Cyber Due Diligence in Public Health Crises

Antonio Coco, Lecturer, School of Law, University of Essex and Talita de Souza Dias, Post-Doctoral Research Fellow, Blavatnik School of Government, University of Oxford [DOI: 10.5526/xgeg-xs42_037]

I. Introduction

Over the past two decades, the internet has become part of our daily lives. As the Covid-19 outbreak unfolds, our dependence on cyberspace has become even greater. Health systems are operated partially through information and communication technologies (ICTs), policymakers share vital and often confidential ideas through digital channels, and public information is disseminated by the media on their websites and mobile apps. The crisis has also forced us to move significant aspects of our personal and professional lives online. Parliaments around the world are holding sessions via video-link, medical appointments are now conducted online, and those who can work from home rely on their internet connections to hold online meetings, send and receive messages.

Whilst cyberspace has become a fertile field for malicious operations that may compound an existing health crisis, it also offers countless opportunities to respond more effectively to such crises. States are bound by several rules of international law requiring them to behave diligently in order to prevent, halt or redress harmful cyber operations — what we call 'cyber due diligence duties'. In this contribution, we explore how compliance with such obligations must be part of States' responses to epidemics and other health crises. On the one hand, failure to implement protective measures of due diligence or reasonable care in cyberspace can have disastrous consequences in the fight against Covid-19 and other diseases — especially when harmful cyber operations target critical infrastructure, such as the healthcare sector. In particular, the inability or unwillingness to prevent or halt cyber operations against hospitals or research facilities can hamper efforts to test and treat patients or to develop a vaccine. On the other hand, cyber due diligence measures can proactively bolster the capacity and resilience of States' online networks and systems, enabling a more rapid recovery from health crises. For instance, with the necessary safeguards in place, contact tracing apps and the dissemination of accurate public health information on social media can help contain the spread of the disease.

The international community already benefits from a suitable — if patchy — international legal and policy framework laying down States' duties to act diligently in preventing, halting and remedying harmful cyber operations against systems and infrastructures which are essential during health crises. States must implement those obligations, *inter alia*, by adopting measures aiming at: establishing an adequate national legal framework; ystems and nfrastructure; engaging in constructive international cooperation and dialogue. By behaving diligently in cyberspace, States will more likely be able to contain the spread of Covid-19, prevent further harm and pursue an effective recovery from the outbreak.

II. States' Reactions to Cyber Operations against the Healthcare Sector

In its 'initial pre-draft report' issued in April 2020, the UN Open-Ended Working Group on cybersecurity (OEWG) reaffirmed the need to implement, at all times, strong protective measures for critical infrastructure against the malicious use of ICTs. Even though the concept of 'critical infrastructure' may vary across States, it is generally understood to

include, at the very least, medical facilities and other healthcare services, electricity grids, water and sanitation systems,[1] as well as financial and electoral services. Interference in the networks and systems of these vital activities could have disastrous consequences not only on a State's national security but also its social, political and economic stability and development.[2]

The risk and impact of malicious cyber operations against such infrastructure are heightened during a public health emergency. For cyber criminals and hacker groups, many of which are notorious State proxies, the public distress and vulnerability caused by the Covid-19 outbreak are an opportunity that can be exploited for personal or political gain.[3] For instance, attempts have been made to steal the results of vaccine clinical trials from Oxford University's database, leading to increased cybersecurity measures.[4] Likewise, hospitals and laboratories in the Czech Republic were targeted by ransomware attacks, forcing delays in scheduled operations.[5] There have also been reports of Covid-19-related phishing messages and fraudulent websites worldwide, whose content has ranged from fully-fledged disinformation campaigns to sales of inexistent medical equipment.[6] The potentially destabilising impact of such operations has prompted strong reactions from several States.

