

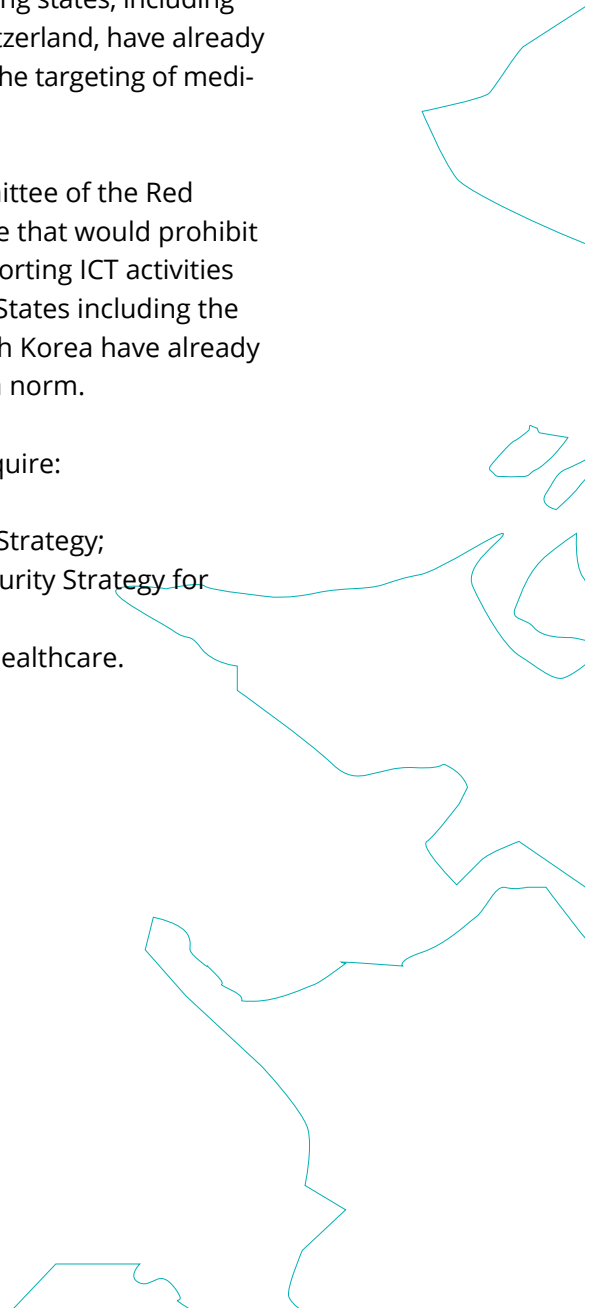


THE BIO-CYBER NORM: EMERGENCE AND OPERATIONALISATION

Sarvjeet Singh
Sharngan Aravindakshan

KEY TAKEAWAYS

- Recent times have shown nations' healthcare systems to be among the systems most essential yet also most vulnerable to external threats such as cyber-attacks and cybercrimes. Reports suggest that cyber-attacks on healthcare systems are increasingly sponsored or directed by states.
- It is becoming clear that healthcare facilities cannot and should not bear the burden of ensuring their cybersecurity on their own.
- Ongoing global cyber-norms-making processes are cognisant of this problem. Under the aegis of the United Nations Open-Ended Working Group on the use of ICTs in the context of international security (OEWG), several leading states, including Australia, France, Germany, Japan, and Switzerland, have already expressed concern over the steady rise in the targeting of medical facilities in cyberspace.
- Within the OEWG, the International Committee of the Red Cross has proposed a norm for cyberspace that would prohibit states from conducting or knowingly supporting ICT activities that target medical services and facilities. States including the Czech Republic, the Netherlands and South Korea have already declared their support for adopting such a norm.
- Operationalizing this norm in India will require:
 - Articulating a National Cyber Security Strategy;
 - Articulating a Sector-Specific Cybersecurity Strategy for the Healthcare Industry;
 - Ensuring Last-Mile Cybersecurity for Healthcare.



The ongoing Covid-19 pandemic has brought the readiness and security systems of medical infrastructure in Asia into sharp focus. Increasing reliance on digital systems, spurred in recent times by Asian countries investing heavily in their digital economies, has served to make healthcare infrastructure viable and easy targets for malicious cyber-actors, which can have dangerous consequences.

