WRITTEN EVIDENCE FROM DR ANTONIO COCO, LECTURER, SCHOOL OF LAW, UNIVERSITY OF ESSEX; VISITING FELLOW, BLAVATNIK SCHOOL OF GOVERNMENT, UNIVERSITY OF OXFORD; DR TALITA DE SOUZA DIAS, POSTDOCTORAL RESEARCH FELLOW, BLAVATNIK SCHOOL OF GOVERNMENT; JUNIOR RESEARCH FELLOW, ST CATHERINE'S COLLEGE, UNIVERSITY OF OXFORD; AND MS TSVETELINA VAN BENTHEM, DPHIL CANDIDATE, FACULTY OF LAW, UNIVERSITY OF OXFORD (COV0213)

The following evidence is based on the interim *findings of the research project on 'Cyber Due Diligence' which is being carried out at the Oxford Institute for Ethics, Law and Armed Conflict (ELAC), Blavatnik School of Government, University of Oxford. A broader analysis of cyber due diligence measures which States must adopt in the context of a public health crisis can be found in A. Coco and T. de Souza Dias, 'Cyber Due Diligence in Public Health Crises', in C. Ferstman, A. Fagan (eds.), 'Covid-19, Law and Human Rights: Essex Dialogues' (University of Essex, 2020), at 297-307. For an even broader analysis of international obligations of due diligence to prevent, halt and redress the spread of COVID-19, please refer to A. Coco and T. de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the COVID-19 Pandemic', (2020) Journal of International Humanitarian Legal Studies.*

1. Background: Digital Threats to the Health Sector and Vaccine Research

As the public health crisis engendered by COVID-19 continues, it is all the more important to protect hospitals, public and private health institutions, laboratories and research facilities against malicious cyber operations directed against them. In the past weeks, cyber criminals and hacker groups — some of which may be sponsored by or act on behalf of States — have tried to take advantage of the vulnerabilities associated with the ongoing emergency for personal and political reasons.[1] For instance, ransomware attacks hit hospitals and laboratories in the Czech Republic, causing delays in scheduled operations.[2] Phishing messages and fraudulent websites related to Covid-19 have been widely reported around the globe, spreading disinformation and deceiving people, for instance, with respect to false cures or sales of inexistent medical equipment.[3] Malicious cyber operations have also targeted vaccine research. Attempts have already been made to steal information relating to the ongoing vaccine clinical trials from Oxford University's database (leading to increased cybersecurity measures).[4] More recently, the United Kingdom (UK)'s National Cyber Security Centre — acting in collaboration with the United States (US) and Canada — announced that allegedly Russian-sponsored cyber operations have attempted to surreptitiously collect information on COVID-19 vaccine research.[5] And Chinese hackers

[1] Winder, 'Cyber Attacks Against Hospitals Have 'Significantly Increased' As Hackers Seek To Maximize Profits', *Forbes*, 8 April 2020; Dunn, 'DDoS attack on US Health agency part of coordinated campaign', *Naked Security (Sophos)*, 18 March 2020; Gallagher, Brandt, 'Facing down the myriad threats tied to COVID-19', *SophosNews*, 14 April 2020.

[2] Cimpanu, 'Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak', *ZDNet*, 13 March 2020.

[3] Cimpanu, 'State-sponsored hackers are now using coronavirus lures to infect their targets', *ZDNet*, 13 March 2020.

[4] Grierson, Devlin, 'Hostile states trying to steal coronavirus research, says UK agency', *The Guardian*, 3 May 2020.

[5] United Kingdom (UK) National Cyber Security Centre, 'UK and allies expose Russian attacks on coronavirus vaccine development', 16 July 2020; UK Foreign and Commonwealth Office, 'Press release — UK condemns

have been accused by the US Justice Department of trying to steal coronavirus research on vaccine, testing technology and treatments.[6] These operations raise even more concern since the development of a vaccine is now an essential component of States' responses to the pandemic. A vaccine may not only save lives but also mitigate the socio-economic impact of the disease by allowing individuals to interact and work more safely.[7]

In this light, more than 130 international lawyers have recently signed the *Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector*,[8] seeking to remind States of the international obligations demanding effective action to protect information and communications technologies (ICTs) invested in curbing the spread of the pandemic. In particular, the applicable international legal framework contains a variety of rules requiring States to prevent, halt and redress a range of harmful cyber operations emanating from or occurring in their territory. The effective implementation of such obligations is crucial to the full recovery from the crisis, given the pervasiveness of ICTs. The present submission will focus on the most pressing measures which the UK should implement to protect the healthcare sector from harmful cyber operations and comply with its positive obligations under international human rights law.

