.*[118]

The analysis is not always so straightforward. What follows is an assessment of whether the different kinds of cyber operations facing the healthcare sector may, by reference to the standard of reasonable foreseeability, constitute a use of force. While it is reasonably foreseeable that disruptive cyber operations against the healthcare sector may result in death or physical injury so as to qualify such operations as a use of force, the standard of reasonable foreseeability is less easily satisfied in cases involving the compromise, theft or publication of medical data ('data breaches') or the dissemination of health-related misinformation or disinformation. In each of these contexts, the presence of other causally relevant conditions or intervening causes, or the imposition of a requirement of directness, will limit the scope of what is reasonably foreseeable, precluding the characterisation of such operations as a use of force.

i. Disruptive Cyber Operations

The healthcare sector is most often faced with disruptive cyber operations, encompassing a range of ransomware and 'denial of service' operations.[119] While ransomware involves the encryption of patient or other data or operating systems pending the payment of a ransom,

118 M Milanovic and MN Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic' (2020) 11 Journal of National Security Law and Policy 247, 255. Although their point is made in relation to the 'rule' of 'sovereignty' the logic is equally applicable here. On sovereignty, see Chapter 4.

119 This includes larger 'distributed denial of service' operations. See CyberPeace Institute, 'Playing with Lives' (n 43) 52-57; D McLaughlin, '"Golden Era for Cyber Attacks as Criminals Take Advantage of Pandemic', The Irish Times (15 January 2022) <https://www.irishtimes.com/life-and-style/golden-era-for-cyber-attacks-as-criminals-take-advantage-of-pandemic-1.4775522> accessed 6 January 2023.

'denial of service' operations overload and thereby disable ICTs so as to render them unavailable in the performance of healthcare-related services. The relevant question is whether the disruption to the provision of healthcare services caused by such operations, including the shutting down of services to prevent further spread of malware,[120] can reasonably foreseeably result in death, physical injury or destruction such that any actual death, physical injury or destruction that results may be described as the legally relevant result of the cyber operation.

Whether in the case of ransomware or 'denial of service' operations, it is reasonably foreseeable that the encryption of patient medical data or the disabling of ICTs necessary for the provision of emergency or acute healthcare services will lead to the interruption of urgent treatment and care, likely causing death or further physical injury to patients. It is not necessary, however, that the precise effects that actually manifested have been reasonably foreseeable. Practical examples illustrate the point well. In 2020, a woman suffering an aortic aneurysm in Düsseldorf, Germany was diverted from the emergency services of the nearest hospital and died as the eventual result of a ransomware operation which denied the hospital access to the ICTs it used 'to coordinate doctors, beds, and treatment, forcing the cancellation of hundreds of operations and other procedures' and 'limit[ing] the hospital's capacity drastically'.[121] It is reasonably foreseeable that the targeting by ransomware of a hospital's emergency services is likely to result in death or physical injury to patients or potential patients, although the death of the specific woman in question need not, for the purpose of the assessment under Article 2(4), have been reasonably foreseeable. The same year, the second largest hospital in the Czech Republic suffered a ransomware operation which disrupted its COVID-19 testing facility at the height of the pandemic, although no deaths were noted in connection with the incident.[122] More

120 This was the necessary result of the ransomware operations against Universal Health Services in the US and Dr Reddy's Laboratories in India, respectively, both in 2020. CyberPeace Institute, 'Playing with Lives' (n 43) 40–41.
121 Ralston (n 40).
122 'Brno University Hospital Ransomware Attack (2020)' (NATO CCDCOE) <https://

recently, in 2021, a series of cyber operations targeting Ireland's Health Service Executive and Department of Health caused the shutting down, amongst others, of radiology services for cancer patients nationwide.[123] In all these cases, the requirement of reasonable foreseeability of effects of death and physical injury, if not destruction, is satisfied.[124] Conversely, where a cyber operation such as the deployment of the 'WannaCry' ransomware has indiscriminate effects, and incidentally happened to have effects on healthcare, amongst other sectors, the case that death, physical injury or destruction are the reasonably foreseeable effects of such an operation is more difficult to make.[125] This is not to exclude the significance of other obligations under international law, which may make indiscriminate cyber operations unlawful or which require states to exercise due diligence in the face of indiscriminate cyber operations.

Where it is not the provision of medical services to individuals that is the target of a cyber operation, the case is less easily made that death, physical injury and destruction are reasonably foreseeable effects. For example, the disabling of ICTs used to provide services ancillary to the provision of healthcare, such as 'patient billing, aid claims submissions, [and] invoice processing', as in the case of the 2020 cyber operation against Life Healthcare in South Africa, are less likely to reasonably foreseeably lead to death, physical injury or destruction.[126] Yet some

cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)> accessed 6 January 2023.

123 C Lally, J Horgan-Jones and A Beesley, 'Department of Health Hit by Cyberattack Similar to that on HSE', The Irish Times (17 May 2021) <https://www.irishtimes.com/news/health/department-of-health-hit-by-cyberattack-similar-to-that-on-hse-1.4566541> accessed 6 January 2023.

124 On the facts, however, none of these cyber operations has been publicly attributed to a state.

125 The 'WannaCry' ransomware operation of 2017 disrupted the functioning of the UK's National Health Service so as to cause the cancellation of over 19,000 medical appointments and procedures. It also variously affected the Russian interior ministry, French car manufacturer Renault, US delivery company FedEx, and several telecommunications and energy companies in Spain. R Cellan-Jones, 'Ransomware and the NHS – The Inquest Begins', BBC News (15 May 2017) <https://www.bbc.co.uk/news/technology-39917278> accessed 6 January 2023.

126 CyberPeace Institute, 'Playing with Lives' (n 43) 40.

have proposed that a 'distributed denial of service' operation (or 'DDoS attack') by State B against a 'virus testing and vaccine research facility' in State A, which 'significantly lessened the ability of State A's population to get tested and obtain test results' and which 'likely caused State A to experience increased rates of infection and mortality from the virus', could constitute a use of force.[127] These consequences, it is argued by these commentators, are 'reasonably foreseeable effects of State B's cyber operation', leading to the suggestion that '[i]f persons in State A in fact fell ill or died at any significant scale as a result of the [distributed denial of service] attack ... , then it may reasonably be characterized as an unlawful use of force against State A by State B'.[128] Although any assessment will need to be made on the facts, the presence of other reasonably foreseeable causes of death or physical injury may prevent the characterisation of such operations as a use of force, effectively limiting what is a reasonably foreseeable effect of the operation in question. In the case at hand, for example, what is reasonably foreseeable may be limited by the decisions of individuals not to comply with social distancing measures, not to use the testing facility, or not to get vaccinated. Simply increasing the risk of death, physical injury or destruction is insufficient to characterise such an operation as a use of force, though it may breach other obligations of states under international law. The use of a standard of reasonable foreseeability in combination with a requirement of directness could lead to the same answer. A slightly different hypothetical scenario, proposed by Norway, suggests that 'cyber operations leading to the destruction of stockpiles of Covid-19 vaccines' could constitute a use of force.[129] In such a case, the destruction of the stockpiles will itself characterise such an operation as a use of force. As in the previous example, whether any subsequent death or physical injury can be said to reasonable foreseeably result from such

127 'Scenario 23: Vaccine Research and Testing' (NATO CCDCOE, Cyber Law Toolkit) para L13 <https://cyberlaw.ccdcoe.org/wiki/Scenario_23:_Vaccine_research_and_testing> accessed 6 January 2023.
128 ibid para L13. Where the effects don't manifest, it is argued, such an operation may nevertheless qualify as a threat of force. ibid.
129 UN GGE Contributions Compendium (n 15) 70 (Norway).

an operation may be more difficult to establish, since the analysis must account for other relevant causes or may be subjected to a requirement of directness of reasonable effects.

As explained above, in Subsection II.A.1.ii, views are divided as to whether the use of a disruptive cyber operation which does not actually lead to death, physical injury or destruction, but is capable of doing so, constitutes a use of force. The 2016 ransomware operation against the Hollywood Presbyterian Medical Centre, for example, which caused the suspension of emergency and other acute healthcare services, did not cause death or physical injury due to the speedy payment of the ransom.[130] Likewise, the targeting by ransomware of three French hospitals in 2021 which, owing to the use of backup procedures and, in one case, early detection of the ransomware, caused minimal disruption.[131] The same is true of ransomware operations against a number of Israeli hospitals the same year.[132] Whichever view is taken as to whether these cyber operations constitute a use of force, such operations may nevertheless be characterised as the attempted use of force or may amount to violations of other rules under international law, such as the prohibition of intervention.[133]

ii. The Compromise, Theft or Publication of Online Data

The monetary value of large sets of patient data and the intellectual property associated with the development of medicines and medical

130 Winton (n 40).
131 'Cyber Attacks Hit Two French Hospitals in One Week, France 24 (16 February 2021) <https://www.france24.com/en/europe/20210216-cyber-attacks-hit-two-french-hospitals-in-one-week> accessed 6 January 2023.
132 'Several Israeli Medical Facilities Targeted with Ransomware Attacks', Haaretz, (17 October 2021) < https://www.haaretz.com/israel-news/2021-10-17/ty-article/.premium/several-israeli-medical-facilities-targeted-with-ransomware-attacks/0000017f-f80d-d47e-a37f-f93d50d70000 > accessed 6 January 2023; 'Top Cyber Official: Hospital Attack "Purely Financial", Likely by Chinese Group', The Times of Israel, (18 October 2021) < https://www.timesofisrael.com/top-cyber-official-hospital-attack-purely-financial-likely-by-chinese-group/ > accessed 6 January 2023.
133 See Chapter 3 Section III.B.

technologies, including data pertaining to clinical trials, has led to unauthorised access to and even theft of such data.[134] In some cases, stolen data is also sold or published on the dark web.[135] Although any assessment will be fact-specific, the theft, compromise or publication of healthcare-related data is unlikely to satisfy the requirement of causation in relation to any eventual death, physical injury or destruction. The standard of reasonable foreseeability is not so strict as to imply 'infinite liability' on the basis of infinite caution.[136] Nor is it a standard of strict liability. Accordingly, it is insufficient justification, for the purpose of attributing legal responsibility, that the cyber operation in question merely increased the risk of death, physical injury or destruction.[137] The prohibition on the use of force would be in constant breach if reasonable foreseeability were so loosely construed. On one view, the foreseeability of intervening causes is key to limiting the scope of what is a reasonably foreseeable result of the conduct. Consider the example of a clinical trial of a COVID-19 vaccine, in which context the confidentiality of datasets in a randomized controlled trial is key to the development and approval of the vaccine. In addition to the unauthorised access to such data, a variety of other causes beyond the compromise of the clinical trial, such as the behaviour of individuals in refusing to get tested, vaccinated or comply with social distancing measures, are also reasonably foreseeable causes of death or physical injury. Similarly, a requirement of directness, in combination with the standard of reasonable foreseeability, could limit what is reasonably foreseeable in this context. A cyber operation targeting the clinical trial of a COVID-19 vaccine may nevertheless constitute a breach of other relevant rules of international law, such as the customary prohibition of intervention in the internal or external

134 CyberPeace Institute, 'Playing with Lives' (n 43) 53-54.

135 In some cases, the publication of stolen data online is part of a 'double extortion' operation. 'CyberPeace Institute, 'Playing with Lives' (n 43) 53, 57. In 2020, for example, the Vastaamo Psychotherapy Center in Finland was subjected to a ransomware operation which included the theft of sensitive patient data. When the ransom was not paid, the stolen data was published online, with individual patients given the option of paying a ransom to have their data removed. ibid 37.

136 Rovine and Hanessian (n 60) 235, 244.

137 See Wright and Puppe (n 57) 492–493.

affairs of another state.[138]

When it comes to the theft of patient medical data, as in the case of the 2017–18 cyber operation against the private healthcare company 'SingHealth',[139] it is reasonably foreseeable that the patients whose data is stolen suffer psychological injury as a result of the fact that their confidential medical records were compromised.[140] The online publication of stolen medical records may, moreover, significantly affect the psychological health of individuals with diagnoses which may ostracize them from their communities, such as substance abuse or HIV/AIDS.[141] This was certainly true of the ransomware operation against the Vastaamo Psychotherapy Centre in Finland, where the patients in question were already seeking psychological services.[142] The characterisation of such an operation as a use of force is likely precluded for other reasons, such as the irrelevance of psychological injury to the characterisation of conduct as a use of force, or the insufficiency of such effects to satisfy the *de minimis* gravity requirement under Article 2(4).[143]

138 See Chapter 3 Section III.B.2.ii.
139 Singaporean Ministry of Communications and Information Committee of Inquiry, 'Public Report on The Cyber Attack On Singapore Health Services Private Limited's Patient Database on or around 27 June 2018' (Report, 10 January 2019) <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/public-report-of-the-coi> accessed 6 January 2023.
140 Shandler and Gomez (n 20).
141 CyberPeace Institute, 'Playing with Lives' (n 43) 45.
142 ibid 37. The nature of the healthcare services in question may be equally relevant to the assessment.
143 On psychological injury, see (n 2) above.

iii. Disinformation and Misinformation Operations

'Influence',[144] 'information'[145] or 'content-based' operations,[146] namely disinformation – the intentional dissemination of false information – and misinformation – the unintentional dissemination of false information – influence the opinions of individuals and, through their dissemination, the public at large.[147] The ability of these operations to spread false information depends in large part on individual initiative to act upon the information received and to further disseminate it.[148]

As with the theft, compromise or publication of online data, it is unlikely that death, physical injury or destruction are the reasonably foreseeable effects of such operations. A range of intervening causes, which in the context of information operations will be many, will be equally foreseeable to the reasonable person. Not least of all in this context is the agency of the individuals who receive the false information and choose whether to act upon it.[149] As one commentator explains, the possibility cannot be excluded that 'the information was considered

144 DB Hollis, 'The Influence of War; The War for Influence' (2018) 32 Temple International and Comparative Law Journal 31; H Lin and J Kerr, 'On Cyber-Enabled Information Warfare and Information Operations' in P Cornish (ed), The Oxford Handbook of Cyber Security (OUP 2021) 251, 252.

145 Oxford Institute for Ethics, Law and Armed Conflict (ELAC), 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' (2021) preambular para 3 <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/> accessed 6 January 2023.

146 T Dias and A Coco, 'Cyber Due Diligence in International Law' (ELAC Report, 2021) 92 <https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf> accessed 6 January 2023.

147 On the distinctions between misinformation and disinformation, see ibid 94-95; M Gebel, 'Misinformation vs. Disinformation: What to Know about Each Form of False Information, and How to Spot Them Online' (Business Insider, 15 January 2021) <https://www.businessinsider.com/guides/tech/misinformation-vs-disinformation?r=US&IR=T> accessed 6 January 2023.

148 Commentators speak of the 'cognitive' dimension of these operations and describe them as 'psychological manipulation'. Hollis, 'The Influence of War; The War for Influence' (n 144) 35–36; Lin and Kerr (n 144) 252.

149 Such an intervening cause is reasonably foreseeable.

but played only a remote, minor part in the decision to act'[150] and, indeed, '[i]t will rarely be possible to rule out that the recipient might have retained agency'.[151] In the context of the COVID-19 pandemic, for example, an individual 'receives the information, processes it and turns it into reasons that form the basis of subsequent behaviour (for example, to ingest a toxic substance that allegedly fends off the coronavirus, to decide against wearing a mask or to not get vaccinated)'.[152] Particularly in light of the various implications of the characterisation of conduct as a use of force,[153] it would be too wide a construction of the standard of reasonable foreseeability to suggest that the intentional or inadvertent dissemination of false health-related information is the cause, for legal purposes, of any subsequent death or physical injury resulting from individual choices and behaviour. Again, as in relation to data breaches, merely increasing the risk of such effects is insufficient to attribute legal responsibility as an unlawful use of force.[154] Such an approach would expand the scope of Article 2(4) excessively and thereby risk rendering the prohibition ineffective. This is not to exclude the possibility that states have other obligations, including positive obligations, to act in the face of misinformation or disinformation.[155]

III. The Right of Self-Defence

A. The Characterisation of Conduct as an Armed Attack

When it comes to the permissibility of the exercise by a state of self-defence under Article 51, the first question to be addressed is whether, and under which conditions, a cyber operation may be characterised as an 'armed attack' so as to trigger the application of the provision. Subsection 1 examines the requirement of an armed attack in Article

150 Lahmann (n 27) 429.
151 ibid 436.
152 ibid 421.
153 See (n 70) above.
154 Wright and Puppe (n 57) 492–493.
155 See Chapter 5 for a discussion of states' positive human rights obligations in relation to the prevention of misinformation and disinformation.

51, while Subsection 2 considers the conditions under which a cyber operation against the healthcare sector might satisfy the requirement of an armed attack. The discussion is necessarily limited by the findings above as to the characterisation of different kinds of cyber operations as a use of force, since an armed attack is by definition a prohibited use of force. Aggression, or the use of armed force by one state against another state, is not separately considered.

In connection with the requirement of an armed attack, the wider scholarship on the law on the use of force raises the question of the permissibility of self-defence against an armed attack which is carried out by a non-state actor but which is not in any way attributable to a state. The question may equally arise in the cyber context, in which cross-border cyber operations are often carried out by non-state actors independently of the states from whose territories they operate. There are competing views on the point, including amongst states, with some arguing that there is as yet no right of self-defence against an armed attack by a non-state actor which is not attributable to a state, and contending that the invocation of the right in such cases is supported by neither the interpretation of Article 51 of the Charter, including by reference to subsequent state practice,[156] nor the requirements under customary international law of state practice and *opinio juris*. However, some states have in fact supported this more expansive view of self-defence.[157] The following discussion does not purport to resolve this debate and simply presumes, in the scenarios considered, that the requirement of attribution is met.

1. The Characterisation of Conduct as an Armed Attack: In General

In principle, if a cyber operation may constitute a threat or use of force under Article 2(4) of the UN Charter, there is no reason why it cannot also be characterised, conditional on the satisfaction of relevant

156 See Vienna Convention on the Law of Treaties (adopted 22 May 1969, entered into force 27 January 1980) 11 UNTS 331 Article 31(3)(b).
157 For an overview of practice since 2001, see Gray (n 18) 206–226.

requirements, as an 'armed attack' under Article 51 of the Charter. There is no qualitative difference between a use of force and an armed attack, the distinction is one of degree. As in the case of Article 2(4), the application of Article 51 is not limited to the use of conventional weapons. Where an 'armed attack' takes place, whether through the use of conventional weapons or other means, including cyber operations, the exercise of the right of self-defence by the targeted state may also take the form of a cyber operation.[158]

What distinguishes an armed attack from other uses of force under Article 2(4) is, according to the ICJ's decision in *Nicaragua*, the 'scale and effects' of the conduct.[159] In other words, it is 'necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms'.[160] One commentary distils three criteria from this jurisprudence, namely 'when force is used on a relatively large scale, is of a sufficient gravity, and has a substantial effect'.[161] The better approach is that the proposed indicators of scale and effects are subsumed within the assessment of gravity.[162] Accordingly, an armed attack is a use of force 'producing (or liable to produce) serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property'.[163]

158 Article 51 of the UN Charter, by referring only to 'the inherent right of individual or collective self-defence', does not specify the form which the right of self-defence must take.

159 Nicaragua (n 5) 103.

160 ibid 102. See also Oil Platforms (Islamic Republic of Iran v. United States of America) (Merits) [2003] ICJ Rep 161 (hereafter 'Oil Platforms') 186–187; Corten (n 6) 400. But see Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 176.

161 Nolte and Randelzhofer (n 30) 1409. On the criteria of scale and effects, see Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 139. For Kretzmer, the identity of the alleged perpetrator and the military nature of the conduct may be additionally relevant. D Kretzmer, 'The Inherent Right to Self-Defence and Proportionality in Jus ad Bellum' (2013) 24 European Journal of International Law 235, 242.

162 For O'Keefe, writing in the context of the crime of aggression, '[i]t is not clear … how the terms "gravity" and "scale" are to be differentiated from each other, although the former would seem to go to the consequences of the act of aggression and the latter to its execution'. R O'Keefe, International Criminal Law (OUP 2015) 159. The same may be said in relation to an armed attack.

163 Dinstein, War, Aggression and Self-Defence (n 12) para 544. See also Roscini, Cyber Operations and the Use of Force in International Law (n 9) 75.

Subject to the requirement of gravity, the criteria used to characterise conduct as a use of force under Article 2(4) may also be considered in the context of an armed attack under Article 51.[164] That the approach taken under Article 51 is consistent with that under Article 2(4) is both necessary and desirable since 'armed attack' is a subset of 'use of force'.[165] The qualification of conduct as an armed attack is thus made on the basis of its effects. First, as in the context of Article 2(4), the effects of death, physical injury and destruction may, conditional on the satisfaction of the criterion of gravity, lead to the characterisation of conduct as an armed attack,[166] including where these effects result from a cyber operation.[167] Relevant effects may pertain either to the public or the private sphere.[168] It is less clear whether other effects might qualify conduct as an armed attack.[169] Secondly, again as in relation to the use of force, the qualification of conduct as an armed attack does not depend on the means used.[170] Means other than conventional weapons may be deployed in a manner capable of relevant effects.[171]

164 O Hathaway, R Crootof, et al, 'The Law of Cyber-Attack' (2012) 100 California Law Review 817, 845–848.

165 Nolte and Randelzhofer (n 30) 1401–1402; Dinstein, War, Aggression and Self-Defence (n 12) para 543.

166 Hathaway, Crootof et al (n 164) 848; K Zemanek, 'Armed Attack', Max Planck Encyclopedia of Public International Law (OUP 2013) para 10.

167 Zemanek (n 166) para 21.

168 Oil Platforms (n 160) 191–192. See also N Ochoa-Ruiz and E Salamanca-Aguado, 'Exploring the Limits of International Law Relating to the Use of Force in Self-Defence' (2005) 16 European Journal of International Law 499, 513; Dinstein, War, Aggression and Self-Defence (n 12) para 574; Roscini, 'World Wide Warfare' (n 21) 116; Roscini, Cyber Operations and the Use of Force in International Law (n 9) 76; Dinstein, 'Computer Network Attacks and Self-Defence' (n 17) 106. Dinstein offers the example of a 'private hospital installation'. ibid.

169 See Tallinn Manual 2.0 (n 7) 342–343; Joyner and Lotrionte (n 12) 855, 863–864. Schmitt questions whether 'it is the nature of the consequences or their seriousness that determines when an action qualifies as an armed attack', proposing that effects other than death, injury and destruction should, if sufficiently serious, qualify relevant conduct as an armed attack. Schmitt, 'The Use of Cyber Force and International Law' (n 88) 1120.

170 Nuclear Weapons (n 7) 244. See also Nolte and Randelzhofer (n 30) 1419; Dinstein, 'Computer Network Attacks and Self-Defence' (n 17) 103; Silver (n 13) 84.

171 The reference here is to the fact of deployment of means capable of relevant effects and not a requirement as to intent. Dinstein offers the example of an unauthorised military border crossing 'even if no fire is opened'. Dinstein, War, Aggression and Self-Defence (n 12) para 559.

As one commentary observes, an armed attack 'may, in principle, also be conducted by electronic weapons', including cyber operations.[172] Finally, whether relevant conduct constitutes an armed attack is not dependent on its target. As commentators warn, the qualification of an armed attack solely on the basis of its targeting of critical infrastructure like healthcare might, in the context of Article 51, lead more easily to the escalation of conflict.[173] It would also conflate the use of force and an armed attack. The targeting of a state's critical infrastructure, such as healthcare, may nevertheless be used to evidence the destructive nature of the effects in question.[174] An additional criterion which is sometimes suggested in relation to an armed attack is the existence or not of hostile intent on the part of the state engaging in the conduct. The criterion of intent being the subject of disagreement and being in any event difficult to ascertain in the case of a state, it is not considered here as being indispensable to the assessment under Article 51.[175]

Although the text of Article 51 does not explicitly articulate a right of self-defence against an armed attack which has not yet occurred, the question has been posed whether such a right nevertheless exists in respect of imminent or even non-imminent (or 'anticipated') armed attacks. Some consider that a right of self-defence exists against imminent armed attacks, although the requirement of imminence is subject to debate.[176] In their view, such an approach is justified in

172 Tallinn Manual 2.0 (n 7) 340–341. See also Nolte and Randelzhofer (n 30) 1419; Silver (n 13) 84; Joyner and Lotrionte (n 12) 855.
173 Hathaway, Crootof et al (n 164) 846.
174 Nolte and Randelzhofer (n 30) 1419–1420; Delerue (n 9) 341.
175 Dinstein uses the criterion of intent to exclude accidents. Dinstein, War, Aggression and Self-Defence (n 12) para 559. Others go further in requiring motive—that an armed attack have been carried out for political or national security reasons. Hathaway, Crootof et al (n 164) 830–832. On the use of the criterion of intent vis-a-vis the criterion of gravity, see Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 166–167; Dinstein, War, Aggression and Self-Defence (n 12) paras 550–553.
176 For a recent demonstration of the difficulties around imminence, see M Milanovic, 'When did the Armed Attack against Ukraine become "Imminent"?' (EJIL Talk!, 20 April 2022) <https://www.ejiltalk.org/when-did-the-armed-attack-against-ukraine-become-imminent/> accessed 6 January 2023. See also Dinstein, War, Aggression and Self-Defence (n 12) paras 611–614.

particular by 'the increasing speed and destructive potential of modern weaponry'.[177] Some go further in contending that a right of self-defence exists against an armed attack which has neither taken place nor is imminent, justifying their view in light of the threats of terrorism and the use of weapons of mass destruction. Others doubt the validity of such reasoning on the basis that it 'open[s] up the floodgates to precisely those risks of abuse that the Charter set out to eradicate'.[178] For them, there is no clear basis for a right of self-defence against either imminent or non-imminent armed attack.[179] Imminent and non-imminent armed attacks must be further distinguished from an inchoate armed attack which has commenced but whose effects, which would qualify it as an armed attack, are yet to manifest. The latter is evidently within the scope of Article 51.[180] The common-sense justification for a right of self-defence against an inchoate armed attack is that the right of a state to defend itself should not be conditional on the completion of such an attack.[181] In contrast, although there are some indications in favour of the emergence of a right of self-defence against imminent armed attacks, state practice and *opinio juris* on the point remain mixed and inconclusive.[182] As one commentator concludes, 'it is impossible

177 Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 257. See also Australian Department of Foreign Affairs and Trade, 'Australia's International Cyber and Critical Technology Engagement Strategy' (Position Paper, 2021) 97–98 <https://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066%20DFAT%20Cyber%20Affairs%20Strategy%202021%20update%20Internals%201%20Acc.pdf> accessed 6 January 2023.

178 Corten (n 6) 408. Additionally, proportionality assessments will be difficult to make in respect of anticipated armed attacks. Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 261.

179 See generally Corten (n 6) Chapter 7; Dinstein, War, Aggression and Self-Defence (n 12) paras 580–598.

180 Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 346; Corten (n 6) 409–410.

181 Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 257.

182 For an overview of state practice from 1945–2001, which overwhelmingly rejected a right of pre-emptive self-defence, see Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 267–305; Gray (n 18) 170–174. On state practice from 2001 onwards, see ibid 330–342; Gray (n 18) 248–261; C O'Meara, 'Reconceptualising the Right of Self-Defence against "Imminent" Armed Attacks"' (2022) Journal on the Use of Force and International Law 1, 11–14.

to identify *de lege lata* a general right of pre-emptive – and *a fortiori* preventive – self-defence'.[183] The following analysis proceeds on the assumption that an inchoate armed attack falls within the scope of Article 51 without resolving whether responses to imminent (or even non-imminent) armed attacks do.[184]

2. The Characterisation of Conduct as an Armed Attack: In the Context of Cyber Operations against Healthcare

A number of states have affirmed in their statements in the UN GGE and UN OEWG that an armed attack under Article 51 of the UN Charter may take the form of a cyber operation, giving rise to a right of self-defence through kinetic or cyber means.[185] Indeed, there is no reason why a cyber operation causing death, physical injury or destruction which satisfies the requisite criterion of gravity will not constitute an armed attack. The assessment of gravity, that is the assessment of the scale of the conduct and its effects, is equally applicable in the context of cyber operations.[186] To the extent that international law recognises that a series of low-level uses of force might, when taken together, constitute

183 Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 342.

184 Conversely, for a discussion of the scope of a right of anticipatory self-defence against an imminent armed attack in the cyber context, see Tallinn Manual 2.0 (n 7) 351–353.

185 Australia Position Paper 2017 (n 15) 48, 90; Canada Position Paper (n 34) para 46; Compendium of statements in explanation of position on the final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (25 March 2021) UN Doc A/AC.290/2021/INF/2 23 (Chile); France Position Paper 2019 (n 15) 8; France, 'Paper Shared with the Open-Ended Working Group Established by Resolution 75/240 - International Law Applied to Operations in Cyberspace' (OEWG Submission, 2021) <https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf> accessed 6 January 2023; Italy Position Paper 2021 (n 15) 9; Japan Position Paper 2021 (n 34) 6; New Zealand Position Paper 2020 (n 15) para 6; Schöndorf (n 15) 399; UN GGE Contributions Compendium (n 15) 30 (Estonia), 43 (Germany), 64 (Netherlands), 69, 73 (Norway), 77 (Romania), 84 (Singapore), 88 (Switzerland), 116 (UK), 137 (US).

186 Tallinn Manual 2.0 (n 7) 339; Dinstein, 'Computer Network Attacks and Self-Defence' (n 17) 103; Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 176; Corten (n 6) 107; Delerue (n 9) 332. Others doubt whether a cyber operation alone could ever amount to an armed attack, even where it results in 'significant physical injury and/or property damage'. Silver (n 13) 93.

an armed attack, the same applies too to cyber operations.[187] The case of a series of repeated, small-scale actions is particularly relevant in the cyber context, though these frequently take the form of 'brief or periodic interruption' to the use of ICTs, which will be difficult to characterise as an armed attack.[188] A cyber operation may also constitute the first step in an inchoate kinetic armed attack even if it does not itself constitute an armed attack.[189]

Conversely, the effects of cyber operations on healthcare other than death, physical injury and destruction, which would not qualify conduct as a use of force, likewise preclude the characterisation of conduct as an armed attack. Accordingly, the 'disruption of communications caused by a temporary [denial of service] attack which does not result in significant human losses or property damage' is unlikely to qualify as an armed attack under Article 51.[190] Nor would a cyber operations causing psychological injury to individuals.[191]

B. The Causal Connection between the Armed Attack and Death, Physical Injury or Destruction

The question of causation discussed in relation to the relevant effects under Article 2(4) of the UN Charter also arises in respect of the characterisation of conduct as an armed attack under Article 51.[192]

187 Dinstein, War, Aggression and Self-Defence (n 12) para 554.
188 Tallinn Manual 2.0 (n 7) 341.
189 Corten considers 'the disruption by computer channels of an anti-aircraft system prior to a bombing campaign'. Corten (n 6) 107. See also P Roguski, 'Violations of Territorial Sovereignty in Cyberspace – An Intrusion-Based Approach', in D Broeders and B van den Berg (eds), Governing Cyberspace: Behavior, Power, and Diplomacy (Rowman & Littlefield 2020) 75–76.
190 Roscini, 'World Wide Warfare' (n 21) 115–116. Conversely, for Joyner and Lotrionte, 'shutting down a state's air traffic control system, … collapsing banking institutions, financial systems and public utilities' might qualify a cyber operation as an armed attack. Joyner and Lotrionte (n 12) 855.
191 As with the threat or use of force, the separate question may be addressed whether psychological injury that satisfies the requirement of gravity is sufficient to characterise conduct as an armed attack.
192 Waxman identifies the issue in this context but does not resolve it. Waxman (n 17)

Recalling the assessment of relevant standards of causation discussed in Section II, which is equally relevant to the assessment of the question of causation under Article 51, Subsection 1 suggests the application under Article 51 of the standard of reasonable foreseeability. Subsection 2 applies this standard to the various kinds of cyber operations facing the healthcare sector to determine whether the effects of these operations are reasonably foreseeable so as to characterise these operations as armed attacks.

1. The Causal Connection: In the Context of Article 51 of the UN Charter

An assessment of gravity under Article 51 of the Charter, that is an assessment of the scale of the conduct and its effects, requires clarification as to which effects might be considered to lead to the characterisation of conduct as an armed attack. For the reasons articulated in relation to relevant standards of causation under Article 2(4), a standard of reasonable foreseeability is equally suited to the determination of causation in respect of an armed attack under Article 51. Amongst the reasons stated in that context, which are equally relevant here, is the need to look beyond the limited application of the requirement of a 'sufficiently direct and certain causal nexus'[193] or the 'but for' test or *conditio sine qua non*. Such a standard would never address, for the purpose of attributing state responsibility, the 'indirect' causing through cyber operations of death, physical injury or destruction of sufficient gravity. The standard of proximity must also be rejected in relation to Article 51, as in relation to Article 2(4), given the wide discretion involved in its application. Given the risk of escalation, consistency and predictability are even more important in the assessment of causation under Article 51.[194] Where the requirement

445.

193 Bosnian Genocide (n 3) 234.

194 The additional implication of the characterisation of conduct as an armed attack is of course that it gives the targeted state a right of individual or collective self-defence. Corten (n 6) 106; Ruys, 'Armed Attack' and Article 51 of the UN Charter (n 18) 55–60; Hathaway, Crootof et al (n 164) 846.

of sufficient gravity is satisfied in relation to relevant indirect effects, and where those effects actually manifest, states must have the right of self-defence. For these reasons, and those discussed in relation to Article 2(4), the standard of reasonable foreseeability is the most suitable under Article 51. It is also worth noting that in the context of an inchoate armed attack, the exercise by a state of self-defence already requires an *ex ante* assessment on its part of the likely effects of the initiated but inchoate conduct, that is, it calls for an assessment of the reasonable foreseeability of relevant effects.[195]

2. The Causal Connection: In the Context of Cyber Operations against Healthcare

In the context of an armed attack under Article 51 of the UN Charter, it is widely recognised that, when it comes to cyber operations, 'the indirect secondary or tertiary effects of cyber-attacks may be much more consequential than the direct and immediate ones'.[196] As Finland suggests, the relevant question is

> *[t]o what extent the definition of a cyberattack comparable to an armed attack should take account of the indirect and long-term impacts of the attack.*[197]

Unlike in respect of Article 2(4) of the Charter, in which context the discussion of causation has been limited, commentators have specifically endorsed the use of a standard of reasonable foreseeability in relation

195 Consider Bethlehem's proposal to consider 'the likely scale of the attack and the injury, loss, or damage likely to result'. D Bethlehem, 'Principles Relevant to the Scope of a State's Right of Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors' (2012) 106 American Journal of International Law 1, 6. Similarly, Dinstein refers to the use of force 'liable to produce' relevant effects and to effects that may be 'reasonably expected from' the use of force. Dinstein, War, Aggression and Self-Defence (n 12) para 544. For Dinstein, '[w]hen no such results are engendered by (or reasonably expected from) a recourse to force, Article 51 does not come into play'. ibid.

196 Waxman (n 17) 437–438.

197 Finland Position Paper 2020 (n 15) 6.

to cyber operations under Article 51.[198] One commentary proposes that the assessment of whether conduct constitutes an armed attack must be based on 'all reasonably foreseeable consequences of the cyber operation'.[199] In respect of a cyber operation 'targeting a water purification plant', for example, it reasons that '[s]ickness and death caused by drinking contaminated water are foreseeable' and thus relevant to the assessment under Article 51.[200] As will be seen below, the same logic extends to the use of cyber operations against the healthcare sector, namely disruptive cyber operations, the theft, compromise or publication of online data, and disinformation and misinformation operations. Subject to the requirement of gravity in respect of the death, injury and destruction in question, it is likely that disruptive cyber operations against healthcare providers responsible for the provision of medical services to individuals will satisfy the requirement of reasonable foreseeability proposed here. Conversely, the compromise, theft and publication of medical data, and the spread of health-related misinformation and disinformation, are unlikely to satisfy this standard.

i. Disruptive Cyber Operations

Disruptive cyber operations like ransomware and 'denial of service' operations may, where they target the provision of healthcare, and subject to the requirement of gravity, constitute an armed attack under Article 51. A handful of states have suggested as much in relation to disruptive cyber operations which target critical infrastructure. For

198 Tallinn Manual 2.0 (n 7) 343; Hathaway, Crootof et al (n 164) 848; Dinstein, War, Aggression and Self-Defence (n 12) para 544. Zemanek takes a wider approach, which he considers to be settled law, that accounts for all 'indirect' effects. In fact, the position is not so clear. See Zemanek (n 166) para 13. The UK also seems to support the use of a standard of reasonable foreseeability in its statements, referring to the consideration of 'the (actual or anticipated) physical destruction of property, injury and death'. UK Foreign, Commonwealth and Development Office, 'Application of International Law to States' Conduct in Cyberspace: UK Statement', (Policy Paper, 3 June 2021) <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement> accessed 6 January 2023.

199 Tallinn Manual 2.0 (n 7) 343.

200 ibid 343.

Norway, a cyber operation which 'severely damages or disables a State's critical infrastructure or functions may … be considered as amounting to an armed attack'.[201] Similarly, Singapore would include within the scope of an armed attack 'a targeted cyber operation causing sustained and long-term outage of Singapore's critical infrastructure'.[202] For France, a cyber operation which 'caused a failure of critical infrastructure with significant consequences or consequences liable to paralyse whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims' would qualify as an armed attack.[203] In such cases, it is not the targeting of critical infrastructure, such as healthcare, that is decisive. Rather, it is the satisfaction of the requirement of gravity through the use of means causing the effects of death, physical injury or destruction which would lead to such a characterisation.[204] As one commentator notes in respect of death, where the '[f]atalities caused by loss of computer-controlled life-support systems' satisfy the requirement of gravity, the conduct may constitute an armed attack.[205] The relevance of various alleged effects is determined on the basis of their reasonable foreseeability, which is satisfied relatively easily in relation to cyber operations targeting the provision of healthcare to individuals, in which context the effects of death and physical injury, if not also destruction, are reasonably foreseeable. That said, the disruptive cyber operations against the healthcare sector to date do not likely satisfy the requirement of gravity so as to constitute an armed attack.

Nor are all disruptive cyber operations targeting the healthcare sector capable of satisfying the requirement of an armed attack. In particular,

201 UN GGE Contributions Compendium (n 15) 70 (Norway).
202 ibid 84 (Singapore). See also New Zealand Position Paper 2020 (n 15) para 8. Switzerland takes note of this approach, although it does not necessarily endorse it. UN GGE Contributions Compendium (n 15) 88 (Switzerland).
203 France Position Paper 2019 (n 15) 16.
204 In the case of the Stuxnet operation, for example, views differed as to whether the disruption of Iran's use of its nuclear reactors was sufficiently destructive as to qualify as an armed attack under Article 51. See e.g. Tallinn Manual 2.0 (n 7) 342; Delerue (n 9) 333.
205 Dinstein, 'Computer Network Attacks and Self-Defence' (n 17) 105.

the 'disruption of communications caused by a temporary [denial of service] attack which does not result in significant human losses or property damage' is unlikely to do so.[206] France seemed to recognise this limitation when it referred to 'limited or reversible effects', which would not, in its view, support the characterisation of conduct as an armed attack.[207] It is nevertheless possible that such operations constitute a part of an inchoate armed attack, where, for example, 'an intrusion … into a computer network has been discovered, although, as yet, it is neither lethal to any person nor tangibly destructive of property'.[208] In such a case, the line between an inchoate armed attack and an imminent or even a non-imminent or anticipated armed attack may be difficult to draw. The securing of unauthorised access to ICTs used for the provision of healthcare may even constitute a threat of force.[209] As two commentators note, 'a cyber-operation that does one thing (e.g., cyberespionage) might simultaneously threaten another (e.g., a prohibited use of force)'.[210]

ii. The Compromise, Theft or Publication of Online Data

The compromise, theft or publication of sensitive online data, such as patient records, clinical trial data or the intellectual property associated with medical research, does not typically disrupt the continued provision of healthcare. Even where the targets of such operations are hospitals or other healthcare providers, the case is not easily made that the reasonably foreseeable effects of such operations include death,

206 Roscini, 'World Wide Warfare' (n 21) 115–116.
207 France Position Paper 2019 (n 15) 7.
208 Dinstein, 'Computer Network Attacks and Self-Defence' (n 17) 111.
209 According to Hollis and van Benthem, the capacity of cyber operations to cause various effects is dependent in large part on the securing of access to 'the targeted system, network or data'. DB Hollis and T van Benthem, 'Threatening Force in Cyberspace', in L Dickinson and E Berg (eds), Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold (forthcoming 2022).
210 ibid. Conversely, one commentator argues that the 'concealed dissemination of disinformation that aims at subtly manipulating the behaviour of the targeted audience' is difficult to construe as a threat to use force. Lahmann (n 27) 425.

physical injury or destruction.[211] Even in the case of the clinical trial of a COVID-19 vaccine, a data breach which causes the state to refrain from authorising the vaccine and thereby prevents individuals from access to life-saving medicine increases the risk of death or physical injury but is not the only reasonably foreseeable cause of any eventual death or physical injury. Various other foreseeable causes will limit what is agreed to be the reasonably foreseeable effect of a data breach, precluding the characterisation of such cyber operations as armed attacks under Article 51. Qualifying reasonable foreseeability by considering only direct foreseeable effects would also tend to exclude the characterisation of a data breach as an armed attack. In any event, the characterisation of such operations as an armed attack is conditioned on the satisfaction of the gravity criterion, which will be difficult to satisfy in relation to the effects of data breaches.

iii. Disinformation and Misinformation Operations

As with the compromise, theft or publication of online data, it is difficult to conclude that disinformation and misinformation operations will reasonably foreseeably lead to death, physical injury and destruction of sufficient gravity as to constitute an armed attack under Article 51. Owing to the nature of these operations, which depend on individual initiative to act upon and to disseminate the false information, the use of a standard of reasonable foreseeability that links any eventual death, physical injury or destruction to such operations would be excessively wide. It is more likely the case that the agency of the individuals concerned, amongst other considerations, is an intervening cause that limits what is a reasonably foreseeable result of a misinformation or disinformation operation. The point has already been made in relation to the potential characterisation of such operations as a use of force.[212] As with the two categories of cyber operations discussed above, relevant

211 An analogous example of conduct which will arguably not constitute an armed attack is the crossing by an armed border patrol into the territory of another state. Nicaragua (n 5) 103; Nolte and Randelzhofer (n 30) 1409.
212 See Section II.B.3.iii in this chapter.

effects will also need to satisfy the requirement of gravity under Article 51, which will preclude the characterisation of many misinformation and disinformation operations as an armed attack. These operations are more suitably regulated in other ways, such as through the compliance by states of their due diligence obligations.[213]

IV. Conclusion

Although there is wide agreement as to the application in principle of the prohibition of the threat or use of force under Article 2(4) of the UN Charter to cyber operations, it is insufficiently clear when a cyber operation may qualify as a use of force. It is at least agreed that a cyber operation which causes effects comparable to conventional operations, namely death, physical injury or destruction, may qualify as a use of force. The consideration of these effects is a suitable means of determining whether a cyber operation constitutes a use of force. Particularly in the context of cyber operations, it is nevertheless unclear when the effects of death, physical injury and destruction may be too indirect or remote or not sufficiently proximate as to be said to result from the cyber operation in question. The determination as to which effects are relevant to the assessment under Article 2(4) must be made by reference to an appropriate standard of causation. Having considered the various standards of causation employed in international law, the standard of reasonable foreseeability is, to the exclusion, on the one side, of the too restrictive standard of a sufficiently direct and certain causal nexus and, on the other side, of the highly discretionary standard of proximity, the most suitable standard of causation in relation to Article 2(4). The use of this standard suggests that, where relevant effects manifest, disruptive cyber operations against the healthcare sector, such as ransomware and 'denial of service' operations, may constitute uses of force, since it is reasonably foreseeable that their use in the context of healthcare may lead to death, physical injury or destruction. Conversely, when it comes to the other kinds of cyber operations with which the healthcare sector

213 See Dias and Coco (n 146).

is faced, such as the theft, compromise or publication of online data, and disinformation and misinformation operations, the reasonable foreseeability of death, physical injury and destruction is either limited by the reasonable foreseeability of other relevant causes or a requirement of directness in the assessment of reasonable foreseeability.