Hospitals and medical facilities are repositories of valuable information, including sensitive medical data, credit card details and insurance information, apart from typically personally identifiable information such as names, addresses, age, sex and so on. Stored in the form of electronic health records (“EHRs”), they are often the most lucrative information for hackers, with their worth estimated at around hundreds or even thousands of dollars.¹ Medical personnel depend on carefully accumulated data in EHRs, which includes patient medical history, diagnoses and so on, to make informed choices regarding patient well-being. Additionally, the availability of healthcare facilities today is often very much dependent on technology. Whether they are critical services, such as those ensuring continuity of care, medical devices and surgery equipment, or administrative services, such as systems dealing with work orders, billing and appointments, any disruption to these services can have a devastating effect on healthcare and consequently on patients’ lives.² Consider, for instance, a doctor conducting a life-saving surgery when a cyber-attack hits his hospital’s networks, rendering systems inoperable.

Until very recently there were no recorded deaths that occurred on account of malicious cyber activities; however, this changed in September 2020 when a woman died as a result of a ransomware attack on a German hospital.³ Moreover, several other countries are already experiencing a taste of the other severe consequences of malicious cyber activities. This includes the loss of patients’ personal health data, as with the cyber-attack on SingHealth

1 Yao, Mariya. 2017. “Your Electronic Medical Records Could Be Worth \$1000 To Hackers.” *Forbes*, 18 April. (<https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/>).

2 Le Bris, Aureore and Walid El Asri. 2017. “State of Cybersecurity & Cyber Threats in Healthcare Organizations – Applied Cybersecurity Strategy for Managers.” *Essec Business School Strategic Report*. (<http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-health-care-strategic-report.pdf>).

3 Staff Reporter. 2020. “German Hospital Hacked, Patient Taken to Another City Dies.” *Associated Press*, 17 September. (<https://apnews.com/cf8f8eee1adce69bc-c864f2c4308c94>).

in Singapore in 2018⁴, which led to the loss of more than a million patients' data, and the shutdown of hospital systems, leading to cancellation of surgeries and even transfer of patients to other hospitals, as happened with the attack on Brno University Hospital in the Czech Republic in 2020.⁵ The attack on Brno University Hospital was particularly pernicious since, as a major testing site for Covid-19 in the Czech Republic, the hospital was playing a crucial role in the government's fight against the pandemic. Importantly, not all of these cyber-attacks are believed to be conducted by opportunist hackers or criminal syndicates, with suspicions being cast on some states possibly taking advantage of lax and diffused focus over cybersecurity during the pandemic.⁶

These incidents have jolted states awake to the vulnerability of their medical infrastructure, both public and private, to such threats, prompting them to raise the issue of ensuring the safety and security of such medical infrastructure in the OEWG an international platform under the aegis of the United Nations concerned with cyber-norms building and cybersecurity. Following the lead of the International Committee of the Red Cross ("ICRC"), states have begun discussing the acceptance of a new norm – "*States should not conduct or knowingly support ICT activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm*"⁷ ("**Bio-Cyber Norm**"). This is an extension of the existing obligation of due diligence in international law, a principle that requires states to ensure their territories are not used to harm other states, which is itself an offshoot of the principle of sovereign equality of states. Importantly, it posits both a negative and a positive obligation on states –

-
- 4 Kwang, Kevin. 2018. "Singapore Health System Hit by 'Most Serious Breach of Personal Data' in Cyberattack; PM Lee's Data Targeted." CNA, 18 October. (<https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318>).
 - 5 Porter, Sophie. 2020. "Cyberattack on Czech Hospital Forces Tech Shutdown during Coronavirus Outbreak." *Healthcare IT News*, 3 April. (<https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak>).
 - 6 Barnes, Julian E., and David E. Sanger. 2020. "Russian Intelligence Agencies Push Disinformation on Pandemic." *The New York Times*, 28 July. (<https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html>).
 - 7 United Nations Open-Ended Working Group. 2020. "Comments by the International Committee of the Red Cross on the Initial 'Predraft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security." (<https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-icrc-on-initial-pre-draft-report-of-oewg.pdf>).

- 1/ It requires states to not conduct or knowingly support harmful ICT activities against medical facilities, and,
- 2/ It also imposes a positive obligation requiring states to actively take measures to ensure the security of medical services. Identifying this obligation as one that states should bear is also generally congruent with policy-making in cyberspace since it is widely acknowledged now that given its interconnected nature, cybersecurity cannot solely be the burden of any individual entity, industry, or sector. Medical and health infrastructure are no exception to this.

