Written evidence submitted by Dr Antonio Coco and Dr Talita de Souza Dias (COR0161)

Dr Antonio Coco, Lecturer, School of Law, University of Essex
Dr Talita de Souza Dias, Post-Doctoral Researcher, Blavatnik School of Government; Junior Research Fellow, St Catherine's College, University of Oxford

1. BACKGROUND

While advancements in information and communication technologies have greatly improved the quality and efficiency of medical treatment and scientific research worldwide, they come with inherent vulnerabilities, risks and costs. In the healthcare sector, there is an increased dependency on technologies such as digital medical records and billing systems, electronic prescriptions, imaging software, surveillance cameras, mobile devices, printers, routers and digital video systems used for online health monitoring and remote procedures. This means that malicious cyber operations targeting any such systems may have disastrous consequences on patients' health, privacy, security, and even their lives. Healthcare facilities are vulnerable not only to the theft, alteration and manipulation of patients' electronic medical records, but also to increasingly sophisticated system breaches that could jeopardise their ability to care for patients and respond to health emergencies. Given the essential nature of medical services and the sensitivity of information in their hands, the healthcare sector is particularly vulnerable to online harms.

For this reason, as early as 2016, the World Medical Association warned that, 'cyber-attacks on healthcare systems and other critical infrastructure represent a cross-border issue and a threat to public health'. It also 'call[ed] upon governments, policy makers and operators of health and other vital infrastructure throughout the world […] to collaborate internationally in order to anticipate and defend against such attacks.'[1]

2. EXTENT OF ONLINE HARMS AGAINST THE HEALTH SECTOR DURING THE COVID-19 PANDEMIC AND EXISTING RESPONSES

As the COVID-19 crisis unfolds, even more pressure is put on already overburdened healthcare systems treating sick patients and research facilities developing a vaccine and a cure for the disease. This vulnerability has been exploited by a range of cybercriminals and hacker groups, seeing the situation of public distress as an opportunity to make personal or political gain or to cause further disruption during the outbreak.[2] Examples include the recent a) ransomware attacks against hospitals in the Czech Republic, France, Spain, the US and Thailand;[3] b) themed phishing or spyware campaigns targeting the WHO as well as labs and pharmaceutical companies in Canada, Japan and South Korea,[4] c) and attempted data breaches of vaccine clinical trial records of the University of Oxford and other research

[1] WMA Statement on Cyber-Attacks on Health and Other Critical Infrastructure, Adopted by the 67th World Medical Assembly, Taipei, Taiwan, October 2016.
[2] https://www.forbes.com/sites/daveywinder/2020/04/08/cyber-attacks-against-hospitals-fighting-covid-19-confirmed-interpol-issues-purple-alert/
[3] https://www.telegraph.co.uk/technology/2020/03/17/battle-fend-cyber-criminals-trying-hold-hospitals-ransom/
[4] https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/; https://pharmaphorum.com/news/covid-19-themed-cyberattacks-hit-healthcare-bodies/

facilities in the UK.[5] At the same time, quarantine, social distancing and other measures to contain the spread of the disease have forced us to move significant parts of our lives online. These range from trivial activities like online shopping, banking and messaging, to parliamentary sessions, education, work meetings and medical appointments. This means that now more than ever cyberspace offers significant challenges but also incredible opportunities in the fight against this pandemic.

In this context, international law emerges as an essential tool to protect medical facilities and other essential services from the disastrous consequences of cyberattacks. It also allows States to safely harness the capabilities that cyberspace has to offer to contain the disease outbreak and effectively recover from it. Thus, it is not surprising that, when condemning recent cyberattacks against the health sector, many governments have called upon all States to comply with existing international law in cyberspace and the so-called 'voluntary, non-binding norms of responsible State behaviour'.[6]

To give some timely examples, in the wake of the attacks against hospitals in the Czech Republic, the Estonian Minister of Foreign Affairs noted that '[c]yber attacks against the medical sector during the ongoing crisis are unacceptable and potentially life-threatening', calling upon all States to respect the 'norms of responsible state behavior and [to uphold] international law in cyberspace.'[7] In its comments to the initial pre-draft report of the Second Substantive Session of the United Nations (UN) Open-Ended Working Group 'on developments in the field of information and telecommunications in the context of international security' (OEWG), the Netherlands expressed that it was: 'appalled by the abuse of the COVID-19 crisis by States to conduct or effectively control non-state actors in launching cyber operations, including the disruption of the healthcare sector, and cyber enabled information operations to interfere with the crisis response in times of urgent crisis.'[8] It also stressed that 'not only are these operations highly deplorable examples of irresponsible state behaviour; in many instances, they constitute violations of international law'.