When it comes to an armed attack under Article 51 of the Charter, the additional assessment of the gravity of the conduct in question requires the consideration of the scale of the conduct and its effects. The relevant effects are, as under Article 2(4), death, physical injury and destruction. As in the context of Article 2(4), the assessment of the effects under Article 51 requires clarification as to which effects may be too indirect or remote or not sufficiently proximate as to be said to result from the cyber operation in question. The assessment as to the relevance of various effects must again be made by reference to a suitable standard of causation. As in respect of Article 2(4), the most suitable standard of causation in the context of Article 51 is the standard of reasonable foreseeability. The application of the standard of reasonable foreseeability specifically in relation to cyber operations against the healthcare sector suggests that disruptive cyber operations, such as ransomware and 'denial of service' operations, may, conditional on the satisfaction of the criterion of gravity, constitute an armed attack. In contrast, owing to the foreseeability of various intervening causes, it is unlikely to be reasonably foreseeable that the theft, compromise or publication of online data and the deployment of disinformation and misinformation will lead to death, physical injury or destruction of sufficient gravity, precluding the characterisation of these operations as an armed attack. Speaking more generally of the range of cyber operations facing the healthcare sector, it is unlikely, though not impossible, that the requirement of gravity will be satisfied in relation to relevant effects.

The formulation by a state of a choice or policy as to healthcare, or the implementation of its preferred choice or policy, whether by a public or a private institution, falls within the domestic jurisdiction of the state and thus within the scope of the prohibition.

Chapter 3

The Application of the Prohibition of Intervention to Cyber Operations against the Healthcare Sector

I. Introduction

This chapter poses the question whether a cyber operation against a state's healthcare sector which is attributable to another state breaches the prohibition of intervention under customary international law.[1] Following the decision of the International Court of Justice (ICJ, the Court) in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (hereafter '*Nicaragua*'), it is widely agreed that the prohibition of intervention addresses 'coercive' intervention in the 'internal or external affairs' of a state,[2] but these requirements have been clearly articulated in neither practice nor scholarship.[3] Likewise, when it comes to cyber operations, there is agreement in general terms as to the application of the prohibition of intervention in relation to information and communications technologies (ICTs),[4] but the existing scholarship has focused almost exclusively on the application of the

1 The relevant literature sometimes substitutes the term 'interference' for 'intervention'. At other times the terms are distinguished, with 'interference' referring to conduct falling short of prohibited 'intervention'. See R Jennings and A Watts (eds), Oppenheim's International Law I (9th edn, OUP 2008) 432–433; A Tzanakopoulos, 'The Right to be Free from Economic Coercion' (2015) 4 Cambridge International Law Journal 616, 620–621 footnote 21; N Aloupi, 'The Right to Non-Intervention and Non-Interference' (2015) 4 Cambridge International Law Journal 566, 575. The chapter consistently uses the term 'intervention'.

2 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits) [1986] ICJ Reports 14, 108.

3 Lowe describes the prohibition of intervention as 'one of the most potent and elusive of all international principles'. V Lowe, International Law (OUP 2007) 104.

4 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135 (hereafter 'UN GGE Report 2021') para 71(c). See also P Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views' (The Hague Program for Cyber Norms Policy Brief, 2020).

prohibition to cyber operations against a state's electoral processes,[5] with far less attention being paid to its application in other contexts, in particular in respect of cyber operations targeting the healthcare sector. Against this backdrop, this chapter clarifies the scope of the customary prohibition of intervention and, on this basis, answers the question whether, and under which conditions, cyber operations targeting the healthcare sector may be said to violate the prohibition of intervention.

Section II fleshes out the prohibition of intervention under customary international law by reference to the resolutions of the UN General Assembly and the jurisprudence of the ICJ.[6] Section III identifies the constituent elements of unlawful intervention and considers whether they are satisfied in the context of cyber operations targeting healthcare. First, Section III.A clarifies what is meant by the 'internal or external affairs' of a state and considers which aspects of healthcare might fall within this definition. Secondly, Section III.B articulates the requirement of coercion and applies it to a range of cyber operations against the healthcare sector to determine which among them, if any, may be coercive. Relevant conduct includes disruptive cyber operations which restrict the provision of healthcare, such as ransomware operations (or 'ransomware attacks') and 'denial of service' operations (or 'DoS attacks'), the compromise, theft and publication of sensitive data, such as patient medical records, clinical trial data or the intellectual property associated with medical research, and 'information' operations involving

5 See e.g. JD Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?' (2017) 95 Texas Law Review 1579; MN Schmitt, 'Foreign Cyber Interference in Elections' (2021) 97 International Law Studies 739; S Wheatley, 'Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about "Coercion"' (2020) 31 Duke Journal of Comparative and International Law 161; MN Schmitt, '"Virtual Disenfranchisement": Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 Chicago Journal of International Law 30.

6 The chapter does not 'interpret' the prohibition of intervention, a rule of customary international law, by reference to the rules for the interpretation of international treaties specified in Articles 31–33 of the Vienna Convention on the Law of Treaties. In support of this methodological approach, see M Fabio Lando, 'Identification as the Process to Determine the Content of Customary International Law' (2022) 42(4) Oxford Journal of Legal Studies 1040.

the dissemination of false health-related information to the public.

While indicating, where relevant, states' positions as to the application in their respective views of the prohibition of intervention to cyber operations, the chapter uses a deductive approach. An inductive approach, more common in the assessment of customary international law, is not suited to the analysis here since states' views as to the manner of the application of the prohibition of intervention to cyber operations are as yet limited to only a small fraction of states.[7] The use of an inductive approach would, in this context, skew the analysis in favour of the limited set of states which have expressed a view. Instead, the positions of the states which have articulated their views as to the application of the prohibition of intervention to cyber operations will be used to illustrate the various possibilities as to the application of the rule in this context.

II. The Prohibition of Intervention in Customary International Law

The prohibition of intervention under customary international law has been closely intertwined with the articulation in various multilateral treaties of its conventional counterparts, so much so that the content of the customary rule is fleshed out in large part by reference to treaty law.[8] What follows is an account of these and other relevant

7 Deductive reasoning is preferred when a question is too new to address through inductive reasoning. S Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion' (2015) 26 European Journal of International Law 417, 421–422. As Talmon notes in relation to the ICJ, '[t]he deductive method is not an alternative to the inductive method but, rather, is complementary to it and may be applied whenever the Court cannot ascertain any rules of customary international law by way of induction'. ibid 423. The logic can be extended too to the question of the application of a rule of customary international law to new facts, as in the characterisation or not of cyber operations as prohibited intervention. Even Schwarzenberger, in making the case for an inductive approach to international law, recognises that inductive reasoning 'presupposes the existence of a fair amount of case material from which plausible generalizations may be attempted'. G Schwarzenberger, 'The Inductive Approach to International Law' (1947) 60 Harvard Law Review 539, 541. This is particular important when fleshing out the content of a rule of customary international law.

8 The crucial contribution of Latin American states in this respect cannot be

developments with a view to the clarification of the content of the customary prohibition of intervention. This account assumes the existence of a prohibition of intervention under customary international law, a position widely affirmed in both practice and scholarship,[9] as 'the corollary of every state's right to sovereignty, territorial integrity and political independence'.[10]

Subsection A traces the attempts in various resolutions of the UN General Assembly – some adopted by consensus, others by a majority vote – to elaborate on the prohibition of intervention under customary international law, including as to the application of the prohibition

overstated. The prohibition of intervention first took concrete form in the plurilateral Montevideo Convention on the Rights and Duties of States of 1933, which declared that '[n]o State has the right to intervene in the internal or external affairs of another'. Convention on Rights and Duties of States adopted by the Seventh International Conference of American States (adopted 26 December 1933, entered into force 26 December 1934) 165 LNTS 19 (hereafter 'Montevideo Convention') art 8. Becker Lorca and Scarfi explain in meticulous detail the laying of the foundations for the prohibition of intervention in the Montevideo Convention, in particular through Latin American initiatives at the 1927 and 1928 pan-American conferences at Rio de Janeiro and Havana respectively, as well as the influential role of the 1933 Anti-War Treaty, signed by six Latin American states. See A Becker Lorca, Mestizo International Law: A Global Intellectual History 1842–1933 (CUP 2014) Chapter 9; JP Scarfi, The Hidden History of International Law in the Americas: Empire and Legal Networks (OUP 2017) Chapters 5–6; A Gurmendi Dunkelberg, 'The Latin American View of Jus ad Bellum' (Opinio Juris, 16 May 2018) <https://www.justsecurity.org/56316/latin-american-view-jus-ad-bellum/> accessed 6 January 2023. In addition to Articles 19 and 20 of the Charter of the Organization of American States (hereafter 'OAS Charter'), referenced in this Section, see Pact of the League of Arab States (adopted 22 March 1945, entered into force 10 May 1945) 70 UNTS 237 art 8; Constitutive Act of the African Union (adopted 11 July 2000, entered into force 26 May 2001) 2158 UNTS 3 arts 4(g)–(h), (j) (art 4(h) as amended by the Protocol on Amendments to the Constitutive Act of the African Union 2003); ASEAN Charter (adopted 20 November 2007, entered into force 15 December 2008) 2624 UNTS 223 arts 2(e)–(f); Treaty of Friendship, Cooperation and Mutual Assistance (adopted 14 May 1955, entered into force 6 June 1955) 219 UNTS 3 (the now defunct 'Warsaw Pact') art 8. Notably, none of these provisions declared the prior existence under customary international law of a prohibition of intervention.

9 See e.g. Oppenheim's International Law (n 1) 428–429; M Jamnejad and M Wood, 'The Principle of Non-Intervention' (2009) 22(2) Leiden Journal of International Law 345, 351–355; C Gray, International Law and the Use of Force (3rd edn, OUP 2018) 75; Aloupi (n 1) 570.

10 Oppenheim's International Law (n 1) 428.

in specific contexts.[11] Subsection B examines the contribution in this respect of the ICJ. The Court has not frequently pronounced on this subject, although its articulation of the rule in *Nicaragua* has served as the largely undisputed basis for subsequent discussions, including as to the application *vel non* of the prohibition in the context of cyber operations.

A. Resolutions of the UN General Assembly

Beginning in 1957, the UN General Assembly adopted a series of resolutions asserting the significance of the prohibition of intervention as a means of securing 'international peace and security and friendly co-operation among States'.[12] It had already made note, in 1949, of the International Law Commission's (ILC, the Commission) 'Draft Declaration on Rights and Duties of States',[13] which reproduced the language of the 1933 Montevideo Convention on the Rights and Duties of States in proposing that '[e]very state has the duty to refrain from intervention in the internal or external affairs of another other State'.[14] The Assembly did not, however, adopt the declaration. Instead,

11 The evidentiary value for customary international law of the non-binding resolutions of the General Assembly on non-intervention is open to debate. See SM Schwebel, 'The Effect of Resolutions of the U.N. General Assembly on Customary International Law' (1979) 73 Proceedings of the Annual Meeting of the American Society of International Law 301–309. For Wood and Jamnejad, 'very few' of the resolutions on non-intervention are 'authoritative, and many were adopted by a heavily divided vote'. Jamnejad and Wood (n 9) 350–351. Conversely, Bowett considered, in relation at least to economic coercion, that relevant resolutions of the UN General Assembly are 'indicative of the gradual acceptance of a concept whose influence cannot be ignored'. DW Bowett, 'International Law and Economic Coercion' (1976) 16 Virginia Journal of International Law 245, 246. See also Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226, 254–255. Mindful of these competing views, the discussion in this Section will account for the voting distributions in the adoption of specific resolutions.

12 UNGA Resolution 1236 (XII) (14 December 1957) UN Doc A/RES/1236(XXI) preambular para 2.

13 The General Assembly considered the draft to be 'a notable and substantial contribution towards the progressive development of international law and its codification'. UNGA Resolution 375 (IV) (6 December 1949) UN Doc A/RES/375(IV) para 2.

14 ibid; Convention on Rights and Duties of States adopted by the Seventh International Conference of American States (adopted 26 December 1933, entered into force 26 December 1934) 165 LNTS 19 art 8.

what later followed was the 1965 'Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty' (hereafter 'Declaration on Intervention'), which affirmed – with no votes against it – the 'principle of the non-intervention of States in the internal and external affairs of other States', articulated by that time in the texts of various regional treaties.[15] Reproducing in large part the text of the Charter of the Organization of American States (hereafter 'OAS Charter'), the General Assembly declared that '[n]o State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State'.[16] Like the OAS Charter, it condemned not only armed intervention but also 'all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements'.[17] So also, and again by reference to the OAS Charter, it declared that '[n]o State may use or encourage the use of economic, political or any other type of measure to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind'.[18] These pronouncements were founded in the right of every state, in the view of the Assembly, 'to choose its political, economic, social and cultural systems, without interference in any form by another State'.[19] Notwithstanding the wording of the UN Charter, which makes no reference to intervention by states, it was also proclaimed that 'the practice of any form of intervention … violates the

15 These treaties were the respective charters of the Organization of American States, the League of Arab States and the Organization of African Unity. See further UNGA Resolution 2131 (XX) (21 December 1965) UN Doc A/RES/2131(XX) preambular para 5. The Declaration was adopted with 109 votes in favour, one abstention and seven states not voting.

16 UNGA Resolution 2131 (XX) (n 15) para 1, reproducing OAS Charter art 19.

17 ibid para 1, reproducing OAS Charter art 19.

18 ibid para 2. Article 20 of the OAS Charter is worded slightly differently, prohibiting member states from 'us[ing] or encourag[ing] the use of coercive measures of an economic or political character in order to force the sovereign will of another State and obtain from it advantages of any kind'.

19 UNGA Resolution 2131 (XX) (n 15) para 5. The resolution was followed by UNGA Resolution 2225 (XXI) (19 December 1966) UN Doc A/RES/2225(XXI), which outlined the obligations of the General Assembly in this respect.

spirit and letter' of the UN Charter.[20]

The next milestone in the General Assembly's work on non-intervention was the 1970 'Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations' (hereafter 'Friendly Relations Declaration'), which was adopted without a vote, that is by consensus.[21] The Assembly again reproduced in large part, as it did in 1965, the relevant provisions of the OAS Charter,[22] with a few minor differences.[23] There remained no clear agreement amongst states as to what intervention falling short of the use of force might look like.[24]

In the years that followed, the General Assembly focused its attention on the application of the prohibition of intervention to means other than military intervention, namely economic means of coercion and, with the end of the Cold War, election-related intervention. Another theme that was briefly raised was '[t]he right of States and peoples to have free access to information and to develop fully, without interference, their

20 UNGA Resolution 2131 (XX) (n 15) para 4. See also ibid preambular para 8. The UN Charter only refers to intervention by the organisation itself. See Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) (hereafter 'UN Charter') art 2(7).

21 UNGA Resolution 2625 (XXV) (24 October 1970) UN Doc A/RES/2625(XXV). On the drafting in parallel of the Declaration on Intervention and the Friendly Relations Declaration, see O Pomson, 'The Prohibition on Intervention under International Law and Cyber Operations' (2022) 99 International Law Studies 180, 191–192.

22 UNGA Resolution 2625 (XXV) (n 21) para 1.

23 First, although not materially different, 'the duty not to intervene' was proclaimed not only by reference to the 'internal or external affairs' of a state but also to 'matters within [its] domestic jurisdiction'. ibid para 2. Secondly, unlike in earlier resolutions, the General Assembly extended the prohibition to intervention by a 'group of States' acting together. ibid para 1. In doing so, the Assembly aligned itself more closely with the text of the OAS Charter.

24 R Higgins, Themes and Theories (OUP 2012) 279; L Fisler Damrosch, 'Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs' (1989) 83 American Journal of International Law 1, 10; Gray (n 9) 75. The main division was between 'advanced capitalist' states, on the one hand, and 'socialist and non-aligned states', on the other. See further S Moyn and U Özsu, 'The Historical Origins and Setting of the Friendly Relations Declaration', in JE Viñuales (ed), The UN Friendly Relations Declaration at 50: An Assessment of the Fundamental Principles of International Law (2020) 35–36.

system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations'.[25] This is not to say that consensus was reached as to the applicability of the rule in these contexts; several of the resolutions that followed were passed by majority. Adopting in 1974 the 'Charter of Economic Rights and Duties of States',[26] the Assembly recognised the right of '[e]very State ... to choose its economic system as well as its political, social and cultural systems in accordance with the will of its people, without outside interference, coercion or threat in any form whatsoever'.[27] A subsequent resolution added that '[n]o State may be subjected to economic, political or any other type of coercion to prevent the free and full exercise of [its] inalienable right' to sovereignty over its 'natural resources and all economic activities'.[28] When it came to elections, the General Assembly affirmed that 'any extraneous activities

25 UNGA Resolution 36/103 (9 December 1981) UN Doc A/RES/36/103 Part I(c). The Declaration recognised '[t]he duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States'. ibid Part II(j). 120 states voted in favour, 22 states voted against, six abstained and nine did not vote.

26 The Charter proclaimed that '[e]conomic as well as political and other relations among States' shall be governed by the principle of non-intervention. UNGA Resolution 3281 (XXIX) (12 December 1974) UN Doc A/RES/3281(XXIX) Chapter I para (d). It was adopted with 120 votes in favour, six votes against, ten abstentions and two states not voting. See also UNGA Resolution 3201 (S-VI) (1 May 1974) UN Doc A/RES/3201(S-VI) para 4(a).

27 UNGA Resolution 3281 (XXIX) (n 26) art 1. In the same spirit, the Assembly condemned 'political coercion through the application of economic instruments with the purpose of inducing changes in the economic or social systems, as well as in the domestic or foreign policies, of other countries'. UNGA Resolution 44/215 (22 December 1989) UN Doc A/RES/44/215 para 4. See also UNGA Resolution 46/210 (20 December 1991) UN Doc A/RES/46/210 para 1.

28 UNGA Resolution 3201 (S-VI) (n 26) para 4(e). The Declaration was adopted without a vote. A later resolution elaborated: 'developed countries should refrain from threatening or applying trade restrictions, blockades, embargoes and other economic sanctions, incompatible with the provisions of the Charter of the United Nations ... against developing countries as a form of political and economic coercion which affects their economic, political and social development'. UNGA Resolution 39/210 (18 December 1984) UN Doc A/RES/39/210 para 2. The focus on intervention by developed countries in developing countries continued in later resolutions. See e.g. UNGA Resolution 40/185 (17 December 1985) UN Doc A/RES/40/185; UNGA Resolution 41/165 (5 December 1986) UN Doc A/RES/41/165; UNGA Resolution 42/173 (11 December 1987) UN Doc A/RES/42/173; UNGA Resolution 44/215 (n 27).

that attempt, directly or indirectly, to interfere in the free development of national electoral processes, … or that intend to sway the results of such processes, violate the spirit and letter of the principles established in the [Friendly Relations Declaration]'.[29] This thematic focus was accompanied by more expansive language than before, likely a response to the increased use during the Cold War of 'a wide range of direct and indirect techniques, including withholding assistance and the threat of withholding assistance, subtle and sophisticated forms of economic coercion, subversion and defamation with a view to destabilization'.[30] To its previous references to 'intervention' and 'interference' the Assembly added 'any form of interference, overt or covert, direct or indirect … in the internal or external affairs of other States'.[31] It also recognised a wide right for each state 'to determine freely, and without any form of foreign interference' 'its relations with other States and international organizations'.[32] Corresponding to this right was the duty of states 'to refrain from any action or attempt in whatever form or under whatever pretext to destabilize or to undermine the stability of another State or of any of its institutions'.[33]

29 UNGA Resolution 44/147 (15 December 1989) UN Doc A/RES/44/147 para 3. The same language was used in UNGA Resolution 45/151 (18 December 1990) UN Doc A/RES/45/151; UNGA Resolution 46/130 (17 December 1991) UN Doc A/RES/46/130; UNGA Resolution 47/130 (18 December 1992) UN Doc A/RES/ 47/130 para 3; UNGA Resolution 48/124 (20 December 1993) UN Doc A/RES/48/124 para 3; UNGA Resolution 50/172 (22 December 1995) UN Doc A/RES/50/172 para 3; UNGA Resolution 52/119 (12 December 1997) UN Doc A/RES/52/119 para 3; UNGA Resolution 54/168 (17 December 1999) UN Doc A/RES/54/168 para 3. This included a call for states 'to abstain from financing or providing, directly or indirectly, any other form of overt or covert support for political parties or groups and from taking actions to undermine the electoral processes in any country'. UNGA Resolution 44/215 (n 27) para 5.

30 UNGA Resolution 31/91 (14 December 1976) UN Doc A/RES/31/91 preambular para 7. This was in reference to states 'seek[ing] to free their economies from foreign control and manipulation'. ibid. See also subsequent UNGA Resolution 32/153 (19 December 1977) UN Doc A/RES/32/153 para 1; UNGA Resolution 33/74 (15 December 1978) UN Doc A/RES/33/74; UNGA Resolution 34/101 (14 December 1979) UN Doc A/RES/34/101; UNGA Resolution 35/159 (12 December 1980) UN Doc A/RES/35/159.

31 UNGA Resolution 31/91 (n 30) para 3.

32 ibid para 1.

33 UNGA Resolution 36/103 (n 25) Part II(e). The Declaration was adopted with 122 votes in favour, 22 votes against, six abstentions and nine states not voting. For some commentators, the Declaration 'was passed against the will of many States and does not

In sum, while states have expressed broad agreement within the General Assembly as to the existence of a customary prohibition of intervention in the internal or external affairs of a state, differences emerge as to its scope and as to the applicability of the prohibition in specific contexts.

B. Decisions of the International Court of Justice

The question of intervention arose tangentially in the first ever contentious proceedings of the ICJ, namely the *Corfu Channel* case, which the UK brought against Albania in respect of the alleged laying of mines by the latter in the North Corfu Strait. When addressing Albania's counterclaims, the Court was required to determine whether the UK's own conduct in the Strait – part of Albania's territorial waters – constituted a violation of Albanian sovereignty.[34] The breach alleged by Albania involved, among others,[35] the minesweeping 'Operation Retail' carried out by the UK in the Strait following the destruction by mines of British warships during what the Court confirmed to be their innocent passage through the Strait. Although Albania did not specifically allege that the UK's conduct amounted a violation of the prohibition of intervention, the Court, when addressing the arguments advanced by the UK, clarified that the UK had neither a right to intervene to secure evidence of Albanian involvement in the laying of the mines nor a defence of self-help.[36] Ultimately, the Court confirmed that the Operation violated Albania's sovereignty but did not also declare that

reflect general international opinion' P Kunig, 'Intervention, Prohibition of' Max Planck Encyclopedia of Public International Law (2008) para 20. See also MN Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) footnote 760; S Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention' in JD Ohlin, K Govern and C Finkelstein (eds), Cyber War: Law and Ethics for Virtual Conflicts (OUP 2015) 262–263.

34 Corfu Channel Case (UK v Albania) (Merits) [1949] ICJ Rep 4 (hereafter 'Corfu Channel') 26.

35 Albania also alleged that the passage through the Strait of a squadron of British warships, without prior notification and by reliance on a right of innocent passage, was a violation of its sovereignty. The Court rejected this contention. ibid 28–32.

36 ibid 34–35.

it constituted a breach of the prohibition of intervention.[37] Conversely, Judge Alvarez in his separate opinion sought to affirm that

> *[t]he intervention of a State in the internal or external affairs of another – i.e., action taken by a State with a view to compelling another State to do, or to refrain from doing, certain things – has long been condemned.*[38]

In Judge Alvarez's view, 'the Court must reaffirm ... that intervention and all other forms of forcible action are not permissible, in any form or on any pretext, in relations between States'.[39] Likewise, Judge Krylov and Judge ad hoc Ečer would have each characterised the UK's conduct as intervention in Albanian affairs.[40] For Judge ad hoc Ečer, Operation Retail was 'an intervention, if not in the political, at least in the police or legal sense', since the UK, through its mine-sweeping operation, effectively 'substituted itself for the Albanian police or judicial authorities in performing an act which was a quasi-judicial or police enquiry in Albanian territorial waters – i.e., an act strictly prohibited by international law'.[41]

It was only in its 1986 decision in the *Case Concerning Military and Paramilitary Activities in and against Nicaragua* that the Court addressed head on the question of the existence under customary international law of a prohibition of intervention. In that case, Nicaragua alleged US intervention in its internal affairs through the provision of various forms of support to the military and paramilitary activities of the opposition group Fuerza Democrática Nicaragüense and through the

37 ibid 35–36. On the other international rules corollary to state sovereignty, see Chapter 4.
38 Corfu Channel (n 34) (Separate Opinion of Judge Alvarez) 47.
39 ibid 47.
40 Corfu Channel (n 34) (Dissenting Opinion of Judge Krylov) 76; Corfu Channel (n 34) (Dissenting Opinion of Judge ad hoc Ečer) 130.
41 Corfu Channel (n 34) (Dissenting Opinion of Judge ad hoc Ečer) 130.

mining of Nicaraguan ports.[42] While clarifying that the prohibition of intervention 'is not, as such, spelt out in the [UN] charter', the Court confirmed its existence under customary international law by reference to 'numerous' expressions of *opinio juris* by states 'backed by established and substantial practice'.[43] The Court assigned particular weight in this exercise to the Friendly Relations Declaration.[44] Characterising the prohibition of intervention as 'a corollary of the principle of the sovereign equality of States' and as founded in 'the right of every sovereign State to conduct its affairs without outside interference',[45] the Court explained that

> *the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.*[46]

The Court went on to affirm that '[t]he element of coercion … defines, and indeed forms the very essence of, prohibited intervention'.[47] Applying the prohibition to the case at hand, the Court restricted itself

42 Nicaragua (n 2) 106. In addition to other forms of support, it was Nicaragua's contention that the US, by damaging Nicaragua's economy and political system, sought to 'coerce the government of Nicaragua into the acceptance of United States policies and political demands'. ibid 123.

43 ibid 106. See also Nicaragua (n 2) (Separate Opinion of Judge Singh) 156; Nicaragua (n 2) (Separate Opinion of Judge Sett-Camera) 199.

44 Nicaragua (n 2) 106–107. The question has been posed whether the Court properly established the existence under customary international law of the prohibition of intervention. See Nicaragua (n 2) (Separate Opinion of Judge Ago) 184, footnote 1; A d'Amato, 'Trashing Customary International Law' (1987) 81 American Journal of International Law 101. But see Gray (n 9) 77.

45 Nicaragua (n 2) 106.

46 Nicaragua (n 2) 107–108.

47 ibid.

to 'only those aspects ... which appear to be relevant to the resolution of the dispute',[48] which in the event included the use of force, 'either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State'.[49] The Court also found that 'training, arming, equipping, financing and supplying the *contra* forces or otherwise encouraging, supporting and aiding military and paramilitary activities in and against Nicaragua' constituted unlawful intervention by the US.[50] When it came to other forms of non-forcible conduct, the Court concluded – without any real explanation – that the US's cessation of economic aid to Nicaragua, the reduction in its quota of sugar imports from Nicaragua, and its eventual trade embargo did not constitute intervention in Nicaragua's affairs.[51] Judge Schwebel, in dissent, proposed a narrower articulation of the customary prohibition of intervention than that articulated by the majority, which would prohibit only 'dictatorial interference by one State in the affairs of the other'.[52] Similarly, Judge Ago expressed his doubts as to whether customary international law 'ha[d] already endorsed all the achievements of treaty law where the prohibition of intervention is concerned.[53]

More recently, in its 2005 decision in *Armed Activities on the Territory of the Congo (DRC v Uganda)* (hereafter *'Armed Activities')*, the Court addressed, among others, the question whether Uganda had violated the prohibition of intervention through conduct that included direct military intervention, the provision of various forms of support to 'irregular forces' operating in the DRC, in particular the Mouvement de Libération du Congo, and the 'illegal exploitation of Congolese

48 ibid.
49 ibid.
50 ibid 146.
51 ibid 126.
52 For Judge Schwebel, the prohibition of intervention in customary international law was, at the time, narrower than that articulated in the OAS Charter. Nicaragua (n 2) (Dissenting Opinion of Judge Schwebel) 620. Judge Schwebel's view seems to exclude the endorsement by the General Assembly in its Resolution 2131 (XX) 1965 of the precise wording of the OAS Charter.
53 Nicaragua (n 2) (Separate Opinion of Judge Ago) 516.

natural resources', which the DRC characterised as 'interference' in its 'economic matters'.[54] The Court relied on its prior articulation of the prohibition of intervention in *Nicaragua* and again on the Friendly Relations Declaration to find that both Uganda's military intervention and its military, logistic, economic and financial support to irregular forces in the DRC constituted 'an interference in the internal affairs of the DRC and in the civil war there raging'.[55] Conversely, it avoided a determination as to whether what it found to be the illegal exploitation by Uganda of Congolese resources likewise constituted a prohibited intervention under customary international law.

Excluding the *Corfu Channel* proceedings in which a finding of a breach of the prohibition of intervention was not ultimately made, the jurisprudence of the ICJ on non-intervention has been limited. It was only in the *Nicaragua* decision, reiterated in *Armed Activities,* that the Court articulated what it considered to be the relevant criteria for determining that non-forcible conduct constitutes unlawful intervention, namely that the conduct in question must amount to intervention in the internal or external affairs of a state and must be coercive. These criteria are elaborated and applied in the context of cyber operations against the healthcare sector below.

III. The Application of the Prohibition of Intervention to Cyber Operations against the Healthcare Sector

When assessing the applicability of the prohibition of intervention to cyber operations against the healthcare sector, the relevant question is whether the cyber operation in question constitutes coercive intervention in the internal or external affairs of the state concerned. The question being one of the application of the existing prohibition of intervention, it is not necessary to establish, by reference to *opinio juris* and state practice, the existence of such a prohibition in the context of

54 Armed Activities on the Territory of the Congo (DRC v Uganda) (Merits) [2005] ICJ Rep 168 (hereafter 'Armed Activities'), 181–186.
55 ibid 227. See also ibid 226–227.

cyber operations.[56] Subsection A addresses the question whether cyber operations against the healthcare sector might constitute intervention in the 'internal or external affairs' of a state. This calls for clarity as to the scope of the 'internal or external affairs' of a state, defined in the existing scholarship by reference to the state's '*domaine réservé*'—those matters on which a state has not undertaken international obligations. Subsection B outlines the conditions under which cyber operations against the healthcare sector might satisfy the requirement of coercion. This warrants prior clarification as to what constitutes coercion by a state, a question with no clear answer in the existing practice.

A. The Internal or External Affairs of a State

1. The Internal or External Affairs of a State: In General

The 'internal or external affairs' of a state, the term used in *Nicaragua,* the Friendly Relations Declaration and various other resolutions of the General Assembly to describe the object of prohibited intervention, refers to matters falling within the domestic jurisdiction of a state,[57] including

56 The application in the cyber context of the prohibition of intervention – a rule of general applicability – need not be supported by a distinct, cyber-specific rule of custom. See D Akande, A Coco and T de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communications Technologies' (2022) 99 International Law Studies 4. Conversely, some have suggested that a prohibition of intervention in relation specifically to cyberspace must develop through state practice and opinio juris. See R Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 International Law Studies 395, 397; Wheatley (n 5) 172–173; Pomson (n 21) 217–218.

57 The Friendly Relations Declaration uses 'domestic jurisdiction' interchangeably with 'the internal or external affairs' of a state. UNGA Resolution 2625 (XXV) (n 21) para 2. According to Higgins, '[t]he whole question of intervention of a non-military character is closely tied up with international law notions of jurisdiction' since '[a]n unacceptable minor, non-military intrusion is a violation of a state's jurisdiction'. Higgins, Themes and Theories (n 24) 273. See also D Tladi, 'The Duty Not to Intervene in Matters within Domestic Jurisdiction', in JE Viñuales (ed), The UN Friendly Relations Declaration at 50: An Assessment of the Fundamental Principles of International Law (2020) 87, 92. This is also likely what Judge Ečer meant in his dissenting opinion in Corfu Channel when he described Operation Retail as 'an intervention 'in the police or legal sense', since the UK 'substituted itself for the Albanian police or judicial authorities in performing an act which was a quasi-judicial or police enquiry in Albanian territorial waters'. Corfu Channel (n 34) (Dissenting Opinion of Judge ad hoc

the choice of its political, economic and cultural systems and its foreign policies.[58] Beyond this, there is little clarity as to what actually constitutes the domestic jurisdiction of a state. As one commentator has observed,

> *[m]atters within the competence of states under general international law are said to be within the reserved domain, the domestic jurisdiction, of states. But this is tautological, and in practice the category of domestic jurisdiction is not very fruitful.*[59]

An attempt to clarify the scope of the domestic jurisdiction of a state was made early on by the Permanent Court of International Justice (PCIJ, the Court) in its 1923 advisory opinion in *Tunis-Morocco Nationality Decrees.* In that context, the Court was asked to determine whether a dispute between the UK and France as to the latter's extension of its own nationality legislation to its protectorates fell within its domestic jurisdiction, thereby excluding the resolution of the dispute in accordance with the relevant procedures of the Covenant of the League of Nations. Referring to Article 15(8) of the Covenant, the Court considered that

> *[t]he words "solely within the domestic jurisdiction" seem … to contemplate matters which, though they may very closely concern the interests of more than one State, are not, in principle, regulated by international law. As regards such matters, each State is sole judge.*[60]

Ečer) 130.

58 Nicaragua (n 2) 107–108.

59 J Crawford, Brownlie's Principles of Public International Law (8th edn, OUP 2012) 453.

60 Tunis-Morocco Nationality Decrees (Advisory Opinion) [1923] PCIJ Rep. Series B No. 4 (hereafter 'Tunis-Morocco Nationality Decrees'), 23–24. A similar explanation was given by the Institut de Droit International in its 1954 Articles 'La determination du domaine réservé et ses effets', which in Article 1 defined the domaine réservé as follows: '[l]a domaine réservé est celui des activités étatiques où la compétence de l'Etat n'est pas liée par le droit international'. That is, the reserved domain is the area of a state's activities where the competence of the state has not been bound by international law (author's translation).

In the view of the Court, any attempt to further circumscribe what it referred to as the '*domaine réservé*' or the '*domaine exclusif*' of the domestic jurisdiction of a state is made more difficult by the fact that the determination is 'an essentially relative question', which 'depends on the development of international relations'.[61] In other words, when a state undertakes international obligations in respect of a particular subject, that subject ceases to fall exclusively within its domestic jurisdiction.[62] The PCIJ's characterisation of the domestic jurisdiction of a state as referring to 'matters which ... are not, in principle, regulated by international law' was meant only to determine whether the dispute in question was to be resolved by reference to domestic law rather than international law.[63] Yet some have taken its approach to Article 15(8) of the Covenant in *Tunis-Morocco Nationality Decrees* to imply that any matter which is the subject of international obligations, and which is therefore not exclusively within the domestic jurisdiction of a state, no longer falls within the scope of the prohibition of intervention.[64] In the

61 Tunis-Morocco Nationality Decrees (n 60) 24. See also Higgins (n 24) 274.

62 See KS Ziegler, 'Domaine Réservé' Max Planck Encyclopedia of Public International Law (2013); Tzanakopoulos (n 1) 623; Aloupi (n 1) 574. Others rely on Ziegler to advance the same position in the cyber context. See Tallinn Manual 2.0 (n 33) 316; MS Helal, 'On Coercion in International Law' (2019) 52 NYU Journal of International Law and Politics 1, 66–67 and footnote 263; T Moulin, 'Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward' (2020) 25 Journal of Conflict and Security Law 423, footnote 20; K Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace', in K Ziolkowski (ed), Peacetime Regime for State Activities in Cyberspace (NATO CCDCOE 2013) 135, 164 and footnote 217.

63 See A Clapham, Brierly's Law of Nations: An Introduction to the Role of International Law in International Relations (7th edn, OUP 2012) 423. In the event, the Court, when determining whether the dispute between the UK and France fell solely within the domestic jurisdiction of the latter, concluded that although the question of nationality was 'in principle' within the reserved domain of a state, such a characterisation is 'relative' as it is 'restricted by obligations which [that State] may have undertaken towards other States'. Tunis-Morocco Nationality Decrees (n 60) 24.

64 Kunig (n 33) para 3; Aloupi (n 1) 574. Likewise, in the context of cyber operations, the Tallinn Manual 2.0 states: 'the fact that one State owes an obligation to another State takes the matter out of the realm of domaine réservé, at least as to the latter state'. Tallinn Manual 2.0 (n 33) 317. See also Watts (n 33) 264; Moulin (n 62) 430–433; Schmitt, 'Foreign Cyber Interference in Elections' (n 5) 746; GP Corn, 'Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention' (Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No 2005, 2020), 8–9.

words of one commentator, '[t]he prohibition of intervention protects states against foreign intrusion into th[e] realm where the liberty of states is intact and unencumbered by international legal obligations'.[65]

The categorical conclusion that the prohibition of intervention is inapplicable to subjects on which states have undertaken international obligations is questionable for several reasons. The first is the particular context in which the domestic jurisdiction of a state has been defined as referring to matters 'not, in principle, regulated by international law', which is not necessarily aligned with the distinct context of the prohibition of intervention.[66] The circumscription to date of the domestic jurisdiction of a state on the basis of its international obligations has been in relation to Article 15(8) of the Covenant of the League of Nations and Article 2(7) of the UN Charter, which were, in one way or another, intended to limit the respective competences of the League of Nations and the United Nations.[67] In *Tunis-Morocco Nationality Decrees,* widely cited for its definition of the *domaine réservé*, the relevant question was whether the dispute between the UK and France addressed a matter falling solely within French jurisdiction such that the dispute could not be resolved by reference to international law. Similarly, in *Interpretation of Peace Treaties with Bulgaria, Hungary and Romania*, the question

65 Helal (n 62) 4. Helal seems to prefer the term 'domaine réservé' to 'domestic jurisdiction' to describe the scope of the prohibition of intervention because the former includes, in his view, 'areas of … foreign policy in which a state has not undertaken international legal obligations'. Ibid. Conversely, he considers that the reference to the 'domestic jurisdiction' of a state would exclude matters of foreign policy from the scope of the prohibition. In fact, there is no reason why a state's foreign policy is excluded from the scope of its domestic jurisdiction. As Tladi explains, 'external affairs' are 'those aspects that, though external, are an integral part of sovereignty or the exercise of sovereign rights, such as recognition of foreign governments and votes in international fora'. Tladi (n 57) 92.

66 Tunis-Morocco Nationality Decrees (n 60) 23–24.

67 Article 15(8) of the Covenant of the League of Nations and Article 2(7) of the UN Charter were both meant to 'reassure States' as to the limits of the relevant organisation. G Nolte, 'Article 2(7)', in B Simma, D-E Khan, G Nolte, A Paulus and N Wessendorf (eds), The Charter of the United Nations: A Commentary I (2nd edn, OUP 2012) 280, 290. Article 15(8) defines the jurisdiction of the Council of the League of Nations, while Article 2(7) of the UN Charter takes the form of a general principle and, unlike Article 15(8), uses the term 'intervention'. Article 15(8) refers to matters 'solely' within the domestic jurisdiction of a state, while Article 2(7) refers to matters 'essentially' within the domestic jurisdiction of a state.

was whether the alleged human rights abuses in Bulgaria, Hungary and Romania could be considered as 'essentially within the domestic jurisdiction'[68] of each state so as to preclude the exercise of the ICJ's advisory jurisdiction.[69] In such contexts, it is indeed the case that the domestic jurisdiction of a state reduces as its international obligations increase[70] and, '[i]n order to remove an area from the sphere of domestic jurisdiction, it is sufficient that this area be regulated by international law only in certain respects'.[71] In contrast, it is not evident why a state, by undertaking international obligations in relation to a given subject, effectively waives the application in respect of that subject of the prohibition of intervention. The point is evidenced too by the absence of any reference to *Tunis-Morocco Nationality Decrees* in the ICJ's own determinations as to the applicability of the prohibition of intervention in *Nicaragua* and *Armed Activities* respectively.

Nor is the approach taken by the PCIJ in *Tunis-Morocco Nationality Decrees* well suited to the question of the applicability of the prohibition of intervention. The relevant question in the non-intervention context, as per *Nicaragua*, is whether the conduct constitutes intervention in 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely'.[72] These 'matters' encompass a state's choices and policies, that is matters of 'legislative regulation or of

68 UN Charter art 2(7).

69 Interpretation of Peace Treaties with Bulgaria, Hungary and Romania (Advisory Opinion) [1950] ICJ Rep 65, 70. The issue was addressed as a response to the suggestion by Bulgaria, Hungary and Romania that the General Assembly, in requesting an advisory opinion as to 'the observance of human rights and fundamental freedoms in the three States', 'was "interfering" or "intervening" in matters essentially within the domestic jurisdiction of States'. The Court rejected the argument since it was only asked to address the question of the interpretation of the dispute settlement clauses of the respective treaties, which it deemed to be a matter of international law. ibid 70.