While much has been written on the nature of the threats faced by medical and healthcare facilities and the technical measures these facilities need to undertake to ramp up their cybersecurity, little focus has been given to operationalising this norm from a governmental or macro perspective. This paper attempts to trace the evolution of the Bio-Cyber Norm and seeks to briefly examine a top-down, whole-of-nation approach to operationalising this norm as a due diligence obligation of a state vis-à-vis its medical services and facilities, contextualising it in the Indian scenario. It envisages the cybersecurity of medical services and facilities as something that can only be maintained by the collective efforts of all stakeholders in the medical ecosystem, including both governing authorities and private facilities. The paper concludes with recommendations to policy-makers. ■

DO NO HARM TO HOSPITALS

Under the law of armed conflict, medical personnel and facilities have traditionally enjoyed a protected status. Article 19 of the Geneva Convention I prohibits parties to a conflict from attacking units of medical services.⁸ Article 18 of the Geneva Convention IV mandates that civilian hospitals organised to give care to the wounded and sick may in no circumstances be objects of attack.⁹ Article 12 of Additional Protocol I and Article 11 of Additional Protocol II require that medical units shall be respected and protected at all times.¹⁰ Under the Statute of the International Criminal Court, additionally, “[i]ntentionally directing attacks against (...) hospitals and places where the sick and the wounded are collected, provided they are not military objectives” constitutes a war crime in both international and non-international armed conflicts.¹¹ There is little dispute that the protected status of medical services and personnel/units during armed conflicts is part and parcel of customary international law.¹²

However, as states are coming to realise, there are no corresponding obligations during peacetime. To be clear, a state employing conventional means to destroy, disrupt or even hinder the work of medical facilities or personnel will still likely fall afoul of certain rules of international law that apply regardless of the nature of the target, such as the prohibition on the threat or use of force under Article 2(4) of the United Nations Charter. But the applicability of these rules in the realm of unconventional warfare, such as in cyberspace, is still heavily disputed. Indeed, cyberspace is often referred to as a “grey zone” in international law due to the lack of clarity on the legality of operations conducted in cyberspace. Cyber operations are also a preferred mode for states to achieve strategically beneficial outcomes given that the inherent structure of cyberspace offers anonymity to states, making it extremely difficult to hold them accountable for any internationally wrongful act in cyberspace. Needless to say, these challenges apply equally to fixing responsibility on non-state actors. The result has been a steady rise

⁸ Art. 19, *Geneva Convention on Wounded and Sick in Armed Forces in the Field, 1949* (Geneva Convention I).

⁹ Art. 18, *Geneva Convention Relative to Protection of Civilian Persons in Time of War, 1949* (Geneva Convention IV).

¹⁰ Article 12 of *Additional Protocol I to the Geneva Conventions, 1977*; Article 11 of *Additional Protocol II to the Geneva Conventions, 1977*.

¹¹ Article 8(2)(b)(ix) and (e)(iv) of the *Rome Statute of the International Criminal Court*.

¹² *Secretary of Defence. 2016. “Principles Related to the Protection of Medical Care Provided by Impartial Humanitarian Organizations During Armed Conflict.”* Washington: Pentagon. (<https://dod.defense.gov/Portals/1/Documents/pubs/Principle-Promulgation-Memo.pdf>).

in state-sponsored or -conducted cyber-attacks in the past decade, with the most insidious being the deliberate attacks on hospitals and medical services engaged in combating the Covid-19 pandemic.

It is no surprise therefore that states are prepared to support a norm uniquely applicable to and aimed at the protection of medical facilities and infrastructure in cyberspace. This emerging cyber norm can in fact be viewed as the result of a gradual evolution of norms in this field. Inter-governmental efforts to understand how to regulate cyberspace from the perspective of international law began with the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (“UN GGE”), first established in 2004. There have been six iterations of the UN GGE since then, with only those since 2010 resulting in any noteworthy outcomes. The 2010 UN GGE recognised the importance of critical infrastructure, emphasising and recommending dialogue between states to “reduce collective risk and protect critical national and international infrastructure”.¹³ The 2013 UN GGE then acknowledged, for the first time, the applicability of international law to cyberspace, noting that “[s]tate sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.”¹⁴ Additionally, the report also recorded several voluntary, non-binding norms on a consensus basis. In this vein, the report noted that states “should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs”.¹⁵ This was subsequently re-affirmed by the 2015 UN GGE report, which besides stating that “[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public”¹⁶, also noted the need for states to take “appro-

¹³ United Nations Group of Governmental Experts. 2010. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” (<https://doi.org/https://undocs.org/A/65/201>).