2. POSITIVE OBLIGATIONS TO PROTECT HUMAN RIGHTS

International human rights law (IHRL) imposes on States positive obligations to safeguard the enjoyment of individual human rights, both online and offline.[9] To comply with such obligations, States must adopt all reasonable measures to protect and ensure the human rights of individuals subject to their jurisdiction. This protection is owed regardless of the origin of the threat: be it a public entity, a private one, or external circumstances, such as natural disasters or epidemics.[10] The standard of conduct against which State compliance with those obligations is measured is usually designated as 'due diligence'.[11] Malicious cyber operations in the context of the COVID-19 crisis, such as those mentioned above, have the potential to interfere with a range of human rights, including in particular the rights to life, health, and privacy.[12]

To the extent that individual lives often depend on medical treatment, public and private acts and omissions in respect of the healthcare sector may infringe the right to life.[13] Violations of

---

Russian Intelligence Services over vaccine cyber attacks', 16 July 2020.

[6] 'China hackers sought to steal coronavirus vaccine research, says US', *The Guardian*, 22 July 2020.

[7] See, e.g., Le Page, '124 coronavirus vaccines are in development – but will any work?', *NewScientist*, 3 June 2020; Honeycomb-Foster, 'Coronavirus vaccine hope as potentially 'game-changing' government-backed candidate enters human trials', *Politics Home*, 15 June 2020.

[8] Available online at https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea. The Statement was cited as a model of how international law applies in cyberspace, in the Dominican Republic's speech, during the recent UN Security Council Arria-Formula meeting on the issue.

[9] 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.

[10] European Court of Human Rights (ECtHR), *Bărbulescu v. Romania*, App. no. 61496/08, 5 September 2017, § 110, with respect to the right to privacy.

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

[12] Milanovic and Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations during a Pandemic', *Journal of National Security Law & Policy*, forthcoming 2020, http://dx.doi.org/10.2139/ssrn.3612019.

[13] See, e.g., ECtHR, *Hristozov and Others v Bulgaria*, Apps. nos. 47039/11 and 358/12, 13 November 2012, § 106.

the right to life might occur in cases where a patient's life is knowingly put in danger by denial of access to life-saving emergency treatment, or in situations of 'systematic or structural dysfunction in hospital services'.[14] Therefore, States have a positive duty to adopt measures necessary to prevent those circumstances to the extent they are avoidable and safeguard the lives of individuals under their jurisdiction.[15] Cyber operations — for instance, those conducted against hospitals and vaccine research facilities — present threats of a scale that could incapacitate a State's healthcare system and slow down the production and delivery of life-saving treatment, thus interfering with patients' right to life. Thus, to comply with their positive obligation to protect this right, States must protect research and healthcare facilities against online harms.

Similarly, malicious cyber operations against healthcare and medical research facilities — especially in the context of a global pandemic — have the potential to affect individuals' enjoyment of their right to the "highest attainable standard of physical and mental health".[16] According to Article 12(2) of the International Covenant on Economic, Social and Cultural Rights (ICESCR), the measures to ensure the progressive realization of the right to health include those necessary for '(c) [t]he prevention, treatment and control of epidemic, endemic, occupational and other diseases', as well as '(d) [t]he creation of conditions which would assure to all medical service and medical attention in the event of sickness'.

Although States are not required to *ensure* good health, they must *take steps* towards the full realisation of the right to health.[17] This right is considered to be one of progressive realisation, dependent on States' capacity to act, including available human and financial resources. To the extent that COVID-19 is a *public* health emergency, even when vaccine research efforts are fully or partly funded by private bodies, States may still have the power and thus the obligation to regulate and administer those efforts. At a minimum, the immediately realisable steps that States must adopt include protecting vaccine development, manufacture and distribution, including through safeguarding the relevant actors' essential networks and systems from malicious cyber operations.

Additionally, the right to health encompasses the right to prevention, treatment and control of diseases. This includes support for the necessary research and development, including for vaccines, new drugs and diagnostic tools,[18] and the creation of a system of urgent medical care in cases of epidemics.[19] In this area, the Committee on Economic, Social and Cultural Rights acknowledges the importance of States' individual *and joint efforts* to, 'inter alia,

---

[14] ECtHR, *Lopes de Sousa Fernandes v Portugal,* App. no. 56080/13, 19 December 2017, §§ 191-192. On this issue, see Stubbins Bates, 'Article 2 ECHR's Positive Obligations–How Can Human Rights Law Inform the Protection of Health Care Personnel and Vulnerable Patients in the COVID-19 Pandemic?', *Opinio Juris*, 1 April 2020.

[15] ECtHR, *LCB v UK*, 14/1997/798/1001, 9 June 1998, § 36; ECtHR, *Brincat and Others v Malta*, Apps. nos. 60908/11, 62110/11, 62129/11, 62312/11 and 62338/11, 24 July 2014, §§ 79-80; cf. Inter-American Court of Human Rights, *Ximenes-Lopes v Brazil* (Merits, Reparations and Costs), Series C No. 149, 4 July 2006, §§ 89-90.