As part of the UK's response, the Secretary of State for Health recognised that 'the network and information systems held by or on behalf of the NHS [National Health Service] in England or those bodies which provision public health services in England must be protected to ensure those systems continue to function to support the provision of services intended to address coronavirus and COVID-19'.[7] For this purpose, executive directions were adopted to enable the National Cyber Security Centre to strengthen the ability of those networks and systems 'to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or

[1] Czech Republic, 'Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security', April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf.
[2] UN Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), 'Second "Pre-draft" report of the OEWG', 27 May 2020, https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf, § 22.
[3] Davey Winder, 'Cyber Attacks Against Hospitals Have 'Significantly Increased' As Hackers Seek To Maximize Profits', *Forbes*, 8 April 2020; John E Dunn, 'DDoS attack on US Health agency part of coordinated campaign', *Naked Security (Sophos)*, 18 March 2020, https://nakedsecurity.sophos.com/2020/03/18/ddos-attack-on-us-health-agency-part-of-coordinated-campaign/amp/; Sean Gallagher, Andrew Brandt, 'Facing down the myriad threats tied to COVID-19', *SophosNews*, 14 April 2020 https://news.sophos.com/en-us/2020/04/14/covidmalware/.
[4] Jamie Grierson, Hannah Devlin, 'Hostile states trying to steal coronavirus research, says UK agency", *The Guardian*, 3 May 2020.
[5] Catalin 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/.
[6] Catalin Cimpanu, 'State-sponsored hackers are now using coronavirus lures to infect their targets', *ZDNet*, 13 March 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/.
[7] UK Department of Health and Social Care, 'The Consent to Activities Related to the Security of NHS and Public Health Services Digital Systems (Coronavirus) Directions 2020', 24 April 2020, https://www.gov.uk/government/publications/security-of-nhs-and-public-health-services-digital-systems-coronavirus-directions-2020, 1.

transmitted or processed data or the related services offered by, or accessible via, those network and information systems.'[8]

In the same vein, referring to recent cyber threats against health and research facilities in the UK, Europe and the US,[9] the UK Foreign Secretary recalled that '[i]nternational law and the norms of responsible state behaviour must be respected and all states have an important role to play to help counter irresponsible activity being carried out by criminal groups in their countries.'[10] Similar calls for compliance with the "norms of responsible state behaviour" and international law applicable to cyberspace to protect the healthcare sector came — among others — from Australia,[11] the Czech Republic,[12] Estonia,[13] the Nordic countries[14] and the US.[15] More tellingly, the European Union, upon condemning 'malicious cyber activities targeting essential operators […] including in the healthcare sector', 'call[ed] upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law'.[16]

It emerges from those declarations that many States believe in the existence of a legal and policy framework to increase cybersecurity and resilience, made up of binding rules and principles of customary and conventional international law; and 'non-binding norms of responsible state behaviour'.[17] Central to such a two-pronged framework is the idea that, as a corollary of their sovereignty, States must exercise "cyber due diligence", that is, act to the best of their abilities to prevent, halt and redress a range of harmful cyber operations emanating from their territory. This, together with the above statements, suggests that, in times of public health emergency, States ought to exercise due diligence in cyberspace.

---

[8] Ibid, Section 2.
[9] UK National Cyber Security Centre, 'Cyber warning issued for key healthcare organisations in UK and USA', 5 May 2020, https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations.
[10] UK Foreign & Commonwealth Office (FCO), 'UK condemns cyber actors seeking to benefit from global coronavirus pandemic', 5 May 2020, https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic.
[11] Stilgherrian, 'Australia and US call out cyber attacks on hospitals during COVID-19 pandemic', *ZDNet*, 27 April 2020, https://www.zdnet.com/article/australia-and-us-call-out-cyber-attacks-on-hospitals-during-covid-19-pandemic/.
[12] Czech Republic, (n. 1).
[13] 'Reinsalu condemns cyber attacks against Czech critical infrastructure', *ERR News*, 20 April 2020, https://news.err.ee/1080058/reinsalu-condemns-cyber-attacks-against-czech-critical-infrastructure.
[14] 'Joint statement from Denmark, Finland, Iceland, Sweden and Norway by Ambassador Mona Juul at the Arria-meeting on Cyber stability and conflict prevention', 22 May 2020, https://www.norway.no/en/missions/UN/statements/security-council/2020/arria-cyber-stability-and-conflict-prevention.
[15] US Department of State, 'The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector', 17 April 2020, https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/.
[16] Council of the European Union, 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic', 30 April 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/. See also the recent call by over 120 academics and experts, 'The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector', *Oxford Institute for Ethics, Law and Armed Conflict*, May 2020, https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.
[17] 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/70/174, 22 July 2015, § 13.