70 Nolte (n 67) 291; Crawford, Brownlie's Principles of Public International Law (n 59) 454.

71 Nolte (n 67) 292. See also Tunis-Morocco Nationality Decrees (n 60) 24.

72 Nicaragua (n 2) 107–108. As Besson notes, the prohibition of intervention applies not only to the domaine réservé but 'more generally' to a state's 'sphere of plenary jurisdiction'. S Besson, 'Sovereignty' Max Planck Encyclopedia of Public International Law (2011) para 126.

administrative activity'[73] left to their discretion, including the manner of the implementation of the state's preferred choices and policies, whether by public or private institutions.[74] The requirement in *Nicaragua* is not equivalent, however, to matters which are not, in principle, regulated by international law—the approach taken in *Tunis-Morocco Nationality Decrees*. As one commentator notes in the context of non-intervention,

> *the fact that a matter is covered by a treaty, or even general international law, does not remove the issue from the domestic jurisdiction of the State concerned. What matters is whether the relevant intervention is directed at a matter over which the State concerned retains the sovereign right to decide freely.*[75]

Although a state may have undertaken international obligations in relation to the exercise of its domestic jurisdiction, the manner of the implementation of those obligations domestically remains in many respects a matter on which it is permitted to freely decide.[76] This is true of obligations under international human rights law, for example, in

73 JHW Verzijl, International Law in Historical Perspective I (AW Sijthoff-Leyden 1968) 272.

74 In the cyber context, Moynihan asks whether the 'function' of the state is implicated. H Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (Chatham House Research Paper, 2019) 34 (a state's 'sovereign functions' includes 'the making of state policies … through its organs and agencies of a legislative, executive and judicial kind') < https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks > accessed 6 January 2023. Others propose a distinction between 'inherently governmental functions' and the domaine réservé, with the latter being relevant in their view to the prohibition of intervention. Tallinn Manual 2.0 (n 33) 24. For Milanovic and Schmitt, '[w]hereas an inherently governmental function is an activity only states perform, the domaine réservé can encompass activities performed by private actors so long as international law allows the state to regulate that activity'. M Milanovic and MN Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations During a Pandemic' (2020) 11 Journal of National Security Law and Policy 247, 256–257.

75 Tladi (n 57) 92.

76 For Aloupi, the domestic jurisdiction of a state is not defined by 'the exclusivity of the state's jurisdiction' but by 'the discretionary nature of its powers and jurisdiction'. Aloupi (n 1) 574. In the cyber context, see Moynihan (n 74) 34; Corn (n 64) 9; TD Gill, 'Non-Intervention in the Cyber Context', in K Ziolkowski (ed) Peacetime Regime for State Activities in Cyberspace (NATO CCDCOE 2013) 222.

which context a state 'possesses a large amount of discretion, as part of its domestic jurisdiction', in determining how to fulfil its obligations.[77] As one commentator explains:

> *Most human rights treaties do not specify in any detail the state conduct they require. They are second order standards which can be satisfied in a variety of ways; it is for the state concerned to decide which.*[78]

There is no reason why the prohibition of intervention should not be equally applicable to the exercise by a state of this discretion, subject of course to the deployment of countermeasures by another state in the event of a breach by the state of the obligation in question—a circumstance precluding wrongfulness.

In sum, the prohibition of intervention applies to the exercise by a state of its domestic jurisdiction, that is the formulation by the state of choices or policies on matters in which it is 'permitted … to decide freely',[79] the implementation of its preferred choices or policies, whether through public or private institutions, and the exercise of its discretion in complying domestically with its international obligations.

77 Nolte (n 67) 298. In the cyber context, the Tallinn Manual 2.0 considers that a coercive operation which seeks to force a state to remove certain online content constitutes unlawful intervention notwithstanding the state's obligations under international human rights law, since 'the regulation of online content … falls within a State's domaine réservé'. Tallinn Manual 2.0 (n 33) 316. Likewise, as Ziolkowski notes, a state that is obliged to protect the right to information under Article 19(1) of the International Covenant on Civil and Political Rights retains discretion in determining which content is 'offensive in terms of morality, security and stability'. Ziolkowski (n 62) 163. See also ibid 164–165.

78 J Crawford, 'Sovereignty as a Legal Value', in J Crawford and M Koskenniemi (eds) The Cambridge Companion to International Law (CUP 2012) 122.

79 Nicaragua (n 2) 107-108.

2. The Internal or External Affairs of a State: In the Context of Cyber Operations against Healthcare

When addressing cyber operations against the healthcare sector, the relevant question is whether and to what extent the provision of healthcare falls within the domestic jurisdiction of a state. This requires the consideration of whether the formulation by the targeted state of choices or policies as to healthcare, or the implementation of the state's preferred choices or policies, are implicated. For the reasons articulated above, the prohibition of intervention will apply irrespective of whether a state has committed itself to relevant international obligations, as many have done, including in respect of the right to health under Article 12 of the International Covenant on Economic, Social and Cultural Rights.[80] States enjoy wide discretion in the implementation of the obligation to achieve the full realisation of the right 'of everyone to the enjoyment of the highest attainable standard of physical and mental health'.[81] This includes, in the context of a pandemic or an epidemic, discretion as to the specific steps to be taken by the state to address the various aspects of prevention, treatment and control.[82] So also, the 'overall management of a public health crisis' remains within the domestic jurisdiction of the state notwithstanding the obligations the state may have under the World Health Organization's International Health Regulations.[83]

The targets of cyber operations within the healthcare sector are wide-ranging, including public and private hospitals and clinics, in particular

80 International Covenant on Economic, Social and Cultural Rights (adopted 19 December 1966, entered into force 3 January 1976) 993 UNTS 3 (hereafter 'ICESCR'). For a discussion of the implications of cyber operations against the healthcare sector on the right to health, see Chapter 5 Section IV.

81 ICESCR art 12.

82 ICESCR art 12(2)(c).

83 'Scenario 20: Cyber Operations against Medical Facilities' (NATO CCDCOE, Cyber Law Toolkit) para L5 <https://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities> accessed 6 January 2023.

those that provide emergency[84] and acute healthcare services,[85] their IT infrastructure[86] and medical devices,[87] research institutions and pharmaceutical companies responsible for the testing and manufacture of COVID-19 vaccines and other medicines and medical technology,[88] the suppliers responsible for the distribution of vaccines and other medicines, and relevant state institutions, such as health ministries. Against the backdrop of the COVID-19 pandemic, states have readily recognised these and other 'medical services and facilities' as being part of a state's 'critical infrastructure' for the provision of public services, which they assert must be protected against malicious cyber operations through the application of the prohibition of intervention and other applicable rules of international law.[89]

84 E.g. W Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', Wired (11 November 2020) <https://www.wired.co.uk/article/ransomware-hospital-death-germany> accessed 6 January 2023.

85 E.g. R Winton, 'Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating', Los Angeles Times (18 February 2016) <https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html> accessed 6 January 2023.

86 E.g. 'New Orangeworm Attack Group Targets the Healthcare Sector in the US, Europe and Asia' (Symantec Enterprise Blogs, 23 April 2018) <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia> accessed 6 January 2023; 'South Africa's Life Healthcare Hit by Cyber Attack', Reuters (9 June 2020) <https://www.reuters.com/article/us-life-healthcare-cyber-idUSKBN23G0MY> accessed 6 January 2023.

87 E.g. T Brewster, 'Medical Devices Hit by Ransomware for the First Time in US Hospitals', Forbes (17 May 2017) <https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4c89894b425c> accessed 6 January 2023.

88 E.g. J Stubbs and C Bing, 'Exclusive: Iran-Linked Hackers Recently Targeted Coronavirus Drugmaker Gilead – Sources', Reuters (8 May 2020) <https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV> accessed 6 January 2023.

89 UN GGE Report 2021 (n 4) para 45; 'Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (10 March 2021) UN Doc A/AC.290/2021/CRP.2 (hereafter 'UN OEWG Report 2021') para 26. Yet the UN GGE and UN OEWG have left it to individual states to determine what constitutes part of their critical infrastructure. UN GGE Report 2021 (n 4) para 44; UN OEWG Report 2021 (n 89) para 18. For states' views, see 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts

As a lowest common denominator, the prohibition of intervention applies at least to 'essential medical facilities', such as emergency medical services.[90] As the UK Attorney General's Office suggests, that '[a]cts like the targeting of essential medical services are no less prohibited interventions … when they are committed by cyber means'.[91] Others propose, in wider terms, that it is the state's 'ability to exercise control over health care in the country' and 'its will with regard to healthcare choices' which are protected by the prohibition of intervention.[92] Accordingly, the prohibition of intervention applies to cases involving significant health-related choices or policies on the part of the state, for example, where the pharmaceutical company targeted is testing a cure for a disease which the state seeks to address. The state's management of the COVID-19 pandemic is a straightforward case. Commentators rightly note that a cyber operation by one state which targets 'the execution of another state's plan for responding to the pandemic', for example where

on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136 (hereafter 'UN GGE Contributions Compendium'). See e.g. ibid 47 (Japan) ('causing physical damage or loss of functionality … against critical infrastructure, including medical institutions, may constitute an unlawful intervention'), 69 (Norway) ('deliberately causing a temporary shutdown of the target State's critical infrastructure'), 83 (Singapore) ('cyber-attacks against our infrastructure'), 116–117 (UK) ('to target the essential medical facilities of another State could … be in violation of the international law prohibition on intervention'), 140 (US) ('attempts to interfere coercively with a State's ability to protect the health of its population – for example, through vaccine research or running cyber-controlled ventilators … during a pandemic'). See also New Zealand Ministry of Foreign Affairs and Trade 'The Application of International Law to State Activity in Cyberspace' (Position Paper, December 2020) (hereafter 'New Zealand Position Paper 2020') para 10 ('causing significant damage to, or loss of functionality in, a state's critical infrastructure, including – for example – its healthcare system') <https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf> accessed 6 January 2023; S Braverman, UK Attorney-General's Office, 'International Law in Future Frontiers' (London, 19 May 2022) <https://www.gov.uk/government/speeches/international-law-in-future-frontiers> accessed 6 January 2023 ('[e]nsuring the provision of essential medical services' is a 'sovereign function' of a State').

90 Moynihan (n 74) 44.

91 J Wright, UK Attorney-General's Office, 'Cyber and International Law in the 21st Century', (London, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 6 January 2023. See also Braverman (n 89).

92 Milanovic and Schmitt (n 74) 258.

the hospital targeted serves as a state's designated COVID-19 test site, constitutes intervention in the exercise of its domestic jurisdiction.[93] To use a practical example, Ireland's implementation of its healthcare policies was arguably implicated in the case of the 2021 ransomware operation against its public healthcare system, the Health Service Executive, which was forced to shut down its IT systems at a national scale during the COVID-19 pandemic.[94] Evidently, the state lost control over the management of the pandemic, along with the implementation of other healthcare policies. As one commentator asserts, 'there can be little doubt that a state's public health policies are part and parcel of its sovereign prerogative'.[95] Even in the absence of a health crisis, a cyber operation which disrupts the provision of healthcare by a state to individuals could amount to intervention in the execution of the state's policy with respect to healthcare.[96] Nor is it relevant for the purpose of the prohibition of intervention whether the choice or policy is ultimately executed by a public or a private institution.[97] That said, the provision of certain services by private entities, which do not further the choice or policy of the state with respect to healthcare, such as cosmetic surgery or services offered by the 'wellness' industry, will not qualify as matters falling within the domestic jurisdiction of the state. It is also unclear whether a state's regulation of ICTs used by individuals to communicate health-related information – such as social media – falls within the scope of its domestic jurisdiction with respect to healthcare. It is more likely

93 ibid 257. See also ibid 258; UN GGE Contributions Compendium (n 89) 140 (US).

94 US Office of Information Security, 'Lessons Learned from the HSE Cyber Attack' (HHS Cybersecurity White Paper, 2 March 2022) <https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf> accessed 6 January 2023.

95 H Lahmann, 'Infecting the Mind: Establishing Responsibility for Transboundary Disinformation' (2022) 33(2) European Journal of International Law 411, 414.

96 Czech Republic, CyberPeace Institute, Microsoft, 'Compendium of Multistakeholder Perspectives: Protecting the Healthcare Sector from Cyber Harm' (2022) 22 <https://www.mzv.cz/un.newyork/en/news_events/the_ministry_of_foreign_affairs_together.html> accessed 6 January 2023; Moulin (n 62) 438.

97 UN OEWG Report 2021 (n 89) para 18; Moynihan (n 74) 44. For Milanovic and Schmitt, this is because the application of the prohibition of intervention to the domaine réservé 'encompass[es] activities performed by private actors so long as international law allows the state to regulate that activity'. Milanovic and Schmitt (n 74) 256–257.

the regulation of the online information environment as an independent exercise of the state's domestic jurisdiction, rather than any link to healthcare, which would trigger the application of the prohibition of intervention to such communications.[98]

B. Coercion

1. Coercion: In General

Not all conduct directed at the exercise of the domestic jurisdiction of a state with respect to healthcare constitutes a prohibited intervention. The Declaration on Intervention and the Friendly Relations Declaration both describe intervention as involving the use by a state of 'economic, political or any other type of measure to coerce another state in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind'.[99] As one commentator laments, this articulation of coercion is 'so vague as to be almost useless',[100] while another points out that, '[a]s a legal proposition, such language is perfectly empty; for if read literally, it would outlaw diplomacy'.[101] For its part, the ICJ has done little to clarify the requirement of coercion, even while noting that it constitutes 'the very essence' of prohibited intervention.[102] In *Nicaragua*, the Court considered that intervention 'bear[s] on matters in which each State is permitted, by the principle of State sovereignty, to decide freely' and that '[i]ntervention is wrongful

98 Tallinn Manual 2.0 (n 33) 316; I Kilovaty, 'The International Law of Cyber Intervention', in N Tsagourias and R Buchan (eds) Research Handbook on International Law and Cyberspace (2nd edn, Edward Elgar 2021) 100.
99 UNGA Resolution 2131 (XX) (n 15) para 2; UNGA Resolution 2625 (XXV) (n 21) para 1.
100 Bowett (n 11) 248.
101 TJ Farer, 'Political and Economic Coercion in Contemporary International Law' (1985) 79 American Journal of International Law 405, 406. Pomson adds that the term 'coercion' was not seriously debated in the drafting of the Friendly Relations Declaration and that '[t]he question of the scope of the prohibition [of intervention] does not appear to have centred on a definition of sorts for the term "coerce"'. Pomson (n 21) 198.
102 Nicaragua (n 2) 107–108.

when it uses methods of coercion in regard to such choices'.[103] The only other elaboration of the requirement of coercion at the Court was offered by Judge Alvarez in the *Corfu Channel* case, in whose view intervention involves 'action taken by a State with a view to compelling another State to do, or to refrain from doing, certain things'.[104]

Other contexts in which coercion has been utilised in international law include the law of treaties and the law of state responsibility, with each attaching distinct consequences to coercion by a state.[105] These areas thus diverge in their respective articulations of coercion. On one side, the Vienna Convention on the Law of Treaties renders a treaty void as a result of the coercion by one state of another and, for this reason, employs a stricter construction of coercion – limited to the threat or use of force – than is warranted in the context of the prohibition of intervention.[106] On the other side, the law of state responsibility does not limit coercion to the threat or use of force but nevertheless defines it in more restrictive

103 ibid.

104 Corfu Channel (n 34) (Separate Opinion of Judge Alvarez) 47.

105 In addition, the EU's proposed 'anti-coercion' regulation of 2021 is tailored to address economic coercion. It purports to apply where a state 'interferes in the legitimate sovereign choices of the Union or a Member State by seeking to prevent or obtain the cessation, modification or adoption of a particular act by the Union or a Member State' or 'by applying or threatening to apply measures affecting trade or investment'. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of the Union and its Member States from Economic Coercion by Third Countries' COM (2021) 775 final art 2(1) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0775> accessed 6 January 2023.

106 Article 52 of the Vienna Convention on the Law of Treaties ('Coercion of a State by the Threat or Use of Force') declares that '[a] treaty is void if its conclusion has been procured by the threat or use of force in violation of the principles of international law embodied in the Charter of the United Nations'. According to Special Rapporteur Waldock, the provision is limited to the threat or use of force since any coercion short of that would leave 'a dangerously wide door to the invalidation of treaties, and hence a threat to the stability of the treaty-making process'. ILC, 'Third Report on the law of treaties, by Sir Humphrey Waldock, Special Rapporteur' (1964) II Yearbook of the ILC 5, 38. See also ibid 26. Incidentally, Article 52 was accompanied by the non-binding 'Declaration on the Prohibition of Military, Political or Economic Coercion in the Conclusion of Treaties' which acknowledged the existence, in the view of some states, of a wider definition of coercion; 'the threat or use of pressure in any form, whether military, political, or economic'.

terms than the General Assembly did.[107] The ILC suggested, in relation to Article 18 of its Articles on the Responsibility of States for Internationally Wrongful Acts, that coercion may involve 'the threat or use of force' or 'intervention, i.e. coercive interference, in the affairs of another State'.[108] In its view, coercion has 'the same essential character as *force majeure*'; '[n]othing less than conduct which forces the will of the coerced State will suffice, giving it no effective choice but to comply with the wishes of the coercing State'.[109] *Force majeure* is in turn defined as 'the occurrence of an irresistible force or of an unforeseen event, beyond the control of the State',[110] which compels the state to act in an 'involuntary' manner or a manner which 'involves no element of free choice'.[111] Conversely, '[i]t is not sufficient that compliance with the obligation is made more difficult or onerous'.[112] The question of how to define coercion as an element of the proposed crime of intervention was also briefly addressed by the Commission in its ultimately discarded Draft Code of Crimes against the Peace and Security of Mankind, but no such definition was agreed.[113]

107 Article 18 of the Articles on the Responsibility of States for Internationally Wrongful Acts provides that, under certain specified circumstances, '[a] State which coerces another State to commit an act is internationally responsible for that act'. ILC, 'Articles on the Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc A/56/10 (hereafter 'ARSIWA').

108 ILC, 'Articles on the Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc A/56/10, reproduced in (2001) II(Part 2) Yearbook of the ILC (hereafter 'ARSIWA Commentary'), 70.

109 ibid 69.

110 ARSIWA art 23(1).

111 ARSIWA Commentary (n 108) 76. The commentary to the ARSIWA describes force majeure as a situation in which 'the State in question is in effect compelled to act in a manner not in conformity with the requirements of an international obligation incumbent upon it'. ibid.

112 ibid 69. See further J Crawford, State Responsibility: The General Part (CUP 2013) 419–421.

113 Special Rapporteur Thiam proposed two alternative definitions of intervention in Draft Article 11(3). The first described intervention broadly, as '[i]nterference' involving 'any act or any measure, whatever its nature or form, amounting to coercion of a State'. The second proposal provided an exhaustive list of unlawful forms of intervention, namely 'fomenting, encouraging or tolerating the fomenting of civil strife or any other form of internal disturbance or unrest in another State' and 'organizing, training, arming, assisting, financing or otherwise encouraging activities against another State, in particular terrorist activities'. ILC, 'Sixth Report on the Draft Code of Crimes against the Peace and Security of Mankind by Doudou Thiam, Special Rapporteur' (1988) UN Doc A/CN.4/411 reproduced

In short, '[t]he nub of the matter is that the word "coercion" has no normative significance; there is nothing illegal about coercion' per se.[114]

Barring the definition of coercion in the Vienna Convention on the Law of Treaties, the coercion by one state of another is not limited to the threat or use of force. Nor is there any reason to so limit it as a requirement for unlawful intervention.[115] On the contrary, the prohibition of intervention would be rendered entirely ineffective if coercion were defined in a manner that coincides with the threat or use of force—a distinct prohibition under international law. Instead, the above practice has been taken to suggest that, to be unlawful, the intervention 'by a state in the affairs of another state'[116] 'must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question'.[117] As has been seen in Subsection A, the 'matter in question' is the choice or policy of the targeted state or its implementation in the exercise of the domestic jurisdiction of the state. To be sure, this articulation of the requirement of coercion leaves considerable discretion in its application to facts. One commentator usefully outlines various possibilities: 'usurp[ing] or undermin[ing] the target state's ability to exercise its exclusive state functions independently', 'seek[ing] to compel an outcome in, or conduct with respect to, the target state's exercise of [its] functions, and 'try[ing] to force the target state into a change of government policy'.[118] There is nothing in the resolutions of the General Assembly or the decisions of

in (1988) II(Part 1) Yearbook of the ILC, 200–201. See also Pomson (n 21) 212.

114 Farer (n 101) 406.

115 In addition to the practice of the UN General Assembly and the ICJ, as well as the work of the ILC on state responsibility, see Jamnejad and Wood (n 9) 348–349; Besson (n 72) para 126; Tladi (n 57) 91.

116 Oppenheim's International Law (n 1) 430.

117 ibid 432. This is similar to Judge Alvarez's articulation. See (n 104) above, Corfu Channel (n 34) (Separate Opinion of Judge Alvarez) 47. Oppenheim is frequently misread as imposing a requirement only of 'forcible or dictatorial' interference. See e.g. G Hafner, 'Present Problems of the Use of Force in International Law' (2009) 73 Annuaire de l'Institut de Droit International 310; Kunig (n 33) para 5; Fisler Damrosch (n 24) footnote 16; Watts (n 33) 256. The additional reference to interference that is 'otherwise coercive' suggests that Oppenheim's articulation of the requirement is not so restrictive.

118 Moynihan (n 74) 44.

the ICJ to suggest that coercion must be accompanied by 'an intention to change the policy of the target state'.[119] Drawing from the work of the ILC, the most that can be said is that the requirement of coercion is ultimately about the loss of the control of the coerced state over the articulation or implementation of choices or policies within the scope of its domestic jurisdiction, in line with the wishes of the coercing state, whether through the threat or use of force or otherwise.[120] Contrariwise, making the state's articulation or implementation of its preferred choice or policy 'more difficult or onerous',[121] or simply 'undermining'[122] the exercise by the state of its jurisdiction, is not coercive.

Various criteria have been proposed to assist with the characterisation of conduct as coercive, that is to establish the fact of the loss of the control of the targeted state over a matter within its domestic jurisdiction. One specification that is sometimes imposed is that the coercion must take the form of a threat intended to secure relevant conduct or consequences through 'fear and a desire to limit or avoid threatened harm' on the part of the targeted state.[123] That is, '[t]he coercing state communicates specific demands to the coerced state and backs those demands with pressure to induce compliance'.[124] To use an example from the cyber context, the 'distributed denial of service' operations (or 'DDoS attacks')[125] that disrupted the services of governmental websites in Estonia in 2007 constituted a coercive threat to the extent that they sought to change the Estonian Government's decision to relocate a contentious Soviet-era statue which had come to symbolise the Soviet occupation of the state.[126] Although a threat of this kind may satisfy

119 Jamnejad and Wood (n 9) 371. See also Tladi (n 57) 92.
120 Moynihan (n 74) 28.
121 ARSIWA Commentary (n 108) 69.
122 Moynihan (n 74) 29.
123 Helal (n 62) 72. See also Ohlin (n 5) 1589–1592.
124 Helal (n 62) 70. See also Helal (n 62) 64–65; Wheatley (n 5) 177; Kilovaty (n 98) 105.
125 See CISA, 'Security Tip (ST04-015): Understanding Denial-of-Service Attacks' (20 November 2019) <https://www.cisa.gov/uscert/ncas/tips/ST04-015> accessed 6 January 2023.
126 N Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle

the requirement of coercion, it is not a necessary condition for conduct to be coercive.[127] Cyber operations targeting critical infrastructure demonstrate that a state may be deprived of control over a matter within its domestic jurisdiction even without being subjected to a coercive threat. As two commentators elaborate, coercion either 'affect[s] the state's *will* to such an extent that its choices are no longer free ones', as in the case of a coercive threat, or it 'deprive[s] the state of the *ability* to exercise ' control' over a matter falling within its domestic jurisdiction.[128]

A second, related suggestion is that the assessment of whether a state's conduct is coercive is to be determined by reference to its intent.[129] The proposition has received the support of a handful of states in the cyber context.[130] Given the difficulties with establishing coercive intent, which

of Non-Intervention in Cyberspace', in D Broeders and B van den Berg (eds), Governing Cyberspace: Behavior, Power, and Diplomacy (Rowman and Littlefield 2020) 48. See also Wheatley (n 5) 184–185. For other examples in the cyber context, see F Delerue, Cyber Operations and International Law (CUP 2020) 238–241.

127 Wheatley illustrates the point well. Wheatley (n 5) 177–182. See also Corn (n 64) 11–12; Kilovaty (n 98) 105.

128 Milanovic and Schmitt (n 74) 256.

129 In support of a criterion of coercive intent in the cyber context, see Tallinn Manual 2.0 (n 33) 321–322; Milanovic and Schmitt (n 74) 257; Tsagourias (n 126) 54–55; Delerue (n 126) 238–241. The Tallinn Manual 2.0 considers that 'the coercive effort must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State'. Tallinn Manual 2.0 (n 33) 318. Put differently, 'a cyber operation that does not seek any change of conduct lacks the requisite coercive element'. ibid. van Benthem, Dias and Hollis refer to this as 'coercive purpose'. T van Benthem, T Dias and DB Hollis, 'Information Operations under International Law' (2022) 55 Vanderbilt Journal of Transnational Law 1217, 1258. Any requirement as to intent is imposed by the primary rule of non-intervention rather than by the law of state responsibility. For this distinction and the exclusion of a general requirement of intent or fault from the law of state responsibility, see O Diggelmann, 'Fault in the Law of State Responsibility – Pragmatism ad infinitum?' (2006) 49 German Yearbook of International Law 293, 294; V Lanovoy, 'Causation in the Law of State Responsibility' (2023) British Yearbook of International Law (forthcoming, advance copy available at <https://doi.org/10.1093/bybil/brab008>), 16.

130 Government of Canada, 'International Law Applicable in Cyberspace' (Position Statement, 2022) (hereafter 'Canada Position Paper') para 22 <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng> accessed 6 January 2023; UN GGE Contributions Compendium (n 89) 5 (Australia), 34 (Germany); New Zealand Position Paper 2020 (n 89) para 9(b); cf DB Hollis, 'From Corollaries to Contents? Elaborating the Principle of Non-Intervention in Cyberspace', in F Delerue and A Géry (eds), International

will need to be inferred from the conduct or its consequences in cases other than those involving a coercive threat, nor is intent an especially useful criterion in establishing coercion.[131]

Setting aside the suggested requirements of a coercive threat and of coercive intent, it is, more often than not, the actual effects of an alleged intervention which demonstrate the fact of the loss of the control of the targeted state over a matter within its domestic jurisdiction.[132] The intensity or severity of the effects[133] and the duration for which the means of coercion were employed might be relevant to the assessment.[134] The question may then be posed whether relevant effects must actually manifest for conduct to be coercive. In other words, is it sufficient that the deprivation of the targeted state of control over a matter within its domestic jurisdiction was a reasonably foreseeable effect of the conduct in question, even if such effects do not manifest? The better

Law and Cybersecurity Governance (EU Cyber Direct 2022) footnote 216.

131 New Zealand Position Paper 2020 (n 89) para 9(b); van Benthem, Dias and Hollis (n 129) 1257–1259.

132 Some assert that 'it is impossible to prejudge whether an act constitutes intervention without knowing its specific context and consequences' since 'the context and consequences of a particular act that would not normally qualify as coercive could raise it to that level.' Tallinn Manual 2.0 (n 33) 319. See also R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 211, 225; Kilovaty (n 98) 107–108.

133 Finnish Ministry of Foreign Affairs, 'International Law and Cyberspace – Finland's National Positions' (Position Paper, October 2020) (hereafter 'Finland Position Paper 2020') 3 <https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859> accessed 6 January 2023; Australian Department of Foreign Affairs and Trade, 'Case studies on the application of international law in cyberspace' (Non-Paper submitted to OEWG, 2020) <https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf> accessed 6 January 2023, at 2; Moynihan (n 74) 36; R Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage', in A-M Osula and H Rõigas (eds), International Cyber Norms: Legal, Policy and Industry Perspectives (CCDCOE 2016) 80; Tsagourias (n 126) 56; Schmitt, 'Foreign Cyber Interference in Elections' (n 5) 747; Moulin (n 62) 444–445. Germany and the UK suggest that cyber operations may be coercive if they are 'comparable in scale and effect to coercion in non-cyber contexts'. UN GGE Contributions Compendium (n 89) 34 (Germany); Braverman (n 89). But see Wheatley (n 5) 186.

134 R Buchan, Cyber Espionage and International Law (Bloomsbury 2019) 226.

view is that the conduct need not actually succeed in depriving the targeted state of control in order to constitute coercive intervention. First, relevant resolutions of the General Assembly clearly evidence the agreement amongst states that even 'attempts' at the various forms of intervention are addressed by the prohibition.[135] The use of this language supports the view that the deployment of means objectively capable of depriving the targeted state of control over a matter within its domestic jurisdiction will satisfy the requirement of coercion, even if the state does not ultimately lose control over the matter. This will be easy to establish where the means employed are inherently coercive, as with the threat or use of force.[136] In other cases, an objective assessment as to reasonable foreseeability may be employed.[137] Secondly, an approach that requires relevant effects to manifest is more limited in its application and creates 'a distinctive risk of excluding otherwise coercive interference in a State's affairs simply because it proves ineffective'.[138] Accordingly, for intervention to be unlawful, it should suffice that the intervening state deploy means capable of depriving the targeted state of control, even if such deployment is ultimately unsuccessful, whether due to a deficiency on the part of the intervening state, the conduct of the targeted state in repelling the intervention, or any other intervening cause.[139]

135 UNGA Resolution 2131 (XX) (n 15) para 1; UNGA Resolution 44/147 (n 29) para 3; UNGA Resolution 36/103 (n 25) Part II(e). The Friendly Relations Declaration used slightly different language: 'all other forms of interference or attempted threats against the personality of the State'. UNGA Resolution 2625 (XXV) (n 21) para 1.

136 O Dörr and A Randelzhofer, 'Article 2(4)', in B Simma, D-E Khan, G Nolte, A Paulus and N Wessendorf (eds), The Charter of the United Nations: A Commentary I (3rd edn, OUP 2012) 210; MC Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale Journal of International Law 421, 428.

137 Reasonable foreseeability as a standard of causation may be imposed in relation to the breach of a primary rule of international law. Alternatively, some construe the requirement of reasonable foreseeability as a presumption as to intent. R Pizzillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', in R Provost (ed), State Responsibility in International Law (Routledge 1992) 9, 12.

138 van Benthem, Dias and Hollis (n 129) 1257. See also Helal (n 62) 79.

139 In 2020, for example, a ransomware operation targeting Hammersmith Medical Research in the UK was identified and repelled without its ICTs or its testing of new vaccines being disrupted. See D Winder, 'COVID-19 Vaccine Test Center Hit by Cyber Attack, Stolen Data Posted Online', Forbes (23 March 2020) <https://perma.cc/E96C-H5R2> accessed 6 January 2023.

2. Coercion: In the Context of Cyber Operations against Healthcare

There is no reason why the above articulation of the requirement of coercion as depriving the targeted state of control over a matter within its domestic jurisdiction cannot be equally applied in the context of cyber operations.[140] For their part, the states that have articulated their views on the application of the prohibition of intervention to cyber operations specifically refer to the requirement of coercion, although they do not necessarily agree on whether the targeted state must actually be deprived of control over the matter in question.[141] On the one hand, states like Canada consider that 'coercive effects that deprive, compel, or impose an outcome on the affected State on matters in which it has free choice' will constitute unlawful intervention.[142] On the other hand,

140 Moynihan (n 74) 28. Some experts at the Tallinn process shared this view. Tallinn Manual 2.0 (n 33) 319. See also Australian Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy (Position Paper, October 2017) 98 <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf> accessed 6 January 2023; Australian Department of Foreign Affairs and Trade (n 133).

141 For an overview, see Hollis, 'From Corollaries to Contents?' (n 130) 55, footnotes 215–216. The language used by Australia is the closest to the requirement of coercion proposed here: '[c]oercive means are those that effectively deprive or are intended to deprive the State of the ability to control, decide upon or govern matters of an inherently sovereign nature.' UN GGE Contributions Compendium (n 89) 5 (Australia). See also Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (Position Paper, 2021) 2 <https://www.mofa.go.jp/files/100200935.pdf> accessed 6 January 2023; UN GGE Contributions Compendium (n 89) 19 (Brazil), 25 (Estonia) (coercing a state 'to take a course of action it would not voluntarily seek'), 34 (Germany) (where 'a State's internal processes regarding aspects pertaining to its domaine réservé are significantly influenced or thwarted and that its will is manifestly bent by the foreign State's conduct'), 57 (Netherlands) ('compelling a state to take a course of action (whether an act or omission) that it would not otherwise voluntarily pursue'), 68 (Norway) ('compel[ling] the target State to take a course of action, whether by act or omission, in a way that it would not otherwise voluntarily have pursued'), 77 (Romania) ('the goal … must be to effectively change the behavior of the target State'), 83 (Singapore) ('to take or forbear a certain course of action'), 87–88 (Switzerland) ('to cause another [state] to act (or refrain from acting) in a way it would not otherwise'). For one commentator, however, the discussion around the application of the prohibition of intervention to cyber operations has 'shift[ed] [from] a strict application of the coercion requirement toward a new emphasis on other kinds of conduct'. H Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' (2021) 32 Duke Journal of Comparative and International Law 61, 100, 106.

142 Canada Position Paper (n 130) para 22. See also German Federal Government,

France subscribes to the view that intervention 'which causes or may cause harm' could constitute unlawful intervention.[143]

Yet others writing in the context of cyber operations emphasise the need for coercive intent, preferring the view that coercion involves conduct 'designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or [to] involuntarily refrain from acting in a particular way'.[144] In their view, 'the coercive effort must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State'.[145] Coercive intent being relatively difficult to establish in relation to the conduct of a state, and in particular in respect of what are typically clandestine cyber operations, the emphasis on intent is not shared here. The divergence in approaches is perhaps resolved by the characterisation of reasonable foreseeability of effects, in some literature, as a presumption as to intent.[146]

The following discussion considers whether the various kinds of cyber operations facing the healthcare sector might satisfy the requirement of coercion articulated above, so as to constitute unlawful

'On the Application of International Law in Cyberspace' (Position Paper, March 2021) (hereafter 'German Position Paper 2021') <https://documents.unoda.org/wp-content/uploads/2021/12/Germany-Position-Paper-On-the-Application-of-International-Law-in-Cyberspace.pdf> accessed 6 January 2023; New Zealand Position Paper 2020 (n 89) para 9(a).

143 France, 'International Law Applied to Operations in Cyberspace - Paper shared by France with the Open-ended Working Group established by Resolution 75/240' (OEWG Submission, 2021) 3 <https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf> accessed 6 January 2023. Similarly, Corn refers to operations that are 'likely to deprive, subordinate, or substantially impair the right of independence in governance … even if inchoate or unsuccessful'. Corn (n 64) 12. See also Tallinn Manual 2.0 (n 33) 322; Helal (n 62) 112.

144 Tallinn Manual 2.0 (n 33) 317. See also Watts (n 33) 256; Milanovic and Schmitt (n 74) 256; Gill (n 76) 218; Tsagourias (n 126) 48; Wheatley (n 5) 191; Ohlin (n 5) 1592; MN Schmitt, "Grey Zones in the International Law of Cyberspace' (2017) 42 Yale Journal of International Law 1, 8; Helal (n 62) 72. Buchan proposes an even looser requirement of coercion, which is not endorsed here ('conduct which compromises or undermines the authority of the state should be regarded as coercive'). Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage (n 133) 78.

145 Tallinn Manual 2.0 (n 33) 318.

146 Pizzillo-Mazzeschi (n 137) 12.

intervention. Relevant conduct includes disruptive cyber operations, the compromise, theft or publication of online data, and misinformation and disinformation operations.

i. Disruptive Cyber Operations

In the context of disruptive cyber operations, such as ransomware or 'denial of service' operations,[147] the relevant question is whether the disruption of a state's use of ICTs in the exercise of its domestic jurisdiction is coercive. The question is especially relevant in relation to healthcare, in which context cyber operations which disrupt the use of healthcare-related ICTs, and thus the provision of healthcare itself, are ubiquitous.[148] Ransomware operations, the most common of the disruptive cyber operations targeting the healthcare sector,[149] typically involve the encryption of operating systems or of patient medical data pending the payment of a ransom. 'Denial of service' operations, while equally disruptive, operate by overloading and thereby disabling ICTs so as to render them unavailable in the performance of various healthcare-related services. The extent of the disruption caused by these operations is substantial. The 'WannaCry' ransomware operation of 2017, for example, disrupted the functioning of the UK's National Health Service to an extent that resulted in the cancellation of over 19,000 medical appointments and procedures.[150] Similarly, the deployment in 2020

147 This includes 'distributed denial of service' operations. See (n 125) above.

148 CyberPeace Institute, 'Playing with Lives: Cyberattacks on Healthcare are Attacks on People' (Report, 2021) 52–57 <https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf> accessed 6 January 2023; D McLaughlin, '"Golden Era" for Cyber Attacks as Criminals Take Advantage of Pandemic', The Irish Times (15 January 2022) <https://www.irishtimes.com/life-and-style/golden-era-for-cyber-attacks-as-criminals-take-advantage-of-pandemic-1.4775522> accessed 6 January 2023.

149 European Union Agency for Cybersecurity (ENISA), Threat Landscape 2021 (Report, 2021) 24 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> accessed 6 January 2023.

150 UK Department of Health and Social Care, 'Securing Cyber Resilience in Health and Care' (Policy Implementation Update Report, 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf> accessed 29 August 2022.

of the Ryuk ransomware against Universal Health Services led to the shutting down of IT services in relation to 250 hospitals and other healthcare facilities across the US.[151] In essence, these cyber operations disrupt the provision of medical and related services, including where these services are shut down to prevent further spread of malware.[152] The targeted institution may also be required to pay a ransom, incur ruinous cybersecurity costs, and remedy any other adverse effects of the disruption.

The requirement of coercion is easily met in the case of cyber operations which significantly disrupt the provision of healthcare. To begin with, such disruption has already been deemed to constitute coercion in the context of other cyber operations. For example, cyber operations which 'hamper [a] state's ability to hold elections', by 'shut[ting] down polling stations'[153] or 'manipulat[ing] ... election results',[154] have been widely considered to satisfy the requirement of coercion. As one commentator observes, a cyber operation that involves 'the disabling of critical state infrastructure ... may be more likely to be coercive because [it] would necessarily have a practical effect on the free will of the target state to exercise its sovereign functions exclusively and effectively over that infrastructure'.[155] Accordingly, the disruption of a state's healthcare-

See also CyberPeace Institute, 'Playing with Lives' (n 148) 34. The WannaCry ransomware operation also affected the Russian interior ministry, French car manufacturer Renault, US delivery company FedEx, and several telecommunications and energy companies in Spain. R Cellan-Jones, 'Ransomware and the NHS – The Inquest Begins', BBC News (15 May 2017) available at <https://www.bbc.co.uk/news/technology-39917278> accessed 6 January 2023.

151 ENISA, Threat Landscape 2021 (n 149) 98.

152 This was the necessary result of the ransomware operations against Universal Health Services in the US and Dr Reddy's Laboratories in India, respectively, both in 2020. CyberPeace Institute, 'Playing with Lives' (n 148) 40–41.

153 Pomson (n 21) 219. See also Schmitt, 'Foreign Cyber Interference in Elections' (n 5) 747.

154 B Egan, 'International Law and Stability in Cyberspace' (2017) 35 Berkeley Journal of International Law 169, 175. See also Finland Position Paper 2020 (n 133) 3; German Position Paper (2021) (n 142) 5–6; New Zealand Position Paper 2020 (n 89) para 10; Wheatley (n 5) 186; Schmitt, 'Foreign Cyber Interference in Elections' (n 5) 747.

155 Moynihan (n 74) 36. See also Wheatley (n 5) 186; Helal (n 62) 112.

related ICTs may lead to the loss of the control of the state over the intended implementation of its choices or policies with respect to the provision of healthcare, whether through public institutions, as in the case of the UK's National Health Service, or private institutions, as in the case of Universal Health Services. A 'denial of service' operation which targets, for example, 'a State-run hospital serving as a virus testing and vaccine research facility' in State A,[156] 'interferes with the crisis response plan developed by State A's Ministry of Health by rendering the … virus testing centre in State A unable to perform its intended function as a key component of State A's plan to manage the public health crisis'.[157] As elaborated by the UK's Attorney General, various other forms of disruption to the healthcare sector, including the disruption of 'systems controlling emergency medical transport' and 'supply chains for essential medicines and vaccines', 'causing hospital computer systems to cease functioning', and 'preventing the supply of power to … healthcare', would also lead to the loss of the control of the state over the provision of healthcare, qualifying such operations as coercive.[158]

ii. The Compromise, Theft or Publication of Online Data

Cyber operations involving unauthorised access to, theft or publication of online date are increasingly common in the healthcare sector given the significant value associated with large sets of patient data, which may be sold on the dark web, as well as the intellectual property associated with the development of medicines and medical technology, which may be valuable from a public health perspective.[159] Generally speaking, the compromise and even theft or publication of online medical data is not disruptive in the same way as ransomware or 'denial of service' operations, since these operations do not interrupt the continued provision of

156 'Scenario 23: Vaccine Research and Testing' (NATO CCDCOE, Cyber Law Toolkit) <https://cyberlaw.ccdcoe.org/wiki/Scenario_23:_Vaccine_research_and_testing> accessed 6 January 2023.
157 ibid para L11.
158 Braverman (n 89).
159 CyberPeace Institute, 'Playing with Lives' (n 148) 53–54.

healthcare.[160] Even in the context of a health crisis, unauthorised access to information held by a health ministry or other relevant institution is not necessarily coercive, since such operations do not deprive the state of control over its response to the crisis. This was the case in the early days of the COVID-19 pandemic, with China's Ministry of Emergency Management and the government of Wuhan being the targets of an unauthorised data breach.[161]

One potential exception to this analysis is an operation in which confidential clinical trial data is accessed,[162] compromising the integrity of the medical research being undertaken.[163] This is because the success of a clinical trial depends on the division of test subjects into a treatment group and a control group in a setting in which none of them is aware of their allocation. Compromising this confidential allocation of test subjects renders the results of a clinical trial unreliable, 'jeopardis[ing] the entire process of regulatory approval'.[164] Where the clinical trial in question pertains to the authorisation of a medicine or medical technology intended for use in the implementation of a state's healthcare policy, a

160 For Wheatley, 'just providing the facts' is not coercive. Wheatley (n 5) 188–189. See also Helal (n 62) 113; Delerue (n 126) 258; 'Scenario 23: Vaccine Research and Testing' (n 156) para L10.

161 CyberPeace Institute, 'Playing with Lives' (n 148) 67.

162 In some cases, data is encrypted and also stolen or published online, typically, but not necessarily, pending the payment of a ransom. Such an operation is referred to as a 'double extortion operation'. CyberPeace Institute, 'Playing with Lives' (n 148) 53, 57. In 2020, for example, the Vastaamo Psychotherapy Center in Finland was subjected to a ransomware operation which included the theft of sensitive patient data. When the ransom was not paid, the stolen data was published online, with individual patients given the option of paying a ransom to have their data removed. ibid 37.

163 A similar argument is made in the context of electoral intervention, where unauthorised access to and theft of voter registration data, as in the case of the 2016 US presidential election, compromises the authenticity of an election. Commentators are divided over whether such conduct alone would be coercive. According to some, the 2016 operation was coercive since it 'caused [the elections] to unfold in a way that they otherwise would not have'. Schmitt, 'Grey Zones' (n 144), 8. See also Helal (n 62) 113–114. But see Ohlin (n 5) 1593.