¹⁴ United Nations Group of Governmental Experts. 2013. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” (<https://doi.org/https://undocs.org/A/68/98>).

¹⁵ Report of the Group of Governmental Experts 2013, 8.

¹⁶ United Nations Group of Governmental Experts. 2015. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” (<https://dig.watch/sites/default/files/UN%20GGE%20Report%202015%20%28A-70-174%29.pdf>). Para. 13(f).

priate measures to protect their critical infrastructure from ICT threats”.¹⁷ This report was also adopted by the United Nations General Assembly.¹⁸ The stage was thus set for a due diligence norm to emerge in cyberspace.

However, as with most international fora, a contestation of interests and ideologies between states ultimately scuttled any further progress and the 2017 UN GGE concluded without being able to achieve consensus on how to apply the norms agreed upon.¹⁹ This allowed some states to successfully argue for and establish the OEWG as a platform for continuing the discussions on cyber norms.²⁰ The OEWG has appeal as an alternative to the UN GGE since it has a mandate largely similar to the UN GGE (insofar as it also involves further developing norms and principles for responsible state behaviour in cyberspace), and its egalitarian structure projects a more open, fair and democratic process in dealing with crucial issues in cyberspace,²¹ whereas each iteration of the UN GGE was composed of 25 select states with membership often changing from one iteration to another.²² Pertinently, however, the General Assembly has renewed the mandate of the UN GGE for the period 2019–2021 and its session is currently ongoing, in parallel with the first session of the OEWG.²³

It was through responses to a Draft Paper issued by the Chair of the OEWG (“Pre-Draft”) that many states’ attention was drawn to the dangerous trend of malicious cyber-activities against hospitals and other medical facilities. The ICRC, in its comments to the draft paper, drew attention to critical infrastructure enabling the delivery of essential services to the population, and, in this vein, stressed the need to explicitly mention the healthcare sector in

¹⁷ *Report of the Group of Governmental Experts 2015*, para. 13(g).

¹⁸ *United Nations General Assembly*. 2015. “Developments in the Field of Information and Telecommunications in the Context of International Security.” A/RES/70/237, 23 December. (<https://undocs.org/A/RES/70/237>).

¹⁹ D’Incau, Fosca and Stefan Soesanto. 2017. “The UN GGE Is Dead: Time to Fall Forward.” *European Council on Foreign Relations*, 15 August. (https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance).

²⁰ De Tomas Colatin, Samuele. 2018. “A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace.” *NATO CCDCOE*. (<https://ccdcoe.org/incyber-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/>).

²¹ Cristiano, Fabio. 2020. “The Road Toward Agonistic Pluralism for International Cyber Norms”. *Council on Foreign Relations*, 6 July. (<https://www.cfr.org/blog/road-toward-agonistic-pluralism-international-cyber-norms>).

²² *Dig.watch*. 2020. “UN GGE and OEWG.” (<https://dig.watch/processes/un-gge>).

²³ *Dig.watch*. 2020. “UN GGE and OEWG.”

the report as being particularly vulnerable to cyber-attacks.²⁴ It then adapted the existing due diligence norm to propose a new one – a norm prohibiting states from harming as well as requiring them to ensure the safety and security of medical services and facilities.²⁵ A number of states, in their own comments to the OEWG draft, also decried and denounced the targeting of these facilities in recent times.²⁶ This has been followed up by a joint proposal from Australia, the Czech Republic, Estonia, Japan, Kazakhstan and the United States of America for including specific text in the OEWG draft that highlighted reports of “attempted and actual damage or impairment by cyber means of the use and operation of critical infrastructure providing services to the public (including healthcare/medical services, facilities and systems, and crisis response organisations) during the Covid-19 global pandemic.”²⁷ The joint proposal moved for the acceptance of slightly different norms that are also reflected in the 2015 GGE Report –

“...A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

...States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cyber-security and the protection of critical infrastructures, and other relevant resolutions.”²⁸

²⁴ United Nations Open-Ended Working Group. 2020. “Comments by the International Committee of the Red Cross on the Initial ‘Predraft’ of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security.” (<https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-icrc-on-initial-pre-draft-report-of-oewg.pdf>).