Without measures of prevention, control and crisis response, overburdened healthcare facilities around the world risk collapsing, and full recovery may be slow if not impossible.

III. Cyber Due Diligence between International Law and Policy

Due diligence has recently gained prominence in the cyber domain as a way to hold States indirectly accountable for hams caused by third parties. Responsibility arises from a failure to prevent or redress harms originating from or transiting through their jurisdiction, without the need to factually or legally attribute the conduct to the State in question. Thus, several States and scholars have supported a customary rule or principle requiring States to exercise due diligence in cyberspace, in what has been termed 'cyber due diligence'.[18] According to one iteration of this rule, States '*must* exercise due diligence in not allowing [their] territory […] or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other states.'[19] However, some governments have been reluctant to accept this formulation as a binding rule of customary international law.[20] Instead, a very similar articulation of cyber due diligence has been recognised by the UN Group of Governmental Experts (GGE) on cybersecurity as well as the UN General Assembly as a voluntary, non-binding norm of responsible State behaviour. It affirms that 'States *should* not knowingly allow their territory to be used for internationally wrongful acts using ICTs.'[21]

The confusion surrounding the concept of cyber due diligence seems to result from its treatment as a standalone obligation or principle. It may well be that a cyber-specific due diligence rule is emerging,[22] but this claim should not detract from the fact that international law in its entirety applies by default to cyberspace — or, more accurately, to ICTs — and States have unanimously and explicitly recognised as much.[23] Thus, the pre-existing range of international obligations of due diligence requiring States to prevent, stop or redress certain harms are already applicable to harmful cyber operations. These include two rules of general application in international law, covering all fields of State activity, as well as rules found in specialised international legal regimes.

The first comes from the 1949 *Corfu Channel* case between the UK and Albania. There, the International Court of Justice (ICJ) held that 'it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'[24] This

---

[18] Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace,' (2015) 125 *Yale LJ Forum* 68.
[19] Michael N. Schmitt, (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge : Cambridge University Press, 2017), Rule 6, 30 (emphasis added).
[20] Liisi Adamson, 'Recommendation 13(c),' in UN Office of Disarmament Affairs, *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (New York: United Nations, 2017), 55, § 12.
[21] UN GGE Report (n. 17), § 13(c) (emphasis added).
[22] See, e.g., France, Ministère des Armées, '*Droit International appliqué aux opérations dans le cyberspace*', 2019, 10; Australia, Department of Foreign Affairs and Trade (DFAT), 'Australia's International Cyber Engagement Strategy — Annex A: Australia's position on how international law applies to state conduct in cyberspace', 2020, https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html#Annex-A; Organization of American States, 'Improving Transparency – International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis)', CJI/doc. 603/20 rev.1, 5 March 2020, §§ 56ff.; Republic of Korea, 'Comments on the pre-draft of the OEWG Report', 14 April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/200414-rok-comment-on-pre-draft-of-oewg.pdf, 2.
[23] See, e.g., UN GGE Report (n. 17), §§ 26-28.
[24] *Corfu Channel Case* (*United Kingdom v Albania*), Merits, 9 April 1949, ICJ Reports (1949) 4, 22 (emphasis added).

particular obligation seems to apply with respect to "acts contrary to the rights of other States", without there necessarily being a violation of a particular rule of international law.[25] It imposes on States a standard of diligent behaviour, i.e. to employ their best efforts, to prevent or stop such acts.[26] It is triggered by actual or constructive knowledge that the acts in question are being or will be committed and limited by a State's capacity to act.[27]