The High Representative for the European Union (EU) Josh Borrel followed suite by expressing the EU's resolve to deter, prevent and respond to exploitative cyberattacks against the healthcare sector, and explicitly '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 and the 2010, 2013 and 2015' UN Group of Governmental Experts on Information and Communication Technologies' (GGE) consensus reports.

Likewise, following a series of attempted and cyberattacks against health facilities in the US and its international partners, US Secretary of State Mike Pompeo expressed 'zero tolerance for malicious cyber activity designed to undermine U.S. and international partners' efforts to protect, assist, and inform the public during this global pandemic.' It also reaffirmed the US' commitment to 'promote a framework of responsible state behavior in cyberspace, including nonbinding norms regarding states refraining from cyber activities that intentionally damage critical infrastructure and knowingly allowing their territory to be used for malicious cyber activities'.

[5] https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency
[6] UN GGE Report 2015, A/70/174, § 13.
[7] Statement by Estonian Minister of Foreign Affairs Urmas Reinsalu (Isamaa), 20 April 2020.
[8] The Kingdom of the Netherlands' response to the pre-draft report of the OEWG, April 2020.

Australia's ambassador for Cyber Affairs, Tobias Feakin also expressed concern 'that malicious cyber actors are seeking to exploit the pandemic for their own gain.' He 'call[ed] on all countries to cease immediately any cyber activity inconsistent with their international commitments' and urged them 'to exercise *increased vigilance* to ensure their territory is not a safe haven for cybercriminals.'[9]

All these statements highlight that, in the fight against COVID-19, States ***should*** and often ***must*** protect their health care systems and other critical infrastructure from harmful cyber operations carried out by other States or non-State entities, in accordance with international law. Of particular importance are two sets of obligations. First, *negative* duties requiring States to refrain from conducting or supporting such activities against third States or individuals, such as those arising from the principles of State sovereignty and non-intervention, as well as under international human rights law and international humanitarian law. Second, *positive* obligations requiring States to exercise *due diligence* and employ their *best efforts* in *preventing*, *halting* and *redressing* such online harms against other States or private entities, applicable under general international law, international human rights law and international humanitarian law.

3. THE CURRENT UK RESPONSE

In the United Kingdom (UK), Foreign Secretary Dominic Raab issued a statement finding that '[a]ttacks by state and non-state actors seeking to undermine the global response to this unprecedented global health crisis endanger lives.' He also stated 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. As cyberspace is essentially borderless, any mitigations or solutions need to be international – it is a foreign policy issue as much as a technical one.'[10] A few days earlier, the UK Health Secretary issues Directions authorising the country's Government Communications Headquarters to carry out activities related to the security of England's public health service network and information systems to protect these systems from malicious cyberoperations during the COVID-19 pandemic.[11]

Yet both initiatives fall short of spelling out what rules of international law are at stake. Crucially, although the UK has in the past recognised the general applicability of the prohibition on the use of force, the principle of non-intervention, international humanitarian law and international human rights law in cyberspace, which are all relevant in the current crises, it has not come forward to recognise the applicability of positive, due diligence duties in cyberspace — thus contributing to the lack of clarity about the content, scope and importance of such international obligations, and weakening the message that the UK is trying to convey to those states which have become safe harbours for malicious actors.

In order to increase certainty, predictability and security in cyberspace and to protect the UK's healthcare sector from online harms in times of COVID-19, the government should consider the following sets of actions which we flesh out below: 1) issuing an official statement explicitly recognising that several international duties of due diligence apply in

---

[9] Statement to ZDNet news platform

[10] Press release: UK condemns cyber actors seeking to benefit from global coronavirus pandemic

[11] https://www.gov.uk/government/publications/security-of-nhs-and-public-health-services-digital-systems-coronavirus-directions-2020

cyberspace generally and, in particular, during the current health crisis; 2) adopting measures of cyber due diligence domestically and internationally.