[16] International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR) art 12(1). On the link with epidemics, see Pearson, 'Towards Human Rights-Based Guidelines for the Response to Infectious Disease Epidemics: Righting the Response' (2018) 24 *Australian Journal of Human Rights* 201.

[17] Committee on Economic, Social and Cultural Rights (CESCR), 'General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)', E/C.12/2000/4, 11 August 2000, § 30.

[18] Office of the United Nations High Commissioner for Human Rights, The Right to Health: Fact Sheet No. 31, at 8. Cf. a decision by Argentina's Federal Administrative Court (Viceconte, Mariela c. Estado Nacional, Amparo Ley 16.986, 2 June 1998), ordering the State to ensure the manufacturing of a vaccine against an endemic disease in compliance with the ICESCR.

[19] CESCR, General Comment 14 (n 17), § 16.

make available relevant technologies, using and improving epidemiological surveillance and data collection on a disaggregated basis, the implementation or enhancement of immunization programmes and other strategies of infectious disease control'.[20]

Finally, the right to privacy or private life, as enshrined, among others, in Article 8 of the European Convention on Human Rights (ECHR),[21] comes into play with respect to the protection of personal information and medical data of individuals who have been tested, infected, treated or subjected to clinical trials. Thus, unauthorised access to such information would constitute an interference with the right to privacy, and States are required to ensure practical and effective protection against such unauthorised access.[22] In the context of COVID-19 vaccine trials and other medical treatment, States are obliged to protect confidential patient information, including when acquired from third States or their nationals, and ranging from personal and medical information, patient questionnaires and journals, most of which are in digital format.[23]

3. SUGGESTIONS FOR ACTION

Positive obligations to protect human rights do not impose on States a pre-determined set of measures but require them to behave diligently and put in place reasonable efforts to prevent and counter harm to such rights, subject to their capacity to act in the circumstances and their knowledge or foreseeability of the harm or risk.[24] Despite this flexibility, at a minimum, such obligations require States put in place the necessary governmental capacity to fulfil them.[25] For instance, the right to life entails a primary duty of States to put in place a legislative and administrative framework designed to provide effective deterrence against threats to life, including the passing of regulations establishing procedures for identifying potential shortcomings in the national framework itself.[26]

As recalled by the International Court of Justice, whether 'due diligence' measures are sufficient to comply with the relevant international obligations will be determined on the basis of an objective but context-dependent assessment.[27] Importantly, any measure adopted by States in this context must be consistent with other international obligations that a State may have, especially negative and positive obligations arising in respect of other human rights or interests affected by the action. In this light, we suggest that the UK consider adopting the following measures to prevent and counter malicious cyber operations which, by targeting the healthcare sector or COVID-19 vaccine research, may interfere with the enjoyment of human rights.

---

[20] *Ibid*.

[21] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

[22] ECtHR, *I. v Finland*, App. No. 20511/03, 17 July 2008, §§ 37-47; ECtHR, *Z. v Finland*, App. No. 22009/93, 25 February 1997, § 95.

[23] See, e.g., 'The Oxford Vaccine Centre COVID-19 Phase II/III Clinical Trial Explained', *COVID-19 Oxford Trial News*, 22 May 2020.

[24] HRC, 'General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life', CCPR/C/GC/36, 30 October 2018 § 21; ECtHR, *Osman v. United Kingdom*, 87/1997/871/1083, 28 October 1998, §§ 115-116.

[25] Besson (n 11), at 5. See generally Koivurova, 'Due Diligence', *Max Planck Encyclopaedia of Public International Law (MPEPIL)* (2010), § 21; Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', 35 *German Yearbook of International Law* (1992) 9, at 26–27.

[26] ECtHR, *Öneryildiz v Turkey*, App. No. 48939/99, 30 November 2004, §§ 89-90.

[27] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, [2017] ICJ Reports 43, 26 February 2007, §§ 430-431.

a) National Legal Framework

Any action plan to implement cyber due diligence measures should start with the establishment of an adequate national legal framework.[28] Such a framework would include, first and foremost, the prohibition or criminalisation of harmful online conduct. Likewise, the availability of civil remedies and the guarantee of effective investigations and prosecutions of malicious cyber behaviour are instrumental in deterring, preventing and redressing ensuing harms.[29] In a context where most ICT infrastructures and many medical research facilities are owned, controlled, operated or funded 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 dis- and misinformation, whether through content moderation or counter-speech; internet security and availability; and software vulnerability — all of which depend on 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.[30]

b) Collection and Dissemination of Relevant Information on Cyber Threats

Effective monitoring of potential cyber threats and risks is an essential component of the protection of ICT infrastructure. States are not required, under IHRL, to anticipate every possible online harm by ostensibly policing the internet and seeking information about potential threats. Arguably, however, they must use their existing technical and financial resources to halt or prevent malicious cyber operations which they know or should have known of — again, to the extent possible and permitted by other rules of international law, in particular the human rights to privacy and freedom of expression.