164 T Dias and A Coco, Cyber Due Diligence in International Law (Oxford Institute for Ethics, Law and Armed Conflict 2021) 72 <https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf> accessed 6 January 2023.

cyber operation that breaches the confidentiality of the trial prevents the state from exercising its choice as to the authorisation or not of the medicine or medical technology, and may thus be coercive. Such effects have already been felt in the context of the COVID-19 pandemic. In 2020, for example, a cyber operation against the Indian pharmaceutical company, Dr Reddy's Laboratory, combined the use of ransomware with the theft of clinical trial data associated with the development of the Sputnik V vaccine, causing the closure of vaccine production facilities across several states.[165] In some cases, the publication of stolen data may even be manipulated, for example, by taking relevant information out of context or presenting it selectively. This was the case the same year when the European Medicines Agency was subjected to the theft and publication of data relating to its authorisation of the Pfizer/BioNTech vaccine.[166] In short, there may be contexts in which a cyber operation which compromises confidential medical data deprives the state of control over the articulation of choices or policies as to healthcare, and are thus coercive.

iii. Disinformation and Misinformation Operations

A third category of cyber operations, referred to as 'influence'[167] or 'content-based' operations,[168] includes disinformation – the intentional dissemination of false information with a view to influencing public opinion – and misinformation – the unintentional dissemination of false information by bots, individuals or both, which might likewise

165 A Millar, 'Five Pharma Cybersecurity Breaches to Know and Learn From' (Pharmaceutical Technology, 17 September 2021) <https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/> accessed 6 January 2023.
166 European Medicines Agency, 'Cyberattack on EMA – Update 5' (15 January 2021) <https://www.ema.europa.eu/en/news/cyberattack-ema-update-5> accessed 6 January 2023; EMA 'Cyberattack on EMA – Update 6' (25 January 2021) <https://www.ema.europa.eu/en/news/cyberattack-ema-update-6> accessed 6 January 2023; 'Pfizer/BioNTech Vaccine Docs Hacked from European Medicines Agency', BBC News (9 December 2020) <https://www.bbc.co.uk/news/technology-55249353> accessed 6 January 2023.
167 H Lin and J Kerr, 'On Cyber-Enabled Information Warfare and Information Operations', in P Cornish (ed), The Oxford Handbook of Cyber Security (OUP 2021) 252.
168 Dias and Coco (n 164) 92.

influence public opinion.[169] Although intentionality is commonly used to differentiate the two sets of operations, it is irrelevant for the purpose of the characterisation of such operations as coercive intervention.[170] A peculiar feature of information operations is that their success depends in large part on individual initiative to act upon the information received and to disseminate it.[171] Such operations have been evidenced in the context of the COVID-19 pandemic, with the World Health Organization expressing its concern that a global 'infodemic' has resulted in 'poor observance of public health measures, thus reducing their effectiveness and endangering countries' ability to stop the pandemic'.[172] In 2020, for example, a cyber operation targeting the Georgian Ministry of Health, Labour and Social Affairs, the National Center for Disease Control and the Richard Lugar Centre for Public Health Research involved the theft of pandemic-related data, a part of which was then published online alongside false information.[173]

169 Dias and Coco (n 164) 94–95; M Gebel, 'Misinformation vs. Disinformation: What to Know about Each Form of False Information, and How to Spot Them Online' (Business Insider, 15 January 2021) < https://www.businessinsider.com/guides/tech/misinformation-vs-disinformation?r=US&IR=T>

170 In contrast, Australia, which takes an approach based on coercive intent, proposes that since misinformation 'has the potential to mislead or deceive but is neither created nor transmitted with the intention of doing so or causing harm', the requirement of coercion is unlikely to be satisfied. Australian Department of Foreign Affairs and Trade, 'Australia's International Cyber and Critical Technology Engagement Strategy' (Position Paper, 2021) 44 <linkhttps://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066 DFAT Cyber Affairs Strategy 2021 update Internals 1 Acc.pdf> accessed 6 January 2023.

171 Commentators speak of the 'cognitive' dimension of these operations and describe them as 'psychological manipulation'. DB Hollis, 'The Influence of War; The War for Influence' (2018) 32 Temple International and Comparative Law Journal 31, 35–36; Lin and Kerr (n 167) 252.

172 WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFCR, 'Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation – Joint Statement' (23 September 2020) <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation> accessed 6 January 2023. See also ENISA, Threat Landscape 2021 (n 149) 109–110.

173 Institute for Development of Freedom of Information, 'Cyberattack on the Ministry of Health and Russian Trace' (IDFI, 3 September 2020) <https://idfi.ge/en/strategy_of_russian_cyber_operations> accessed 6 January 2023. See also E Tucker, 'US Officials: Russia Behind Spread of Virus Disinformation', AP News (28 July 2020) available at <https://

Whether it comes to the dissemination by a state of misinformation or disinformation, the relevant question is whether the cyber operation in question is capable of having coercive effect, that is of depriving the targeted state of control over a matter within its domestic jurisdiction.[174] The difficulty that arises in answering this question is whether any ensuing loss of the control of the state over the articulation or implementation of healthcare choices or policies is sufficiently proximate to the information operation in question so as to be attributed to it. Some commentators have considered, in the context of the COVID-19 pandemic, that the requirement of coercion will be satisfied in the case of a misinformation operation which 'directly causes part of the target state's crisis management plan to fail'.[175] In contrast to the requirement of direct effect suggested by these commentators, New Zealand has taken the view that even 'a prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic' may be coercive.[176] What is required to resolve these different views is the articulation of a suitable standard of causation to 'determine' whether the causal chain or link should be severed at any intermediate point, because beyond that point the wrongdoer could not have foreseen the result of his acts, or the results were too remote and not proximate'.[177] Instead of excessively limiting responsibility using a strict requirement of a 'sufficiently direct and certain causal nexus',[178]

apnews.com/article/virus-outbreak-ap-top-news-health-moscow-ap-fact-check-3acb089e6a333e051dbc4a465cb68ee1> accessed 6 January 2023.

174 Schmitt considers an assessment of the actual scale and effects of such operations as being a necessary part of the analysis. Schmitt, 'Foreign Cyber Interference in Elections' (n 5) 749.

175 Milanovic and Schmitt (n 74) 269. In line with the approach taken in the Tallinn Manual 2.0, Milanovic and Schmitt add that the misinformation operation must also have been 'designed' to lead to such effects.

176 New Zealand Position Paper 2020 (n 89) para 10. See also Italian Government, 'Italian Position Paper on "International Law and Cyberspace"' (Position Paper, September 2021) 5 <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf> accessed 6 January 2023.

177 Lanovoy (n 129) 14.

178 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Merits) [2007] ICJ Rep 2007 43, 234.

which would exclude anything but the most direct effects, or engaging in variable determinations as to causation by reference to the excessively flexible standard of proximity,[179] an objective standard of reasonable foreseeability is best suited to address the effects of information operations.[180] Judged by the standard of reasonable foreseeability, there will likely be many circumstances in which any eventual effects of an information operation on a state's choices or policies as to healthcare, or the implementation of its preferred choices or policies, will be too remote to give rise to the responsibility of the state disseminating the false information. This is at least in part because causing such effects depends on the dissemination by individuals of the false information such that a sufficient number of them act upon it rather than on the guidance of the state. Depending on the circumstances, these individual actions may be more or less foreseeable. Moreover, the agency of individuals who act deliberately and not on the basis of the false information they receive may be constitute an intervening cause that breaks the chain of causation. As one commentator explains,

> *By itself, the dissemination of information does not lead to any adverse consequences. What is required is an individual that receives the information, processes it and turns it into reasons that form the basis of subsequent behaviour (for example, to ingest a toxic substance that allegedly fends off the coronavirus, to decide against wearing a mask or to not get vaccinated.* [181]

Some commentators make the distinct argument that since information operations cause individuals to willingly change their views on a given subject, these operations cannot be characterised as coercive.[182] Others

179 Lanovoy (n 129) 54, 57.
180 For more detailed scrutiny of these standards of causation in the context of the law on the use of force, see Chapter 2 Section II.B.
181 Lahmann, 'Infecting the Mind' (n 95) 421.
182 See e.g. Lin and Kerr (n 167) 253; Hollis, 'The Influence of War; The War for Influence' (n 171) 41.

use similar logic to argue the opposite, that information operations deceive individuals into changing their views and thus satisfy the requirement of coercion.[183] The better view is that the willingness or unwillingness of the individuals concerned is irrelevant to the analysis, since 'coercing' individuals – to use the generic meaning of the term – to change their views would not necessarily imply coercion – for the purpose of non-intervention – of the targeted state.

IV. Conclusion

The relevant resolutions of the General Assembly and the ICJ's decision in *Nicaragua* indicate that the prohibition of intervention under customary international law addresses coercive intervention in the internal or external affairs of a state. Beyond this articulation, neither the requirement of intervention in the internal or external affairs of a state nor the requirement of coercion has been sufficiently elaborated through practice or scholarship. The internal or external affairs of a state, or the domestic jurisdiction of a state, is better defined in the context of the prohibition of intervention as referring to a state's choices and policies rather than the *domaine réservé*, which refers to matters not regulated by international law, for the distinct purpose of allocating jurisdictional competence between the domestic and international levels. The requirement of coercion refers to the loss of the control of the targeted state over matters within its domestic jurisdiction, that is the articulation of the state's choices or policies and their implementation. Even where the state is not ultimately deprived of control over such matters, coercion may be established on the basis of the reasonable foreseeability of such effects.

This articulation of the prohibition of intervention suggests that cyber operations against the healthcare sector may, in some circumstances, constitute violations of the prohibition of intervention. The formulation by a state of a choice or policy as to healthcare, or the implementation

183 Wheatley (n 5) 191–195.

of its preferred choice or policy, whether by a public or a private institution, falls within the domestic jurisdiction of the state and thus within the scope of the prohibition. Certain kinds of cyber operations will satisfy the requirement of coercion. Disruptive cyber operations, like ransomware and 'denial of service' operations, are capable of depriving the targeted state of control over the implementation of health-related choices or policies and may, on this basis, be coercive. Conversely, the compromise, theft or publication of online medical data is not coercive since these operations do not interrupt the provision of healthcare. One exception is a cyber operation which compromises clinical trial data and thereby prevents the approval by a state of a medicine or medical technology intended for use in the implementation of a health-related policy. Information operations are the most difficult to characterise as coercive since any alleged loss of the control of the targeted state over the articulation or implementation of health-related choices or policies will be difficult to attribute to the information operation, in particular owing to intervening causes, not least the conduct of the individuals disseminating the false information.

Given that most cyber operations against the healthcare sector are carried out remotely and do not involve the usurpation of a governmental function, their physical effects … provide the clearest basis on which to characterise such operations as violations of the territorial sovereignty of the targeted state.

Chapter 4

The Application of the Rule Prohibiting Conduct in Violation of a State's Territorial Sovereignty to Cyber Operations against the Healthcare Sector

I. Introduction

This chapter addresses the question whether and, if so, under which conditions a cyber operation against the healthcare sector may be said to breach the rule prohibiting conduct that violates a state's 'sovereignty' or 'territorial sovereignty'.[1] In general terms, 'territorial sovereignty' describes the state's 'plenary competence'[2] or its 'capacity as the entity entitled to exercise control over its territory'.[3] As a consequence of a state's territorial sovereignty, certain conduct carried out by another state within its territory is, in the absence of prior consent, prohibited. Such conduct evidently includes the threat or use of force and coercive intervention in its affairs.[4] Likewise, it is prohibited to make, without prior consent, an aerial, maritime or land-based incursion into the territory of another state. Where, moreover, the conduct involves, in the absence of prior consent, the exercise of enforcement jurisdiction or any other governmental function by one state in the territory of another, it may be presumed to be non-consensual and thereby a violation of the prohibition. In the cyber context, it is conceivable that, like aerial, maritime and land-based incursions, the carrying out of a

1 The report uses the two terms interchangeably unless otherwise specified.
2 J Crawford, Creation of States in International Law (2nd edn, OUP 2007) 89.
3 J Crawford, Brownlie's Principles of Public International Law (8th edn, OUP 2012) 432.
4 The prohibition on the threat or use of force and the prohibition of intervention, both corollaries of the sovereignty of a state over its territory, are addressed separately in Chapters 2 and 3 respectively of this report.

cyber operation by one state through the physical presence of its agent in the territory of another state constitutes a violation of the latter's territorial sovereignty. For example, it may be unlawful for the agent of one state while physically present in another state to insert malware into information and communications technologies (ICTs) in the latter state. In reality, however, most cross-border cyber operations are carried out remotely, avoiding the need for any physical presence in the targeted state. The more relevant question is therefore whether and, if so, on what basis a remote cyber operation against the healthcare sector may be said to violate the sovereignty of a state over its territory.

Section II identifies the rule prohibiting the violation of the sovereignty of a state over its territory. In addition to specifically prohibiting intervention in the affairs of another state and the threat or use of force, addressed elsewhere in this report, the rule generally prohibits non-consensual conduct by a state in the territory of another state. Section III considers the manner of the application of this prohibition to cyber operations. It first finds that cyber operations carried out through the physical presence of the agent of one state in the territory of another is, like an aerial, maritime or land-based incursion, prohibited as a violation of the sovereignty of the targeted state. Secondly, it asks whether remote cyber operations which 'interfere' with the exercise by a state of a governmental function are prohibited even if they do not constitute a prohibited intervention in the affairs of another state. Finally, it examines the proposition that remote cyber operations causing relevant effects in the territory of another state violate its territorial sovereignty. Having scrutinised these various bases for a finding of unlawfulness, Section III considers the question of the lawfulness or not of three kinds of cyber operations facing the healthcare sector, namely disruptive cyber operations, the compromise, theft or publication of data, and disinformation and misinformation operations.

II. The International Legal Rules Corollary to a State's Territorial Sovereignty

What is referred to as 'sovereignty' or 'territorial sovereignty' is shorthand for the exercise by the state's government of 'supreme, and normally exclusive, authority',[5] power[6] or control[7] in its territory.[8] It is, in the words of the *Island of Palmas* arbitral award, 'the exclusive right to display the activities of a State'.[9] Territorial sovereignty implies that 'a sovereign State may exercise in its territory, to the exclusion of other subjects of international law, all the powers of a State, be they legislative, judicial or executive'.[10] Deriving from a state's territorial sovereignty is its 'jurisdiction, prima facie exclusive, over a territory',[11] that is the exercise of the 'competence … to regulate the conduct of natural and juridical persons' within the territory.[12]

The exclusivity of a state's sovereignty over its territory gives rise to a corresponding obligation on other states not to engage in certain forms of conduct in the territory without the consent of the territorial state.[13]

5 R Jennings and A Watts (eds), Oppenheim's International Law vol I (9th edn, 2008) 564. See also M Sørenson (ed), Manual of Public International Law (Palgrave Macmillan 1968) 313; Crawford, Brownlie's Principles of Public International Law (n 3) 89; J Crawford, 'Sovereignty as a Legal Value' in J Crawford and M Koskenniemi (eds) The Cambridge Companion to International Law (CUP 2012) 120.

6 G Schwarzenberger and ED Brown (eds), A Manual of International Law (6th edn, 1976) 76; Oppenheim's International Law I (n 5) 564.

7 Crawford, Brownlie's Principles of Public International Law (n 3) 432; A Clapham (ed), Brierly's Law of Nations: An Introduction to the Role of International Law in International Relations (7th edn, OUP 2012) 139.

8 Crawford, 'Sovereignty as a Legal Value' (n 5) 131.

9 Island of Palmas case (Netherlands/US) [1928] II RIAA 829, 839.

10 A Manual of International Law (n 6) 76. See also Manual of Public International Law (n 5) 316.

11 Crawford, Brownlie's Principles of Public International Law (n 3) 431. In the words of the PCIJ, a state's 'title to exercise jurisdiction rests in its sovereignty'. The Case of the SS Lotus (France v Turkey) (Merits) [1927] PCIJ Rep Series A No. 10 (hereafter 'SS Lotus') 19. See also Crawford, Brownlie's Principles of Public International Law (n 3) 192; Manual of Public International Law (n 5) 314; Brierly's Law of Nations (n 7) 168; S Besson, 'Sovereignty', Max Planck Encyclopedia of Public International Law (2011) para 118.

12 Crawford, Brownlie's Principles of Public International Law (n 3) 440.

13 Oppenheim's International Law I (n 5) 385, 564; Crawford, Brownlie's Principles

Such conduct includes, but is not limited to, intervention in the internal or external affairs of a state, whether through the threat or use of force or otherwise.[14] In the words of the Permanent Court of International Justice (PCIJ) in the *SS Lotus* case, a state

> *may not exercise its power in any form in the territory of another State. In this sense, jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.* [15]

The more recent articulation of the prohibition arising from territorial sovereignty by the International Court of Justice (ICJ) in *Certain Activities Carried Out by Nicaragua in the Border Area and Construction of a Road in Costa Rica Along the San Juan River* addressed, in equally broad terms, the exercise of 'any authority' or the carrying out of 'any activity' in the territory of another state.[16] In accordance with this approach, the Court rejected Nicaragua's claim that Costa Rica, through the construction of a road within its own territory, violated Nicaragua's territorial integrity due to the formation in its territory of deltas of 'sediment eroded from the road'.[17] There was 'no evidence that Costa Rica exercised any authority on Nicaragua's territory or carried out any activity therein'.[18]

The question may be posed as to what conduct is actually addressed by the prohibition on the exercise of the 'power' or 'authority' of one state

of Public International Law (n 3) 432–433; Crawford, 'Sovereignty as a Legal Value' (n 5). In the Corfu Channel case, the ICJ reiterated that '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations. Corfu Channel Case (UK v Albania) (Merits) [1949] ICJ Rep 4 (hereafter 'Corfu Channel') 35.

14 See Chapters 2 and 3 of this report.

15 SS Lotus (n 11) 18–19.

16 Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica) (Merits) [2015] ICJ Rep 665 (hereafter 'Certain Activities') 738.

17 ibid 738.

18 ibid 738.

in the territory of another. In the absence of prior consent, certain forms of conduct may be easily presumed to be unlawful. To begin with, the exercise of a state's jurisdiction to enforce within the territory of another state is, without the latter's consent, prohibited as a violation of its territorial sovereignty.[19] Relevant conduct includes the carrying out of police or other investigations, the execution of arrests, the detention of suspects, the taking of evidence, the conduct of judicial proceedings, the recognition and enforcement of judgments, and the carrying out of sentences.[20] In addition to the exercise of enforcement jurisdiction, the exercise of other governmental functions in the territory of another state may also, in the absence of prior consent, be presumed to violate the sovereignty of the territorial state.[21] The ICJ has declared various forms of conduct to be violations of sovereignty[22] or territorial sovereignty[23] on this basis. In the *Corfu Channel* case, the Court declared the UK's minesweeping 'Operation Retail' in Albanian territorial waters as a violation of Albania's sovereignty.[24] So also, in the *Certain Activities* case, Nicaragua's excavation of caños in Costa Rica's territory was considered to be a violation of Costa Rica's sovereignty.[25] In both these cases, there

19 This is in contrast with the exercise of a state's jurisdiction to prescribe.

20 See Crawford, Brownlie's Principles of Public International Law (n 3) 462–466; Oppenheim's International Law I (n 5) 386; MT Kamminga, 'Extraterritoriality', Max Planck Encyclopedia of Public International Law (2020) para 23; R O'Keefe, International Criminal Law (OUP 2015) 740. Somewhat exceptionally, Jamnejad and Wood consider extraterritorial enforcement jurisdiction to be a violation of the customary prohibition of intervention. M Jamnejad and M Wood, 'The Principle of Non-Intervention' (2009) 22(2) Leiden Journal of International Law 345, 372.

21 SS Lotus (n 11) 19. See also Crawford, Brownlie's Principles of Public International Law (n 3) 461–462; C Staker, 'Jurisdiction' in M Evans (ed) International Law (5th edn, OUP) 290, 311; V Lowe, International Law (OUP 2007) 184.

22 Corfu Channel (n 13) 36; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits) [1986] ICJ Reports 14 (hereafter 'Nicaragua') 147.

23 Certain Activities (n 16) 703.

24 Corfu Channel (n 13) 26.

25 Certain Activities (n 16) 703. Having found that relevant conduct constituted a violation of Costa Rica's sovereignty, the Court did not deem it necessary to additionally address whether the same conduct also constituted a violation of the prohibition on the threat or use of force. ibid 704. For Heller, the Court was of the view that 'merely crossing the border on land' constitutes a violation of territorial sovereignty. KJ Heller, "In Defense of Pure Sovereignty in Cyberspace' (2021) 97 International Law Studies 1432, 1468. In fact,

was a presumption that the exercise of a governmental function by one state in the territory of another constitutes the exercise of power or authority in violation of the latter's territorial sovereignty. This is in part because

> *international law defines 'territory' not by adopting private law analogies of real property but by reference to the extent of governmental power exercised, or capable of being exercised, with respect to some territory and population. Territorial sovereignty is not ownership of but governing power with respect to territory.*[26]

This is not to say that only conduct constituting the exercise of a governmental function in the territory of another state falls foul of the prohibition. Although the carrying out of such a function creates a presumption as to the non-consensual nature of the conduct, the ICJ's jurisprudence indicates that a violation of territorial sovereignty need not always involve the carrying out of a governmental function.[27] In its *Nicaragua* decision, for example, the Court considered the US's laying of mines in Nicaragua's territorial waters and its 'directing or authorizing

the Court was more concerned with the exercise of authority or the carrying out of relevant activities in the territory of another state. See H Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (Chatham House Research Paper, 2019) 16 <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks> accessed 6 January 2023.

26 Crawford, Brownlie's Principles of Public International Law (n 3) 56.

27 Many cases involve land-based, maritime or aerial incursions into the territory of another state. When it comes to land-based incursions, relevant practice pertains to the exercise of enforcement jurisdiction as a violation of the prohibition on the exercise of governmental functions in the territory of another state. In the maritime context, practice has involved the exercise of enforcement jurisdiction on the high seas as well as in states' territorial seas, with only the latter being relevant for present purposes. Since aerial incursions do not typically involve the exercise of a governmental function, states' reactions to aerial incursions make a convincing case that they consider non-consensual incursions to constitute violations of their territorial sovereignty, although states have in such contexts been equally, if not at times exclusively, concerned with compliance with other, more specific rules as to conduct in their airspace. See also T Ruys, 'The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?' (2014) 108 American Journal of International Law 159, 189–191.

[of] overflights of Nicaraguan territory' by US aircraft, 'for purposes of intelligence-gathering and supply to the *contras* in the field' and 'to intimidate the population',[28] as violations of Nicaragua's sovereignty.[29] It declared that '[t]he principle of respect for territorial sovereignty is ... directly infringed by the unauthorized overflight of a State's territory by aircraft belonging to or under the control of the government of another State'.[30] The Court took the same view in respect of maritime incursions, describing the US's mining operations in Nicaragua's ports as unlawful 'incursions into [Nicaragua's] territorial and internal waters'.[31] The Court has taken a similar approach to land-based incursions. In *Certain Activities*, it characterised the establishment by Nicaragua of a military presence in Costa Rica's territory as a violation of Costa Rica's sovereignty.[32] In these cases, it was not, or not only, the exercise of a governmental function in the territory of another state that qualified relevant conduct as unlawful. Rather, it was the fact of an unauthorised incursion by one state into the territory of another that the Court deemed as an unlawful exercise of power or authority in the territory of another state. Like the ICJ, the International Law Commission has also suggested that aerial, maritime and land-based incursions might violate the 'obligation to respect the sovereignty and territorial integrity' of other states.[33] Given that non-consensual aerial, maritime and land-based incursions are prohibited, the execution of 'clandestine operations'

28 Nicaragua (n 22) 22.
29 ibid 147. See also ibid 128.
30 ibid 128. The U-2 incident of 1960, the unauthorised flying of Israeli military aircraft across Lebanese territory in 2003, and the recent incursions by Russia into Estonian airspace are all instances of states alleging violations of their territorial sovereignty through aerial incursions. For an overview of relevant practice, see ILC, '"Force Majeure" and "Fortuitous Event" as Circumstances Precluding Wrongfulness: Survey of State Practice, International Judicial Decisions and Doctrine' (27 June 1977) UN Doc A/CN.4/315, reproduced in (1978) II(Part 2) Yearbook of the ILC 98–104; O Corten, The Law Against War: The Prohibition on the Use of Force in Contemporary International Law (2nd edn, Bloomsbury 2021) 64–76.
31 Nicaragua (n 22) 128.
32 Certain Activities (n 16) 703. Judge ad hoc Dugard additionally considered that 'encouraging members of the Guardabarranco Environmental Movement to trespass on Costa Rican territory' should have constituted a violation of Costa Rica's territorial sovereignty. Certain Activities (n 16) (Separate Opinion of Judge ad hoc Dugard) 843.
33 UN Doc A/CN.4/315 (n 30) 98.

abroad,[34] such as the abduction or assassination of individuals by the agents of one state within the territory of another, would also arguably constitute a violation of the sovereignty of the territorial state if carried out without its prior consent.[35] In the end:

> *Whether one chooses to call it sovereignty, or territorial sovereignty, or territorial integrity, or something else entirely … there is a primary rule of international law that requires one state to refrain from taking a public act or exercising authority in the territory of another state.*[36]

It is less clear whether the exercise of a governmental function that does not involve a physical presence in the territory of another state is likewise prohibited as a consequence of the sovereignty of a state over its territory. Outside the cyber context, the question may be relevant in cases involving, for example, the issue of summons or orders for the production of documents by the authorities of one state in the territory of another. Such conduct being an exercise of a state's jurisdiction to enforce with effects in the territory of another state, summons or orders from one state received in the territory of another could be considered as the unlawful exercise of enforcement jurisdiction.

34 Oppenheim's International Law I (n 5) 386.
35 Kamminga (n 20) paras 23, 26; Corten (n 30) 66.
36 P Spector, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017) 111 AJIL Unbound 219, 222.

III. The Application of the Rule Prohibiting Conduct in Violation of a State's Territorial Sovereignty to Cyber Operations against the Healthcare Sector

A. The Application of the Rule to Cyber Operations Generally

1. Cyber Operations involving a Physical Presence in the Targeted State

An analogy with aerial, maritime and land-based incursions into the territory of another state supports the conclusion that a cyber operation may, if carried out without prior consent in the territory of another state, violate its territorial sovereignty.[37] In the words of one commentary, 'a violation of sovereignty occurs whenever one State physically crosses into the territory or national airspace of another State without either its consent or another justification in international law'.[38] This implies that 'physically manipulating hardware' within the territory of another state – for example, the manual insertion of malware into critical infrastructure through the use of a USB device – would be unlawful in the same way as the laying of mines in another state's territorial waters.[39] This includes the exercise of enforcement jurisdiction or another governmental function through the use of a cyber operation, which will constitute a violation of the sovereignty of the state in which the operation is being carried out.

37 F Delerue, Cyber Operations and International Law (CUP 2020) 213–214; L Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0' (2019) 20 Melbourne Journal of International Law 349, 369–370; P Roguski, 'Violations of Territorial Sovereignty in Cyberspace—an Intrusion-Based Approach', in D Broeders and B van den Berg (eds), Governing Cyberspace: Behavior, Power, and Diplomacy (Rowman and Littlefield 2020), 65, 74; Heller (n 25) 1470; H Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' (2021) 32 Duke Journal of Comparative and International Law 61, 98.

38 MN Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) 19.

39 ibid 19; T Dias and A Coco, 'Cyber Due Diligence in International Law' (Oxford Institute for Ethics, Law and Armed Conflict (ELAC) Report, 2021) 66 <https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf> accessed 6 January 2023.

In reality, however, cyber operations are used precisely because their execution does not require a physical presence in the territory of the targeted state. In some cases, such as data breaches, cyber operations involve the penetration through cyber means of ICTs in another state's territory. In others, like 'denial of service' operations, websites or other ICTs operating in one state cease to function simply because they are flooded with remote requests. The limited applicability in these cases of the prohibition on non-consensual incursions into the territory of another state has led to the suggestion, discussed below, that even remote cyber operations involving no physical presence in the territory of another state may violate a state's territorial sovereignty.

2. Remote Cyber Operations

Several justifications have been offered to support the view that cyber operations carried out remotely, rather than through a physical presence in or incursion into the territory of the targeted state, may constitute violations of its territorial sovereignty. The first is that remote cyber operations which 'usurp' or 'interfere' with the exercise by the territorial state of governmental functions within its territory are prohibited as a violation of the state's territorial sovereignty. A second justification is that remote cyber operations causing relevant effects in another state's territory – whatever those effects may be – will violate its territorial sovereignty. Each is addressed in turn below.

i. The 'Usurpation' of or 'Interference' with the Exercise of Governmental Functions in the Territory of Another State

Some states and scholars assert that remote cyber operations which 'usurp' or 'interfere' with the exercise of the governmental functions of a state violate its territorial sovereignty.[40] Usurpation of a governmental

40 See 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13

function has been taken in the existing commentary to address, in the main, 'the exercise of law enforcement functions within another State's borders in the absence of either an allocation of authority under international law or consent'.[41] As with the issue of summons or orders for the production of documents by the authorities of one state in the territory of another, the exercise of enforcement jurisdiction remotely through the use of cyber operations may likewise be prohibited by territorial sovereignty. For example, it is surely prohibited to use a remote cyber operation to carry out a 'law enforcement operation against a botnet in order to obtain evidence for criminal prosecution by taking over its command and control servers located in another state'.[42] If the exercise of enforcement jurisdiction or another governmental function through the physical presence of the agent of one state in the territory of another is prohibited, remote cyber operations used to achieve the same effect will also be prohibited.

When it comes to interference with the exercise of governmental functions, some argue that 'a cyber operation that interferes with data or services that are necessary for the exercise of inherently governmental functions is prohibited as a violation of sovereignty'.[43] This has been said to include the interference with 'online services that are necessary for the delivery of social services', such as healthcare.[44] Other areas include 'law enforcement, administration of elections, tax collection, national

July 2021) UN Doc A/76/136 (hereafter 'UN GGE Contributions Compendium'), 57 (Netherlands), 68 (Norway), 87 (Switzerland); see also Government of Canada, 'International Law Applicable in Cyberspace' (Position Statement, 2022) (hereafter 'Canada Position Paper') paras 13, 18 <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng> accessed 6 January 2023. See also Tallinn Manual 2.0 (n 38), 21–24; M Milanovic and MN Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations During a Pandemic' (2020) 11 Journal of National Security Law and Policy 247, 255; R Buchan, Cyber Espionage and International Law (Bloomsbury 2019) 51.

41 Tallinn Manual 2.0 (n 38) 22.

42 ibid 22.

43 ibid 22. Elsewhere, the Tallinn Manual 2.0 refers to cyber operations which 'prevent or disregard another State's exercise of its sovereign prerogatives'. ibid 17.

44 ibid 23.

defence and the conduct of international relations'.[45] As a matter of existing law, 'interference' of this kind may be prohibited as a violation of territorial sovereignty if it constitutes a prohibited intervention in the affairs of another state. That is, where relevant requirements for prohibited intervention are met, remote cyber operations interfering with the exercise by a state of governmental functions will constitute a violation of the prohibition of intervention and thereby also a violation of territorial sovereignty.[46] Conversely, where the relevant requirements for prohibited intervention are not met, territorial sovereignty does not otherwise prohibit 'interference' with the exercise by the territorial state of a governmental function unless the conduct causes prohibited effects in the territory of that state. Such effects are discussed below.

ii. The Causing of Effects in the Territory of Another State

In addition to the usurpation of governmental functions in the territory of another state, the characterisation of remote cyber operations as violations of territorial sovereignty may be based on the causing of relevant effects within the territory of the targeted state.[47] Several

45 Canada Position Paper (n 40) para 18. See also Tallinn Manual 2.0 (n 38) 22.

46 The Tallinn Manual 2.0 considers that such conduct might 'in some cases' also constitute a violation of the prohibition of intervention. Tallinn Manual 2.0 (n 38) 22. See also B Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', in K Ziolkowski (ed), Peacetime Regime for State Activities in Cyberspace (NATO CCDCOE, 2013) 203. On the applicability to cyber operations against the healthcare sector of the prohibition of intervention, see Chapter 3 of this report.

47 Tallinn Manual 2.0 (n 38) 20; Milanovic and Schmitt (n 40) 253; P Wrange, 'Intervention in National and Private Cyberspace and International Law', in J Ebbesson, M Jacobsson, MA Klamberg, D Langlet and P Wrange (eds), International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi (Brill 2014) 307, 314–315. Delerue (n 37) 227 (describing 'distributed denial of service' operations as remote cyber operations with effects within the territory of the targeted state). Others oppose this approach. Watts and Richard cite the US Department of Defense memorandum of 2017 as declaring that 'there is insufficient evidence of state practice or opinio juris to support the assertion that sovereignty acts as a binding legal norm, proscribing cyber actions by one State that results in effects occurring on the infrastructure located in another State, or that are manifest in another State'. J O'Connor, General Counsel of the US Department of Defense, 'International Law Framework for Employing Cyber Capabilities in Military Operations' (Memorandum, 19 January 2017); cf S Watts and T Richard, 'Baseline Territorial Sovereignty and Cyberspace' (2018) 22 Lewis and Clark Law Review 771, 829.

states consider that remote cyber operations carried out in one state and having effects in another state may constitute violations of the latter's territorial sovereignty, as expressed in their statements in the UN 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (GGE) and the UN 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (OEWG).[48] Yet not all of these states distinguish between the relevance, in their respective views, of the effects of cyber operations taking place through the presence of the agent of one state in the territory of another state, on the one hand, and the effects of cyber operations carried out remotely, on the other.[49] It cannot be ruled out that

48 Canada Position Paper (n 40) paras 15–16 ('significant harmful effects' above 'de minimis effects', including 'loss of functionality' but excluding 'remote activities … carried out on or through the cyber infrastructure'); Finnish Ministry of Foreign Affairs, 'International Law and Cyberspace – Finland's National Positions' (Position Paper, October 2020) 2 ('producing effects' of 'material harm', 'loss of functionality' and 'modif[ying] or delet[ing] information') < https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859> accessed 6 January 2023; France, 'International Law Applied to Operations in Cyberspace - Paper shared by France with the Open-ended Working Group established by Resolution 75/240' (OEWG Submission, 2021) (hereafter 'France OEWG Position Paper') 3 ('any effects') < https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf > accessed 6 January 2023; Italian Government, 'Italian Position Paper on "International Law and Cyberspace"' (Position Paper, September 2021) 4 ('harmful effects') < https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf > accessed 6 January 2023; Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (Position Paper, 2021) (hereafter 'Japan Position Paper 2021') 2–3 ('physical damage or loss of functionality') < https://www.mofa.go.jp/files/100200935.pdf > accessed 6 January 2023; New Zealand Ministry of Foreign Affairs and Trade 'The Application of International Law to State Activity in Cyberspace' (Position Paper, December 2020) para 14 ('significant harmful effects' but not 'every unauthorised intrusion') <https://dpmc.govt.nz/sites/default/files/2020-12/The Application of International Law to State Activity in Cyberspace.pdf> accessed 6 January 2023; UN GGE Contributions Compendium (n 40) 18 (Brazil) (referring to 'extraterritorial effects'), 33 (Germany) (non-negligible 'physical damage to cyber infrastructure components per se and physical effects of such damage on persons or other infrastructure' as well as 'functional impairments with regard to cyber infrastructures'), 67 (Norway) ('physical damage'), 87 (Switzerland) ('material damage').

49 Exceptionally, Canada, noting the distinction between the two approaches, suggests that 'cyber activities with effects in another State do not constitute physical

one or more of these states considers the effects of cyber operations to be relevant in simply establishing the fact of unlawful, non-consensual conduct within the territory of the targeted state.

Were remote cyber operations to be prohibited on the basis of their effects on the targeted state, the lack of agreement as to what kinds of effects will qualify a cyber operation as a violation of territorial sovereignty leaves the scope of the prohibition unclear. The most expansive view, proposed by France, is that 'any effects produced on French territory by digital means' will constitute a violation of its sovereignty.[50] A slightly different view is that 'any remote penetration of a computer system, even penetration that does not cause any harm, violates the territorial sovereignty of the State in which the computer system is located'.[51] A handful of states have suggested as much, putting remote cyber intrusions on par with aerial, maritime or land-based intrusions.[52] Others, like Brazil, go even further in considering

presence in the territory of that State' and, '[a]s such, [that] territorial sovereignty is not violated by virtue merely of remote activities having been carried out on or through the cyber infrastructure located within the territory of another State'. Canada Position Paper (n 40) para 15. Such operations must cause 'loss of functionality' with 'significant harmful effects' rather than 'de minimis effects' to constitute a violation of territorial sovereignty. ibid 16–17.

50 France OEWG Position Paper (n 48) 3.

51 Heller (n 25) 1468. See also Roguski (n 37) 74, 79; Delerue (n 37) 222; Buchan (n 40) 51; WH von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 International Law Studies 123, 129; Wrange (n 47) 322. Similarly, one group of commentators recognises the existence of 'national sovereignty over cyber infrastructure, entities, behaviour as well as relevant data and information on [state] territory'. Chinese Academy of Social Sciences et al, 'Sovereignty in Cyberspace: Theory and Practice (Version 2.0)' (World Internet Conference, 2020) 3–4 <https://www.wuzhenwic.org/download/SovereigntyinCyberspaceTheoryandPractice(Version2.0).pdf> accessed 6 January 2023. On this basis, prohibited conduct includes, in their view, the 'unauthorized penetration into the network systems in the territory or within the jurisdiction of another country'. ibid 4.

52 Iran Armed Forces Cyberspace Center, 'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace' (Nournews, 18 August 2020) ('unlawful intrusion') <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat> accessed 6 January 2023; US Department of Defense Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (1999) 71 International Law Studies 460, 485 ('unauthorized electronic intrusion into another nation's computer systems' a violation of 'territorial sovereignty'); UN GGE Contributions Compendium (n 40) 87 (Switzerland) ('unauthorised intrusion').

'any cyber operations against information systems located in another State's territory', as well as the 'interception of telecommunications', as prohibited by territorial sovereignty.[53] The general rationale for these propositions is that 'penetrating a computer system in another State is a form of exercising power on that State's territory'.[54] Whether due to the causing of 'any effects' in or the fact of a cyber 'incursion' into ICTs in the territory of another state, the practical implication of declaring remote cyber operations unlawful on these bases is that 'the sovereignty of states would technically be in a constant state of violation', thereby 'increas[ing] the risk of confrontation and escalation'.[55]

Other states set the bar for prohibited cyber intrusions somewhat higher. The US Department of Defense argues, for instance, that 'there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory'.[56] More specifically, 'international law ... does not prohibit espionage *per se* even when it involves some degree of physical or virtual intrusion into foreign territory'.[57] States in this group suggest that it is only the causing of physical damage and perhaps also the loss of functionality of ICTs which would qualify a cyber operation as a violation of territorial sovereignty.[58] Where a remote cyber operation causes knock-on effects of death, injury or destruction, the conduct may additionally qualify as a use of force and, based on the assessment

53 UN GGE Contributions Compendium (n 40) 18 (Brazil).
54 Heller (n 25) 1465. See also Roguski (n 37) 75. For Roguski, certain forms of 'computer intrusion or interference' constitute 'an exercise of state power and thus a violation of the territorial sovereignty of the targeted state'. ibid 79.
55 Moynihan (n 25) 20. See further Tallinn Manual 2.0 (n 38) 69–71.
56 PC Ney Jr, Former General Counsel of the Department of Defense, 'DOD General Counsel Remarks at US Cyber Command Legal Conference', (U.S. Cyber Command Legal Conference, 2 March 2020) <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/> accessed 6 January 2023.
57 ibid.
58 See Tallinn Manual 2.0 (n 38) 20–21; von Heinegg (n 51) 128–129. In support of a de minimis requirement as to effects, see Chircop (n 37) 362.

of gravity, as an armed attack.[59] Conversely, cases involving the loss of functionality alone, and those causing effects other than physical damage or the loss of functionality, are more difficult to characterise as violations of territorial sovereignty. Canada proposes that causing the loss of functionality of ICTs in a state will qualify a cyber operation as a violation of territorial sovereignty if the cyber operation 'causes significant harmful effects similar to those caused by physical damage to persons or property'.[60] This is likely to include cases in which a cyber operation 'necessitat[es] repair or replacement of physical components of cyber infrastructure' even without causing physical damage to ICTs.[61] It is less clear, according to the proponents of this view, whether a range of other effects, such as the securing of unauthorised access to ICTs, precipitating the reinstallation or reboot of ICTs, causing ICTs to 'operate differently … altering or deleting data stored in cyber infrastructure … and causing a temporary … loss of functionality', would qualify such an operation as a violation of territorial sovereignty.[62] At least some of these cases might be characterised as the loss of functionality on the ground that the targeted ICTs stop functioning as they should.[63]

In the specific context of healthcare, it is the causing of physical damage, in particular harm to individuals, that is of greatest concern. The causing of physical damage is the least contentious basis, in accordance with both the approaches discussed above, for determining that there has been a violation of a state's territorial sovereignty. The

59 See Chapter 2 for a detailed analysis of the conditions under which a cyber operation against the healthcare sector might qualify as a use of force and an armed attack respectively.

60 Canada Position Paper (n 40) para 16.

61 Tallinn Manual 2.0 (n 38) 21. See also Canada Position Paper (n 40) para 16. As Dias and Coco elaborate, it is not necessary that the cyber operation target hardware through a physical presence in the territory of the targeted state; a cyber operation targeting software or firmware on which the operation of hardware depends can also cause damage to hardware. Dias and Coco (n 39) 67–69.

62 Tallinn Manual 2.0 (n 38) 21.

63 A Coco, T Dias and T van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) European Journal of International Law (forthcoming, advance copy available at <https://doi.org/10.1093/ejil/chac063>), 5–6.

following assessment thus focuses on the causing of physical damage as the basis for characterising cyber operations against healthcare as violations of a state's territorial sovereignty. Conversely, it does not address whether other effects on the ICTs themselves, such as the loss of their functionality or an unauthorised intrusion into ICTs, which are more contentious and are in any event not specific to healthcare, qualify as a violation of territorial sovereignty in the absence of physical damage.