4. OFFICIAL STATEMENT RECOGNISING THE APPLICABILITY OF DUE DILIGENCE OBLIGATIONS IN CYBERSPACE

In the last few years, States, non-governmental organizations and scholars have debated whether international law provides for a specific rule of 'cyber due diligence'. This rule would require States not to knowingly allow their territory or ICT infrastructure under their jurisdiction to be used for certain malicious cyber operations against third States or other entities. The group of independent experts who drafted the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* supported its existence in the following terms:

> "[a] State must exercise due diligence in not allowing its territory, or 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."[12]

A 'voluntary, non-binding norm' of similar content was recognised by the UN Group of Governmental Experts (GGE) on cybersecurity in its 2015 report. It affirms that 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.'[13]

But the reluctance of several governments to frame those duties as binding rules or principles of international law has put their customary status in question.

Whilst it is reasonable to assume that a cyber-specific rule of due diligence is — at the very least — emerging, one should not forget that States have agreed that existing international law applies, in its entirety, to cyberspace. In fact, the concept of 'due diligence' is a standard of conduct, which requires states to behave in a reasonable way by employing their best efforts to prevent, stop and redress certain harms. This standard is found in a range of international *obligations of conduct* under treaty and customary international law, with some applying generally and others grounded in specialised regimes. They are already applicable to malicious cyberoperations and require states to prevent, stop or redress certain harms. The following applicable rules are the ones most relevant to current crisis:

a. **What we call the 'Corfu Channel' principle or *dictum***, according to which 'it is every State's obligation not to allow knowingly its territory to be used for *acts contrary to the rights of other States'*;[14]

b. **The no-harm principle**, articulated in several international cases,[15] as well as by the International Law Commission (ILC),[16] which requires States to 'take all

[12] Tallinn Manual 2.0, Rule 6, 30.
[13] UN GGE Report 2015, A/70/174, § 13(c).
[14] Emphasis added. *Corfu Channel Case* (*United Kingdom v Albania*), Merits, 9 April 1949, ICJ Reports (1949) 4, at 22.
[15] See, e.g., *Alabama Claims Arbitration (USA v UK)* (1872) 29 RIAA 125, at 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), at 3041; *Neer Case (USA v Mexico)* (1926) 4 RIAA 60, at 61-62. See also *Trail Smelter Case (USA v Canada)*, (1941) 3 RIAA 1911, at

appropriate measures to prevent significant transboundary *harm* or […] to minimize the risk thereof'

c. **Positive duties to protect and ensure human rights online**. With respect to Covid-19, it is helpful to recall that international human rights law (IHRL) imposes on States positive obligations to safeguard 'virtually' individual human rights, including civil, political, economic, social and cultural rights. 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.[17] Due diligence, in this context, describes the standard of conduct against which compliance with those obligations is measured.[18] Cyberattacks against the healthcare sector, in particular, have the potential to harm individuals' rights to life, health, and privacy — just to mention a few. Accordingly, under IHLR, States must prevent, stop and remedy such attacks to the extent that they emanate from their jurisdiction, regardless of their particular cause. While the substance of those duties is well-accepted, some controversy exists as to the scope of States' extraterritorial jurisdiction for positive human rights duties, a particularly vexing problem in cyberspace. Although this issue is beyond the scope of this contribution, it suffices to note that any model of extraterritorial jurisdiction over human rights online — spatial, personal or functional — is subject to the capacity of a State to act, as well as the foreseeability of the harm or threat.

Tellingly, the applicability of this comprehensive, yet fragmented framework in cyberspace has received support from several States in times of Covid-19. As mentioned earlier, States such as Australia,[19] the Czech Republic[20], as well as France[21] and Austria,[22] 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.