²⁵ United Nations Open-Ended Working Group. 2020. “Comments by the International Committee of the Red Cross.”

²⁶ United Nations Open-Ended Working Group. 2020. “Comments Submitted by the Czech Republic in Reaction to the Initial ‘Pre-Draft’ Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.” (<https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf>); United Nations Open-Ended Working Group. 2020. “France’s Response to the Pre-Draft Report from the OEWG Chair.” (<https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf>); United Nations Open-Ended Working Group. 2020. “The Kingdom of the Netherlands’ Response to the Pre-Draft Report Of the OEWG.” (<https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf>).

²⁷ United Nations Open-Ended Working Group. 2020. “Joint Proposal from a Number of Member States on the Protection of Health Infrastructure.” (<https://front.un-arm.org/wp-content/uploads/2020/05/final-joint-oewg-proposal-protection-of-health-infrastructure.pdf>).

²⁸ Report of the Group of Governmental Experts 2015, para. 13(f) and 13(g).

But the proposal also notes that member states of the OEWG all considered medical services and medical facilities to be critical infrastructure for the purpose of these suggested norms.²⁹ Hence, there is no reason to believe that the extent of protection for medical services and facilities will not remain the same as or equivalent to the proposal by the ICRC. ■



OPERATIONALISING THE BIO-CYBER NORM

Asian countries, including those in the Indian subcontinent, face a somewhat paradoxical problem. Most of their populations (barring countries like Singapore, Malaysia and South Korea), have a substantial digital divide that their governments are rigorously attempting to bridge with the goal of harnessing the full benefits of a digital economy.³⁰ At the same time, this impetus to the digital revolution in these countries also means that as more and more sectors digitise and take their operations online, they open themselves up to cyber threats. The interconnected nature of cyberspace means that a vulnerability or weakness in one sector automatically renders other sectors also vulnerable to exploitation.³¹ This makes cybersecurity in any given sector a national priority and an area that the government should take the lead in, through laying down regulations, or investments, or any of a host of other policy measures available to them.³² At the same time, a heavily networked cyber environment also means that other stakeholders, such as private players, will also need to ensure they play an equal role to shore up, maintain and safeguard cybersecurity. These realities mean that the burden of ensuring cybersecurity for a given sector has to be a shared responsibility between the government and other stakeholders, which, in other words, calls for a multi-stakeholder approach. This is especially so in the medical and healthcare industry, which while currently not regulated in terms of cybersecurity, requires specialised standards- or regulations-setting, necessitating the cooperation and co-option of expertise from the medical industry.

From a macro-perspective, implementing the Bio-Cyber Norm *inter alia* requires action in three key areas:

³⁰ ASEAN. 2010. “2010 Master Plan on ASEAN Connectivity: One Vision, One Identity, One Community.” (<https://cil.nus.edu.sg/wp-content/uploads/formidable/18/2010-Master-Plan-on-ASEAN-Connectivity.pdf>).

³¹ United Nations Counter-Terrorism Centre. 2018. “The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium of Good Practices.” (https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf).

³² NATO Cooperative Cyber Defence Centre for Excellence. 2013. “National Cyber Security Strategy Guidelines.” (https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf).



1. Articulating a National Cyber Security Strategy

The cyber-attacks on hospitals and healthcare facilities cannot be responded to or dealt with solely on an individual or case-to-case basis. Weak healthcare cybersecurity is also symptomatic of problematic policy priorities, such as lack of regulations, inadequate incentivisation, and so on. Additionally, cybersecurity policy goals for the healthcare industry (both public and private) should ideally be congruent with measures in other sectors, given that its major units, like hospitals, are themselves highly dependent on other services such as power, energy and transportation. In any case, no matter the sector, a well-functioning critical information infrastructure ecosystem requires policy-makers to address cybersecurity on a national level.³³ A national cybersecurity strategy provides guidance to policy-makers and other stakeholders regarding a nation's cybersecurity policy priorities. A properly articulated national cybersecurity strategy (i) enables government departments to identify strategic objectives, (ii) translates the policy-maker's vision into coherent and implementable policies, (iii) pinpoints the resources to fulfil the strategic objectives and specifies how these resources are to be used; (iv) clarifies how the nation might act in international affairs and within the context of relevant international organisations; and (v) states how it is to be linked to other, related strategies.³⁴ A national strategy for cybersecurity signals to relevant stakeholders what macro-objectives the government plans to achieve for national cybersecurity, offering some predictability, which in turn allows stakeholders to align their own courses of action with governmental objectives. These strategies also usually include, or are accompanied by, the clear identification of governmental agencies or regulators responsible for implementing the policies identified.