If, at a minimum, the causing of physical damage in the territory of another state qualifies a remote cyber operation as a violation of territorial sovereignty, the question of the remoteness of such effects must be addressed. In other words, when might any ensuing physical damage be, in causal terms, too indirect or remote or not sufficiently proximate as to qualify a remote cyber operation as a breach of the targeted state's territorial sovereignty? The question is especially relevant in the case of a remote cyber operation which does not physically damage the targeted ICTs – hardware, software and data – but leads in turn to physical damage. In particular, remote cyber operations which cause the targeted ICTs to cease to function often cause physical damage as a result of the unavailability of the ICTs in the provision of public services like healthcare. In such cases, states like Germany and others propose that '[i]f functional impairments result in substantive secondary or indirect physical effects in the territory of the target State (and a sufficient causal link to the cyber operation can be established), a violation of territorial sovereignty will appear highly probable'.[64] A suitable standard of causation is thus needed to assess the relevance of physical effects beyond physical damage to the targeted ICTs. Some commentators assert that the 'requisite consequences for breach may be caused directly or *indirectly*'.[65] This seems to suggest a loose standard of proximity of effects which deems many 'indirect' effects as relevant. Such a standard leaves a wide margin of discretion when determining

64 UN GGE Contributions Compendium (n 40) 33 (Germany). See also ibid 67 (Norway); Canada Position Paper (n 40) para 16.

65 Milanovic and Schmitt (n 40) 254. Milanovic and Schmitt speak of 'the intensity of the causal connection between the cyber operation and some concrete harm'. ibid 255.

the relevance or not of various effects. Alternatively, were the standard of reasonable foreseeability of effects – proposed elsewhere in this report[66] – to apply, many of the knock-on effects of cyber operations would likewise be relevant to the characterisation of such operations as violations of territorial sovereignty. That said, reasonable foreseeability is not the same as strict liability—it is not so strict as to include all possible effects and every possible eventuality. As will be seen below, whether on the basis of the proximity of effects or the reasonable foreseeability of effects, remote cyber operations against the healthcare sector could be considered as unlawful on the basis that they cause physical damage. In contrast, the stricter 'but for' test or the *conditio sine qua non* standard of causation would not consider the indirect effects of such operations to be relevant to the analysis, precluding the characterisation of such operations as unlawful. Whichever of the three standards of causation is preferred, the 'direct' effect of causing physical damage to the targeted ICTs will likely qualify remote cyber operations as violations of the rule prohibiting violations of territorial integrity. The question of causation in respect of the physical damage caused by remote cyber operations targeting the healthcare sector is discussed in greater detail below.

B. The Application of the Rule to Cyber Operations against the Healthcare Sector

The analogy with land-based, maritime or aerial incursions suggests that cyber operations against the healthcare sector which involve a non-consensual physical presence in the territory of another state may violate the latter's territorial sovereignty. In reality, however, the range of cross-border cyber operations facing the healthcare sector tend to be conducted remotely. As the provision of healthcare becomes more dependent on the internet, so too does its vulnerability to remote cyber

66 On the use of reasonable foreseeability in the context of cyber operations, see Chapter 2 Section II.B.2.iii. On the use of a standard of reasonable foreseeability in international law, see generally V Lanovoy, 'Causation in the Law of State Responsibility' (2023) British Yearbook of International Law (forthcoming, advance copy available at <https://doi.org/10.1093/bybil/brab008>).

operations. Hospitals and other healthcare providers increasingly use a wide range of internet-connected medical devices and technologies which increase the exposure of the sector to remote cyber operations.[67] These remote operations may be more effectively addressed on the basis of their effects in the territory of another state. On one view, all remote cyber operations targeting healthcare constitute unlawful 'incursions' into a state's critical infrastructure irrespective of their effects. On another view, to use Japan's articulation, '[a]n act of causing physical damage or loss of functionality by means of cyber operations against critical infrastructure, including medical institutions, ... may constitute a violation of sovereignty'.[68] Although different approaches have been proposed to the assessment of effects, it is at least agreed that causing physical damage will qualify a cyber operation as a violation of territorial sovereignty. In the context of healthcare, this generally refers to harm to individuals, but may also include other forms of physical damage, such as rendering medical supplies unusable. Irrespective of which approach is preferred, there are thus certain contexts in which remote cyber operations against healthcare will be clearly unlawful. The following analysis seeks to identify these contexts by considering three categories of cyber operations, namely disruptive cyber operations which encrypt ICTs, the compromise, theft and publication of online data (or 'data breaches'), and disinformation and misinformation operations. Although these various cyber operations may also be prohibited on the basis that they amount to the usurpation of governmental functions by the territorial state, this has not been the case in reality in the context of healthcare and is not therefore addressed.

1. Disruptive Cyber Operations

67 Czech Republic, CyberPeace Institute, Microsoft, 'Compendium of Multistakeholder Perspectives: Protecting the Healthcare Sector from Cyber Harm' (Report, 2022) 9 <https://www.mzv.cz/un.newyork/en/news_events/the_ministry_of_foreign_affairs_together.html> accessed 6 January 2023.

68 Japan Position Paper 2021 (n 48) 2–3. On the targeting of critical infrastructure, see Chapter 2 Section II.A.1.iii.

Disruptive cyber operations like ransomware operations (or 'ransomware attacks') and 'denial of service' operations (or 'DoS attacks') are ubiquitous in the healthcare sector. To the extent that causing physical damage in the territory of a state constitutes a violation of its territorial sovereignty, disruptive cyber operations that physically damage medical devices, IT systems or other parts of the critical infrastructure on which the provision of healthcare depends could qualify as unlawful.[69] In most cases, however, disruptive cyber operations do not cause physical damage to the targeted ICTs but cause them to cease to function or to function sub-optimally, which in turn affects the provision of healthcare.[70] Where the ICTs targeted are not physically damaged, the loss of their functionality alone – whether through encryption or overload – may be insufficient to constitute such a violation. In such cases, the further physical effects resulting from the loss of functionality, namely the disruption to the continued provision of medical services to patients, which may be delayed, suspended or delegated to other healthcare providers, may qualify such an operation as unlawful. As two commentators explain, a remote cyber operation that 'renders medical equipment inoperable' and thereby 'interferes with the immediate delivery of medical care' may violate the targeted state's territorial sovereignty.[71] These effects are particularly felt when cyber operations like ransomware disrupt the provision of emergency or acute healthcare services.[72]

69 On cyber operations targeting the IT systems used by the healthcare sector, see e.g. 'New Orangeworm Attack Group Targets the Healthcare Sector in the US, Europe and Asia' (Symantec Enterprise Blogs, 23 April 2018) <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia> accessed 6 January 2023; 'South Africa's Life Healthcare Hit by Cyber Attack', Reuters (9 June 2020) <https://www.reuters.com/article/us-life-healthcare-cyber-idUSKBN23G0MY> accessed 6 January 2023.

70 See e.g. T Brewster, 'Medical Devices Hit by Ransomware for the First Time in US Hospitals', Forbes (17 May 2017) <https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4c89894b425c> accessed 6 January 2023.

71 Milanovic and Schmitt (n 40) 253. Such an operation may also constitute a breach of the prohibition of non-intervention. See Chapter 3.

72 See e.g. R Winton, 'Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating', Los Angeles Times (18 February 2016) <https://www.latimes.com/business/

Where disruptive cyber operations cause the loss of functionality of targeted ICTs and thereby interrupt the provision of healthcare, the causal chain or link between the cyber operation and the physical damage in terms of the provision of healthcare must be established. This is easily done when using the standard of proximity or the standard of reasonable foreseeability of effects, discussed above, in either case leading to the characterisation of such operations as unlawful. Accordingly, a remote ransomware or 'denial of service' operation 'against a website providing information on virus testing', for example, would violate territorial sovereignty if the effects of 'the information's unavailability is an increase in the numbers of infected individuals or exacerbation of the illness's severity due to individuals not having access to timely testing'.[73] Such operations will be unlawful not on the basis of physical damage to the targeted ICTs but because, in such a case, they 'cause individuals to be unable to secure COVID-19 treatment or preventative measures, and illness or aggravation of illness'.[74] Certainly, when considering the standard of the reasonable foreseeability of effects in the context of a pandemic, 'almost any interference with the provision of medical care and public health activities would foreseeably impact the health of individuals'.[75] In contrast, a stricter standard of causation limited to the consideration of the 'direct' effects of a cyber operation – that is, the effects on the targeted ICTs – is likely to preclude the characterisation of such operations as a violation of territorial sovereignty.

As opposed to the provision of healthcare, where remote cyber operations disrupt the functioning of the ICTs on which medical research institutes or pharmaceutical companies depend, establishing the causal chain or link between the cyber operation and any ensuing physical

technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html> accessed 6 January 2023; W Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', Wired (11 November 2020) <https://www.wired.co.uk/article/ransomware-hospital-death-germany> accessed 6 January 2023.

73 Milanovic and Schmitt (n 40) 254.

74 ibid 254.

75 ibid 255.

damage in terms of the provision of healthcare will prove more difficult. Certainly, if using the standard of proximity, establishing the causal chain or link needed will pose challenges. The case for the reasonable foreseeability of such effects may also be difficult to make, given the more tenuous connection with the actual provision of healthcare to individuals and the role of intervening causes, which will tend to limit what is reasonably foreseeable. In the case of the disruption of medical research, for example, it may not even be known whether the research would have successfully led to a cure, making it difficult to attribute any harm to individuals to the targeting, through cyber means, of the research. In other words, the less proximate the effects on individual health, the less likely it is that the standard of reasonable foreseeability is met. Such operations are thus less likely to be unlawful on the basis that they cause physical damage in terms of the provision of healthcare.

2. The Compromise, Theft and Publication of Online Data

In addition to disruptive cyber operations, the healthcare sector is increasingly faced with cyber operations involving the compromise, theft or online publication of sensitive data, such as patient medical history and confidential datasets pertaining to clinical trials. One of the largest such operations took place in 2017–18, when SingHealth, a private healthcare company in Singapore, was subjected to an elaborate phishing operation involving the exfiltration over months of the personal information and, in some cases, medical records, of nearly 1.5 million patients.[76] Other targets of these operations include pharmaceutical companies, research institutes, insurance companies, and even distributors.[77] The targeting, for example, of the COVID-19

76 Singaporean Ministry of Communications and Information Committee of Inquiry, 'Public Report on The Cyber Attack On Singapore Health Services Private Limited's Patient Database on or around 27 June 2018' (Report, 10 January 2019) i <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/public-report-of-the-coi> accessed 6 January 2023.

77 There have several cases involving the large-scale compromise or theft of confidential medical records, including in Finland, Georgia, the UK and the US. See CyberPeace Institute, 'Playing with Lives: Cyberattacks on Healthcare are Attacks on People'

vaccine 'cold supply' chain, which 'ensur[es] the safe preservation of vaccines in temperature-controlled environments during their storage and transportation',[78] compromised 'sensitive information about vaccine distribution plans and processes'.[79]

These data breaches target data or the 'content layer' of ICTs in ways that cause neither physical damage nor the loss of functionality of the hardware and software used to store the data.[80] Although prompting a cybersecurity response, these cyber operations do not generally restrict the continued provision of healthcare. This precludes the characterisation of many such operations as unlawful on the basis of physical damage caused in the territory of the targeted state. The less tangible effects of such operations are the loss of public confidence in the ability of healthcare providers, insurance companies and others to secure their medical records, the confidence of regulators and the public in the outcomes of clinical trials in which confidential data has been compromised, and the loss of the intellectual property associated with the development of medicines and medical technology.[81] When it comes to medical research in particular, '[e]ven minor breaches of confidentiality of data … can undermine public confidence therein, halting regulatory approval of research outputs and their use by the general population'.[82] None of these effects are comparable to physical damage nor even the loss of functionality of ICTs. If the lawfulness of cyber operations is assessed on the basis of their physical effects in the territory of another state, remotely accessing confidential medical data is unlikely to be prohibited as a violation of territorial sovereignty. The

(Report, 2021) 39 <https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf> accessed 6 January 2023.

78 Dias and Coco (n 39) 72–73.

79 ibid.

80 As Roguski explains, access to data would not 'interfere' with the functioning of a computer system in the territory of another state'. Roguski (n 37) 79.

81 Dias and Coco speak of the 'economic, social, political, reputational and physical damage to states, non-state entities, such as corporations, and individuals' resulting from 'harms to or through data'. Dias and Coco (n 39) 75.

82 ibid 80.

logic applies too to the theft of data.[83] This is not to exclude the possible characterisation of such operations as unlawful on the distinct basis that they violate the prohibition of intervention in the affairs of other states.[84]

In exceptional cases involving 'the deletion or alteration of data' where, for example, medical professionals are unable to rely on the accuracy of compromised patient medical records, physical damage to the health of individuals could be said to result from such operations.[85] These effects will satisfy either the standard of proximity or the standard of reasonable foreseeability, discussed above, when patient medical records used for the provision of treatment are compromised. Such operations will qualify more easily as violations of the territorial integrity of the targeted state. In contrast, where the compromised data is not required for the provision of healthcare to individuals, as with clinical trial data or intellectual property associated with the development of medicines or medical technology, the requirement of causation in respect of any ensuing physical damage – whether in terms of proximity or reasonable foreseeability – will be more difficult to establish. Taking the wider view, however, that all remote cyber 'intrusions' into the critical infrastructure used by the healthcare sector are violations of a state's territorial sovereignty would qualify a wider range of data breaches as unlawful on this basis.[86]

83 Milanovic and Schmitt (n 40) 254. On states' views in the cyber context, see Heller (n 25) 1459–1460.

84 See Chapter 3 Section III.B.2.ii.

85 Roguski (n 37) 79. Roguski does not consider it necessary for the deletion or alteration of data to have physical effects in order to constitute a violation of territorial sovereignty. ibid 79. The Tallinn Manual 2.0 also takes a different approach in considering that the deletion or alteration of data constitutes 'interference' with the exercise of governmental functions, such as 'the delivery of social services', which amounts to a violation of territorial sovereignty. Tallinn Manual 2.0 (n 38) 22.

86 For Roguski, a cyber operation which compromises 'the integrity of data' is a violation of territorial sovereignty. Roguski (n 37) 78. While expressly rejecting an effects-based assessment – presumably referring to physical effects – Roguski considers that 'actions taken against specific computers or networks, even if undertaken remotely, ultimately manifest themselves in the territory of the state where the physical infrastructure is located'. ibid 78. This includes, in his view, cases in which 'a foreign state damages, deletes,

3. Disinformation and Misinformation Operations

'Influence',[87] 'information'[88] or 'content-based' operations[89] comprising disinformation[90] and misinformation[91] use social media, email and other messaging services to disseminate false or misleading information to the public. As the COVID-19 pandemic demonstrates, such operations can 'jeopardize' the functioning of core public services' like healthcare:

> *Recent examples include the spread of false information about COVID-19, its treatments and vaccines, which lead to a number of individuals to die or get seriously ill from drinking bleach or alcohol, and others to dismiss the seriousness of the virus or reject government approved vaccines.*[92]

Like data breaches, information operations affect neither the physical integrity nor the functionality of ICTs. Nor do they in and of themselves prevent healthcare providers from continuing to provide their services. To the extent that physical damage – in particular, damage to individuals acting on false information – can be attributed to information operations, they may nevertheless be characterised as breaching a state's territorial

deteriorates, alters, or suppresses data stored on a computer system within the territory of another state'. ibid 79.

87 DB Hollis, 'The Influence of War; The War for Influence' (2018) 32 Temple International and Comparative Law Journal 31–46; H Lin and J Kerr, 'On Cyber-Enabled Information Warfare and Information Operations' in P Cornish (ed), The Oxford Handbook of Cyber Security (OUP 2021) 251, 252.

88 ELAC, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' (2021) <https://elac.web.ox.ac.uk/the-oxford-Statement-on-the-regulation-of-information-operations-and-activities> accessed 6 January 2023.

89 Dias and Coco (n 39) 92.

90 The intentional dissemination of false information with a view to influencing the public.

91 The unintentional dissemination of false information online with a view to influencing the public.

92 Dias and Coco (n 39) 74.

sovereignty. However, the relevance of various effects to the causal assessment is open to question. According to the approach preferred by some commentators, 'any of the cyber operations attributable to a state that have negatively affected the health of any individuals on the state's territory' will constitute violations of territorial sovereignty.[93] This wide view will prohibit, as a consequence of a state's territorial sovereignty, the dissemination of 'a false or misleading piece of information [that] induce[s] citizens of the target state to ingest a supposedly remedial, but in fact harmful, substance that results in severe illness or even death'.[94] Since 'the dissemination of information does not [itself] lead to any adverse consequences', it is still necessary to establish a causal chain or link between the dissemination of the false information and the individual decision to act upon it.[95] Establishing that the harm to an individual was the result of their exposure to false information may be difficult, given that it is the 'individual that receives the information, processes it and turns it into reasons that forms the basis for subsequent behaviour'.[96] That the individual acted at least in part on the basis of the false information may be challenging to establish from an evidentiary perspective. Given the complexity of establishing a causal chain or link, the application of a standard of reasonable foreseeability may be better suited to the context of information operations. Yet the standard of reasonable foreseeability is not so strict as to require the foreseeability of every possible eventuality, particularly when the circumstances involve individual decision-making, warranting caution in the use even of this more permissive standard of causation. Disinformation and misinformation operations, whether attributed to a state or not, may nevertheless trigger other obligations for states, in particular obligations of due diligence[97] and a variety of obligations

93 Milanovic and Schmitt (n 40) 253.
94 H Lahmann, 'Infecting the Mind: Establishing Responsibility for Transboundary Disinformation' (2022) 33(2) European Journal of International Law 411, 415.
95 ibid 421.
96 ibid.
97 Dias and Coco (n 39).

under international human rights law.[98]

IV. Conclusion

International law prohibits states from engaging in certain forms of conduct as a consequence of the sovereignty of a state over its territory. In principle, the prohibition applies equally to cyber operations. An analogy with non-consensual aerial, maritime and land-based incursions by one state into the territory of another suggests that cyber operations carried out through a physical presence of the agent of one state in the territory of another may constitute a violation of the latter's territorial sovereignty. Given, however, that the vast majority of cyber operations are conducted remotely, the question of their lawfulness may be assessed on other bases. First, a cyber operation may be prohibited on the basis that it usurps the exercise of a governmental function by the territorial state even where it is carried out remotely. Secondly, the view is advanced, although not universally accepted, that remote cyber operations with effects in the territory of another state may violate the territorial sovereignty of that state. There is no clear agreement, however, as to which effects are relevant to the assessment. It is open to question whether the loss of functionality of the targeted ICTs or the fact of a cyber 'incursion' alone might qualify a remote cyber operation as a violation of territorial sovereignty. At a minimum, it is agreed that the causing of physical damage in the territory of another state will qualify a remote cyber operation as a violation of the territorial sovereignty of the targeted state.

Given that most cyber operations against the healthcare sector are carried out remotely and do not involve the usurpation of a governmental function, their physical effects – both on the targeted ICTs and on the provision of healthcare – provide the clearest basis on which to characterise such operations as violations of the territorial

98 See Chapter 5.

sovereignty of the targeted state. Although there is as yet no agreement as to the relevance of various effects to the assessment, the causing of physical damage in the territory of another state is widely considered as qualifying a remote cyber operation as a violation of territorial sovereignty. This includes not only physical damage to the targeted ICTs but also, where causally relevant, physical damage to individuals harmed by the interruption of healthcare services. Disruptive cyber operations, like ransomware and 'denial of service' operations, typically target the functionality of ICTs and in turn cause physical damage by disrupting the provision of healthcare services. Subject to the satisfaction of causal requirements, which is in this context easily done, such operations as likely prohibited as violations of territorial sovereignty. The compromise, theft and publication of confidential medical data cause neither physical damage nor the loss of functionality of ICTs. Nor do data breaches interrupt the provision of healthcare, except where compromised data can no longer be relied on in the provision of medical care to individuals. Using a standard of reasonable foreseeability of effects, such exceptional cases may be construed as violations of territorial sovereignty. Finally, disinformation and misinformation do not target ICTs in the same way as disruptive cyber operations and data breaches but, through the dissemination of false information, affect healthcare widely. In many cases, the causal chain or link between such operations and any eventual physical damage – notably, the health of an individual subjected to the false information – is tenuous, even when using the standard of reasonable foreseeability. Setting aside the consideration of the effects of remote cyber operations, were the assessment of their lawfulness to be carried out by reference simply to the fact of an unauthorised 'incursion' into ICTs in the territory of another state, a much wider range of cyber operations, including data breaches, might qualify as violations of territorial sovereignty.

…all three types of cyber operations targeting the healthcare sector covered in this report – disruptive operations, data breaches and information operations – may engage the … rights [to] life, health, privacy and the freedoms of expression and information.

Chapter 5

The Application of International Human Rights Law to Cyber Operations against the Healthcare Sector

I. Introduction

The healthcare sector has been conceived and put in place to tend to the needs of human beings. As such, it implicates states' duties to respect, protect and fulfil several human rights recognised in international law and enshrined in different legal instruments, including core human rights treaties and customary international law. First and foremost, the provision of healthcare through hospitals and other institutions is not only a means to protect the rights to life and physical integrity but also calls into question states' duties to respect those rights whilst individuals undergo medical treatments. Similarly, without appropriate healthcare it would be impossible for states to fulfil their obligations to ensure the right to health. Moreover, in the pursuit of their functions, healthcare institutions routinely collect and store vast amounts of data, of a personal and sensitive nature, bringing into play the right to privacy of those individuals to whom the data pertains. Likewise, access to adequate healthcare and medical treatment is logically dependent on one's ability to obtain the necessary information, and on the right of a number of stakeholders – from healthcare professionals and scientists to journalists and ordinary individuals – to provide information and express their ideas freely.

The digitalisation of health services, in this respect, is creating opportunities and vulnerabilities at the same time, especially when the smooth running of such services is dependent on information and communication technologies (ICTs). Operational downtime for

healthcare structures targeted by malicious cyber operations may run for days, during which the relevant healthcare personnel may be entirely unable to access patient data and may have to revert to pen and paper, assuming this is even possible.[1] Furthermore, the interoperability of healthcare systems across states and the sharing of data to enable cross-border provision of health services[2] have created additional channels for the spread of malware and other vectors of harmful cyber operations. Even mere intrusions into hospital systems and databases can be damaging or at least disruptive to the provision of healthcare, if they result in a lack of trust in the integrity, confidentiality and/or reliability of data like health records.[3] Such intrusions may be particularly damaging to the integrity of data pertaining to medical research of treatments and vaccines.

This chapter analyses the dangers posed to these rights by cyber operations targeting the healthcare sector, and the applicable international legal framework. This framework includes – among other treaties and in addition to customary international human rights law (IHRL) – the International Covenant on Civil and Political Rights (ICCPR),[4] the International Covenant on Economic, Social and Cultural Rights (ICESCR),[5] and regional human rights treaties such

1 As, for instance, happened in the case of the ransomware attack against the Tokushima hospital in Japan: 'Ransomware Attack Forced Tokushima Hospital to Halt Operations for Two Months' The Japan Times (24 January 2022) <https://www.japantimes.co.jp/news/2022/01/24/national/ransomware-attack-hospital-server/> accessed 7 January 2023. More examples are discussed at 'Data to Dissect the Harm of Cyberattacks' (CyberPeace Institute, 18 March 2022) <https://cyberpeaceinstitute.org/news/data-to-dissect-the-harm-of-cyberattacks/> accessed 7 January 2023.

2 As, for instance, promoted within the European Union: see C Botrugno, 'Working on a Right to Health for the Digital Era' in G Ziccardi Capaldo (ed), The Global Community Yearbook of International Law and Jurisprudence 2020 (OUP 2021) 150.

3 E.g. C Cimpanu, 'Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak' (ZDNet, 13 March 2020) <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/> accessed 7 January 2023.

4 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

5 International Covenant on Economic, Social and Cultural Rights (adopted 19 December 1966, entered into force 3 January 1976) 993 UNTS 3.

as the African Charter of Human and People's Rights (ACHPR),[6] the American Convention on Human Rights (ACHR),[7] and the European Convention on Human Rights (ECHR),[8] as interpreted by the relevant treaty bodies and in state practice.

The said legal framework establishes two main types of obligations applicable offline as well as online, including in the healthcare context. On the one hand, states bear 'negative' obligations to *respect* human rights, that is, to refrain from engaging in cyber operations that violate human rights.[9] Identifying a breach of such negative human rights obligations requires the attribution of the relevant conduct to a state, which in turn presupposes tracing the factual origin of the harmful operation.[10] On the other hand, states are bound by 'positive' obligations to adopt all the necessary and feasible measures to *protect* the human rights of persons under their jurisdiction against threats posed or harms caused by their own agents or other entities — including foreign governments, companies, criminals, or other actors.[11] They must also *fulfil* or *ensure*

6 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217.

7 Charter of the Organization of American States (OAS) (adopted on 22 January 1969, entered into force 13 December 1951) 119 UNTS 3.

8 Convention for the Protection of Human Rights and Fundamental Freedoms (adopted on 4 November 1950, entered into force 3 September 1953) ETS No 5.

9 See e.g. ICCPR art 2(1) and UN Human Rights Committee (HRC), 'General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.1 (hereafter 'CCPR General Comment 31') paras 3, 5–6 and 10.

10 E.g. T van Benthem, T Dias and D Hollis, 'Information Operations under International Law' (2022) 55 Vanderbilt Journal of Transnational Law 1217, 1230, 1233–1235; M Milanovic and MN Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations During a Pandemic' (2020) 11 Journal of National Security Law and Policy 247, 251–252, 262. For an example of attribution, see e.g. The White House, 'FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government' (15 April 2021) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/> accessed 7 January 2023.

11 See e.g. ICCPR art 2(1) and CCPR General Comment 31 (n 9) paras 6, 8; Bărbulescu v Romania (App no. 61496/08) (European Court of Human Rights (ECtHR), 12 January 2016) para 110, with respect to the right to privacy. In this sense, see also Milanovic and Schmitt (n 10), 270ff.

those rights, that is create the conditions for their full enjoyment.[12] Such positive obligations do not require states to successfully preclude all human rights violations by third parties. Rather, states must discharge them by exercising due diligence, that is, by exercising their best efforts to prevent, stop or redress those violations, insofar as they know or should have known of such acts and are capable of taking the necessary steps in the circumstances.[13]

States' positive human rights obligations containing a due diligence standard must not be confused with the related concept of corporate 'human rights due diligence', that is, the non-binding responsibility of businesses to mitigate the human rights impact of their activities.[14] These responsibilities are not within the scope of this study, which focuses solely on states' human rights obligations. Although the scope of states' positive human rights obligations in the cyber context has been extensively discussed elsewhere,[15] this chapter will focus on the extent to which both negative and positive obligations apply when cyber operations target or affect the healthcare sector.

As noted in previous chapters, such cyber operations may take three main forms: a) disruptive operations, which hamper or restrict healthcare

12 See CCPR General Comment 31 (n 9) paras 3 and 8. See also Committee on Economic, Social and Cultural Rights (CESCR), 'General Comment No. 3: The Nature of States Parties' Obligations (Art. 2, Para. 1, of the Covenant)' (14 December 1990) UN Doc E/1991/23 para 1; Velasquez Rodriguez v Honduras (Inter-American Court of Human Rights (IACHR) Series C No. 4) (29 July 1988) paras 166–167.

13 CCPR General Comment 31 (n 9) para 8; S Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!' (2020) 9(1) ESIL Reflections 2, 4-5; Milanovic and Schmitt (n 10) 270, 279–282.

14 On this principle, see J Bonnitcha and R McCorquodale, 'The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights' (2017) 28(3) European Journal of International Law 899; JG Ruggie and JF Sherman, 'The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights: A Reply to Jonathan Bonnitcha and Robert McCorquodale' (2017) 28(3) European Journal of International Law 921.

15 T Dias and A Coco, 'Cyber Due Diligence in International Law' (Oxford Institute for Ethics, Law and Armed Conflict (ELAC) Report, 2021) <https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf> accessed 7 January 2023.

providers' ability to deliver vital services, such as ransomware operations (or 'ransomware attacks') and 'denial of service' operations (or 'DoS attacks'); b) data breaches, which involve the compromise, theft and publication of sensitive data, such as patient records, clinical trial data, or the intellectual property associated with vaccine research; and c) and information operations, including disinformation and misinformation, and comprising the exfiltration, manipulation and dissemination of false or misleading health information to the public.[16] In this light, this chapter focusses on the human rights most relevant to such operations, namely the rights to a) life; b) health; c) privacy; and d) freedom of expression and information.

Before delving into how different human rights might be implicated by such operations, it is important to highlight three general challenges facing the application of IHRL in cyberspace. First, while there is no question that human rights apply online, the scope of states' obligations to respect, protect and fulfil those rights remotely, that is, in the absence of physical control of a territory, space or individual, remains contested. This relates to the broader question of extraterritorial application of human rights obligations, to which we turn in the next section. Secondly, for both negative and positive human rights obligations, the wrongful action or omission must be attributed to a state. Yet, attribution of cyber operations to states is notoriously difficult.[17] On the one hand, despite advances in cyber forensics, it is often impossible to trace with confidence the factual origin of certain operations, given the Internet's decentralized nature, user anonymity and the use of spoofing techniques.[18] On the

16 See Chapter 1 Section II and CyberPeace Institute, 'Playing with Lives: Cyberattacks on Healthcare are Attacks on People' (Report, 2021) 51 <https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf> accessed 7 January 2023.

17 R Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 Journal of Conflict and Security Law 429, 432.

18 See JA Shamsi, S Zeadally, F Sheikh and A Flowers, 'Attribution in cyberspace: techniques and legal implications', (2016) 9 Security and Communications Networks (2016) 2886, 2886–2887; F Skopik and T Pahi, 'Under False Flag: Using Technical Artifacts for Cyber Attack Attribution' (2020) 8 Cybersecurity 1, 6–7, 14; PA Yannakogeorgos, 'Strategies for Resolving the Cyber Attribution Challenge' (Air Force Research Institute Perspectives on Cyber Power, December 2013) 9, 13–16 <https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_

other hand, the legal standards for attributing the conduct of private groups or individuals to states are exacting.[19] Though we acknowledge these practical difficulties, for the sake of simplicity, we assume that the cyber operations discussed below are either attributable to a state (in the case of negative duties), or that official state organs failed to prevent, stop, or redress them (in the case positive obligations). Thirdly, acquiring actual or constructive knowledge of harmful cyber operations, as is necessary to trigger positive human rights obligations, is often difficult in practice, given the speed and secrecy with which such operations unfold. At the same time, the active pursuit of such knowledge may have implications for other human rights, most notably, the right to privacy.

II. The Extent of States' Jurisdiction for the Purposes of Human Rights Obligations

Under certain human rights treaties – for instance the ICCPR, the ACHR and the ECHR[20] – a state only bears negative and positive obligations with respect to activities that fall under its jurisdiction.[21] The extent of a state's jurisdiction in IHRL undoubtedly covers persons, objects or events in its territory – for instance, operations affecting information technology (IT) infrastructure, those occurring in the physical premises of tech companies or perpetrated by individuals located in a state's own territory.

In addition, where certain conditions are fulfilled, a state's jurisdiction extends over certain physical spaces, persons or events located or occurring outside of a state's borders, that is, extraterritorially. Rules of international law determining the extent of extraterritorial jurisdiction are particularly important with respect to ICTs, given their multi-layered and

CHALLENGE.PDF> accessed 7 January 2023.

19 See T Mikanagi and K Mačák, 'Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case' (2020) 9 Cambridge International Law Journal 51, 60–64.

20 See e.g. ICCPR art 2(1); ECHR art 1; ACHR art 1(1).

21 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174 (hereafter 'UN GGE Report 2015') para 28(b).

transnational nature, comprising cross-border physical infrastructure or hardware, logical systems or software, data and human activity.[22]

A first, relatively uncontroversial rule posits that individuals over which the state exercises some form of physical control or authority fall within that state's extraterritorial jurisdiction.[23] This so-called 'personal' model of extraterritorial jurisdiction applies to both negative and positive human rights obligations, according to numerous human rights bodies[24] and commentators.[25]

Secondly, several human rights treaty bodies have affirmed that a state's extraterritorial jurisdiction extends to the reasonably foreseeable human rights impact of the activities of entities, such as companies that are incorporated in or located on its territory, or are otherwise subject to such state's effective control[26] — albeit this view is not uncontroversial.[27] The idea is that, if a state enjoys regulatory control over entities that

22 C Sullivan, 'The 2014 Sony Hack and the Role of International Law' (2017) 8 Journal of National Security Law and Policy 438, 454, footnote 88.

23 CCPR General Comment 31 (n 9) para 10.

24 See e.g. Coard et al (United States), IACommHR Report N. 109/99 (29 September 1999) para 37; Al-Skeini and others v United Kingdom (App no 55721/07) (ECtHR, 7 July 2011) paras 136–139.

25 M Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (OUP 2011) 119. But the ECtHR has been reluctant to recognize this model in relation to extraterritorial kinetic force in the absence of governmental control (see Banković and others v Belgium and others (Appl. no 52207/99) (ECtHR, 12 December 2001) paras 74–82; and Al-Skeini (n 24) paras 136–137). For a recent analysis, see M Milanovic, 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life' (2020) Human Rights Law Review 1, 23–24.

26 HRC, 'General Comment No. 36 Article 6: Right to Life' (3 September 2019) UN Doc CCPR/C/GC/36 (hereafter 'CCPR General Comment 36') para 22, CESCR, 'General Comment No. 14: The Right to the Highest Attainable Standard of Health' (11 August 2000) UN Doc E/C.12/2000/4 (hereafter 'CESCR General Comment 14') para 39; CESCR, 'General Comment No. 15: The Right to Water (Arts. 11 and 12 of the Covenant)' (20 January 2003) UN Doc E/C.12/2002/para 33; CESCR, 'Statement on the Obligations of States Parties regarding the Corporate Sector and Economic Social and Cultural Rights' (20 May 2011) UN Doc E/C.12/2011/1 para 5; The Environment and Human Rights, Advisory Opinion OC-23/17, (IACHR Series A No 23) (15 November 2017) paras 101–102; African Commission on Human and Peoples' Rights (ACommHPR), 'General Comment no. 3 on the African Charter of Human and Peoples' Rights: The Right to Life (Article 4)' (November 2015) (hereafter 'ACommHPR General Comment 3') para 14. See also Milanovic and Schmitt (n 10) 281–282.

27 See Besson (n 13).

control the relevant infrastructure or data, jurisdiction extends to such entities and their activities.[28]

Thirdly, a state may be said to have extraterritorial jurisdiction over a certain person or activity if it exercises functional control over the victim's enjoyment of a certain human right, even if such control is exercised remotely, that is, in a non-physical manner.[29] Thus, this model is particularly well-suited for online activities. A prime example would be the use of electronic surveillance equipment or spyware software to access an individual's personal data. Whilst still controversial, the so-called 'functional' model of extraterritorial jurisdiction has been endorsed by several academics[30] and the UN Human Rights Committee[31] and the courts of at least one state,[32] receiving stronger support in its application to negative human rights obligations when compared with positive human rights obligations.[33]

28 HRC, 'The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014') UN Doc A/HRC/27/37 (hereafter 'Right to Privacy in the Digital Age') paras 31-36.

29 CCPR General Comment 36 (n 26) paras 21, 63.

30 E.g. SH Cleveland, 'Embedded International Law and the Constitution Abroad' (2010) 110 Columbia Law Review 225; Y Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law' (2013) 7 The Law and Ethics of Human Rights 47.

31 ibid.

32 German Constitutional Court (Bundesverfassungsgericht, or 'BVerfG'), Bundesnachrichtendienst (19 May 2020) 1 BvR 2835/17 <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html> accessed 7 January 2023.

33 Milanovic, Extraterritorial Application of Human Rights Treaties (n 25) 209; R Goodman, C Heyns and Y Shany, 'Human Rights, Deprivation of Life and National Security: Q&A with Christof Heyns and Yuval Shany on General Comment 36' (Just Security, 2019) questions 1, 2 <https://www.justsecurity.org/62467/human-life-national-security-qa-christof-heyns-yuval-shany-general-comment-36/> accessed 7 January 2023; Sergio Euben Lopez Burgos v Uruguay (Comm No R.12/52) (HRC, 29 July 1981) para 12.3; Lilian Celiberti de Casariego v Uruguay (Comm no 56/1979) (Human Rights Committee, 29 July 1981) para 10.3; Issa and others v Turkey (App No 31821/96) (ECtHR, 16 November 2004) para 71. On the contrary, many oppose its applicability to positive human rights obligations, fearing the lack of necessary government powers beyond a state's territory or spatial control. See e.g. the account of the debate in Milanovic, 'The Murder of Jamal Khashoggi' (n 25) 19–20; and Milanovic, Extraterritorial Application of Human Rights Treaties (n 25) 209, 210–212, 219–220.

Irrespective of one's approach to extraterritorial jurisdiction pursuant to certain human rights treaties, it is worth stressing that human rights under customary international law apply irrespective of jurisdictional restrictions under specific treaties, even if their exact scope remains unclear.[34] Likewise, social, economic and cultural rights recognised in the ICESCR are not subject to any jurisdictional requirement.[35]

III. The Right to Life

Life is an individual's most fundamental human right. It inheres in each human being irrespective of personal characteristics or circumstances and is a necessary pre-condition to the enjoyment of all other human rights.[36] As such, under some human rights treaties, the right to life is non-derogable, including in times of armed conflict or other public emergencies.[37] It is also arguably a rule of *jus cogens*,[38] even if the exact scope of the right may be limited in some circumstances, such as during armed conflict. Given the importance of this right, it must not be

34 ACmmHPR General Comment 3 (n 26) para 14; R Fisher (ed), Operational Law Handbook (The Judge Advocate General's Legal Center and School, 2022) 96 <https://tjaglcs.army.mil/documents/35956/56931/2022+Operational+Law+Handbook.pdf/4e10836e-2399-eb81-768f-7de8f6e03dc5?t=1652119179075> accessed 7 January 2023; W Johnson (ed), Operational Law Handbook (The Judge Advocate General's Legal Center and School, 2013) 45 <https://irp.fas.org/doddir/army/oplaw2013.pdf> accessed 7 January 2023, stating that "[international human rights law] IHRL based on [customary international law] CIL binds all states in all circumstances, and is thus obligatory at all times. For official U.S. personnel (i.e., 'state actors' in the language of IHRL) dealing with civilians outside the territory of the United States, CIL establishes the human rights considered fundamental, and therefore obligatory." See also R Goodman, 'The United States' Long (and Proud) Tradition in Support of the Extraterritorial Application of International Human Rights Law', (Just Security, 10 March 2014) <https://www.justsecurity.org/8035/united-states-long-and-proud-tradition-supporting-extraterritorial-application-international-human-rights-law/> accessed 7 January 2023.

35 See ICESCR art 2.

36 CCPR General Comment 36 (n 26) para 2.

37 ibid para 1; ACmmHPR General Comment 3 (n 26) para 7.

38 M Nowak, UN Covenant on Civil and Political Rights: CCPR Commentary (2nd edn, NP Engel 2005) 122; PM Taylor, A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights (CUP 2020) 139; ACmmHPR General Comment 3 (n 26) para 5.

interpreted narrowly.[39] The right to life is also intrinsically connected to the protection of human health, as well as other economic, social, and cultural rights.[40] This means that the content of these rights, particularly the right to health, assessed below, should inform the interpretation and application of the right to life.[41]

It is easy to see why cyber operations against the healthcare sector directly implicate the right to life. On the one hand, those *already* undergoing medical treatment in hospitals or care units may suffer life-threatening harm or face the risk of such harm from disruptive cyber operations against hospital systems or equipment. In *Ximenes Lopes*, for example, a case involving the state's failure to prevent the suicide of patient in a psychiatric facility, the Inter-American Court of Human Rights (IACHR) stressed that:

> *As to the persons who are under medical treatment, and since health is a public interest the protection of which is a duty of the states, these must prevent third parties from unduly interfering with the enjoyment of the rights to life and personal integrity, which are particularly vulnerable when a person is undergoing health treatment. […]*
>
> *The Inter-American Court considers that any person who is in a vulnerable condition is entitled to special protection, which must be provided by the states if they are to comply with their general duties to respect and guarantee human rights.*[42]

39 CCPR General Comment 36 (n 26) para 3, ACmmHPR General Comment 3 (n 26) para 6.

40 ACmmHPR General Comment 3 (n 26) paras 6, 43; Suárez-Peralta v Ecuador (IACHR Series C No 261) (21 May 2013 paras 130–131.

41 CCPR General Comment 36 (n 26) para 2.

42 Ximenes-Lopes v Brazil (IACHR Series C No 149) (4 July 2006) paras 89 and 103 (emphasis added). For a similar case and conclusion, see Storck v Germany, (Application No. 61603/00) (ECtHR, 16 June 2005) para 103.

Similar findings have been made by the UN Human Rights Committee (HRC), the IACHR and the European Court of Human Rights (ECtHR) in cases involving the health of detainees under state custody.[43]

In the cyber context, 'distributed denial of service' (DDoS) operations (or 'DDoS attacks') targeting a hospital's operational technology control systems, that is, systems controlling the functioning of physical medical equipment such as ventilators, surgical equipment, or examination machines, could immediately affect a patient's treatment and lead to death or significant physical harm. Similarly, ransomware operations affecting the availability of patient data could lead to significant delays, suspension, or cancellation of life-saving health treatment.

On the other hand, even if patients are not *yet* being treated by any health provider, malicious cyber operations targeting healthcare can have devastating consequences for their well-being. Think of the health-related disinformation and misinformation campaigns during the COVID-19 pandemic, which led many to resort to unsafe, life-threatening 'cures', such as consuming high doses of alcohol, bleach, or dangerous medicines prescribed for other diseases.[44] Likewise, if the functioning of hospitals is disrupted by cyber operations such as ransomware or DDoS operations, new patients, including those in need of emergency care, may not be admitted for treatment. These are just a few examples of how cyber operations targeting the healthcare sector can have devastating consequences for the right to life.

According to the HRC, the right to life is 'the entitlement of individuals to be free from acts and omissions that are intended or may be expected to cause their unnatural or premature death, as well as to enjoy a life with dignity'.[45] This means that it protects individuals from deprivation

43 CCPR General Comment 36 (n 26) para 25; Denis Vasilyev v Russia (App No. 32704/04) (ECtHR, 17 December 2009) paras 115–116. See also V Stoyanova, 'Causation between State Omission and Harm within the Framework of Positive Obligations under the European Convention on Human Rights' (2018) 18 Human Rights Law Review 309, 330.
44 Milanovic and Schmitt (n 10) 266.
45 CCPR General Comment 36 (n 26) para 2.

of life, that is, intended or otherwise foreseeable and avoidable death, life-terminating injury or harm, whether physical or mental, caused by an act or omission.[46] Thus, the right to life can only be violated if a state, through its agents, intends to deprive an individual of their life, or else knows or should have known, based on the information available at the time, of a life-threatening situation created by its own agents or third parties. Protection against such foreseeable and preventable life-terminating injuries or harms is effected by imposing on states both negative and positive human rights obligations. As will become clearer in the remainder of this section, the right to life, along with the positive and negative duties arising therefrom, apply both to states that perpetrate cyber operations against the healthcare sector and states targeted by them.