The second rule of international law establishing a due diligence duty of general application is the "no-harm" or "good neighbourliness" principle. Although this principle has gained most prominence in the environmental context, its origins go far back to nineteenth century State-to-State disputes about the treatment of aliens abroad.[28] The rule was most clearly articulated in the 1941 *Trail Smelter* award, where the arbitral tribunal held that a State 'owes at all times a duty to protect other states against injurious acts by individuals from within their jurisdiction.'[29] The principle is now embodied in the ILC's 2001 Articles on Prevention of Transboundary Harm from Hazardous Activities,[30] which are deemed to reflect customary international law, at least in significant part.[31] Article 3, in particular, acknowledges that States have a duty to 'take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof.' The ICJ sanctioned the customary nature of this duty in the 1996 *Nuclear Weapons* Advisory Opinion,[32] while the ILC itself recognised its applicability beyond the environmental realm.[33] Unlike the rule articulated in *Corfu Channel*, the no-harm principle requires States to prevent transboundary harm even if caused by activities that are lawful or not contrary to the rights of other States.[34] As it explained, this is an obligation of due diligence, not

[25] The Tallinn Manual 2.0, going beyond the ICJ reasoning, argues that such acts are limited to internationally wrongful acts by a State, or acts committed by other entities that would have been internationally wrongful if committed by the State from where the harm originates or through which it transits. See Schmitt, *Tallinn Manual* (n. 19) 39, § 34; 34, § 14, 35–36, § 21.
[26] See e.g. Schmitt, Tallinn Manual (n. 19) 30; Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?,' (2014) 14 *Baltic Y Intl L* 5; International Law Association (ILA), 'Study Group on Due Diligence in International Law, Second Report,' July 2016, 2.
[27] Robert Kolb, 'Reflections on Due Diligence Duties and Cyberspace,' (2015) 58 *GerY Intl L* 123–24; Schmitt, *Tallinn Manual* (n. 19) 44–45, §§ 7-9; 47, §§ 16-18; Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm,' (2016) 21(3) *J Confl & Sec L*441–42.
[28] See, e.g., *Alabama Claims Arbitration (USA v UK)* (1872) 29 RIAA 125, 127, 129, 131-132; *Wipperman Case (USA v Venezuela)* (1887), reprinted in John Bassett Moore, History and Digest of the International Arbitrations to Which the United States Has Been a Party, vol. 3 (1898–1906), 3041; *Neer Case (USA v Mexico)* (1926) 4 RIAA 60, 61-62. See also *Trail Smelter Case (USA v Canada)*, (1941) 3 RIAA 1911, 1963-1965.
[29] *Trail Smelter Case*, ibid, 1963.
[30] ILC, 'Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries', in 'Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001)', UN Doc. A/56/10, 144-170.
[31] Timo Koivurova, 'Due Diligence,' *Max Planck Encyclopedia of Public International Law*, February 2010, § 10.
[32] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ GL No 95, [1996] ICJ Rep 226, para 29.
[33] ILC, Draft articles on Prevention of Transboundary Harm (n. 30), 148-149. See also Jutta Brunée and Tamar Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance,' (2015) 58 *Ger Y Intl L* 134–35; Koivurova (n. 31), §§ 16, 23, 44-45.
[34] Failure to exercise the requisite diligence leads to liability to redress the harm by compensation, once it materialises — with international responsibility arising if the State fails to effect such redress.ILC, Draft articles on Prevention of Transboundary Harm (n. 30), 150.

requiring States 'to guarantee that the harm would not occur' but 'to exert [their] best possible efforts to minimize the risk' thereof.[35]