We appreciate the UK Health Secretary's decision to 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'.[31] Likewise, the recent advisory issued by the National Cyber Security Centre, with detection and mitigation advice for organisations involved in coronavirus vaccine development targeted with custom malware by APT29 is also a welcome effort,[32] although similar initiatives must be taken *in advance of* such attacks. Looking ahead of malicious cyber operations to safeguard the human rights of individuals requires investment in the detection of existing security vulnerabilities, such as data breaches or software flaws, and the identification of areas for improvement in the cybersecurity of critical infrastructure.

Therefore, whilst we encourage the UK to continue in such protective efforts, we also suggest that more should be done to facilitate the *early*, *accessible and comprehensive* dissemination

[28] HRC, General Comment 31 (n 11), §§ 7, 13; HRC, General Comment 36 (n 24), §§ 4, 13, 22.
[29] Cf. ECtHR, *Nicolae Virgiliu Tănase v. Romania*, App. no. 41720/13, 25 June 2019, § 127; HRC, General Comment 31 (n 11), §§ 8, 18; HRC, General Comment 36 (n 24), §§ 13, 19, 27-28.
[30] HRC, General Comment 36 (n 24), § 21.
[31] 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, Section 4.
[32] UK National Cyber Security Centre, 'Advisory: APT29 targets COVID-19 vaccine development', 16 July 2020.

of available information on threats, detection and mitigation to relevant stakeholders, including other States whose networks are essential to the functioning of the UK's healthcare and are willing to cooperate in increasing cybersecurity.

c) International Cooperation and Capacity-Building

Given the transboundary nature of both cyberspace and efforts to contain the pandemic, we renew the call for the UK to cooperate with other countries in countering malicious cyber operations and thus facilitating a speedier recovery from the global public health crisis. As the 2015 report issued by the United Nations Group of Governmental Experts on ICTs rightly acknowledges, '[i]nternational cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use'.[33] In the same vein, the World Health Organization (WHO) has not ceased to remind States that COVID-19 is a highly contagious disease and that international solidarity is essential to restoring global health security.[34]

State cooperation may also be necessary to build or enhance the technical and financial capacity of less developed States to prevent and counter harmful cyber operations. One ought to remember that, in our interconnected world, security vulnerabilities in one State may compromise the integrity of systems beyond national borders. In the particular context of the right to health, the Committee on Economic, Social and Cultural Rights has noted that 'depending on the availability of resources, States should facilitate access to essential health facilities, goods and services in other countries, wherever possible, and provide the necessary aid when required'.[35] This wording, though granting to States significant navigational space, does provide a basis for a requirement to cooperate internationally, to the extent that this is feasible in the circumstances.

Recent developments show the importance of cooperation in halting the spread of COVID-19. In a resolution adopted on July 10th, 2020, the European Parliament set out principles for its future EU health strategy, including global cooperation and affordable access to COVID-19 vaccines and treatments for all people worldwide as soon as they are available.[36] On June the 1st 2020, the WHO launched its 'Solidarity Call to Action to realize equitable global access to COVID-19 health technologies through pooling of knowledge, intellectual property and data'.[37] This initiative, supported by thirty-nine States so far, recognises that, to halt the rapid transmission of the coronavirus and reverse the trend of consequential global distress, it is essential that 'everyone, everywhere can access the health technologies they need for COVID-19 detection, prevention, treatment and response'. In the same vein, on July 15th, it was announced that 'seventy-five countries have submitted expressions of interest to protect their populations and those of other nations through joining the COVAX Facility, a mechanism designed to guarantee rapid, fair and equitable access to COVID-19 vaccines worldwide'.[38] Efforts to increase cybersecurity with the aim of protecting human rights

---

[33] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), UN Doc. A/70/174, 22 July 2015, § 19.
[34] See World Health Organization, 'Making the response to COVID-19 a public common good', 2020; Lurie, Developing Covid-19 Vaccines at Pandemic Speed, *New England Journal of Medicine* 2020.
[35] CESCR, General Comment 14 (n 17), § 39.
[36] 'Health threats: boosting EU readiness and crisis management', News – European Parliament, updated 10 July 2020.
[37] Available at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/global-research-on-novel-coronavirus-2019-ncov/covid-19-technology-access-pool/solidarity-call-to-action.
[38] World Health Organization, 'More than 150 countries engaged in COVID-19 vaccine global access facility', 15 July 2020.

should similarly benefit from international cooperation in support of efforts to curb the pandemic. Thus, we strongly encourage the UK to express its support for those calls in fulfilling its obligations to protect human rights.

23/07/2020