For those reasons, we call upon the UK Government and/or its Parliament to follow the example of its international counterparts and adopt the **following official statement expressing is view that**:

> 'According to existing international law, when a State is or should be aware of a cyber operation that emanates from its territory or infrastructure under its jurisdiction or control, and which will produce adverse consequences for health-care facilities abroad, the State

---

1963-1965.

[16] Koivurova, 'Due Diligence', *Max Planck Encyclopaedia of Public International Law (MPEPIL)* (2010), para 10.

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

[18] HRC, GC 31, note 71, § 8; Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9:1 *ESIL Reflections* (2020) 2, 4-5.

[19] 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.

[20] Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security, 11 March 2020.

[21] France's response to the pre-draft report from the OEWG Chair, 1 April 2020.

[22] Pre-Draft Report of the OEWG - ICT: Comments by Austria, 31 March 2020.

must take all feasible measures to prevent or stop the operation, and to mitigate any harms threatened or generated by the operation.'

5. 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 risk. Thus, their extent varies on the basis of available resources, the degree and type of 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 significant degree of flexibility and deference to States, but minimal action to acquire the necessary governmental infrastructure is nonetheless required.[23] This means that, beyond this minimal threshold, each State may have different due diligence obligations in different scenarios. Due diligence calls for an *in concreto* or contextual assessment of State behaviour.[24] It is also worth recalling that any cyber due diligence measures must be consistent with States' other international obligations, especially their negative duties not to violate human rights.

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. This is because efforts to tackle cyber harms or threats usually involve limitations to fundamental human rights and therefore presuppose sufficiently accessible and foreseeable legislation. Likewise, the availability of civil remedies alongside provisions for effective investigations and prosecutions of malicious cyber behaviour are instrumental in deterring, preventing and redressing their ensuing harms.[25] In a context of 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 applicable due diligence standards, to the extent they have extraterritorial jurisdiction over such activities. Such measures should address online disinformation and content moderation, internet security and availability, as well as software vulnerability, all of which depend on corporate action.

b) Monitoring

States should and — to the extent practicable — must adopt at all times, including during health crises effective monitoring or surveillance of cyberspace. To be sure, the obligation to 'police' the internet does not necessarily require States to do the impossible to continuously anticipate all cyber harms. But it does impose on States to use their existing technical and

---

[23] ILC Draft Articles with Commentary, at 155-156; Commentary to Article 3, para. 17; Article 5 and Commentary; Koivurova, para 21; Pisillo-Mazzeschi, 26–27; Kolb, 117, 127.
[24] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Merits, 26 February 2007 ICJ Reports (2007) 43, §§ 430-431
[25] Tanase, § 127; HRC, GC 31, paras 8, 18; GC 36, paras 13, 19, 27-28.

financial resources to halt or prevent malicious cyber operations which they know or should have known if this action is indeed feasible in the circumstances. 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.[26]

c) Confidence-building

The implementation of methods enhancing the security of critical cyber infrastructure, also known as 'confidence-building' measures, are also necessary to counter and prevent cyberattacks against health facilities during Covid-19 and other public emergencies. Such measures may be required to the extent that they can address existing security vulnerabilities, such as password breaches, or increase resilience to recover from cyberattacks, such as the creation of 24/7 Cyber Emergency Teams.

d) International cooperation and capacity-building

As neither the internet nor the pandemic knows territorial boundaries, international cooperation and institutional dialogue are crucial to preventing further outbreaks, containing the spread of the disease and eventually eliminating 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'.[27] Such calls for increased cooperation are not merely hortatory but may be required under existing international law. Importantly, State cooperation is also needed to build the technical and financial capacity of less developed States to prevent, stop and respond to online harms. In an interconnected world, security vulnerabilities in one State may open the doors to malicious cyber operations across the border.

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 stop the spread of Covid-19, recover from it and prevent further outbreaks. This arises not only as a matter of policy and good governance but is also required by existing international law. Although there may not be sufficient evidence that a specific obligation requiring diligent State behaviour in cyberspace has achieved *lex lata* status, 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.

May 2020

---

[26] https://www.theguardian.com/world/video/2020/may/08/how-covid-19-contact-tracing-can-help-beat-the-pandemic; https://hms.harvard.edu/news/crowdsourcing-covid-19.

[27] §19.