Duties of due diligence can also be found in specialised bodies of international law, which, as noted earlier, apply by default to ICTs in the absence of carve-outs. With respect to Covid-19, it is helpful to recall that international human rights law (IHRL) imposes on States positive obligations to safeguard the enjoyment individual human rights, including civil, political, economic, social and cultural rights, online and offline.[36] These positive obligations entail a range of due diligence duties requiring States to adopt all reasonable measures to protect and ensure the human rights of individuals subject to their jurisdiction against threats posed by private or public entities or external circumstances, such as natural disasters or epidemics.[37] Due diligence, in this context, describes the standard of conduct against which State compliance with those obligations is measured.[38] Covid-19-themed or related cyberattacks, such as those described in Section II above, have the potential to harm *inter alia* individuals' rights to life, health, privacy and freedom of expression.[39] Accordingly, States must do their best to prevent, stop and remedy such cyber operations — to the extent that they occur within a State's territory or jurisdiction — whether or not they are perpetrated by State agents, private individuals or simply result from an accident.[40] In this respect, one should recall that identifying the scope of a State's jurisdiction for IHRL purposes is particularly problematic in respect to cyberspace or ICTs,[41] given their transboundary nature and the different 'layers' of which they are made — physical, logical and personal.[42] Although this issue is beyond the scope of this contribution, it suffices to note that any model of extraterritorial jurisdiction over human rights online[43] is subject to a State's the capacity to act, as well as the foreseeability of the harm or threat.

---

[35] Ibid, 154.

[36] See also UN Human Rights Council, Resolution 32/13, 'The promotion, protection and enjoyment of human rights on the Internet', UN Doc. A/HRC/RES/32/13, 31 July 2016, § 1.

[37] *Bărbulescu v. Romania*, Appl. no. 61496/08, 5 September 2017, § 110, with respect to the right to privacy.

[38] HRC, General Comment No. 31, UN Doc. CCPR/C/21/Rev.1/Add. 13, 26 May 2004, § 8; Samantha Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!,' *ESIL Reflections* 9, no. 1, 28 April 2020, 4–5.

[39] Marko Milanovic and Michael N. Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations during a Pandemic,' *J Natl Sec L & Pol*, forthcoming, http://dx.doi.org/10.2139/ssrn.3612019.

[40] In the context of cyberspace, see Schmitt, *Tallinn Manual* (n. 19) Rule 36, 196–201; Milanovic and Schmitt, (n. 39), 22. See generally *Velásquez-Rodríguez v Honduras* (Merits), Ser. C. No. 4, 29 July 1988, §§ 172-173; *Öneryıldız v. Turkey*, Appl. No. 48939/99, 30 November 2004, §§ 89-90, 97-110; *Rantsev v. Cyprus and Russia*, Appl. No. 25965/04, 7 January 2010, §§ 218-223; *M. Özel and Others v. Turkey*, Appl. nos. 14350/05, 15245/05 and 16051/05, 17 November 2017, §§ 173-174.

[41] Marko Milanovic, 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life,' (2020) 20(1) *Hum Rts LR* 21–24,.

[42] Clare Sullivan, 'The 2014 Sony Hack and the Role of International Law,' (2015-16) 8(3) *J Natl Sec L & Pol* 454, fn 88.

[43] Different human rights bodies and scholars have oscillated between different models of extraterritorial jurisdiction: a) spatial, requiring control over physical infrastructure (e.g. a server or satellite; see e.g. *Banković v. Belgium* (Admissibility), App no 52207/99, 12 December 2001, §§ 74-82); b) personal, requiring control of the individual victim/right-holder (see e.g HRC, General Comment 31 (n. 38), § 10); c) activity-based, whereby control must be exercised over the activity in question (e.g. the acts hacking a computer; see e.g. HRC, 'General Comment No. 36: Right to Life (Art. 6)", UN Doc. CCPR/C/GC/35, 3 September 2019, § 22); or d) functional, requiring control over the enjoyment or exercise of the rights in question, broadly defined (e.g. HRC, General Comment 36, ibid, § 63; Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law,' (2013) 7(1) *Law & Ethics of Hum Rts* 47.