In what follows, we delve deeper into the negative (Subsection A) and positive (Subsection B) duties arising from the right to life, as well as the types of threats that might trigger them (Subsection C) and whether or not causation between state actions or omissions and said threats is required (Subsection D).

A. Negative Obligations to Respect the Right to Life

First, states have negative obligations to refrain from *arbitrarily* depriving individuals of their lives. This obligation is breached by actions attributable to a state.[47] Though Article 2 of the European Convention on Human Rights (ECHR) does not explicitly refer to arbitrariness, it lays down tightly constrained circumstances in which limitations on the right to life are permitted and thus not arbitrary.[48] These are: the execution of a death penalty provided by law, the use of force for a legitimate purpose and in an absolutely necessary manner, or during lawful acts

46 ibid para 6.
47 See ICCPR art 6(1); ACHR art 4(1); ACHPR art 4; CCPR General Comment 36 (n 26) paras 4, 7.
48 ECHR art 2.

of war following a proper derogation.[49] Assessment of the arbitrariness of a deprivation of life includes but is not limited to inconsistency with the law. According to the HRC and the African Commission on Human and Peoples' Rights (ACmmHPR), it also encompasses elements of inappropriateness, injustice, lack of predictability, due process of law, reasonableness, necessity, and proportionality.[50] In short, unlawfulness is just the starting point; all relevant factors must be taken into account on a case-by-case basis.

This assessment may be complicated when more than one legal regime applies simultaneously. For example, a killing or death might be lawful under domestic law or international humanitarian law (IHL) but may still be unlawful under other legal regimes, such as the prohibition on the use of force or *jus ad bellum*.[51] According to the HRC, in those instances, any act of aggression *resulting in deprivation* of life would *ipso facto* violate the right to life.[52] This view is arguably sound, though there is no reason not to extend it to *any* violation of the prohibition on the use of force[53] that results in deprivation of life. Accordingly, if a state launches a cyber operation against a hospital or healthcare facility in another state that results in loss of life and can be qualified as a prohibited use of force or an act of aggression, this would *ipso facto* violate the right to life.[54] Nevertheless, the state's aggressive or otherwise illegal forceful actions that *ipso facto* violate its negative and positive duties to respect and protect the right to life should be distinguished from any deprivations of life caused by *individual* combatants fighting for the aggressor state

49 ECHR art 2 and 15(2).
50 CCPR General Comment 36 (n 26) para 12; ACmmHPR General Comment 3 (n 26) para 12.
51 CCPR General Comment 36 (n 26) para 70.
52 ibid.
53 Recall that the use of force in self-defence in line with Article 51 of the UN Charter or authorised by the UN Security Council under Chapter VII of the Charter would not breach the prohibition on the use of force under Article 2(4) of the UN Charter or its customary counterpart.
54 See M Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) 334, Rule 9, para 9(a). For a discussion of the prohibition of the threat or use of force, see Chapter 2.

consistently with IHRL or IHL standards.[55] The latter actions will not in principle violate a state's obligation to respect the right to life.[56]

In cyber and healthcare contexts, a state may violate its negative obligation to respect life if its organs or agents launch cyber operations that intentionally, recklessly, or foreseeably threaten the life of victims within its jurisdiction in an arbitrary manner. Again, actual death or life-threatening harm is not necessary, but only a risk of such harm ensuing.

B. Positive Obligations to Protect and Ensure the Right to Life

States also have positive obligations to protect the right to life from acts or omissions emanating from state or non-state agents.[57] This duty is explicitly laid down in Article 6(1) of the ICCPR, Article 2(1) of the ECHR, and Article 4(1) of the ACHR, all of which stipulate that the right to life 'shall be protected by law'. As a minimum, this obligation requires states to put in place criminal laws prohibiting and punishing serious types of homicide, such as murder and manslaughter, though further protection can be achieved by civil and administrative laws on the matter.[58] However, the scope of a state's duty to protect the right to life goes well beyond simply outlawing arbitrary killings.

As noted by several human rights monitoring bodies, including the HRC, the ACmmHPR, the IACHR and the ECtHR, the right to life also requires states to take *all* reasonable measures to protect life from *all* reasonably foreseeable threats, including threats emanating from a state's own agents[59] as well as private persons and entities.[60] Simply put, legislation

55 See, mutatis mutandis, McCann and Others v United Kingdom (App. no. 18984/91) (ECtHR, 27 September 1995) paras 194-214.
56 CCPR General Comment 36 (n 26) para 12.
57 ibid para 18.
58 Nowak (n 38) 123
59 CCPR General Comment 36 (n 26) para 13.
60 ibid para 18; ACmmHPR General Comment 3 (n 26) paras 7–9; Lopes de Sousa Fernandes v Portugal (App No 56080/13) (ECtHR, 15 December 2015) para 165. On reasonable foreseeability, see Chapter 2 Section II.B.2.iii.

or regulation might not be enough to discharge a state's positive obligation to protect the right to life. In addition to that, a state may have to adopt administrative, judicial, and other reasonable measures, such as carrying out effective investigations,[61] providing access to justice and an effective remedy, as would be necessary to ensure that individuals' right to life is protected.[62] Notably, life-threatening situations that must be prevented, stopped, or redressed include 'general conditions in society that may give rise to direct threats to life or prevent individuals from enjoying their right to life with dignity'.[63]

The duty to protect the right to life from life-threatening situations or conditions by measures going beyond legislation derives from states' general obligation to protect, ensure, and fulfil all human rights within their jurisdiction.[64] Under Article 2(1) of the ICCPR for example, states parties undertake not only to respect but also ensure to all individuals within their territory and subject to their jurisdiction the rights recognised in the Covenant. The same goes for Article 1 of the ECHR and Article 1 of the ACHR.

Examples of general conditions from which individuals must be protected include violence, disease, poor sanitation, malnutrition and hunger, environmental degradation, natural or man-made disasters, and, most importantly for present purposes, 'massive cyber-attacks resulting in disruption of essential services'.[65] According to the HRC, states should put in place contingency and disaster management plans designed to increase preparedness and address these and other situations,[66] though, as due diligence obligations, these are subject to a state's capacity to

61 cf McCann (n 55) 161; Velasquez Rodriguez (n 12) 174; The Public Committee Against Torture in Israel v The Government of Israel [2006] HCJ 769/02 para 40.
62 Nowak (n 38) 124; CCPR General Comment 36 (n 26) paras 13, 18; ACmmHPR General Comment 3 (n 26) para 38.
63 CCPR General Comment 36 (n 26) para 26; ACmmHPR General Comment 3 (n 26) paras 41–42.
64 Nowak (n 38) 124.
65 CCPR General Comment 36 (n 26) para 26. See also ACmmHPR General Comment 3 (n 26), para 41.
66 CCPR General Comment 36 (n 26) para 26.

act. In the specific context of healthcare, the HRC has found that 'as a minimum, states parties have the obligation to provide access to existing health-care services that are reasonably available and accessible when lack of access to the health care would expose a person to a reasonably foreseeable risk that can result in loss of life'.[67] Similarly, the ACmmHR has opined that, to address chronic yet pervasive threats to life, states must establish functioning health systems and eliminate practices that impact on individuals' and groups' ability to seek healthcare.[68]

This means that states must ensure that *access* to *existing* healthcare services within their jurisdiction is not hampered by cyber operations, insofar as the resulting lack of access could foreseeably lead to life-threatening harm. The procedural duties to investigate, punish and provide redress for violations of the right to life by state or non-state actors are also key components of states' positive obligation to protect life, including in the healthcare sector.[69] Thus, states must investigate the causes of deaths or life-threatening situations in health institutions, including those arising from cyber operations. States must also prosecute and appropriately punish those responsible, and provide victims, including relatives of dead patients, with an effective remedy.

However, as we have noted elsewhere, positive obligations to protect, fulfil, and ensure human rights, including the right to life, do not require states to do the impossible to successfully prevent, stop or redress avoidable and foreseeable threats to life or other rights.[70] Rather, these are obligations of conduct, requiring states to exercise due diligence, or their best efforts to achieve those aims.[71] As such, positive human rights

67 Nell Toussaint v Canada (Comm No 2348/2014) (HRC, 24 July 2018) para 11.3. Similarly, M.B. v Canada (Comm No 358/1989) (HRC, 5 November 1991) para 7.5.
68 ACmmHPR General Comment 3 (n 26) para 42.
69 CCPR General Comment 36 (n 26) para 27; ACmmHPR General Comment 3 (n 26) paras 15-21; Kotilainen and others v Finland (App No 62439/12) (ECtHR, 17 September 2020) paras 91–94.
70 A Coco and T Dias, "Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32(3) European Journal of International Law 771, 787.
71 ibid 774–775.

obligations are highly contextual, with the necessary and appropriate measures depending on the circumstances at hand, including how much knowledge a state has or should have about the threat and its capacity to avert or respond to it.[72] Nonetheless, lack of capacity does not completely exempt states from their obligation to protect life and other human rights.[73] This is because the obligation also entails a duty to acquire the necessary capacity to discharge it, at the very least by putting in a place a minimally functioning state apparatus that is able to enact legislation on the matter.[74]

While a state's positive duty to protect life extends to both public and private contexts,[75] the provision of public services, such as education and healthcare, whether by the state itself or private entities under concession agreements or other forms of outsourcing, imposes on states a heightened duty of care.[76] This is so for two main reasons. First, under conventional and customary international human rights law, states are responsible for the provision of certain public services to ensure or fulfil social, economic and cultural rights.[77] Second, state interference with individual privacy will usually be justified in the public interest to safeguard the provision of essential public services.[78] According to the IACHR, this heightened duty to ensure the provision of public services entails, at the very least, effective supervision and inspection of the service in question.[79]

72 V Stoyanova, 'Fault, Knowledge and Risk within the Framework of Positive Obligations under the European Convention on Human Rights' (2020) 33 Leiden Journal of International Law 601, 604, 618.
73 Coco and Dias, 'A Patchwork of Protective Obligations' (n 70) 788.
74 R Pisillo-Mazzeschi, 'The Due Diligence: Rule and the Nature of the International Responsibility of States', 35 German Yearbook of International Law (1992) 9, 26; Buchan (n 17) 434–439.
75 CCPR General Comment 36 (n 26) para 18.
76 Gonzales Lluy y otros v Ecuador (IACHR, Series C No 298) (1 September 2015) para 184; Suárez-Peralta (n 40) paras 144, 149–150; Ximenes-Lopes (n 42) para 96. See also, mutatis mutandis, CCPR General Comment 36 (n 26) para 25 (in the context of private detention facilities).
77 See e.g. ICESCR.
78 See e.g. ICCPR art 17(1); ECHR art 8(2); ACHR art 11.
79 Gonzales Lluy (n 76) para 184; Suárez-Peralta (n 40) paras 144, 149-150;

Two general interrelated questions surrounding states' obligations to respect and protect life that are particularly important in the context of cyber operations against the healthcare sector concern the types of threats triggering the right to life, and the issue of causation between states' actions or omissions and the relevant harm or life-threatening conduct or situation.

C. Threats to Life

It is uncontroversial that, across the main international and regional human rights instruments, mere threats to life suffice to trigger the corresponding right. However, some human rights monitoring bodies have referred to attributes such as 'real', 'immediate' or 'imminent' risk to life. For example, the HRC has found that:

> *[T]he duty to respect and ensure the right to life requires states parties to refrain from deporting, extraditing or otherwise transferring individuals to countries in which there are substantial grounds for believing that a real risk exists that their right to life under article 6 of the Covenant would be violated.*[80] *[…]*
> *And that [r]eturning individuals to countries where there are substantial grounds for believing that they face a real risk to their lives violates articles 6 and 7 of the Covenant.*[81]

Ximenes-Lopes (n 42) para 96. See also, mutatis mutandis, CCPR General Comment 36 (n 26) para 25 (in the context of private detention facilities).

80 CCPR General Comment 36 (n 26) para 30 (emphasis added).

81 ibid para 55 (emphasis added). See also Y.Sh. v Russian Federation (Comm No 2815/2016) (HRC, 13 March 2020) para 8.5 (finding that the claim was inadmissible because 'the author does not claim that the authorities had in their possession specific information about a planned shooting, which accidentally caused the death of the author's daughter; nor has the author shown that the level of lawlessness and violence in the city reached such high levels as to put all the inhabitants at real risk to their lives', emphasis added).

Likewise, in *Osman v the United Kingdom*, the ECtHR reasoned that:

> *[H]aving regard to the nature of the right protected by Article 2, a right fundamental in the scheme of the Convention, it is sufficient for an applicant to show that the authorities did not do all that could be reasonably expected of them to avoid a real and immediate risk to life of which they have or ought to have knowledge.*[82]

Using similar terminology, the ACmmHPR opined that '[t]he state has a positive duty to protect individuals and groups from *real and immediate* risks to their lives caused either by actions or inactions of third parties'.[83]

Does this mean that a state only breaches its *negative* duty to respect the right to life when its agents pose a real and imminent or immediate risk to an individual's life? Is the *positive* duty to protect life only violated when a state fails to exercise due diligence in preventing, stopping, or redressing real and imminent or immediate risks to an individual's life caused by its agents or third parties?

Arguably, the two qualifiers ought to be separated, and whether or not they apply to a state's duties to respect and protect life depends on the type of obligation and the circumstances at hand. As others have noted, a 'real risk' is one that is likely or 'objectively given and not merely speculative'.[84] Thus, it seems that the requirement of a real risk is just a reflection of the need for an objective test of reasonable foreseeability of the risk to life, an element of both negative and positive duties discussed earlier.

Conversely, an immediate or imminent risk is one that is present and will materialise in a relatively short period of time.[85] If such an attribute

82 Osman v The United Kingdom (App. Nos 23452/94) (ECtHR, 28 October 1998) para 116 (emphasis added).
83 ACmmHPR General Comment 3 (n 26) para 41 (emphasis added).
84 Stoyanova, 'Causation' (n 43) 339.
85 ibid.

were required for each and every life-threatening situation, the scope of the right to life would be significantly reduced. In particular, general conditions in society that may objectively threaten the right to life, but only once a certain period of time elapses, would be excluded. As seen earlier, this does not seem to be case, at least for a state's positive obligation to protect the right to life. It is also likely that a state would breach its negative duty to respect life if its own agents actively caused such life-threatening general conditions in society, such as an armed conflict, pollution, or a nuclear disaster, irrespective of their timing. Thus, immediacy or imminence do not seem to be general elements of a state's negative or positive obligations arising from the right to life. At the same time, in situations when one or more specific individuals are either the target or the source of a life-threatening behaviour or situation, it does seem reasonable to limit at least some of a state's *positive* duties of *prevention* to imminent or immediate threats to life.

To be sure, irrespective of any *specific* threat to life, a state has a *broad* duty to put in place an appropriate set of preventive measures to ensure public safety and deter a variety of life-threatening situations affecting individuals or society in general. As noted by the HRC, these include 'massive cyberattacks resulting in disruption of essential services'.[86] Healthcare is a prime example of an essential service directly implicating the right to life. Yet it is one of the most ICT-dependent sectors, making it extremely vulnerable to cyber operations.[87] Thus, states must adopt a range of preventive measures to deter and stop cyber operations that would result in the disruption of healthcare services with a real and foreseeable risk to the lives of patients. This is a broad regulatory duty that encompasses the enactment, implementation, and supervision of a regulatory framework to protect life.[88] It is breached by generalised, systemic failures, as opposed to errors of judgment or negligence by one

86 CCPR General Comment 36 (n 26) para 26.
87 J Zarocostas, 'Health under cyberattack' (4 September 2021) 398(10303) The Lancet 829; CyberPeace Institute, 'Playing with Lives' (n 16) 16.
88 Kotilainen (n 69) para 66-68, 75; Lopes de Sousa Fernandes (n 60) paras 186–188; Ximenes-Lopes (n 42) paras 98–99; Suárez-Peralta (n 40) para 135.

or a few individuals.[89] Drawing on the right to health,[90] assessed below, the IACHR has found that the regulatory duty to protect life requires availability, accessibility, acceptability, and quality of medical services, in theory and in practice.[91]

Cyber operations targeting the healthcare sector may affect one or more of such attributes. For one, disruptive cyber operations may affect the availability and quality of health services provided, insofar as they may lead to interruptions and delays in patient care. Such consequences were seen in the infamous WannaCry ransomware operation, for example. This operation targeted 40% of public healthcare providers in the UK, leading to thousands of appointment and surgery cancellations as well as patient diversions whose impact can still be felt today.[92]

The regulatory duty to protect life arises once the state is or should be in possession of knowledge or information about specific or systemic risks to life arising from certain dangerous activities, such as crime or environmental harm.[93] This level of constructive knowledge should be judged without the benefit of hindsight.[94] However, the more dangerous the situation at hand, the higher the burden is on states to acquire more information and remain vigilant about its risks to life,[95] whether by carrying out risk assessments or scientific research.[96] Similarly, states

89 Kotilainen (n 69) paras 66–68; Lopes de Sousa Fernandes (n 60) paras 165, 189; Fernandes de Oliveira v Portugal (App No 78103/14) (ECtHR, 31 January 2019) paras 105–106.
90 See CESCR General Comment 14 (n 26) para 12.
91 Suárez-Peralta (n 40) para 152.
92 UK National Audit Office, 'Investigation: WannaCry cyber attack and the NHS' (Report by the Comptroller and Auditor General, 25 April 2018) <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf> accessed 7 January 2023; CyberPeace Institute, 'Playing with Lives' (n 16) 34.
93 Y.Sh. (n 81) para 8.5.
94 O'Keeffe v Ireland (App No 35810/09) (ECtHR, 28 January 2014) paras 143 and 152. Stoyanova, 'Fault, Knowledge and Risk (n 72) 608, 611.
95 See Stoyanova, 'Fault, Knowledge and Risk (n 72) 608.
96 CCPR General Comment 36 (n 26) para 62.

have a duty to ensure access to such information by potential victims.[97] The extent to which such precautionary measures will be required depends, of course, on a state's capacity to carry them out, including its financial and human resources.[98] Furthermore, the more predictable a certain life-threatening situation is, the more demanding the positive measures required from states will be.[99] In sum, the level of knowledge, the seriousness of the harm, and a state's capacity to act will affect the nature and scope of measures that states must put in place to discharge their positive obligation to protect life from life-threatening situations.

Concretely, this means that states must acquire information about systemic risks posed by cyber operations against the healthcare sector, including by investing in research and information-gathering about the potential impact of those operations. Based on the risks that are already known to states, they must also enact, supervise, and implement a basic regulatory framework for the prevention of those cyber operations, including by outlawing the most serious types of operations affecting the healthcare sector, such as DDoS and ransomware operations.

This positive regulatory duty is separate from the duties that arise or the measures that must be put in place when a *specific* threat to life exists. When a specific life-threatening situation exists, states must adopt *additional* measures to prevent or stop violations of the right to life. The ECtHR has referred to these as 'preventive operational measures' to protect citizens or society at large from *identifiable* threats to life, such as police intervention.[100] Yet, even when a state knows or should have known about such a specific threat to life, actual operational measures only become appropriate and necessary when the threat is imminent and, thus, about to materialise. Otherwise, the positive duty to protect

97 ibid; Vilnes and Others v Norway (App Nos 52806/09 and 22703/10) (ECtHR, 5 December 2013) para 243–244.
98 Stoyanova, 'Fault, Knowledge and Risk (n 72) 608,
99 Stoyanova, 'Causation' (n 43) 324; Finogenov and Others v Russia (App nos 18299/03 and 27311/03) (ECtHR, 20 December 2011) para 243.
100 Kotilainen (n 69) para 69.

the right to life would impose on states an insurmountable burden, diverting resources and efforts from the implementation of other fundamental human rights.

According to the ECtHR, the additional duty to adopt preventive operational measures arises in three sets of exceptional circumstances, two of which are specific to the healthcare context. First, when an individual patient's life is knowingly put in danger by denial of access to life-saving emergency treatment. Second, where a 'systemic or structural dysfunction in hospital services results in a patient being deprived of access to life-saving emergency treatment and the authorities knew about or ought to have known about that risk'.[101] Third, when a given individual poses a real and imminent risk of committing criminal acts towards unidentified members of the public, such as when dangerous prisoners are granted leave or conditional release.[102] Cyber operations against the healthcare sector could cause or contribute to these three types of scenarios. In the first case, significantly disruptive cyber operations may well impede the access of individuals to emergency treatment, as was the case with the WannaCry ransomware operation. The second scenario could result from systemic failures to put in place robust cybersecurity systems in health institutions or a resilient health information environment, whose exploitation by disruptive cyber operations, data breaches, misinformation or disinformation could result in denial of life-saving emergency treatment. Finally, identified state actors or cyber criminals could be at the origin of specific cyber operations threatening the lives of individuals.

101 Lopes de Sousa Fernandes (n 60) paras 185–189, 192.

102 See Kotilainen (n 69) paras 70–73; Mastromatteo v Italy [GC] (App. no. 37703/97) (ECtHR, 24 October 2002) para 69; Maiorano and Others v Italy (App no 28634/06) (ECtHR, 15 December 2009) para 107; and Choreftakis and Choreftaki v Greece (App no 46846/08) (ECtHR, 17 January 2012) paras 48–49.

D. Causation

The second question highlighted above addresses causation: what, if any, test of causation is required between state action or inaction and the deprivation of life? Answering this question is crucial here because most types of cyber operations targeting the healthcare will only have indirect effects on the victims' right to life.[103] Granted, cyber operations targeting operational technology used to control life-saving physical devices, such as ventilators or defibrillators, raise a clear and direct risk to patients' lives.[104] But in the case of cyber operations compromising the availability or confidentiality of patient or hospital data, such as ransomware, it is not the data theft per se that will kill or cause life-threatening harm to patients. Rather, it is the disruption and delays in patient treatment following on from the unavailability of data and the efforts expended on repairing affected systems that risk affecting patients' lives.[105] Similarly, in the case health misinformation or disinformation, it is not the dissemination of false information about diseases or medical treatment that will immediately affect addressees' lives; victims still need to act upon the false or misleading information received to suffer life-threatening harm, such as by drinking bleach or refusing to take a vaccine.[106]

Very little has been written on causation in the law of state responsibility generally and in the context of international human rights law. And there is controversy on which legal or normative considerations should be added to a purely factual causation analysis.[107] Some insist on an

103 See Milanovic and Schmitt (n 10) 262.
104 See CyberPeace Institute, 'Playing with Lives' (n 16) 43, 53–56.
105 ibid 43.
106 T van Benthem, T Dias and D Hollis (n 10) 1269. See also H Lahmann, 'Infecting the Mind: Establishing Responsibility for Transboundary Disinformation' (2022) 33(2) European Journal of International Law 411, 421.
107 See generally, V Lanovoy, 'Causation in the Law of State Responsibility' (2022) British Yearbook of International Law (forthcoming, advance copy available at <https://doi.org/10.1093/bybil/brab008>), 44–78. For a detailed discussion of relevant standards of causation and on the relationship between 'factual causation' and 'legal causation', see Chapter 2 Section II.B.1.

exacting 'but for' causation test, necessitating a sufficiently direct[108] connection between cause and effect. Conversely, others have proposed more flexible standards based on normative considerations, such as reasonableness and foreseeability, to assess causation in a certain chain of events.[109] Further uncertainty and confusion pervade the matter in the case law of different human rights bodies, particularly due to the inconsistent use of terminology on applicable standards of causation.[110] Assessing causation is even more challenging for positive obligations given the factual difficulty of proving a causal link in the case of omissions, that is, to what extent a state's lack of diligence caused or contributed to the relevant result.

The ECtHR has erratically referred to different standards of causation, such as '(direct) causal link', 'direct and immediate link', 'proximity', 'strong enough link', 'sufficient nexus' and 'significant influence'.[111] In the case of omissions, the Court has generally found that 'a failure to take reasonably available measures [must] have had a real prospect of altering the outcome or mitigating the harm'[112]. However, it has not applied the 'real prospect' test consistently.[113] For its part, the HRC has not delved into the applicable standard of causation. It has simply noted that, for a breach of the right to life, an intentional or otherwise

108 E.g., Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Merits) [2007] ICJ Rep 43, 233; The M/V 'Saiga' (No 2) (Saint Vincent and Grenadines v Guinea) (Judgment) ITLOS Reports 1999 para 172; German-US Mixed Claims Commission 'Administrative Decision No II' (1923) VII RIAA 23, 29; Dix Case (1903) IX RIAA 119, 121.
109 Lanovoy (n 107) 57–60, 78–79.
110 Stoyanova, 'Causation' (n 43) 310.
111 ibid 316–318.
112 E.g. O'Keeffe (n 94) para 149; Opuz v Turkey (App No 33401/02) (ECtHR, 9 June 2009) para 136; Premininy v Russia (App No 44973/04) (ECtHR, 10 February 2011) para 84; Bljakaj and Others v Croatia (App No 74448/12) (ECtHR, 18 September 2014) para 124.
113 Stoyanova, 'Causation' (n 43) 317–318.

foreseeable and preventable life-terminating harm or injury must be *caused* by an act or omission.[114] Importantly, however, the HRC has found that:

> *The obligation of states parties to respect and ensure the right to life extends to reasonably foreseeable threats and life-threatening situations that can result in loss of life. States parties may be in violation of article 6 even if such threats and situations do not result in loss of life.*[115]

As seen earlier, this means that the right to life is not only violated when an actual deprivation of life occurs. Rather, mere *threats* to life suffice to breach this right, provided that they are real and foreseeable. And these threats may be caused by duty-bearer states or third parties. To be sure, the actual death or life-threatening injury *potentially* caused by a state agent or private entity must be reasonably foreseeable to the state. This means that the effect of death or life-threatening injury must be projectable results of the public or private behaviour or situation at hand. But if no actual harm is necessary, then causation between a state's actions or omissions and any such harm is not strictly necessary either. For breaches of the *negative* duty to *respect* life, a state's actions need only cause a life-threatening *situation*, such as an armed conflict or environmental disaster. However, because the state is the principal 'perpetrator' of such breaches, it is reasonable to conclude that the state ought to actually engage in the life-threatening behaviour at hand. In other words, given the structure and focus of negative human rights obligations, nothing short of direct causation between the state conduct and the life-threatening situation should be expected.

Conversely, for positive obligations to protect life, what seems to be required is the mere *existence* of a life-threatening situation that the

114 CCPR General Comment 36 (n 26) para 6.
115 ibid para 7 (emphasis added).

state should have foreseen, failed to avoid or redress, and yet could have done so in the circumstances. Here, causation between state conduct and life-threatening situation does not seem to be necessary, at least in a strict sense. Rather, any assessment of causation between state conduct and 'result' is purely hypothetical or counterfactual: should the state have foreseen the existence of the life-threatening situation, and could it have been avoided? In a way, this assessment of projected or predictive causation is blended in with considerations of foreseeability and capacity to act.[116] As discussed earlier, for preventive operational measures, this assessment of predicted causation is naturally more exacting, insofar as the threat to life must not only be real but also immediate or imminent. But for the broad regulatory duty to protect life to kick in, including in situations involving healthcare and cyber operations, only objective foreseeability of the life-threatening situation – such as a cyber operation against the healthcare sector – and capacity to prevent it are required.

A more stringent test of causation is nonetheless required when actual deprivation of life ensues, and victims claim reparations from the state whose alleged omissions led to it.[117] In those cases, the ECtHR's 'real prospect' test seems reasonable, at least as a general matter. It asks whether a protective measure available to the state in the circumstances could have obviated or mitigated the result,[118] *in casu*, the deprivation of life. As other counterfactual tests of causation for omissions, this test should not look to find a direct causal link between the state's failure to act and the result. Instead, it should query about the extent to which the state's lack of due diligence *contributed* to the deprivation of life, even if it was not the sole or most significant factor in the chain of events leading up to it. This is because positive human rights obligations are about preventing or remedying the actions of third parties. If direct or proximate causation were required between a state's omission and the

116 Stoyanova, 'Causation' (n 43) 315–316; Stoyanova, 'Fault, Knowledge and Risk (n 72) 618–619.
117 Kotilainen (n 69) para 104; Lanovoy (n 107) 80–82.
118 Stoyanova, 'Causation' (n 43) 317–318.

result, the scope of states' positive duties to protect life and other human rights would be significantly narrower than it actually is.

As hinted at earlier, different types of cyber operations targeting the healthcare sector may, directly or indirectly, affect the lives of different victims—from patients already undergoing medical treatment to individuals who need medical care and members of the general public. The most obvious life-threatening impact of such operations, especially disruptive ones like ransomware, are delays in and interruption of patient care.[119] For example, the Ryuk ransomware operation in September 2020 left over 250 hospitals in the United States without access to computer and phone systems. As a result of the operation, staff lost access to patient files and history, including exams such as X-rays or CT scans, were forced to revert to pen and paper, and to redirect ambulances or relocate surgeries. Some affected staff members even linked the operation to the death of certain patients.[120] At least one study has found that losing access to medical records and life-saving medical devices affects the ability of healthcare professionals to effectively care for their patients and administer medicines and other medical treatment in time.[121] Insofar as such operations could be attributed to a state actor, the requisite causal link between state action and foreseeable threat to life would be easily met. And irrespective of attribution, state failure to adopt reasonable measures to prevent or mitigate the impact of disruptive operations, including regulation, cybersecurity protocols, and law enforcement action, can certainly be said to contribute to their heightened risk to patients' lives. After all, there is evidence that all such measures, especially increased cyber hygiene, could potentially reduce or mitigate the risk of such cyber operations occurring in the first place or their impact on patients' lives and wellbeing.[122]

119 CyberPeace Institute, 'Playing with Lives' (n 16) 42.
120 ibid 43.
121 J Snair and D Henry, 'Risks of Cyber Attacks on the Healthcare Sector Leave Public Health of Communities Vulnerable' (NACCHO Voice, 24 October 2013) <https://www.naccho.org/blog/articles/risks-of-cyber-attacks-on-the-healthcare-sector-leave-public-health-of-communities-vulnerable> accessed 7 January 2023.
122 See e.g. AJ Coronado and TL Wong, 'Healthcare cybersecurity risk management:

In the same vein, cyber operations affecting the confidentiality of healthcare data, including patient, hospital, or research data, may cause significant delays in patient care. For one thing, restoring databases and patching up software vulnerabilities requires hospitals and other healthcare facilities to divest time, human and financial resources originally allocated to patient care. A study on the relationship between breach remediation efforts and hospital care quality found evidence that hospitals targeted by data breaches increased patient mortality in 30% in the two to three years following the incident.[123] This was mainly due to delays in the provision of critical patient care, such as electrocardiograms to patients suffering from chest pain.[124] Likewise, breaches of confidentiality of research data, such as clinical trials of vaccines and other medical treatments, may lead to delays in their regulatory approval process.[125] Such operations may also undermine public trust in institutions and medical treatments, which may affect their general intake and effectiveness in society. If attributed to a state actor, these types of operations would undoubtedly increase the risk of life-threatening harm in affected health institutions or society as a whole. Likewise, a state's failure to adopt general regulatory measures (including the enactment, implementation and supervision of the necessary regulation), as well as specific operational measures, such as the deployment of cyber incident response teams, in the event of a specific data breach against one or more hospitals, may be said to contribute to an increased risk of life-threatening harms in affected institutions or society.

Even though disinformation, misinformation, and other health-related information operations still require individual addressees to act upon

keys to an effective plan', (2014) Biomedical Instrumentation Technology 26 <doi.org/10.2345/0899-8205-48.s1.26> accessed 7 January 2023; L Coventry and D Branley, 'Cybersecurity in healthcare: A narrative review of trends, threats and ways forward' (2018) 113 Maturitas 48.

123 CyberPeace Institute, 'Playing with Lives' (n 16) 42.

124 SJ Choi, ME Johnson and CU Lehmann 'Data breach remediation efforts and their implications for hospital quality' (2019) 54(5) Health Services Research 971.

125 Dias and Coco, 'Cyber Due Diligence in International Law' (n 15) 72.

the information received, they may also give rise to or increase the risk of life-threatening situations.[126] This risk is particularly high when the false or misleading information promotes medical treatments that seriously threaten individuals' lives or well-being, such as dangerous home remedies or unapproved medicines, or raises doubts about treatments or measures that can save lives, such as vaccines, social-distancing or mask-wearing.[127] However, other types of disinformation or misinformation may not easily be said to increase the risk of life-threatening harm, such as those relating to the origin of the COVID-19 virus. If a state orchestrates or carries out an information operation that does create or contribute to a life-threatening situation, then causation between the state action and said situation may be established. If a state fails to exercise due diligence to prevent or mitigate the effects of such types of operations, such as by regulating the dissemination of health disinformation or misinformation on online platforms, debunking health myths or promoting the distribution of accurate health information, then this omission might be said to contribute to increased life-threatening risks arising from such information operations.

IV. The Right to Health

Health could be defined as 'a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity'.[128] Desirable as it may be, existing international legal instruments do not establish an unconditional 'right to be healthy'[129] and, evidently, not even the most willing and able state can guarantee – at the present stage of medical knowledge – that individuals will enjoy good health at all times.[130] As such, the right to health in international law can be better understood as having an aspirational and progressive nature, as a right

126 Similarly, Milanovic and Schmitt (n 10) 262.
127 ibid 267.
128 Constitution of the WHO (adopted 22 July 1946, entered into force 7 April 1948) 14 UNTS 185 art 28(i).
129 CESCR General Comment 14 (n 26) para 8.
130 ibid para 9. cf E Riedel, 'Health, Right to, International Protection' Max Planck Encyclopaedia of Public International Law (2011) para 29.

'to enjoy the conditions that will maximize the potential for individuals to enjoy health'.[131] The opportunity to attain the highest standard of health invariably depends on a range of other socio-economic factors allowing individuals to conduct a healthy life, like the availability of food, water, sanitation, housing in the relevant national and regional context, and the lack of discrimination in access to such resources.[132] Conditions that will maximize the potential to enjoy health comprise 'a system of health protection, including health care and the underlying determinants of health, which provides equality of opportunity for people to enjoy the highest attainable standard of health'.[133]

The World Health Organization (WHO) identified 'six essential building blocks' upon which the full realisation of the right to the highest attainable standard of health rests, namely 'good health services'; a 'well-performing health workforce;' a 'well-functioning health information system' ensuring 'the production, analysis, dissemination and use of reliable and timely information on health determinants, health systems performance and health status'; 'medical products, vaccines and technologies'; 'a good health financing system'; and 'leadership, governance, stewardship' by the relevant authorities.[134] Clearly, all of such 'building blocks' are to be conceived dynamically and flexibly in

131 J Tobin and D Barrett, 'The Right to Health and Health-Related Human Rights' in Lawrence O Gostin and Benjamin Mason Meier (eds), Foundations of Global Health & Human Rights (OUP 2020) 68.

132 CESCR General Comment 14 (n 26) para 4. See also UNGA, 'Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health' (8 August 2007) UN Doc A/62/214 paras 45–48.

133 ECOSOC, 'Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health, Paul Hunt' (11 February 2005) UN Doc E/CN.4/2005/51 para 42.

134 WHO, 'Everybody's Business: Strengthening Health Systems to Improve Health Outcomes' (2007) cited in B Saul, D Kinley and Jacqueline Mowbray, The International Covenant on Economic, Social and Cultural Rights: Commentary, Cases, and Materials (OUP 2014) 1045. See also Human Rights Council, 'Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health' (31 January 2008) UN Doc A/HRC/7/11 para 70; and 'Declaration of Alma-Ata' (International Conference on Primary Health Care, Alma-Ata, 6-12 September 1978) defining the concept of 'primary health care'.

time, as susceptible of being adapted to technological advancements and new knowledge in medical and other sciences.[135]

A. Cyber Threats against the Right to Health

There is no question that cyber operations targeting the healthcare sector can directly or indirectly pose a threat to the enjoyment of the right to health. Whilst the right to health cannot be reduced to a right to healthcare, as seen earlier, a well-functioning healthcare system is undeniably one of the right's key components. Interruption of the functioning of infrastructure that supports health services could jeopardize, in certain circumstances, an individual's ability to attain the highest standard of health[136] and, in the most extreme cases, even result in death.[137] Moreover, compromises with detrimental effects on the enjoyment of the right to health may arise, for instance, in the form of delays in the approval process, production and distribution of vaccines.[138]

The collection in digital form of huge quantities of personal data about patients is an effect of the increased digitalisation of healthcare, in addition to being a fundamental tool to inform public health policies and strategies, and even decisions on treatment and/or therapy in

135 Riedel (n 130) para 31.

136 H McDermott, 'Application of the International Human Rights Law Framework in Cyber Space' in D Akande et al (eds), Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment (OUP 2020) 197. See e.g. what happened when the Waikato Health Board in New Zealand was the subject of a massive ransomware attack: 'Waikato DHB Ransomware Attack: Documents Released Online', RNZ, (29 June 2021) <https://www.rnz.co.nz/news/national/445735/waikato-dhb-ransomware-attack-documents-released-online> accessed 7 January 2023.

137 For instance, a ransomware attack against the University hospital in Dusseldorf – on 11 September 2020 – determined that a 78-year-old patient had to be diverted to another hospital 32 km away. The patient died on the way. See W Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', Wired (11 November 2020) <https://www.wired.co.uk/article/ransomware-hospital-death-germany> 7 January 2023.

138 See e.g. what happened when the vaccine-maker Dr Reddy was the object of a ransomware attack : 'Dr Reddy's: Covid Vaccine-Maker Suffers Cyber-Attack' BBC News (22 October 2020) <https://www.bbc.com/news/technology-54642870> accessed 7 January 2023.

individual cases.[139] Such data is vulnerable to theft, compromise or publication. These, in turn, could affect not only the right to privacy of the individuals to whom the data pertains[140] but also their right to health if individuals decide not to seek or communicate sensitive information in the fear that such data could be subject to unwanted access and/or their anonymity may be lost.[141] The issue is particularly sensitive for women. In this regard, the Committee on the Elimination of Discrimination against Women (CEDAW) has recalled that '[w]hile lack of respect for the confidentiality of patients will affect both men and women, it may deter women from seeking advice and treatment and thereby adversely affect their health and well-being. Women will be less willing, for that reason, to seek medical care for diseases of the genital tract, for contraception or for incomplete abortion and in cases where they have suffered sexual or physical violence.'[142] The problem was in the news recently in the wake of the overturning of the *Roe v Wade* precedent by the United States Supreme Court, recognising the right to abortion – with women worldwide fearing that their sensitive data may be illegally accessed, *inter alia* by anti-abortion activists.[143]

Importantly, another key component of the right to health is the ability to access accurate and reliable information about health matters.[144] Information operations are the biggest threat against this component of the right to health. This is especially so if one considers the wide availability of health-related information online, and the increasing

139 Botrugno (n 2) 148–149.
140 ibid 154. See e.g. what happened in the Waikato DHB Ransomware incident: 'Waikato DHB Ransomware Attack: Documents Released Online', RNZ (n 136). See also Section V on the right to privacy below.
141 McDermott (n 136) 195.
142 On the dangers, see CEDAW, 'General Recommendation No. 24 (20th session, 1999) (article 12: Women and health)' (1999) UN Doc A/54/38/Rev.1, Chapter I, para 12(d).
143 R Chandran and D Baptista, 'Analysis: After Roe v Wade, Healthcare Data Privacy Fears Grow Worldwide' Reuters (12 July 2022) <https://www.reuters.com/legal/litigation/after-roe-v-wade-healthcare-data-privacy-fears-grow-worldwide-2022-07-12/> accessed 7 January 2023.
144 Riedel (n 130) para 31.

provision of digital healthcare services, for example by way of remote doctor-patient interactions, whose reliability could be potentially threatened by such operations.[145]

In the face of such threats, how does international human rights law safeguard and promote the right to health? Health has always been a pillar of a human-oriented international law, since the days of its mention in Article 55 of the UN Charter and the creation, in 1946, of the WHO.[146] Though not a binding legal provision per se, Article 25 of the Universal Declaration of Human Rights signalled early on the importance of health as an aim of international law. It provides that 'everyone has the right to a standard of living adequate for the health and well-being of himself and his family, including food, clothing, housing and medical care and necessary social services'. Article 12(1) of the 1966 ICESCR then established that 'States Parties to the present Covenant recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health'. Article 12(2) adds that

> *[t]he steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for (a) The provision for the reduction of the stillbirth-rate and of infant mortality and for the healthy development of the child; (b) The improvement of all aspects of environmental and industrial hygiene; (c) The prevention, treatment and control of epidemic, endemic, occupational and other diseases; (d) The creation of conditions which would assure to all medical service and medical attention in the event of sickness.*

In similar terms, the right to health is recognised inter alia in regional human rights treaties, for instance in Article 11 of the European Social

145 Botrugno (n 2) 142. See also CyberPeace Institute, 'Playing with Lives' (n 16) 60.
146 Riedel (n 130) para 5.

Charter, in Article 16 of the ACHPR and in Article 10 of the Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights. Health is also internationally protected by specialized human rights conventions, such as the Convention on the Elimination of All Forms of Racial Discrimination (Article 5(e)(iv)), CEDAW (especially Article 12), and the Convention on the Rights of the Child (especially Article 24). A strong argument can also be made that all humans enjoy a right to health as a matter of customary international law, considering how even states that are not Parties to the ICESCR appear to include it among their international human rights obligations.[147]

For ease of reference, the remainder of this section will analyse the content of the obligations deriving from the ICESCR, whilst referring to other conventional or customary obligations where appropriate. Considerations about the protection of the right to health as enshrined in the ICESCR can be applied to the other treaty regimes and custom *mutatis mutandis*.

B. Negative and Positive Obligations to Respect, Protect and Fulfil the Right to Health

As with other human rights obligations, international legal instruments establish obligations to respect, protect and fulfil the right to health, violations of which may take the form of either direct action or omission. Pursuant to their duty to respect the right to health, states must 'refrain from interfering directly or indirectly with the enjoyment of the right to health'.[148] For instance, states must refrain from enacting policies or laws, or engaging in conduct that impedes equal access to health services and facilities for particular individuals or groups as well as withholding or misrepresenting vital health-related information, such

147 See country reports cited in William A Schabas, The Customary International Law of Human Rights (OUP 2021) 309. Among other documents, health is described as a 'fundamental human right' also in the 1978 Alma-Ata Declaration (n 134), I.
148 CESCR General Comment 14 (n 26) para 33.

as information on appropriate medical treatment.[149] The core, non-derogable obligations to respect the right to health, in addition, include the duty not to limit access to health facilities, services, and goods on a discriminatory basis[150] and to ensure their equitable distribution[151] – something that a state could violate when it carries out or sponsors harmful cyber operations abroad. Evidently, carrying out or supporting cyber operations that interfere with the right to health by disrupting access to healthcare – such as ransomware or DDoS operations against healthcare infrastructure – would constitute one such violation.[152] Mere support to a cyber operation that cannot be attributed to a state would violate the right to health insofar as it would contribute to impeding access to health by individuals.