Many, if not most, countries in Asia, including members of significant groups like ASEAN, have neither developed nor implemented comprehensive national cybersecurity strategies. While India has already articulated a cybersecurity strategy previously in 2013, it was less a comprehensive cybersecurity strategy than a policy

33 "National Cyber Security Strategy Guidelines" 7.

34 "National Cyber Security Strategy Guidelines" 7.

document identifying some goals for cybersecurity³⁵ and is also largely outdated. On the positive side, India is currently in the process of articulating an updated, fully comprehensive national cybersecurity strategy, although it is unclear when it will be released.

2. Articulating a Sector-Specific Cybersecurity Strategy for the Healthcare Industry

While a *national* cybersecurity strategy identifies goals for a nation's cybersecurity system and identifies a roadmap to achieve those goals, *sectoral* cybersecurity strategies do the same for specific sectors. Identifying key sectors vital to ensuring the cyber health of a nation is also important. This is already being done in most nations in the form of identifying "critical information infrastructure" ("CII"). Notably, a General Assembly resolution from as far back as 2004 called upon states to take action to identify and protect their CII.³⁶ India's nodal agency for protecting CII is the National Critical Information Infrastructure Protection Centre ("NCIIPC").³⁷ Under Section 70 of India's Information Technology Act, 2000, CII is defined as a "computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety".³⁸ However, the CII identified in India include only the defence, banking and financial, ICT and telecommunications, transportation, power and energy sectors, the Ministries of Home Affairs, External Affairs and Heavy Industries as well as the Niti Aayog (previously known as the Planning Commission).³⁹ The medical or healthcare sector is currently conspicuously absent from this classification.

Aside from this, preparing a sectoral cybersecurity strategy for the healthcare sector will also, needless to say, require a thorough understanding of the unique attributes of this sector

³⁵ Centre for Communication Governance. 2020. "Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020." New Delhi, National Law University Delhi.

³⁶ United Nations General Assembly. 2013. "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures." A/RES/58/199 2004, 23 December 2013. (<https://digitallibrary.un.org/record/509571?ln=en>).

³⁷ Government of India, Department of Electronics and Information Technology. 2014. "Notification." (<https://www.meity.gov.in/>).

³⁸ Section 70, Information Technology Act, 2000.

³⁹ Government of India, National Critical Information Infrastructure Protection Centre. 2013. "Guidelines for the Protection of Critical Information Infrastructure, Version 1.0." (<https://www.cii.in/uploads/1Guidelines%20for%20Protection%20of%20NCII-CoverPage599.pdf>).

as well as the motivations of malicious actors targeting healthcare facilities. Sectoral risk profiles that quantitatively assess the cyber threat landscape as well as current levels of sectoral cybersecurity maturity will also prove beneficial since they can serve as a reference for all organisations in the sector, instead of each organisation separately undertaking this exercise and expending resources.⁴⁰

Designating the medical or healthcare sector as critical information infrastructure will go a long way towards ensuring their cyber resilience and the continuity of these essential services. The NCIIPC in India, for instance, is responsible for taking “all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorised access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders.”⁴¹ It periodically lays down guidelines for the protection of critical information infrastructure and its guiding principles include adopting risk management approaches, ensuring compliance with its guidelines, advisories and alerts, and facilitating sharing of information on emerging threats, cyber-attacks, vulnerabilities, etc. with CII.⁴² If the healthcare sector is classified as CII, it would also come under the ambit of the NCIIPC, which, through consultations with the relevant stakeholders, could begin to standardise cybersecurity measures in the sector through regulations uniquely tailored to healthcare. Additionally, it is also part of the NCIIPC’s mandate to establish sectoral Computer Emergency Response Teams or CERTs to deal with critical sector-specific issues – in this regard, a Med-CERT with the relevant expertise could do much to alleviate the healthcare sector’s cybersecurity woes as a first responder. Currently, the Indian Computer Emergency Response Team or CERT-In is operational, with the stated objectives of securing the Indian cyberspace, preventing and responding to cyber-attacks against the Indian cyberspace and enhancing cybersecurity awareness among common citizens.

⁴⁰ International Telecommunication Union. 2018. “Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity.” (https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018).