International humanitarian law (IHL) also establishes a range of due diligence obligations.[44] Cyberwarfare has become a common feature of modern armed conflicts. Malicious cyber operations have the potential to intentionally or indiscriminately render civilian infrastructure dysfunctional, disrupting the provision of services essential to the civilian population.[45] Thus, during armed conflict and even in peacetime, States must behave diligently in adopting measures to protect civilians against the effects of violent cyberattacks.[46] Likewise, they have a general duty to act with due diligence to ensure that parties to an armed conflict do not violate IHL, including in cyberspace.[47]

Crucially, the applicability of this comprehensive, yet multifaceted and patchy framework in cyberspace has received support from several States, especially in times of Covid-19. For instance, France,[48] Austria,[49] Australia,[50] and the Czech Republic[51] have not only expressed concern for cyberattacks against health and research facilities but also explicitly recognised the binding nature of due diligence obligations under international law, IHRL and/or IHL.

The "voluntary, non-binding norms of responsible state behaviour", first outlined in the 2015 GGE Report and reaffirmed in the context of the pandemic,[52] also seem to embrace a preventive and precautionary approach in respect of harmful cyber operations. They send a message that resonates even more clearly during a public health crisis: States should take reasonable steps and appropriate measures to protect their critical infrastructure from ICT threats, especially those that can compound the crisis or hinder an effective response to the outbreak. Of particular importance in this context are the following measures that States are encouraged to take: enactment of domestic legislation,[53] monitoring,[54] confidence-building,[55] and international cooperation and capacity-building.[56]

---

[44] See e.g. Marco Longobardo, 'The Relevance of the Concept of Due Diligence for International Humanitarian Law,' (2020) 37(1) *Wisc Intl LJ* 44.
[45] ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts — ICRC position paper', 28 November 2019, , 5.
[46] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I), 8 June 1977, Art. 58; Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press, 2005), Rules 22-24.
[47] Geneva Conventions of 1949, common Art.1; AP I, Art. 1(1).
[48] France, 'France's response to the pre-draft report from the OEWG Chair', April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf.
[49] Austria, 'Pre-Draft Report of the OEWG - ICT: Comments by Austria', 31 March 2020, https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf.
[50] Australia, 'Australia's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG)', 16 April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/final-australia-comments-on-oewg-pre-draft-report-16-april.pdf.
[51] Czech Republic, (n. 1).
[52] See, e.g., n. 48, 49, 50 above.
[53] See, e.g. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/68/98, 24 June 2013, § 32(a).
[54] See, e.g., 'Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', December 2019, https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf, 17.
[55] UN GGE Report (n. 17), §§ 16-18.
[56] Ibid, §§ 19-23.

But the responsibility to adopt those measures arises *not only* from voluntary commitments made in that report, the OEWG and other fora, or the resulting social expectation. These various measures may be required in different circumstances by the range of international obligations of due diligence outlined earlier — to the extent that such measures would be a way to prevent, halt and redress harmful cyber operations.

IV. Cyber Due Diligence Measures and their Impact on the Pandemic

The general thrust of due diligence obligations is to require States to do what they *can* do. Such duties do not impose pre-determined measures, but demand from States reasonable efforts to prevent, stop or redress harm, subject to their capacity to act in the circumstances and their knowledge or foreseeability of the harm or risk. Thus, their extent varies on the basis of available resources, the degree and type of harm or risk they seek to avert, as well as a State's capacity to influence the behaviour of the perpetrators. In this way, due diligence obligations afford a degree of flexibility and deference to States, but they are accompanied by a core procedural obligation of result to put in place the necessary governmental capacity to fulfil applicable obligations.[57] This means that, beyond this minimal threshold, each State may be required to adopt different due diligence measures depending on the circumstances. As the ICJ recalled in the *Bosnian Genocide* case, due diligence calls for an *in concreto* or contextual assessment of State behaviour.[58] Also, any cyber due diligence measures must be consistent with other international obligations that a State may have, especially their negative and positive obligations in respect of human rights affected by adopted measures.