A state's duty to protect the right to health can be met with a range of measures. Examples include adopting an appropriate national legal framework on the provision of health services, especially if they are to be privatized,[153] or ensuring that health professionals are trained to the highest possible standards[154] — what nowadays must include basic cyber hygiene and data protection practices.[155] The enactment and implementation of adequate cybersecurity regulations and practices in healthcare infrastructure has effectively become an important dimension to the protection of the right to health. The failure to take all necessary measures to protect individuals from interferences with their right to health by third parties – such as those that could occur by means of cyber operations – may amount to a violation of the obligation.[156]

149 ibid paras 34, 50; Riedel (n 130) para 36.
150 cf also CESCR General Comment 14 (n 26) para 43(a).
151 cf also ibid para 43(e).
152 Milanovic and Schmitt (n 10) 261.
153 CESCR General Comment 14 (n 26) para 35; Saul, Kinley and Mowbray (n 134) 992.
154 CESCR General Comment 14 (n 26) para 35; Riedel (n 130) para 37.
155 In this sense also K Denney-Turner, 'State Responsibility for Healthcare: Human Rights Obligations in Relation to Cyberattacks' (CyberPeace Institute, 5 April 2022) <https://cyberpeaceinstitute.org/publications/state-responsibility-for-healthcare-human-rights-obligations-in-relation-to-cyberattacks/> accessed 7 January 2023.
156 CESCR General Comment 14 (n 26) para 51.

As to the duty to ensure or fulfil the right to health, it essentially requires states to adopt all necessary steps to create the conditions for the enjoyment of said right. These include, for instance, the adoption of a national health policy aimed at maximising the chances of everyone attaining the highest possible standard of health, the creation of a sufficient and well-functioning public health infrastructure, and, more generally, the expenditure of public resources to ensure equal enjoyment of the right.[157] Again, such measures should include the acquisition of state-of-the-art cybersecurity products (where the state has available resources to do so), the adoption of data protection policies, and the promotion of cyber hygiene in healthcare.[158]

The realisation of the right to health is intended to be progressive and subject to the technical and economic capabilities of each state. Thus, lack of adequate state action will not always constitute a violation of the positive duties arising from said right. This will occur when a state is unwilling to use its *available* resources to protect and fulfil the right to health. When a state does not have adequate resources and is, thus, unable to meet its obligations under the ICESCR, it still bears the burden of showing that it has made every reasonable effort towards that objective.[159] Yet, as noted earlier with respect to states' positive duties to protect the right to life, lack of technical or financial capability is not an excuse for non-compliance with the positive obligations to protect and ensure the right to health. States are, in fact, bound by some immediate obligations, including to guarantee that this right will be enjoyable by all without any discrimination, and the actual taking of steps towards its full realisation.[160]

As seen earlier, cyber operations can pose a threat to the enjoyment and progressive realisation of the right to health. According the Committee on Economic, Social, and Cultural Rights (CESCR or 'the Committee'),

157 ibid paras 36–37, 52; Riedel (n 130) para 38.
158 In this sense also Denney-Turner (n 155).
159 CESCR General Comment 14 (n 26) para 47.
160 ibid para 30.

such realisation rests upon four essential and interconnected features of a health system: availability, accessibility, acceptability, and quality.[161] *Availability* designates a state's health system that provides a sufficient amount of well-functioning facilities, goods, services and programmes, whilst *accessibility* posits that such facilities, goods, services and programmes are placed at everyone's disposal without discrimination.[162] Disruptive cyber operations may endanger such availability in the short, medium or long term, thus affecting individuals' right to health. Of particular interest to the present discussion, accessibility is conceived by the CESCR as including 'information accessibility', namely 'the right to seek, receive and impart information and ideas concerning health issues'.[163] Thus, information operations aimed at misleading the public about issues such as medical treatment, health conditions or vaccines may hamper this particular dimension of the realisation of the right to health.[164] For instance, data relating to the regulatory approval of the COVID-19 BioNTech-Pfizer vaccine was leaked from the European Medicines Agency (EMA) and subsequently published in manipulated format. According to the EMA, this could undermine public trust in the vaccines and relevant health institutions thereby hindering efforts to curb the COVID-19 pandemic.[165]

161 ibid para 12. See also Tobin and Barrett (n 131) 72.
162 CESCR General Comment 14 (n 26) para 12.
163 CESCR General Comment 14 (n 26) para 12(b).
164 As implied, for instance, by independent experts : Office of the High Commissioner of Human Rights (OHCHR), 'COVID-19: Governments Must Promote and Protect Access to and Free Flow of Information during Pandemic – International Experts' (19 March 2020) <https://www.ohchr.org/en/press-releases/2020/03/covid-19-governments-must-promote-and-protect-access-and-free-flow> accessed 7 January 2023. For a similar view, see Milanovic and Schmitt (n 10) 268. For a closer examination of how information operations may harm the right to health and other human rights, see van Benthem, Dias and Hollis (n 10); CyberPeace Institute, 'Playing with Lives' (n 16) 42; HRC, 'Disinformation and freedom of opinion and expression Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan' (13 April 2021) UN Doc A/HRC/47/25 paras 2, 21, 49.
165 J Stubbs, 'Hackers steal Pfizer/BioNTech COVID-19 vaccine data in Europe, companies say', Reuters (9 December 2020) <https://www.reuters.com/article/us-ema-cyber-idINKBN28J2Q7> accessed 7 January 2023; CyberPeace Institute, 'Playing with Lives' (n 16) 61.

A third feature required for a 'healthy' health system is, for the CESCR, its *acceptability*: this expression designates respect for medical ethics, consideration of cultural factors, and respect for confidentiality of personal data involved in medical consultations, treatment, and research.[166] In fact, the Committee warned that even the above-mentioned accessibility of information 'should not impair the right to have personal health data treated with confidentiality'.[167] Cyber operations that result in the theft, compromise or publication of electronic data – or the lack of adequate protection against them – could impair the right to health, especially if they erode individuals' trust in the confidentiality of their own personal data, disincentivising them from seeking healthcare services. Breaches of confidential patient data may have long-term effects on victims, such as fraud and social stigmatisation, as was the case with the 2019 data breach of Singapore's HIV registry.[168] This can ultimately lead to distrust in the healthcare sector as a whole, as found in a study conducted by the CyberPeace Institute in Kenya and Botswana.[169]

Finally, the realisation of the right to health depends on the *quality* of a health system, which is shaped by factors like its scientific and medical advancement, the presence of skilled personnel, the availability and resort to 'scientifically approved and unexpired drugs and hospital equipment, safe and potable water, and adequate sanitation'.[170] In light of the increased and increasing digitalisation of healthcare, such quality may nowadays be said to include the availability of and resort to state-of-the-art ICTs, cybersecurity tools, and skilled IT personnel, insofar as the state is able to put those in place.

166 CESCR General Comment 14 (n 26) para 12.
167 ibid para 12(b).
168 CyberPeace Institute, 'Playing with Lives' (n 16) 45, citing Snair and Henry (n 121) and 'LGBT+ people in Singapore "more fearful" after HIV data leak', The Economist Times CISO (30 January 2019) https://ciso.economictimes.indiatimes.com/news/lgbt-people-in-singapore-more-fearful-after-hiv-dataleak/67749845> accessed 7 January 2023.
169 CyberPeace Institute, 'Playing with Lives' (n 16) 45.
170 CESCR General Comment 14 (n 26) para 12.

Even when healthcare or related services (including IT services) are privatised, states are still bound by their positive human rights obligations. Thus, they must ensure that private actors entrusted with providing health services do not interfere with the enjoyment of the right to health, by threatening 'the availability, accessibility, acceptability and quality of health facilities, goods and services'.[171]

Importantly, the international legal framework on the right to health is not limited to duties borne out by a state towards individuals located on its territory but includes obligations with respect to the right to health of individuals located elsewhere, that is, in other states. As noted above, Article 12 ICESCR (like the Covenant more generally)[172] does not provide for any jurisdictional or territorial limitation to the obligations it places on states.[173] Thus, at the very least, states have an obligation to refrain from adopting or sponsoring measures that might jeopardize or impair the enjoyment of the right to health in other states.[174] Likewise, they must protect the enjoyment of the right to health of individuals by doing what they can to prevent non-state actors from harming or threatening such enjoyment in other states, insofar as feasible in the circumstances.[175]

171 ibid para 35.

172 See ICESCR art 2(1), which lays out the Convention's scope of application without referring to the concept of 'jurisdiction'.

173 Saul, Kinley and Mowbray (n 134) 992–993.

174 CESCR General Comment 14 (n 26) para 39; CESCR, 'General Comment No. 24 on state obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities' (10 August 2017) UN Doc E/C.12/GC/24 (hereafter 'CESCR General Comment 24') paras 27–29; Milanovic and Schmitt (n 10) 265; Saul, Kinley and Mowbray (n 134) 993. See also the International Commission of Jurists, Maastricht Principles on Extraterritorial Obligations of States in the area of Economic, Social and Cultural Rights (29 February 2012) Principle 13: 'states must desist from acts and omissions that create a real risk of nullifying or impairing the enjoyment of economic, social and cultural rights extraterritorially. The responsibility of states is engaged where such nullification or impairment is a foreseeable result of their conduct. Uncertainty about potential impacts does not constitute justification for such conduct.' See also Principles 20 and 21.

175 CESCR General Comment 14 (n 26) para 39; CESCR General Comment 24 (n 174) paras 30–33; Tobin and Barrett (n 131) 78; Saul, Kinley and Mowbray (n 134) 994. See also Maastricht Principles (n 174) Principle 24: 'All states must take necessary measures to ensure that non-state actors which they are in a position to regulate ... such as private individuals and organizations, and transnational corporations and other business enterprises, do

This is especially the case if the harmful conduct originates from their own territory but has effects abroad. If states have sufficient resources, they should also cooperate with other states to facilitate access to essential health services abroad, including by providing assistance when so required[176] and cross-border capacity-building.[177] International cooperation required as part of the duties to protect and fulfil the right to health also includes the conclusion of adequate international agreements—either aimed specifically at realising the right to health or, at the very least, ensuring that agreements do not interfere with the enjoyment of the right to health.[178]

As to the relevant standard of causation – for both positive and negative obligations – the Committee on the Rights of the Child, in rendering its views concerning harm caused by climate change and subsequent environmental damage to (inter alia) the claimants' right to health, held that 'the alleged harm suffered by the victims needs to have been reasonably foreseeable to the state party at the time of its acts or omissions even for the purpose of establishing jurisdiction'.[179]

V. The Right to Privacy

Whoever seeks or receives medical care is, by that very act, revealing something about themselves and inviting other people – particularly medical professionals and service providers – into their private life. This is such a sensitive matter that one of the pillars of medical ethics, Hippocrates' oath, makes doctors swear that

not nullify or impair the enjoyment of economic, social and cultural rights. These include administrative, legislative, investigative, adjudicatory and other measures. All other states have a duty to refrain from nullifying or impairing the discharge of this obligation to protect.'

176 CESCR General Comment 14 (n 26) para 39.

177 Denney-Turner (n 155).

178 CESCR General Comment 14 (n 26) para 39.

179 See e.g. Chiara Sacchi and others v Germany (Comm no 107/2019) (Children's Rights Committee, 22 September 2021) para 9.7.

> *All that may come to [their] knowledge in the exercise of [their] profession or outside of [their] profession or in daily commerce with men, which ought not to be spread abroad, [they] will keep secret and will never reveal.* [180]

Medical doctors may well be bound by confidentiality as a matter of professional deontology, but the whole healthcare enterprise exposes details of individuals' private life to a number of other actors. Medical care and treatment necessitate the sharing of sensitive information by the patient, and the collection of such information within the broadly defined healthcare system. It is therefore self-evident how cyber operations against healthcare – if they involve unauthorised access to said information – may interfere with, and harm, individuals' right to privacy.

This right, recognised already in the Universal Declaration of Human Rights (Article 12), is enshrined in Article 17 of the ICCPR, which holds that:

> *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks.*

The right to privacy is also protected by specialized international human rights treaties. These include the Convention on Migrant Workers (Article 14, affirming that '[n]o migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy…') and the Convention on the Rights of the Child (Article 16, for which '[n]o child shall be subjected to arbitrary or unlawful interference

180 E Wicks, Human Rights and Healthcare (Hart Publishing 2007) 124. See also Baroness Hale's opinion in Campbell v Mirror Group Newspapers Ltd [2004] UKHL 22, cited in Wicks (n 180) 125.

with his or her privacy…'), and by regional human rights treaties, like the ECHR (Article 8, which speaks of everyone's 'right to respect for his private and family life'), the ACHR (Article 11, establishing that '[n]o one may be the object of arbitrary or abusive interference with his private life…'), the Arab Charter on Human Rights (Article 21, by which '[n]o one shall be subjected to arbitrary or unlawful interference with regard to his privacy…') and the African Charter on the Rights and Welfare of the Child (Article 10, stating that '[n]o child shall be subject to arbitrary or unlawful interference with his privacy…'). All these instruments provide that beneficiaries have the right to be protected by law against prohibited interferences with their privacy.

Adequate protection of individuals' private life and, more generally, the full enjoyment of the right to privacy is a prerequisite for the fruition of other human rights, like the right not to be discriminated on grounds impermissible under international human rights law, or the rights to freedom of expression, association, and assembly. Similarly, the protection of the right to privacy is necessary for the enjoyment of the right to the highest attainable standard of health. As the provision of health services concerns very sensitive information about the individual, related to their dignity and some their most intimate features, fears that the confidentiality or anonymity of this information may be in jeopardy could result in the individual refraining from seeking medical attention and/or communicating sensitive information to health professionals.[181] In short, guaranteeing respect for and protection of the right to privacy is propaedeutic to the right to health, in that it preserves the confidence of individuals in the proper functioning and reliability of the healthcare system.[182] As noted above, concerns of this kind recently surfaced, for instance, in the United States after the overturning of the Supreme Court's *Roe v Wade* precedent on the right to abortion. It has been feared that women may stop using useful health-tracking apps or turning up to abortion clinics and rights groups, worrying that the confidentiality of

181 HRC, 'Right to Privacy in the Digital Age' (n 28) para 14.
182 Z. v Finland (App No 22009/93) (ECtHR, 25 February 1997) para 96.

the data collected therein may be compromised.[183]

A. Privacy, Personal Information, and Data Protection

In practice, protecting the privacy of individuals means protecting information that pertains to the individual person's private sphere. In fact, the protection of personal information constitutes the core, and least controversial, aspect of the protection of the right to privacy.[184] Such information can be extracted from data that has been collected about individuals, often voluntarily surrendered in exchange for access to certain goods, services or information.[185] The distinction between 'data' and 'information' is subtle: 'data' designates the object of interpretation, whilst 'information' represents what is perceived through interpretation.[186] Such provision of information, in the contemporary era, takes place through digital means constantly and continuously. Data is used by companies not only to provide services and goods but also to improve the quality of the services and goods they offer, to innovate, and to better target potential clients. At the same time, it is used by governments to enhance and inform practices of public administration, provide more tailored and higher quality public services, and strengthen national security. Data has effectively become an asset, a resource, not differently than capital or labour.[187] Nonetheless, with respect to data collection, processing, and use, the interests of individuals, companies, and governments are not always aligned.

It is, thus, no surprise that the UN Special Rapporteur on Privacy has identified

183 Chandran and Baptista (n 143). See also, with respect to a different kind of health app, L Eftychiou and C El Morr, 'Mobile Mental Health Virtual Communities: Challenges and Opportunities' in L Menvielle, AF Audrain-Pontevia and William Menvielle (eds), The Digitization of Healthcare (Palgrave MacMillan 2017) 266.
184 Wicks (n 180) 119.
185 HRC, 'Right to Privacy in the Digital Age' (n 28) para 18.
186 BJ Richards, M Taylor and SS Jacobson, Technology, Innovation and Healthcare: An Evolving Relationship (Edward Elgar 2022) 108. For the purposes of this report, the two concepts will be used as synonymous, for the sake of simplicity.
187 UNGA, 'Report of the Special Rapporteur on the Right to Privacy' (17 October 2018) UN Doc A/73/438 para 103.

the protection of personal information online as a priority.[188] Likewise, the 2022 'Declaration on the future of the Internet' – a programmatic document sponsored by the United States and recently signed by over 60 states[189] – committed signatories to strive to '[p]rotect individuals' privacy, their personal data, the confidentiality of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic and international law'. More importantly, binding legal instruments have been adopted nationally and internationally to attain such objectives. At the supranational level, prominent among them are the Council of Europe's Convention n. 108 on the automatic processing of data,[190] which was updated as recently as 2018,[191] and the European Union's General Data Protection Regulation (GDPR), which came into force in 2018.[192]

Thanks to these efforts by policy-makers and law-makers, the discourse on privacy online has become almost one and the same as the discourse on data protection and data governance. Confidentiality of personal data is seen as an indispensable ingredient in the realisation of individuals' right to privacy.[193] Of course, different jurisdictions and different legal instruments adopt different definitions of personal information or data, varying in scope. Yet, all seem to share the minimum common

188 HRC, 'Report of the Special Rapporteur on the Right to Privacy' (16 October 2019) UN Doc A/HRC/40/63 para 105.

189 US Bureau of Cyberspace and Digital Policy, 'Declaration for the Future of the Internet' (Policy Statement, 2022) <https://www.state.gov/declaration-for-the-future-of-the-internet> accessed 7 January 2023.

190 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985) ETS No 108.

191 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 18 May 2018) CETS No 223.

192 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016] OJ L/119/1. Because of the worldwide importance of the European market, and because of the so-called 'Brussels effect' according to which the GDPR has become the model for data governance legislation also in other states, this section will make reference to it when helpful to clarify how to implement the international human rights legal framework.

193 Richards, Taylor and Jacobson (n 186) 108.

denominator of designating information that either identifies or may reasonably identify an individual.[194] For instance, according to the GDPR,

> *… 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*[195]

In this context, and with respect to the present report, medical and health-related data assumes central importance. Whilst health data has also been generated by wearable devices like smartwatches and by direct-to-consumer services like genetic ancestry testing, the provision of healthcare remains one of the activities that produces the largest amounts of such data.[196] Use of data in healthcare has increased over time and is on an upward trajectory for the foreseeable future.[197] Medical data is of great interest not only for healthcare professionals and patients but also other stakeholders.[198] For instance, it is extremely valuable for pharmaceutical companies, since it may be used in the research and development of new treatments, including personalised ones, as well as to target clients.[199] As seen above, seeking and/or receiving medical attention means sharing intimate information with healthcare professionals and service providers, usually with the expectation that such data 'will be used to provide safe and effective

194 UN Doc A/73/438 (n 187) paras 58–59.
195 GDPR (n 192) art 4(1).
196 Richards, Taylor and Jacobson (n 186) 106.
197 ibid.
198 UN Doc A/HRC/40/63 (n 188) para 114.
199 C Boullenois, 'China's Data Strategy: Creating a State-Led Market' (European Union Institute for Security Studies Brief, October 2021) 5 <https://www.iss.europa.eu/content/chinas-data-strategy> accessed 7 January 2023.

care and not used inappropriately'.[200] Yet the growth in importance of health data is directly proportional to surging risks that personal information contained in such data become the object of unauthorised access or usage.[201] For instance, it has been noted how telemedicine creates dangers for patients' privacy, if the IT system used to administer it is compromised.[202] Considering how most data is stored for a long time and used asynchronously with respect to the moment in which it is collected, the risk of breaches for every concerned individual may span over a long time.[203] Considering that this information can be incredibly sensitive, breaches of the confidentiality of the relevant data may be cause for 'enormous concern'[204] not only for the privacy of the individuals to whom the data relates but also for their overall safety and dignity.

For those reasons, according to the GDPR, health data must be considered as a 'special category of data', whose processing is subject to heightened restrictions and protections.[205] Likewise, pursuant to Convention 108, the processing of health data must be accompanied by special safeguards established by law.[206] In recognition of health data's importance, the UN Special Rapporteur on the Right to Privacy, with help from a task force appointed for this specific purpose, issued a detailed 'Recommendation on the protection and use of health-related data', as a baseline or minimum standard of protection for health-related data by all states—regardless of whether they are already bound by data protection legislation or whether they are yet to develop it. According to the Recommendation, '"health-related data" means all personal data

200 Richards, Taylor and Jacobson (n 186) 106.
201 Botrugno (n 2) 154.
202 A Loute and JP Cobbaut, 'What Ethics for Telemedicine?' in Loick Menvielle, AF Audrain-Pontevia and W Menvielle (eds), The Digitization of Healthcare (Palgrave MacMillan 2017) 402.
203 M Mrcela and I Vuletic, 'Healthcare, Privacy, Big Data and Cybercrime: Which One Is the Weakest Link?' (2018) 27 Annals of Health Law 257, 258–259.
204 UNGA, 'Report of the Special Rapporteur on the right to privacy' (5 August 2019) UN Doc A/74/277 para 3.
205 GDPR (n 192) art 9.
206 ETS No 108 (n 190) art 6. See also UNGA, 'Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci' (27 July 2020) UN Doc A/75/147 para 32.

concerning the physical or mental health of an individual, including the provision of health-care services, that reveal information about the individual's past, current and future health', including genetic data.[207] A health-related data breach is defined as 'the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or prevention of lawful access to (including unlawful lock-in practices), or sale of, health-related data transmitted, stored or otherwise processed', with the notable exception of intentional lawful destruction.[208] Different types of malicious cyber operations carried out against healthcare infrastructure – as it will be explained below – may easily result in such breaches.

B. Negative and Positive Obligations to Respect, Protect and Fulfil the Right to Privacy

How does international human rights law protect individuals' privacy, especially with respect to personal data collected and/or used in the provision of healthcare services? At the outset, it must be noted that 'any capture of communications data is potentially an interference with privacy and, [...] the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used'.[209] Nonetheless, the right to privacy is a relative one and, therefore, individual's privacy may be subject to interference, provided that it is not 'unlawful' or 'arbitrary'. The prohibition of 'unlawful' interference with privacy implies that such interference may only lawfully occur if envisaged by law.[210] The qualifier 'arbitrary' was added because, even when an interference is envisaged by law, it must still accord with 'the provisions, aims and objectives of the Covenant and

207 UN Doc A/74/277 (n 204) Annex, Recommendation para 3.
208 ibid.
209 HRC, 'Right to Privacy in the Digital Age' (n 28) para 20.
210 HRC, 'General Comment No. 16 - Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc HRI/GEN/1/Rev.9 191ff (hereafter 'CCPR General Comment 16') para 3.

should be, in any event, reasonable in the particular circumstances'.[211] According to the HRC, this means that 'the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant'.[212] The text of the ECHR is even clearer, in that it states that an interference with the right to privacy may be lawful insofar as 'as [it] is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.[213] Thus, the test for the lawfulness of an interference with privacy is fourfold: an interference is lawful only where it is provided by law, pursues a legitimate public aim (such as those exhaustively listed in Article 8(2) ECHR), and is necessary and proportionate to achieve this aim.[214]

As with many other human rights obligations, the state is not only obliged to refrain from interfering with privacy itself but must also adopt positive measures to protect this right against unlawful interference from third parties, and to ensure that beneficiaries enjoy said right.[215] States must ensure the practical and effective protection against unauthorised access of personal information and medical data – inter alia – of individuals who have been tested, infected, treated or subjected to clinical trials.[216] To this end, the HRC has reiterated that '[t]he gathering

211 ibid 4; HRC, 'Right to Privacy in the Digital Age' (n 28) para 21.
212 CCPR General Comment 16 (n 210) para 7.
213 ECHR art 8(2).
214 UN Doc A/HRC/40/63 (n 188) para 18; HRC, 'Surveillance and Human Rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (28 May 2019) UN Doc A/HRC/41/35 para. 24; HRC, 'Right to Privacy in the Digital Age' (n 28) paras 21–30.
215 See CCPR General Comment 16 (n 210) para 10 and, in the ECHR system, X and Y v the Netherlands (App no 8978/80) (ECtHR, 26 March 1985) para 23; Bărbulescu (n 10) para 108; Hämäläinen v Finland (App no 37359/09) (ECtHR 16 July 2014) para 62; Nicolae Virgiliu Tănase v Romania (App no 41720/13) (ECtHR, 25 June 2019) para 125.
216 I. v Finland (App. No. 20511/03) (ECtHR, 17 July 2008) paras 37–47; Z. (n 182) para 95.

and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law'.[217] Legal protection of the right to privacy through data regulation should include, inter alia, the possibility for every individual to verify whether and what personal data is stored in automatic data files, for what purposes and which public authorities or private entities may control such files, the right to request rectification or elimination of incorrect or unlawfully collected or processed personal data,[218] effective and independent oversight mechanisms,[219] and opportunities for effective remedy in case of violations.[220]

With specific respect to health-related data, the UN Special Rapporteur on Privacy has explicitly affirmed that medical confidentiality is an essential component of the human right to privacy.[221] This includes personal information disclosed to healthcare professionals when seeking or receiving medical treatment of health services.[222] Patients also have a right to be accurately and transparently informed by healthcare professionals about how their personal information will be processed and used.[223] Due to the digitalization of healthcare, more and more data is being produced. This results in more complete patient profiles, easier sharing of data between healthcare professionals, and, overall, better health information.[224] But the flipside is that 'the confidentiality and protection of [patients'] health-related data in electronic health record systems must be rigorously managed',[225] processed and shared

217 CCPR General Comment 16 (n 210) para 10.
218 ibid. cf the stance taken by the Court of Justice of the EU (CJEU) in Case C-131/12 Google Spain v AEPD and Mario Costeja González [2014] OJ C212/4 paras 89–99. cf also Articles 16 and 17 of the GDPR (n 192).
219 UNGA Resolution 68/167 (21 January 2014) UN Doc A/RES/68/167 para 4(d).
220 HRC, 'Right to Privacy in the Digital Age' (n 28) paras 39–41; CCPR General Comment 16 (n 210) para 11. See also UN Doc A/74/277 (n 204) Annex, Recommendation paras 12.3 and 31.3.
221 UN Doc A/HRC/40/63 (n 188) para 112. See also Wicks (n 180) 119.
222 Z. (n 182) 95-96.
223 UN Doc A/HRC/40/63 (n 188) para 111.
224 UN Doc A/75/147 (n 206) para 29.
225 UN Doc A/74/277 (n 204) Annex, Recommendation para 18.1.

only according to 'the highest legal and ethical standards'.[226] Such data processing should also be subject to appropriate verification and auditing processes.[227] Of course, individuals are entitled to give up part of their privacy by sharing personal data and allowing for their collection and processing, even by electronic means, as they routinely do to receive medical goods, services, and information.[228] However, individuals' consent to the sharing and processing of personal data must consist of 'a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to her or him, such as by a written statement, including by electronic means, or an oral statement'.[229]

C. Threats to Privacy by Means of Cyber Operations against the Healthcare Sector

When assessing potential breaches of individual privacy, a common focus for international human rights law scholarship is on the threat posed by mass surveillance put in place by governments territorially and, at times, extraterritorially.[230] Any such operation by digital means, including when it concerns healthcare systems, may constitute an unlawful interference with victims' right to privacy.

226 UN Doc A/HRC/40/63 (n 188) para 113.
227 UN Doc A/74/277 (n 204) Annex, Recommendation para 13.3.
228 HRC, 'Right to Privacy in the Digital Age' (n 28) para 18.
229 UN Doc A/74/277 (n 204) Annex, Recommendation para 3. See also L Williatte, 'Use of New Information and Communication Technologies in the Health Sector: The Legal Reason for Differences Between International and European Standards' in L Menvielle, AF Audrain-Pontevia and W Menvielle (eds), The Digitization of Healthcare (Palgrave MacMillan 2017) 390.
230 See e.g. M Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 81; A Deeks, 'An International Legal Framework for Surveillance' (2014) 55 Virginia Journal of International Law 291; V Rusinova, 'Privacy and the Legalisation of Mass Surveillance: In Search of a Second Wind for International Human Rights Law' (2022) 26 The International Journal of Human Rights 740; K Lachmayer and N Witzleb, 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective Thematic: Communications Surveillance, Big Data and the Law' (2014) 37 University of New South Wales Law Journal 748.

In general, any intrusion into a healthcare ICT infrastructure, with unauthorized access to personal information, can be deemed a violation of individuals' right to privacy. It has been estimated that, from 2005 to 2019, the personal data of about 250 million individuals were affected by healthcare data breaches,[231] with this number increasing every year.[232] Single incidents may interfere with the right to privacy of millions of individuals at a time. To give one example, an intrusion into the UCLA Health System's computer network, discovered in 2015, exposed sensitive information of as many as 4.5 million patients.[233]

Hacking incidents – by means of ransomware, credential-stealing malware, or other means – are one of the most common threats against personal health-related data,[234] and have been rapidly increasing over the past few years.[235] Ransomware, in particular, may have devastating consequences for individual privacy when they threaten to release personal information if the ransom request is not met. For instance, the data of at least 520 patients were published online in the aftermath of the 2021 ransomware operation against the Irish Health Service Executive.[236] Breaches directly aimed at the theft of data in the healthcare system are all but uncommon. Medical data, for example patients' complete record files, are extremely valuable on the black market and, therefore, constitute a very enticing target for criminal hackers.[237] Furthermore, data collected for medical treatment are often

231 AH Seh et al 'Healthcare Data Breaches: Insights and Implications' (2020) 8(2) Healthcare 133.s 1.","plainCitation":"Adil Hussain Seh and others, 'Healthcare Data Breaches: Insights and Implications' (2020

232 Health Insurance Portability and Accountability Act (HIPAA) Journal, 'Healthcare Data Breach Statistics' (2022) <https://www.hipaajournal.com/healthcare-data-breach-statistics/> accessed 7 January 2023.

233 C Terhune 'UCLA Health System data breach affects 4.5 million patients' Los Angeles Times (17 July 2015) <https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html> accessed 7 January 2023.

234 Seh et al (n 231) Section 4.

235 ibid 6.

236 C Gallagher, 'HSE confirms data of 520 patients published online' The Irish Times (28 May 2021) <https://www.irishtimes.com/news/crime-and-law/data-of-520-patients-published-online-hse-confirms-1.4578136> accessed 7 January 2023.

237 Seh et al (n 231) Section 4.2.1.

stored for a long time for reasons of documentation or research, at times for decades,[238] increasing the risk that such data be eventually accessed by unauthorised entities.[239]

When medical research is subject to espionage or data theft, personal information may be exposed and individuals' privacy violated. Although much controversy exists as to whether espionage per se, including by cyber means, is prohibited under international law, there is growing support for the view that certain types of data access and theft are or ought to be prohibited by international law, including by international human rights law.[240] For instance, members of the G20 recently affirmed that:

> *no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.*[241]

Alarmingly, often individuals are not even aware that their privacy has been breached. To redress such problem, the GDPR (Article 33) and Convention 108 (Article 7(2)) require EU member states and parties, respectively, to ensure that the competent supervisory authority is notified of personal data breaches 'unless [they are] unlikely to result in a risk to the rights and freedoms of natural persons' (GDPR), and of 'those data breaches which may seriously interfere with the rights and

238 UN Doc A/HRC/40/63 (n 188) para 119.
239 In this sense, among others, Mrcela and Vuletic (n 203) 258–259.
240 See A Coco, T Dias and T van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) European Journal of International Law (forthcoming, advance copy available at <https://doi.org/10.1093/ejil/chac063>).
241 'G20 Leaders' Communiqué', (Antalya, 16 November 2015) para 26 <https://pm.gc.ca/en/news/statements/2015/11/16/g20-leaders-communique> accessed 7 January 2023.

fundamental freedoms of data subjects' (Convention 108). Arguably, these types of provisions are conducive to the protection of the right to privacy under international human rights law. In addition, Article 34 of the GDPR establishes that '[w]hen the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay'. Yet other legal instruments, especially national ones, often lack clear guidelines or rules as to whether – and, if so, how promptly and precisely – the data subjects concerned and the general public needs to be informed of data breaches.[242] To reduce the dangers of long-term data retention, which exposes personal information to unlawful interference over time, the Special Rapporteur on the Right to Privacy has recommended that states adopt continuous deletion programmes, or 'sunset clauses' to ensure that personal data is not held for longer than needed.[243]

It is paradoxical, however, that cybersecurity practices to protect against malicious cyberoperations directed at the healthcare sector may carry their own risk for the right to privacy. Cybersecurity incident reporting procedures must not themselves constitute an unlawful interference with the privacy of the individuals concerned. Likewise, the confidentiality of their personal data must not be unduly compromised in the process of the responding to a potential cyber incident.

VI. The Rights to Freedom of Expression and Information

The right to freedom of expression is recognised in several human rights treaties.[244] For instance, Article 19(2) of the ICCPR, which is thought to reflect customary international law,[245] stipulates that

242 UN Doc A/HRC/40/63 (n 188) para 139.
243 UNGA, 'Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci' (23 July 2021) UN Doc A/76/220 paras 112(n), 112(o).
244 See ICCPR art 19 ICCPR; ECHR art 10; ACHR art 13 ACHR, and ACHPR art 9.
245 A Lowe, 'Customary International Law and International Human Rights Law: A Proposal for the Expansion of the Alien Tort Statute' (2013) 23 Indiana International and Comparative Law Review 523, 535, 537.

> *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.* [246]

As the text of this provision indicates, the right includes not only freedom of expression per se but also freedom of information, that is, the right to seek and receive information.[247] Neither limb of the right can be territorially bound, since information itself is not physical and can be easily transmitted to individuals located abroad by using different means of communication.[248] This arguably means that any requirement of jurisdiction ought to be effectively extraterritorial in the context of this right, at the very least with respect to negative duties arising therefrom. Likewise, the types of information and media covered are not limited in any way.[249] This means that any type of information, views or ideas is *in principle* protected, 'including those that may shock, offend or disturb, and irrespective of the truth or falsehood of the content'.[250] There is also no question that the rights to freedom of expression and information

246 Emphasis added.

247 See Gauthier v Canada (Comm no 633/1995) (HRC, 7 April 1999) paras 13.4–13.5.

248 See Milanovic and Schmitt (n 10) 268–269; UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression And "Fake News", Disinformation and Propaganda' (3 March 2017) (hereafter 'Joint Declaration') para 1(c) <https://www.osce.org/files/f/documents/6/8/302796.pdf> accessed 7 January 2023; HRC, 'General comment No. 34 - Article 19: Freedoms of opinion and expression' (12 September 2011) UN Doc CCPR/C/GC/34 (hereafter 'CCPR General Comment 34') para 11.

249 CCPR General Comment 34 (n 248) paras 11–12; Nowak (n 38) 443–444.

250 UN Doc A/HRC/47/25 (n 164) para 38, citing CCPR General Comment 34 (n 248) paras 11, 47, 49; Handyside v the United Kingdom (App no 5493/72) (ECtHR, 7 December 1976) para 49; Salov v Ukraine (App no 65518/01) (ECtHR, 6 September 2005) para 113 (noting that "Article 10 of the [ECHR] does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful"). See also Joint Declaration (n 248) preambular para 7.

apply online as they do offline.[251]

Different cyber operations against the healthcare sector may engage these rights in a variety of circumstances.[252] The most obvious examples are misinformation and disinformation campaigns as well as other information operations, that is, 'any coordinated or individual deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience'.[253] As will be discussed further, while in principle protected forms of expression, these operations may affect the right of audiences to seek, receive and even impart information.[254] Disruptive cyber operations and data breaches against the healthcare sector may also engage the rights to freedom of expression and information. For one thing, individuals are entitled to have access to relevant information about those cyber operations, especially considering their actual and potential impact on the healthcare sector and human health more generally. For another, when responding to such operations, states must not unduly restrict the rights of individuals – whether victims or the general public – to receive, seek or impart information.

In what follows, we assess these and other situations where cyber operations against the healthcare sector may have a bearing on the rights to freedom of expression and information. To do so, we tackle two core issues: a) states' negative obligations to respect the rights to freedom of expression and information and how they interact with states' positive duties to protect life, health and privacy in the context of different cyber operations; and b) states' positive obligations to protect freedom of expression and information in the health context, including the extent to which individuals have a right to receive true information.

251 UN Doc A/HRC/47/25 (n 164) para 37.
252 See Milanovic and Schmitt (n 10) 272–279.
253 ELAC, 'Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' (2021) preambular para 3 <https://elac.web.ox.ac.uk/the-oxford-Statement-on-the-regulation-of-information-operations-and-activities> accessed 7 January 2023; van Benthem, Dias and Hollis (n 10) 1218, footnote 1.
254 UN Doc A/HRC/47/25 (n 164) paras 2, 49.

A. Negative Obligations to Respect the Rights to Freedom of Expression and Information

As discussed earlier, states have positive duties to protect the rights to life, health, and privacy from the harmful effects of cyber operations. This may include an obligation to supress certain types of health misinformation or disinformation that threaten the life or health of individuals.[255] Likewise, to effectively prevent and respond to certain disruptive cyber operations or data breaches against hospitals and other health institutions, states may need to act in secrecy, keeping entire operations or some of their details hidden from the public eye. The protection of sensitive research or confidential patient data also requires states to restrict the information available to the public. Thus, the question arises as to how states may reconcile the protection of life, health, and privacy with their duties to *respect* individuals' rights to seek, receive and impart information.

This negative duty entails first and foremost that states may not interfere with individuals' free expression and access to information, online or offline.[256] Yet these rights are not absolute — if they were, the achievement of key societal aims would be arguably difficult, if not impossible.[257] Thus, Article 19(3) of the ICCPR, for example, states that:

> *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> *(a) For respect of the rights or reputations of others;*
>
> *(b) For the protection of national security or of public order (ordre*

255 Milanovic and Schmitt (n 10) 274.
256 CCPR General Comment 34 (n 248) para 7; Nowak (n 38) 440–441, 443, 446.
257 Nowak (n 38) 449, 456–458.

> *public), or of public health or morals.* [258]

Similar provisions are found in Article 10(2) of the ECHR and Article 13(2) of the ACHR. In essence, they all recognise that the rights to freedom of expression and information may be limited in some circumstances where the public interest so demands, but only in line with strict requirements.[259] These make up the so-called 'tripartite test' of legality, legitimacy, and necessity.[260]

Legality stands for the requirement that any limitation on freedom of expression and information be grounded in law. While 'law' is not synonymous with written law,[261] it does imply adoption by an independent legislative body.[262] 'Law' must also be accessible and foreseeable to an ordinary person.[263] Legitimacy refers to the different public interest grounds that may justify a restriction on freedom of expression or information.[264] Though the list of legitimate grounds is exhaustive in the ICCPR, ECHR and ACHR, each ground is broad and flexible enough to accommodate a variety of public interests in different states, provided that their interpretation is consistent with other human rights, particularly non-discrimination.[265] Two such grounds are public health and the rights of others, which include the rights to life and privacy.[266] The 'rights of others' also comprise the rights to freedom of expression and information of other individuals,[267] whose protection

258 Emphasis added.
259 See EM Aswad 'To Protect Freedom of Expression, Why Not Steal Victory from the Jaws of Defeat?' (2020) 77(2) Washington and Lee Law Review 609, 622.
260 ibid 618.
261 KJ Partsch 'Freedom of conscience and expression, and political freedoms' in L Henkin (ed), The International Bill of Rights: The Covenant on Civil and Political Rights (Columbia University Press 1981) 220.
262 CCPR General Comment 34 (n 248) para 24.
263 ibid para 25.
264 Aswad, 'To Protect Freedom of Expression' (n 259) 625.
265 CCPR General Comment 34 (n 248) paras 26, 32.
266 ibid para 28.
267 Nowak (n 38) 463.

will be assessed in the following subsection. Finally, necessity refers to the least restrictive means to achieve the legitimate aim in question and includes an assessment of the proportionality between the means chosen and the aim sought.[268]

Applying the tripartite test means that limitations on the freedoms of expression and information must be exceptional, grounded in sufficiently clear laws, and well-calibrated to the importance of the legitimate aim justifying their adoption.[269] This is necessarily a case-by-case assessment that depends on specific factual circumstances, particularly the content of the speech and the broader societal context in which it is disseminated.[270]

The negative duty to respect the rights to freedom of expression and information constrains any measure that states might adopt to prevent, stop, or redress cyber operations against the healthcare sector that might interfere with said rights.[271] And it is the tripartite of legality, legitimacy, and necessity that must guide any balancing act between the protection of health, life, privacy, and other relevant rights or interests, on the one hand, and the limitations that such protection will entail on the rights to freedom of expression and information, on the other hand. For example, when adopting measures to curb the harmful effects of misinformation and disinformation on the rights to life and health, states must ground them in accessible and foreseeable laws, which must be necessary and proportionate to the aims of protecting life and health in the particular circumstances at hand.[272] As noted by the special rapporteurs and representatives for freedom of expression of different international and regional institutions on various occasions, this means that general prohibitions on the dissemination of false information – or other information operations for that matter – would be

268 CCPR General Comment 34 (n 248) paras 33–36.
269 ibid para 21.
270 Milanovic and Schmitt (n 10) 268, 277.
271 ibid 272, 274–279.
272 ibid 275.

inherently disproportionate.[273] Instead, to ensure that the fight against health misinformation and disinformation is consistent with the rights to freedom of expression and information, states must enact specific laws or regulations clearly laying down a) what types of speech acts are subject to limitations, and b) what kinds of limitations to such acts will be adopted.[274] As one of us has argued elsewhere, when it comes to the freedoms of expression and information, legality applies not only to the *behaviour* constrained but also to *how* it is constrained: individuals must not only have notice of what they cannot say online or offline but also the consequences of disregarding those limitations.[275]

Furthermore, even if grounded in clear laws enacted to protect the healthcare sector from malicious cyber operations, any restrictions on misinformation and disinformation must be necessary and proportionate to achieve that aim in the circumstances. This means that before outlawing health misinformation or disinformation, states must consider if other, less restrictive measures, such as the dissemination and prioritisation of verifiable information from official sources such as the WHO, the labelling of different types of content as verifiable or not, or the use of digital nudges to redirect users to such types of content, could achieve the same aim.[276] In many societies, especially those with a more robust information environment and resilient audiences, health misinformation and disinformation can be effectively curbed by ensuring

273 Joint Declaration (n 248) para 2(a). See also Milanovic and Schmitt (n 10) 275–277; Amnesty International, 'Silenced and misinformed: Freedom of expression in danger during Covid-19' (19 October 2021) <https://www.amnesty.org/en/documents/pol30/4751/2021/en/> accessed 7 January 2023, 34.

274 See van Benthem, Dias and Hollis (n 10) 1246; UN Doc A/HRC/47/25 (n 164) paras 40–41; UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (9 October 2019) UN Doc A/74/486 paras 31–32.

275 T Dias, 'Hate Speech and the Online Safety Bill: Ensuring Consistency with Core International Human Rights Instruments' (Evidence Submission to the UK House of Commons Digital, Culture, Media and Sport Sub-committee on Online Harms and Disinformation, September 2021) 6–8, 9–15 <https://committees.parliament.uk/writtenevidence/38393/pdf/> accessed 7 January 2023.

276 E Douek, 'Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability' (2021) 121(3) Columbia Law Review 759, 826.

the free flow of and access to accurate information.[277] Where this is the case, and audiences voluntarily follow official health information whilst spotting and discrediting harmful misinformation and disinformation, the prohibition of these and other information operations will be unnecessary. Still, any other restrictions on speech acts, such as digital nudges and labels, must still be provided by law and well-calibrated to the seriousness of the speech acts they target. This means that, in the fight against health misinformation and disinformation, adopting a basic legal framework for content regulation or moderation is imperative. This is true whether such measures are mandated by public authorities or private entities insofar as states have duties to both respect and protect the freedoms of expression and information, as will be discussed below.

In less resilient societies, where less stringent measures such as the dissemination of official information are an insufficient antidote to health misinformation and disinformation, it may be necessary to tackle the problem by adopting stricter measures, such as legal prohibitions. Even so, those prohibitions should be calibrated to the harms sought to be curbed. This means that the criminalisation of information operations, even when they affect life and health, should be reserved to only the most serious types of speech acts.[278] As noted by the HRC and different UN Special Rapporteurs for Freedom of Expression in the context of online hate speech, criminalisation of expression should be limited to cases where there is, at the very least, an intention to cause harm and an imminent risk of violence or serious harm resulting from the speech act.[279] At the same time, it would almost invariably be disproportionate to prohibit or impose any form of liability, whether civil or criminal, on misinformation, that is, the non-intentional dissemination of false

277 Amnesty International (n 273) 7.
278 Milanovic and Schmitt (n 10) 278.
279 UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (7 September 2012) UN Doc A/67/357 para 46; HRC, 'Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred' (11 January 2013) UN Doc A/HRC/22/17/Add.4 para 29.

or misleading information by individuals.[280] Yet this does not mean that states or their agents may disseminate or promote information that they know or should have known is false or misleading.[281] Quite the contrary. As will be discussed in the next subsection, states have a positive obligation to promote accurate information as part of their duty to protect the right of individuals to freedom of information.[282]

Other extreme measures, such as prior censorship through content-filtering systems, Internet shutdowns, and blanket intermediary liability, would likely be disproportionate means to fight health-related information operations. Prior censorship turns free expression into an exception, jeopardising the right itself.[283] It removes an individual's ability to have their speech acts assessed in context, including the extent to which any limitations thereto are necessary for and proportionate to the legitimate aim sought.[284] Internet shutdowns are inherently indiscriminate, affecting entire states or regions rather than particular types of speech acts, as required by the necessity test.[285] Intermediary liability, that is, the imposition of liability for the mere hosting of content, would result in third parties being liable for the speech acts of others. Arguably, this measure would only be necessary and proportionate when intermediaries are required by relevant authorities to act upon certain pieces of unlawful content yet fail to do so in a reasonable amount of time.[286] But it remains contested whether and to what extent online

280 Joint Declaration (n 248) para 1(e).
281 ibid 2(c).
282 Milanovic and Schmitt (n 10) 272; UN Doc A/HRC/47/25 (n 164) paras 88, 93.
283 See CCPR General Comment 34 (n 248) para 21 (noting that "the relation between right and restriction and between norm and exception must not be reversed"); Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism, Advisory Opinion OC-5/85 (IACHR, Series A No 5) (13 November 2985) (hereafter 'Compulsory Membership') para 38.
284 Nowak (n 38) 457; Joint Declaration (n 248) para 1(g); UN Doc A/74/486 (n 274) para 34.
285 UN Doc A/HRC/47/25 (n 164) paras 51, 85; Milanovic and Schmitt (n 10) 278–279.
286 Joint Declaration (n 248) para 1(d); UN Doc A/74/486 (n 274) paras 30-33; Delfi AS v Estonia [GC] (App no. 64569/0916) (ECtHR, 16 June 2015) paras 140–162.

platforms are mere intermediaries or actual content curators,[287] given the role of their ranking and recommendation algorithms in promoting or demoting third-party content.[288]

The same tripartite test for assessing the lawfulness of limitations on speech applies when states interfere with the rights to receive, seek and impart information to curb other types of cyber operations, including disruptive operations and data breaches. As noted earlier, in an effort to prevent, stop, or respond to such operations, states may encroach upon the right of individuals to impart, seek and receive information about certain matters. This could happen, for example, when confidential cybersecurity or cyber hygiene measures are put in place, requiring the imposition of limits on the accessibility and disclosure of sensitive information, including through legal prohibitions.

To be consistent with states' negative obligations to respect the rights to freedom of information and expression, these restrictive measures must be grounded in sufficiently clear laws, adopted for a legitimate purpose, such as the protection of life, health or national security, and put in place in a necessary and proportionate manner. Thus, to avoid unlawful interference with the freedoms of expression and information whilst fighting cyber operations against the healthcare sector, such as ransomware or DDoS operations, states must enact cybersecurity laws that include the prevention of or responses to such operations as grounds for ostensive or covert cyber measures. Pandemic preparedness is an example of such a

287 See Case of Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary (App. No. 22947/13) (ECtHR, 2 February 2016) para 79; Council of Europe, 'Recommendation CM/Rec(2011)7 on a new notion of media' (21 September 2011) para 7, and Appendix, paras 20–21, 26, 29–36 <https://edoc.coe.int/en/media/8019-recommendation-cmrec20117-on-a-new-notion-of-media.html> accessed 7 January 2023; EM Aswad, 'The Future of Freedom of Expression Online' (2018) 17 Duke Law and Technology Review 26, 55; T Gillespie, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media (Yale University Press, 2018) 206.

288 See Douek (n 276) 797; UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (28 August 2018) UN Doc A/73/348 para 12.

legitimate ground that needs to be clearly laid out in law. Preventive or responsive cyber strategies must also be tailored to the seriousness of the health or cyber threat as well as the importance of combatting it.

B. Positive Obligations to Protect the Rights to Freedom of Expression and Information

While states' duties to protect life, health, privacy, and other fundamental human rights might clash with individuals' rights to freedom of expression and information, the protection of both sets of rights may also converge. This is because the freedoms of expression and information entail not only negative state obligations but also positive duties to protect those rights from interference by third parties, including by other individuals.[289] In the words of the IACHR, those rights have a dual individual and social or collective dimension that must be simultaneously upheld.[290] The former safeguards individual expression from state interference.[291] The latter requires states to take action to protect such individual freedom. It is grounded in the idea that freedom of expression is a means for the exchange of ideas and information, and for mass communications among human beings.[292]

Thus, during health crises, including in the context of cyber operations against the healthcare sector, positive obligations arising from the rights to health, life, and the freedoms of expression and information come together to require states to ensure the free flow of accurate health-related information.[293] As noted by Amnesty International with respect to the COVID-19 pandemic

289 See ICCPR art 2(1); CCPR General Comment 34 (n 248) para 7; Nowak (n 38) 440–441.
290 Compulsory Membership (n 283) paras 30, 33.
291 ibid para 31.
292 ibid para 32. See also Nowak (n 38) 438–440.
293 UN Doc, A/HRC/47/25 (n 164) para 38; Joint Declaration (n 248) paras 3(a), 3(d); Milanovic and Schmitt (n 10) 274-275, 278; Council of Europe's Committee of experts on media environment and reform (MSI-REF), 'Mitigating a global health crisis while maintaining freedom of expression and information' (2020) 1 <https://rm.coe.int/en-mitigating-a-global-health-crisis-while-maintaining-freedom-of-expr/16809e2d1e> accessed 7 January 2023.

> *A free flow of accurate, evidence-based and timely information ensures higher levels of awareness about health risks and how to deal with them, fosters trust in and compliance with public health guidelines, and enables civil society to hold governments accountable for their policy responses and their effects on different sectors of society.* [294]

This duty includes, in particular, the publication of corrections and clarifications as more information becomes available about health risks and impacts, which may prompt changes in government responses to health crises.[295] As seen earlier, states must also refrain from spreading information that they know or should have known is false or misleading, including in the context of health crises.[296] But the question remains as to whether and to what extent individuals have the right to receive truthful information.

Some commentators as well as the ECtHR's case law do suggest that individuals have a right to be 'properly informed' and thus to receive accurate or truthful information.[297] However, even if this is the case, it does not mean that states must necessarily prohibit, sanction or successfully curb the dissemination of false or misleading information. As seen earlier, the right to receive, seek and impart information is not limited to accurate or truthful information, and individuals are not generally precluded from spreading lies.[298] This is especially important

294 Amnesty International (n 273) 7.
295 MSI-REF (n 293) 1.
296 Joint Declaration (n 248) para 2(c); UN Doc A/HRC/47/25 (n 164) para 88.
297 Partsch (n 261) 219; Nowak, (n 38) 446, 459; The Sunday Times v United Kingdom (App no 6538/74) (ECtHR, 26 April 1979) para 66; NIT S.R.L v Moldova [GC] (App no 28470/12) (ECtHR, 5 April 2022) para 192; Manole and others v Moldova (App no 13936/02) (ECtHR, 17 September 2009) para 100; Verlagsruppe News GMBH v Austria (no 2) (App no 10520/02) (ECtHR, 14 December 2006) (Separate Opinion of Judge Herndl) para 1; Observer and Guardian v United Kingdom (App no 13585/88) (ECtHR, 26 November 1991) (Separate Opinion of Judge Morenilla) para 7; and Rashkin v Russia (App no 69575/10) (ECtHR, 7 July 2020) (Separate Opinion of Judge Elosegui) para 17.
298 CCPR General Comment 34 (n 248) para 49; UN Doc A/HRC/47/25 (n 164) para

with respect to scientific matters, such as in the health and technology contexts, where the truth might be contested or is constantly evolving.[299]

What a right to be properly informed does entail is a positive duty on the part of states to ensure a plural, independent and robust media and information environment, favourable to public debate and critique.[300] This includes a duty to promote accurate information.[301] Likewise, states must ensure access to diverse content and media, as well as prevent media concentration.[302] States also have a heightened responsibility to ensure that journalists inform society about the truth in an impartial and objective manner, given their special roles as public watchdogs.[303] As with other positive human rights obligations, these are not obligations of result, but ones of due diligence, that is, duties to exercise one's best efforts towards achieving a certain aim.[304] Thus, the obligation to protect the rights to freedom of expression and information requires states to exercise their best efforts to prevent and mitigate the impact of misinformation and disinformation in society, including during health crises.[305] Yet, in doing so, they must still respect the rights of other

38; Salov (n 250) para 113; Milanovic and Schmitt (n 10) 275–276; Amnesty International (n 294) 39.

299 Milanovic and Schmitt (n 10) 276; Amnesty International (n 294) 27; The Royal Society, The online information environment: Understanding how the internet shapes people's engagement with scientific information (Report, January 2022) 8 <https://royalsociety.org/-/media/policy/projects/online-information-environment/the-online-information-environment.pdf?la=en-GB&hash=691F34A269075C0001A0E647C503DB8F> accessed 7 January 2023.

300 Joint Declaration (n 248) preambular para 9; CCPR General Comment 34 (n 248) paras 14, 40; Dink v Turkey (App nos 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09) (ECtHR, 14 September 2010) para 137.

301 Milanovic and Schmitt (n 10) 272; UN Doc A/HRC/47/25 (n 164) paras 38, 88, 93.

302 HRC, 'General Comment No. 10: Article 19 (Freedom of Opinion" (29 June 1983) (hereafter 'CCPR General Comment 10') para 2; UN Doc A/HRC/47/25 (n 164) para 38; NIT S.R.L (n 297) paras 101, 185; Centro Europa 7 S.R.L. and Di Stefano [GC] (App no 38433/09) (ECtHR, 7 June 2012) paras 129–30.

303 See UN Doc A/67/357 (n 279) paras 72, 90; Milanovic and Schmitt (n 10) 275.

304 See generally Coco and Dias, 'A Patchwork of Protective Obligations' (n 70) 795–797.

305 See Özgür Gündem v Turkey (App no 23144/93) (ECtHR, 16 March 2000) para 43 (noting that 'The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States, the difficulties involved in policing modern societies and the choices which must be made in terms of priorities and resources.

individuals to freedom of expression and information, including by applying the tripartite test described above.[306]

The duty to protect the rights to freedom of expression and information also does not entail an obligation to ensure that *all* sorts of ideas and information have a platform or to grant *every* individual a right to express themselves in the media of their choice, public or private.[307] Dictating who can publish and what they can publish would impose on states an unsurmountable burden.[308] At the same time, ensuring a diverse, plural, and robust media environment may require the imposition of certain limits on public and private media, which, once again, must be provided by law, legitimate, and necessary. For instance, effective measures such as a basic legal and administrative framework guaranteeing media pluralism might be necessary to prevent control of the media as would interfere with the right of everyone to freedom of expression and information.[309] Other examples include TV broadcasting and radio licensing regulations, as well as professional journalistic standards.[310] Whether and to what extent those limitations might be required is always highly contextual. As noted by the ECtHR in *NIT v Moldova*:

> *Diversity is sometimes best achieved when people can freely enter the "marketplace of ideas" without any governmental constraints; at other times and in other places, the survival of various political views and cultural values necessitates state intervention.*[311]

Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities').

306 See UN Doc A/HRC/47/25 (n 164) paras 39–42; Fuentes Bobo v Spain (App no 39293/98) (ECtHR, 29 February 2000) para 43.

307 Hertzberg et al v Finland (Comm no 061/1979) (Human Rights Committee, 2 April 1982) para 10.2 and Separate Opinion of Mr. Opsahl: Mr. Rajsoomer Lallah, Mr. Walter Surma Tarnopolsky.

308 See Özgür Gündem (n 305) para 43.

309 CCPR General Comment 10 (n 302) para 2; CCPR General Comment 34 (n 248) para 40; NIT S.R.L (n 297) paras 148, 186; Manole (n 297) para 99; Compulsory Membership (n 283) para 34.

310 NIT S.R.L (n 297) paras 174-175, 179-182, 190, 193; Manole (n 297) paras 100–101.

311 NIT S.R.L (n 297) para 102.

While states themselves *must* follow the tripartite test when directly intervening, restrictions imposed on private media outlets with respect to individual speech acts *should* but *need not exactly* mirror said test, including the public grounds that may justify limitations on otherwise free speech.[312] Private media companies, including online platforms have their own commercial interests[313] and states are neither required nor allowed to micromanage their editorial or curation choices. Otherwise, the protection of free expression and information would be a pretext for public censorship.[314] Further, even if media companies themselves, including online platforms, lack human rights under certain instruments like the ICCPR,[315] their owners are still entitled to freedom of expression and information, private property as well as other rights.[316] Ultimately, both limbs or dimensions of the freedoms of expression and information – private and public, negative and positive – must be reconciled.[317] This means that, when regulating or otherwise intervening in the media sector, whether online or offline, states must strike a fair balance between the interests of individuals and the community as a whole.[318] In some instances, the scale will tip in favour of requiring companies to make public interest assessments when limiting online speech, whereas in other instances, these interests should play a smaller role.

312 See Hertzberg et al (n 307) Separate Opinion of Mr. Opsahl, Mr. Rajsoomer Lallah, Mr. Walter Surma Tarnopolsky (arguing that "nobody – and in particular no state – has any duty under the Covenant to promote publicity to information and ideas of all kinds. Access to media operated by others is always and necessarily more limited than the general freedom of expression. It follows that such access may be controlled on grounds which do not have to be justified under article 19 (3)). See also Taylor (n 38) 575; Joint Declaration (n 248) para 4(a). cf Aswad, 'The Future of Freedom of Expression Online' (n 287) 52–67 (questioning whether online platforms should follow Article 19(3) of the ICCPR when designing and implementing their speech policies but ultimately arguing in favour of this approach).

313 Aswad, 'The Future of Freedom of Expression Online' (n 287) 54.

314 Compulsory Membership (n 283) para 33.

315 Aswad, 'The Future of Freedom of Expression Online' (n 287) 40-41, citing ICCPR art 2(1) ICCPR and CCPR General Comment 31 (n 9) para 9.

316 Nowak (n 38) 463.

317 Compulsory Membership (n 283) para 33.

318 Palomo Sánchez and Others v Spain [GC] (App nos 28955/06, 28957/06, 28959/06 and 28964/06) (ECtHR, 12 September 2011) para 62; Özgür Gündem (n 305) para 43.

Large online platforms can be said to make up today's digital public space.[319] As others have also noted, given their market power, these platforms have assumed a fiduciary role with respect to information relating to health and other public goods.[320] Thus, the public interest in regulating their content and in doing so consistently with chiefly public grounds, such as the protection of health, national security, and public order, is perhaps more salient than for smaller platforms.[321] When requiring large platforms to restrict online content, including health misinformation and disinformation, states should apply the tripartite test of legality, legitimacy, and necessity.[322] This means requiring companies to have accessible and foreseeable content moderation policies, and that any limitations on online content be necessary and proportionate to any public interest aims sought.[323] In the context of cyber operations against the healthcare sector, the legitimacy test for limitations on speech acts will be met insofar as the protection of public health is sought. But states must still adopt a clear legal framework in which to ground such limitations and ensure that content moderation measures – ranging from deletion and user suspension to nudges and labels – are necessary and proportionate

319 TM Scanlon, The Difficulty of Tolerance: Essays in Political Philosophy (CUP, 2019) 157; D Kaye, 'A New Constitution for Content Moderation', (OneZero, 25 June 2019) <https://onezero.medium.com/a-new-constitution-for-content-moderation-6249af611bdf> accessed 7 January 2023; Aswad, 'The Future of Freedom of Expression Online' (n 287) 30-31.

320 B Sander and N Tsagourias, 'The Covid-19 Infodemic and Online Platforms as Intermediary Fiduciaries under International Law' (2020) 11(2) Journal of International Humanitarian Legal Studies 331, 341–345.

321 See HRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (6 April 2018) UN Doc A/HRC/38/35 paras 42–48; Aswad, 'The Future of Freedom of Expression Online' (n 287) 54–57, 64–67; Aswad, 'To Protect Freedom of Expression' (n 259) 612-613. For a contrary view, see E Douek, 'U.N. Special Rapporteur's Latest Report on Online Content Regulation Calls for 'Human Rights by Default,' (Lawfare Blog, 6 June 2018) <https://www.lawfareblog.com/un-special-rapporteurs-latest-report-online-content-regulation-calls-human-rights-default> accessed 7 January 2023; A Clooney and P Webb, 'The Right to Insult in International Law' (2017) 48(2) Columbia Human Rights Review 1.

322 See Milanovic and Schmitt (n 10) 273–274; Aswad, 'To Protect Freedom of Expression' (n 259) 657–658.

323 UN Doc A/HRC/47/25 (n 164) paras 40–42; UN Doc A/HRC/38/35 (n 321) paras 46–47; Aswad, 'To Protect Freedom of Expression' (n 259) 619–627; Aswad, 'The Future of Freedom of Expression Online' (n 287) 49–52.

to the protection of the relevant health goal or institution.[324]

Under Article 20 of the ICCPR, states have a special positive duty to enact legislation prohibiting content that amounts to propaganda for aggressive war or advocacy of national, racial, or religious hatred that constitutes incitement to hostility, discrimination or violence. Though an important response to inflammatory speech acts that led to World War II,[325] the customary nature of this provision is contested,[326] especially considering that several states have made reservations thereto.[327] For states that are bound by it, Article 20 of the ICCPR still requires consistency with Article 19(3)'s tripartite test.[328] Thus, when prohibiting said forms of war propaganda or incitement online and offline, states must adopt accessible and foreseeable laws whose sanctions are necessary to punish relevant speech acts and proportionate to their seriousness. Again, this means reserving criminal sanctions to only the most serious types of war propaganda and incitement, such as where there is an intent to cause harm and a serious and imminent risk of such harm ensuing.[329] In the healthcare context, online posts advocating for life-threatening or otherwise harmful cyber operations against hospitals in another state or inciting individuals to physically attack healthcare institutions, patients or professionals likely fall under the scope of Article 20 of the ICCPR and must therefore be prohibited by law.

324 Aswad, 'The Future of Freedom of Expression Online' (n 287) 52.
325 Nowak (n 38) 475.
326 See HRC, 'General Comment No. 24: Issues Relating to Reservations Made upon Ratification or Accession to the Covenant or the Optional Protocols thereto, or in Relation to Declarations under Article 41 of the Covenant' (4 January 1994) UN Doc. CCPR/C/21/Rev.1/Add.6 para 8; van Benthem, Dias and Hollis (n 10) 1243–1244.
327 For the reservations, see 'ICCPR' (UN Treaty Collection) <https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND> accessed 7 January 2023.
328 HRC, 'CCPR General Comment No. 11: Article 20 Prohibition of Propaganda for War and Inciting National, Racial or Religious Hatred' (1983), para 2; CCPR General Comment 34 (n 248) para 52; UN Doc A/HRC/22/17/Add.4 (n 279) paras 18, 22; UN Doc A/67/357 (n 279) para 41; UN Doc A/HRC/38/35 (n 321) para 8; UN Doc A/74/486 (n 274) para 13; Aswad, 'To Protect Freedom of Expression' (n 259) 629.
329 UN Doc A/HRC/22/17/Add.4 (n 279) para 29; UN Doc A/67/357 (n 279) paras 46–47, 79; UN Doc A/74/486 (n 274) paras 14–15.

VII. Conclusion

Under certain human rights treaties, such as the ICCPR, the ECHR, and the ACHR, the application of human rights to any subject-matter, including cyber operations targeting the healthcare sector, is subject to a requirement of jurisdiction. In the context of those treaties, jurisdiction can be either territorial, that is, extend over a state's own territory, or extraterritorial, applying beyond national borders. We have argued that extraterritorial jurisdiction may be established through a state's effective control over a geographical space, a person, a company whose activities foreseeably impact on an individual's human rights abroad, and, arguably, over the enjoyment of those rights, irrespective of any physical control. Given the remote and often cross-boundary nature of cyber operations, understanding extraterritorial jurisdiction as a type of functional, rather than physical, control over the enjoyment of human rights is the most appropriate way to ensure that the healthcare sector and other frequent targets of such operations are within the scope of international human rights law.

As seen earlier, all three types of cyber operations targeting the healthcare sector covered in this report – disruptive operations, data breaches and information operations – may engage the four rights discussed in this chapter, that is, life, health, privacy and the freedoms of expression and information. Each of these rights entails both negative obligations to respect and positive duties to protect human rights online and offline. Negative human rights obligations may be breached when the state itself, through its agents, engages in conduct that interferes with these rights. Conversely, positive duties may be breached when a state fails to exercise due diligence to prevent, stop or redress human rights violations by its own agents or third parties, including other states and non-state actors, or when the state fails to put in place measures necessary to ensure the full enjoyment of the relevant right. Although conflicts of rights may occur, the four rights discussed earlier are interdependent in that the realisation of one often requires respecting or protecting another.

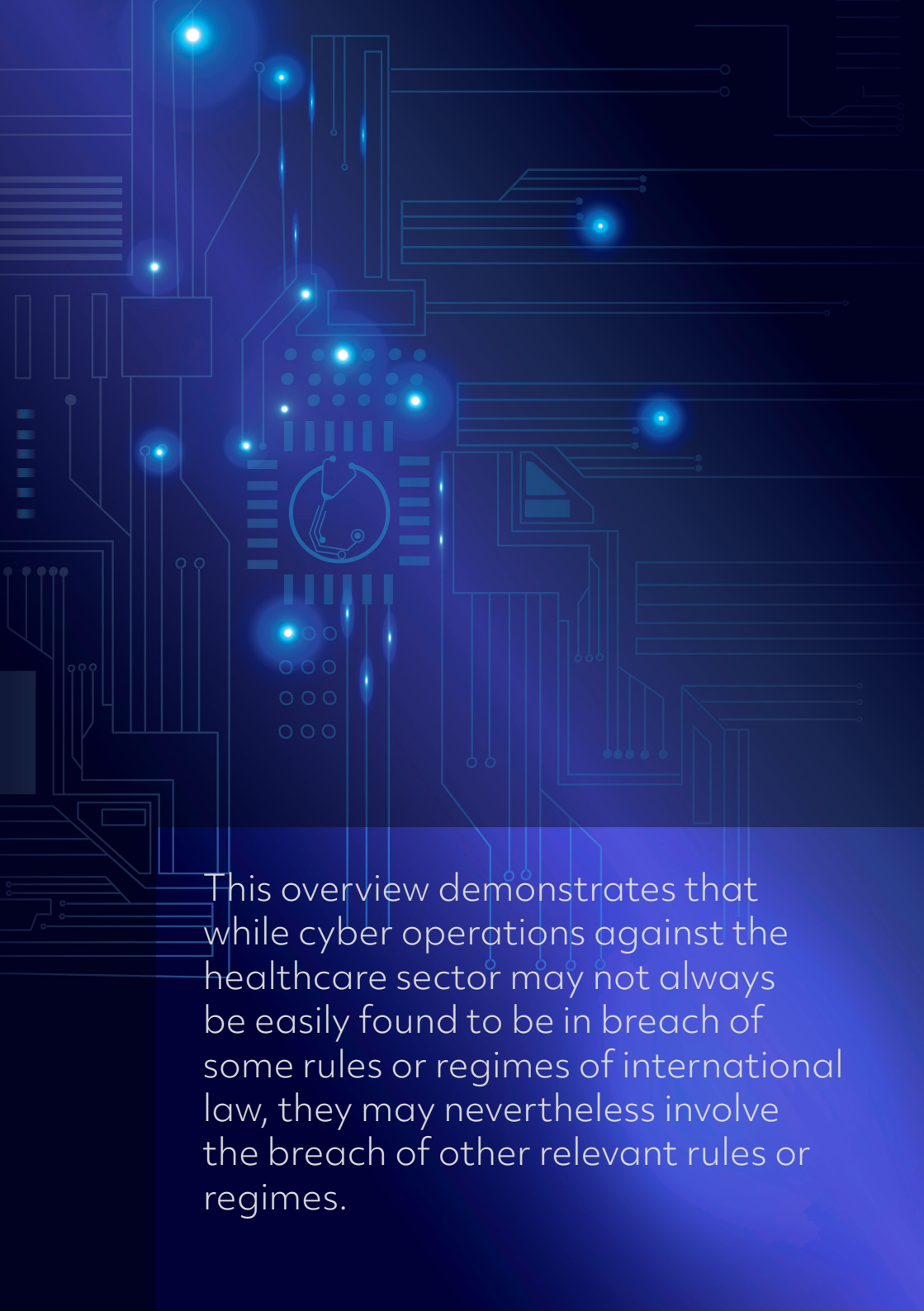
This chapter has found that a violation to the right to life under international human rights law will occur if a state engages in or fails to reasonably protect individuals from *any* foreseeable threat to life. This includes general conditions in society that may directly prevent individuals from enjoying their right to life with dignity, such as cyber operations targeting the healthcare sector that risk deprivation of life or life-threatening harm. Examples include disruptive operations targeting hospital equipment or essential patient data, systemic data breaches that hinder the provision of healthcare, and misinformation or disinformation campaigns involving emergency health treatments or measures. These cyber operations may foreseeably risk the lives of actual or potential healthcare patients or members of the public. Though these threats to life must be foreseeable and, thus, real, they need not be imminent unless they target a specific victim or emanate from an identifiable source. As there is no need for an actual deprivation of life to ensue, any requirement of causation is limited to a finding that the state either engaged in or failed to prevent the foreseeable life-threatening behaviour or situation in question.

The right to health may be equally undermined by cyber operations targeting the healthcare sector. This right requires states to not only refrain from limiting access to health facilities or providing healthcare on a discriminatory basis but also exercise their best efforts to provide individuals with the conditions to achieve the highest attainable standard of health. In the age of telemedicine and other manifestations of digital healthcare, the fulfilment of this duty requires not only the adoption of a traditional legal framework for healthcare but also the implementation of robust cybersecurity and data protection measures. One of the key components of the right to health is a well-functioning health information system, including the availability of accurate and reliable health information. Thus, health-related misinformation and disinformation operations directly undermine this component of the right to health. Likewise, by affecting essential qualities of healthcare, namely, availability, accessibility, acceptability, and quality, other types

of cyber operations may breach states' duties to respect, protect and fulfil the right to health.

Privacy is another key human right at stake in the context of cyber operations targeting the healthcare sector. As noted earlier, health data, particularly patient data, is a special category of private information, deserving heightened protection. The negative limb of the right to privacy proscribes arbitrary or unlawful interferences with patient data, including by cyber means such as electronic surveillance or ransomware. This means that any interference must be provided by law and reasonable in the circumstances. Conversely, the positive duties to protect and fulfil the right to privacy, as it concerns health-related personal information, include protection against unauthorised access by third parties and granting individuals the rights to data verification, correction, and deletion.

Finally, this chapter has addressed the importance of the rights to freedom of expression and information in the cyber and healthcare contexts. Whenever adopting measures to protect the rights to life, health, and privacy from cyber operations targeting the healthcare sector, states must respect the right of individuals to receive, seek, and impart information and ideas of all kinds, online and offline. This means that, even if legitimately grounded in the protection of health or other human rights, any limitation on freedom of expression or information must be grounded in law, necessary, and proportionate to the specific aim sought. Moreover, states themselves must not engage in health misinformation or disinformation or other harmful information operations. The positive duty to protect the freedoms of expression and information requires states to exercise their best efforts to ensure a free flow of accurate, verifiable health-information online and offline, as well as a diverse, plural, and robust media environment, including during health crises.



This overview demonstrates that while cyber operations against the healthcare sector may not always be easily found to be in breach of some rules or regimes of international law, they may nevertheless involve the breach of other relevant rules or regimes.

Chapter 6 Conclusion

This report has offered a detailed assessment of whether a variety of cyber operations facing the healthcare sector violate international law. Chapters 2, 3, 4 and 5 addressed relevant rules and regimes of international law applicable to states, namely the prohibition of the threat or use of force (Chapter 2), the prohibition of intervention in the affairs of other states (Chapter 3), the prohibition of conduct that violates a state's territorial sovereignty (Chapter 4), and relevant obligations under international human rights law (Chapter 5). Although there is emerging agreement amongst some states and commentators as to the applicability in general terms of these rules and regimes to cyber operations, there is as yet insufficient clarity as to how they might apply to different kinds of cyber operations and in the specific context of healthcare. Accordingly, the report has included within its scope a range of cyber operations facing the healthcare sector, each causing different effects and divided for the purpose of the analysis into: (1) disruptive cyber operations, such as ransomware operations (or 'ransomware attacks') and 'denial of service' operations (or 'DoS attacks'), (2) cyber operations involving the compromise, theft or publication of online data (or 'data breaches'), and (3) misinformation and disinformation operations. The report has also conceived of the healthcare sector widely, including not only hospitals and other healthcare providers, but also research institutes and pharmaceutical companies, including those developing COVID-19 vaccines, medical suppliers and distributors, health ministries and regulators, and the World Health Organization.

The discussions in the various chapters of the report reveal common themes that arise across the relevant rules and regimes of international law. To begin with, barring states' positive obligations under international human rights law, the violation of relevant rules and regimes of international law requires the attribution of a cyber operation to a state. Without satisfying the requirement attribution, such operations may not qualify as breaches of international law at all. Relatedly, a

common issue across the various chapters is the difficult forensic task of determining the source of a cyber operation so as to satisfy, amongst others, the requirement of attribution. This may be a difficult endeavour given the clandestine nature of most cyber operations.

The discussions across the various chapters also point to the need to identify a suitable standard of causation with which to determine what are the legally relevant effects of cyber operations. This is a particular problem in the context of healthcare, where the effects of concern are not the effects on targeted ICTs but the knock-on effects on the provision of medical care to individuals as well as public health. Where, by reference to the most appropriate standard of causation, a cyber operation may be said to cause death, physical injury or destruction, it may constitute a breach of the prohibition of the threat or use of force. Where, again by reference to a suitable standard of causation, a cyber operation may be said to cause a wider range of physical effects and perhaps even the loss of functionality of ICTs, it may constitute a breach of the prohibition of conduct in violation of a state's territorial sovereignty. The question of causation is not one which has been sufficiently addressed in international law generally. Although it is beyond the scope of this report to exhaustively address the question of the applicable standards of causation, Chapter 2 examines in some detail the question of the suitability of relevant standards of causation in relation to the threat or use of force and armed attack respectively. The reasonable foreseeability of relevant effects, proposed as the most suitable standard of causation in that context, is also tentatively discussed in relation to other relevant rules and regimes in other chapters alongside other standards of causation used in international law.

What follows is a recollection of the various arguments made in each chapter of the report. This overview demonstrates that while cyber operations against the healthcare sector may not always be easily found to be in breach of some rules or regimes of international law, they may nevertheless involve the breach of other relevant rules or regimes.

It ought to go without saying that the analysis proposed in this report addresses the most common scenarios that are likely to arise in the context of the healthcare sector and that any more specific assessment is necessarily fact dependent.

Chapter 2 examined the applicability to cyber operations against the healthcare sector of the prohibition of the threat or use of force and the right of self-defence against an armed attack under Articles 2(4) and 51 respectively of the UN Charter and under customary international law. These rules are applicable to cyber operations on the basis at least of the causing of effects comparable to those caused by conventional weapons, namely death, physical injury and destruction. When it comes to an armed attack, the additional requirement of gravity, comprising requirements as to the scale of the conduct and its effects, must also be satisfied.[1] Death and physical injury, if not also destruction of property, is certainly conceivable in the context of cyber operations targeting the provision of medical care to individuals and, in some cases, even medical research and development. A particular problem that arises in this context is whether any ensuing effects of death, physical injury or destruction are in causal terms too indirect or remote or not sufficiently proximate as to qualify such operations as a use of force and an armed attack respectively. Having considered the various standards of causation used in international law, the standard of reasonable foreseeability is found to be the most suitable standard of causation in relation to Articles 2(4) and 51. The use of this standard means that, where relevant effects manifest, disruptive cyber operations against the healthcare sector, such as ransomware and 'denial of service' operations, may amount to the use of force, since it is reasonably foreseeable that their use in the context of healthcare may lead to death, physical injury or destruction. Conversely, when it comes to the other kinds of cyber operations with which the healthcare sector is faced, such as data breaches and disinformation and misinformation operations,

1 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits) [1986] ICJ Reports 14, 93.

the standard of reasonable foreseeability may not be satisfied, either because of the foreseeability equally of intervening causes, or because of the use alongside reasonable foreseeability of a requirement of directness. The satisfaction of the standard of reasonable foreseeability notwithstanding, in reality many cyber operations targeting the healthcare sector will violate neither the prohibition of the threat or use of force nor constitute an armed attack since they fall below the *de minimis* threshold for a use of force under Article 2(4) and are even less likely to satisfy the requirement of gravity in respect of an armed attack under Article 51.

More likely than the violation of the prohibition of the threat or use of force is the violation of the prohibition of intervention in the affairs of other states, discussed in **Chapter 3**. For a prohibited intervention to occur, the cyber operation in question must satisfy the requirements of 'coercive' intervention in the 'internal or external affairs' of a state, articulated in the decision of the International Court of Justice (ICJ, the Court) in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*.[2] The internal or external affairs of a state, or the domestic jurisdiction of a state, is better defined in the context of the prohibition of intervention as referring to a state's choices and policies rather than the *domaine réservé*, which refers to matters not regulated by international law for the purpose of allocating jurisdictional competence between the domestic and international levels. Certainly, the formulation by a state of a choice or policy as to healthcare, or the implementation of its preferred choice or policy, whether by a public or a private institution, falls within the domestic jurisdiction of the state and thus within the scope of the prohibition. The requirement of coercion refers to the loss of the choice of the targeted state over matters within its domestic jurisdiction, including the loss of its control over the articulation of its choices or policies or their implementation. Accordingly, some cyber operations against the healthcare sector are more likely than others to constitute violations of the prohibition of intervention. Disruptive cyber

2 ibid 108.

operations, like ransomware and 'denial of service' operations, interrupt the provision of healthcare, deprive the targeted state of control over the implementation of health-related choices or policies and, on this basis, may be coercive. Conversely, the compromise, theft or publication of online medical data is not coercive since these operations do not interrupt the provision of healthcare. One potential exception is a cyber operation which compromises clinical trial data and thereby prevents the approval by a state of a medicine or medical technology intended for use in the implementation of a health-related policy. Information operations are the most difficult to characterise as coercive since any alleged loss of the control of the targeted state over the articulation or implementation of health-related choices or policies will be difficult to link to such an operation.

Beyond the prohibition of the threat or use of force and the prohibition of intervention in the affairs of states, which may be violated by certain kinds of cyber operations facing the healthcare sector, **Chapter 4** considered whether these or other kinds of cyber operations may also violate the rule prohibiting conduct that violates a state's 'sovereignty' or 'territorial sovereignty'. In the absence of prior consent, the conduct of one state in the territory of another state is prohibited. Accordingly, a cyber operation by one state through the physical presence of its agent in another state may constitute a violation of the latter's territorial sovereignty. In reality, however, most cross-border cyber operations are carried out remotely, avoiding the need for any physical presence in the targeted state. The more relevant question addressed by Chapter 4 is therefore whether and, if so, on what basis a remote cyber operation against the healthcare sector may be said to violate the sovereignty of a state over its territory. First, a cyber operation may be prohibited on the basis that it usurps the exercise of a governmental function by the territorial state even where it is carried out remotely. Although generally applicable to cyber operations, such usurpation has not occurred to date in the context of governmental functions in relation to healthcare. Secondly, the view has been advanced that remote cyber operations

with effects in the territory of another state may violate the territorial sovereignty of that state. There is no clear agreement, however, as to which effects are relevant to the assessment. It is not widely agreed by states that the loss of functionality of the targeted ICTs or the fact of a cyber 'incursion' alone would qualify a remote cyber operation as a violation of territorial sovereignty. In contrast, it is at least agreed that, as a minimum, causing physical damage in the territory of another state will qualify a remote cyber operation as a violation of the territorial sovereignty of the targeted state. In the context of healthcare, relevant effects include the loss of functionality of the targeted ICTs and knock-on physical damage and could include death and physical injury to individuals.

Subject to the satisfaction of causal requirements, disruptive cyber operations which target the functionality of ICTs and in turn cause physical damage by interrupting the provision of medical services may violate the rule prohibiting conduct in violation of a state's territorial integrity. In contrast, data breaches typically cause neither the loss of functionality of ICTs nor physical damage, except perhaps where compromised data can no longer be relied on in the provision of medical care to individuals. Using a standard of reasonable foreseeability of effects, such exceptional cases might be construed as violations of territorial sovereignty. When it comes to disinformation and misinformation operations, which affect healthcare widely, the requirement of causation will be more difficult to satisfy. Were the assessment of the lawfulness of cyber operations to be carried out by reference to the fact of an unauthorised 'incursion' into ICTs in the territory of another state, or were the loss of functionality of ICTs sufficient to constitute such a breach, a wider range of cyber operations might qualify as violations of territorial sovereignty. In the absence of agreement on the point, the unlawfulness of the various cyber operations discussed is more easily established by reference to the prohibition of intervention discussed in Chapter 3.

Finally, obligations in respect of human rights may exist for states even

where the other rules and regimes of international law, discussed above, are not breached. Chapter 5 scrutinised the key human rights which may be violated by cyber operations targeting the healthcare sector, or which may otherwise give rise to state obligations in the context of healthcare. These are the right to life, the right to health, the right to privacy and the right to freedom of expression and freedom of information, variously articulated in human rights treaties and under customary international law. International human rights law encompasses two sets of obligations for states, namely: (1) negative obligations to respect human rights by refraining from engaging in cyber operations that violate relevant rights, and (2) positive obligations to protect and fulfil or ensure rights owed to individuals through the exercise of due diligence. An overarching consideration when addressing the range of human rights obligations that may be implicated in the context of healthcare is the scope of states' obligations to respect, protect and fulfil these rights remotely, that is, in the absence of physical control of a territory, space or individual. Amongst the various approaches that are proposed to address the question, the functional model is apposite in the context of cyber operations, extending a state's jurisdiction to its exercise of functional control over an individual's enjoyment of a human right, even where such control is exercised remotely.

A violation to the right to life under international human rights law will occur if a state engages in or fails to reasonably protect individuals from any foreseeable threat to life. This includes general conditions in society that may directly prevent individuals from enjoying their right to life with dignity, such as cyber operations targeting the healthcare sector that risk deprivation of life or life-threatening harm. Examples include disruptive operations targeting hospital equipment or essential patient data, systemic data breaches that hinder the provision of healthcare, and misinformation or disinformation campaigns involving emergency health treatments or measures. These cyber operations may foreseeably risk the lives of actual or potential healthcare patients or members of the public. Though these threats to life must be foreseeable

and, thus, real, they need not be imminent unless they target a specific victim or emanate from an identifiable source. As there is no need for an actual deprivation of life to ensue, any requirement of causation is limited to a finding that the state either engaged in or failed to prevent the foreseeable life-threatening behaviour or situation in question.

The right to health may be equally undermined by cyber operations targeting the healthcare sector. This right requires states to not only refrain from limiting access to health facilities or providing healthcare on a discriminatory basis but also exercise their best efforts to provide individuals with the conditions to achieve the highest attainable standard of health. In the age of telemedicine and other manifestations of digital healthcare, the fulfilment of this duty requires not only the adoption of a traditional legal framework for healthcare but also the implementation of robust cybersecurity and data protection measures. One of the key components of the right to health is a well-functioning health information system, including the availability of accurate and reliable health information. Thus, health-related misinformation and disinformation operations directly undermine this component of the right to health. Likewise, by affecting essential qualities of healthcare, namely, availability, accessibility, acceptability, and quality, other types of cyber operations may breach states' duties to respect, protect and fulfil the right to health.

Privacy is a key human right at stake in the context of cyber operations targeting the healthcare sector. As noted earlier, health data, particularly patient data, is a special category of private information, deserving of heightened protection. The negative limb of the right to privacy proscribes arbitrary or unlawful interferences with patient data, including by cyber means such as electronic surveillance or ransomware. This means that any interference must be provided by law and must be reasonable in the circumstances. Conversely, the positive duties to protect and fulfil the right to privacy, as it concerns health-related personal information, include protection against unauthorised access

by third parties and granting individuals the rights to data verification, correction, and deletion.

Lastly, Chapter 5 addressed the rights to freedom of expression and information in the cyber and healthcare contexts. Whenever adopting measures to protect the rights to life, health, and privacy from cyber operations targeting the healthcare sector, states must respect the right of individuals to receive, seek, and impart information and ideas of all kinds, online and offline. This means that, even if legitimately grounded in the protection of health or other human rights, any limitation on freedom of expression or information must be grounded in law, necessary, and proportionate to achieve the specific aim sought. Moreover, states themselves must not engage in health misinformation or disinformation or other harmful information operations. The positive duty to protect the freedoms of expression and information requires states to exercise their best efforts to ensure a free flow of accurate, verifiable health-information online and offline, as well as a diverse, plural, and robust media environment, including during health crises.


BLAVATNIK
SCHOOL OF
GOVERNMENT
UNIVERSITY OF
OXFORD
OXFORD INSTITUTE FOR
ETHICS, LAW AND
ARMED CONFLICT