The following measures are particularly suitable, if not essential, to any attempt at preventing, halting and redressing online harms that may either compound ongoing health problems or jeopardise the effective recovery therefrom.

a) National legal framework

Any plan of action to implement cyber due diligence measures ought to begin with the establishment of an adequate national legal framework.[59] An adequate national legal framework in this sense would include, first and foremost, the prohibition or criminalisation of harmful cyber conduct. Likewise, the availability of civil remedies alongside provision for effective investigations and prosecutions of malicious cyber behaviour are instrumental in deterring, preventing and redressing ensuing harms.[60] In a context where most ICT infrastructures are owned, controlled or operated by multinational or foreign corporations, States must also pass appropriate national legislation regulating their human rights impact and imposing relevant corporate due diligence standards. Such measures should address: online disinformation, whether through content moderation or counter-speech; internet security and availability; as well as software vulnerability — all of which depend on

[57] ILC, Draft articles on Prevention of Transboundary Harm (n. 30), 155-156, in particular commentary to Article 3, § 17 and commentary to Article 5. See also Koivurova (n. 31), § 21; Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States,' (1992) *Ger Y Intl L* 26–27; Kolb (n. 27), 117, 127. Koivurova, para 21; Pisillo-Mazzeschi, 26–27; Kolb, 117, 127.
[58] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Merits, [2017] ICJ Reports 43, 26 February 2007§§ 430-431.
[59] HRC, General Comment 31, (n. 38), §§ 7, 13; HRC, General Comment 36, (n. 43), §§ 4, 13, 22.
[60] *Nicolae Virgiliu Tănase v. Romania*, Appl. no. 41720/13, 25 June 2019, § 127; HRC, General Comment 31, ibid, §§ 8, 18; HRC, General Comment 36, ibid, §§ 13, 19, 27-28.

corporate action. Other legislative measures of particular relevance in a health crisis include the provision of response and preparedness plans for cyber emergencies, along with an effective system for monitoring compliance with the law by State officials and third parties, to the extent permitted by international law.[61]

b) Monitoring

This brings us to the second type of cyber due diligence measures that States should and often must — to the extent practicable — adopt at all times, including during health crises: effective monitoring or surveillance of cyberspace. To be sure, obligations of due diligence do not necessarily require States to do the impossible to anticipate all possible online harms by ostensibly policing the internet and seeking information about potential threats. But they do require States to use their existing technical and financial resources to halt or prevent malicious cyber operations which they know or should have known about, again, to the extent possible and permitted by other rules of international law — in particular, the human rights to privacy and freedom of expression.

Notably, in light of recent cyber threats facing the healthcare sector, Australia urged all States to "exercise increased vigilance to ensure their territory is not a safe haven for cybercriminals."[62] In the same spirit of vigilance, the UK Health Secretary put the Government Communications Headquarters (GHCQ) in charge of monitoring "any information relating to the security of any network and information system held by or on behalf of the NHS or a public health body during the period ending on 31st December 2020."[63] Digital technologies may also be used to monitor spaces and individuals to contain the spread of Covid-19, consistently with international law. Examples include video surveillance, contact tracing technologies and crowdsourcing systems.[64]

c) Confidence-building

The implementation of methods to enhance cybersecurity and mutual trust among States, also known as "confidence-building" measures,[65] may also be necessary to counter and prevent harmful cyber operations against the healthcare sector and other critical infrastructure during the Covid-19 outbreak and other public emergencies. Such measures may be required to the extent that they can address existing security vulnerabilities, such as data breaches or software flaws, or increase resilience in the recovery from harmful cyber operations, such as the creation of 24/7 Cyber Emergency Teams.[66]

These measures may also be required, moreover, to comply with the IHL rule stipulating that '[t]he civilian population and individual civilians shall enjoy general protection against

---

[61] HRC, General Comment 36, (n. 43) § 21.
[62] Australia, DFAT and Australian Cyber Security Centre, 'Unacceptable malicious cyber activity: Joint Statement', 20 May 2020, https://www.dfat.gov.au/news/news/unacceptable-malicious-cyber-activity; Stilgherrian, (n. 11).
[63] UK, Coronavirus Directions 2020, (n. 7), Section 4.
[64] Josh Toussaint-Strauss, Alex Hern, Simon Roberts, Joseph Pierce, Paul Boyd and Ryan Baxter, 'How Covid-19 contact tracing can help beat the pandemic', *The Guardian*, 8 May 2020; Nancy Fiesler, 'Crowdsourcing COVID-19', *Harvard Medical School: News & Research*, https://hms.harvard.edu/news/crowdsourcing-covid-19.
[65] UN GGE Report (n. 17), §§ 16-18.
[66] Ibid, § 17(c).

dangers arising from military operations.'[67] Precautionary measures are particularly important in cyberwarfare, given the co-dependency and interconnectivity between civilian infrastructures and lawful military objectives.[68] Thus, they may play a key role in preventing cyberattacks directed against military targets from spilling over onto civilian systems, including hospitals and other critical infrastructure.[69]

d) International cooperation and capacity-building

As neither the internet nor the pandemic knows territorial boundaries, international cooperation and institutional dialogue are crucial to prevent further outbreaks, contain the spread of the disease and eventually eliminate it. As the 2015 GGE report rightly acknowledges, '[i]nternational cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use.'[70]

Thus, it not surprising that several governments have recently called upon other States to cooperate with each other as well as with international institutions, particularly the World Health Organisation, in the context of the pandemic. The Czech Republic, for example, noted that "[t]he rising number of cyberattacks on medical facilities worldwide reinforce [sic] the need for coordinated global action to protect [the] public health care sector from malicious ICT activities."[71] Similarly, Estonia affirmed that '[t]he international community should urgently address cyberattacks against hospitals and other essential medical services that threaten already strained healthcare entities.'[72] Likewise, facing questions about its response to such threats, the UK reminded that it is 'working closely with [its] allies to hold the perpetrators to account and deter further malicious cyber activity around the world.'[73]

Such calls for increased cooperation are not merely hortatory but may be required under existing international law. In particular, the Corfu Channel and no-harm principles may require States to alert or notify third States about the risk of malicious cyber operations emanating from or transiting through their territory. During armed conflict, States must cooperate with other States and with the UN to ensure respect for IHL.[74]

Importantly, State cooperation may also be necessary to build the technical and financial capacity of less developed States to prevent, stop and redress online harms. In an interconnected world, security vulnerabilities in one State may compromise the integrity of systems beyond national borders.

---

[67] AP I, Art. 51.
[68] Ibid, Art. 52(2).
[69] Laurent Gisel, Tilman Rodenhäuser, 'Cyber operations and international humanitarian law: five key points', *Humanitarian Law & Policy*, 28 November 2019, https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.
[70] UN GGE Report (n. 17), § 19.
[71] Czech Republic, (n. 1).
[72] 'Reinsalu condemns cyber attacks against Czech critical infrastructure' (n. 13).
[73] FCO, 'UK condemns cyber actors', (n. 10).
[74] Henckaerts and Doswald-Beck (n. 46), Rule 144: Practice, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule144.

V. Conclusion

As essential services are now more than ever connected to the internet and other digital networks, measures of cyber due diligence are necessary to contain the spread of Covid-19, prevent further outbreaks and ensure a full recovery from the current crisis. Such measures are not only required as a matter of policy and good governance, but also by existing international law. Whether or not a standalone principle or rule of "cyber due diligence" exists, the international community already benefits from a comprehensive legal and policy framework to tackle online harms in times of Covid-19 and other health crises, even if it is spread across different international legal regimes. This framework — a true patchwork of different obligations — includes at the very least the Corfu Channel and no-harm principles, and positive State obligations under specific bodies of law such as IHRL and IHL. Their interpretation and implementation are guided and complemented by the norms of responsible State behaviour and other voluntary commitments made by States. Accordingly, States cannot reasonably invoke the absence of a specific binding international rule governing of cyber harms as an excuse for inaction in the fight against Covid-19 and other health crises.