⁴¹ Datta, Saikat. 2016. “Defending India’s Critical Information Infrastructure – The Development and Role of the National Critical Information Infrastructure Protection Centre (NCIIPC).” *Internet Democracy Project 2*. (<https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf>).

⁴² Government of India, National Critical Information Infrastructure Protection Centre. 2015. “Guidelines for the Protection of Critical Information Infrastructure, Version 2.0.” (https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf).

A Med-CERT would greatly streamline CERT-In's abilities to secure medical and healthcare facilities.

Sectoral focus for healthcare is vital to operationalising the Bio-Cyber Norm. This is all the more so given that the Indian government is set to digitise health-related information on a massive scale. The government's National Health Stack ("NHS") project is intended to be a digital infrastructure built with the aim of making the health insurance system more transparent and robust.⁴³ Among other things, it is proposed to consist of an "electronic national health registry", intended to serve as a single source for health data in the nation, with access to hospitals, labs, insurance companies, etc.⁴⁴ The National e-Health Policy released in 2017 also discusses leveraging an "integrated health information system" that "serves the needs of all stake-holders and improves efficiency, transparency, and citizen experience."⁴⁵ Both the National e-Health Policy⁴⁶ as well as the National Health Stack⁴⁷ suggest using the national identification number or "Aadhaar Number" for identification purposes. The implications of a cybersecurity breach in such envisaged systems would be massive. Separately, on the bright side, India is also on the cusp of passing the Personal Data Protection Bill 2019, under which medical or health-related information will fall under the "sensitive personal data" category, thereby commanding a higher level of protection as opposed to other personal data such as names, addresses and so on.⁴⁸

This regulation will ensure that healthcare facilities will be held accountable if they do not ensure the implementation of adequate safeguards to secure personal and medical data. While the focus of the legislation is not on cybersecurity, it will certainly assist in bringing relevant stakeholders up to standard in some respects, with regard to personal data at least.

⁴³ Ghosh, Abantika. 2019. "Stack and Blueprint – Building Digital Infrastructure for National Health Database." *The Indian Express*, 5 November. (<https://indianexpress.com/article/explained/explained-stack-and-blueprint-building-digital-infrastructure-for-national-health-database-6103245/>).

⁴⁴ Niti Aayog, Government of India. 2020. "National Health Stack- Strategy and Approach." (https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Documents-for-consultation.pdf).

⁴⁵ Ministry of Health and Family Welfare, Government of India. 2017. "National Health Policy 2017." (https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf).

⁴⁶ Ministry of Health and Family Welfare. 2017. "National Health Policy 2017."

⁴⁷ Niti Aayog. 2020. "National Health Stack- Strategy and Approach."

⁴⁸ Clause 2(36), Personal Data Protection Bill 2019; Clause 33, Personal Data Protection Bill 2019; Clause 34 Personal Data Protection Bill 2019.

But these disparate measures need to come together in the form of a coherent and cogent policy that, while promoting the harnessing of the full benefits of healthcare technology, ensures adequate safety and security of both the data and services involved.

3. Ensuring Last-Mile Cybersecurity for Healthcare

A cybersecurity ecosystem is only as strong as its weakest link. Hence, although it is essential for the government to implement policy measures, including regulations, it is possibly even more important for healthcare facilities and stakeholders to do their bit to support robust cybersecurity. From an organisational perspective, hospitals will need to allocate sufficient funds to information security. Most hospitals do not have dedicated information or cybersecurity teams, instead delegating the management of cybersecurity issues to their IT teams, which may not have the relevant expertise. Another problem with this is variance in objectives – IT teams often aim to make systems easy-to-use, whereas cybersecurity teams aim to make them secure.⁴⁹ This often leads to discarding of cybersecurity objectives in favour of IT ones.⁵⁰ Thus, security policies in hospitals need to be carefully drafted in order to make sure adequate attention is paid to cybersecurity. These security policies will necessarily have to assess and identify the appropriate systems/networks/databases that are most important vis-à-vis cybersecurity and threat perspectives. Equally importantly, these policies will have to be strictly enforced.

At the technical level, it is highly important that all hospital staff are properly trained in basic cyber hygiene. This will greatly reduce the potential for security breaches and vulnerabilities. For context, the SingHealth cyber-attack was caused by weak administrator password practices and phishing emails.⁵¹ The cooperation and diligence of all relevant hospital staff will be of utmost importance in order to avoid incidents on account of these failings. Additionally, while evermore interdependent

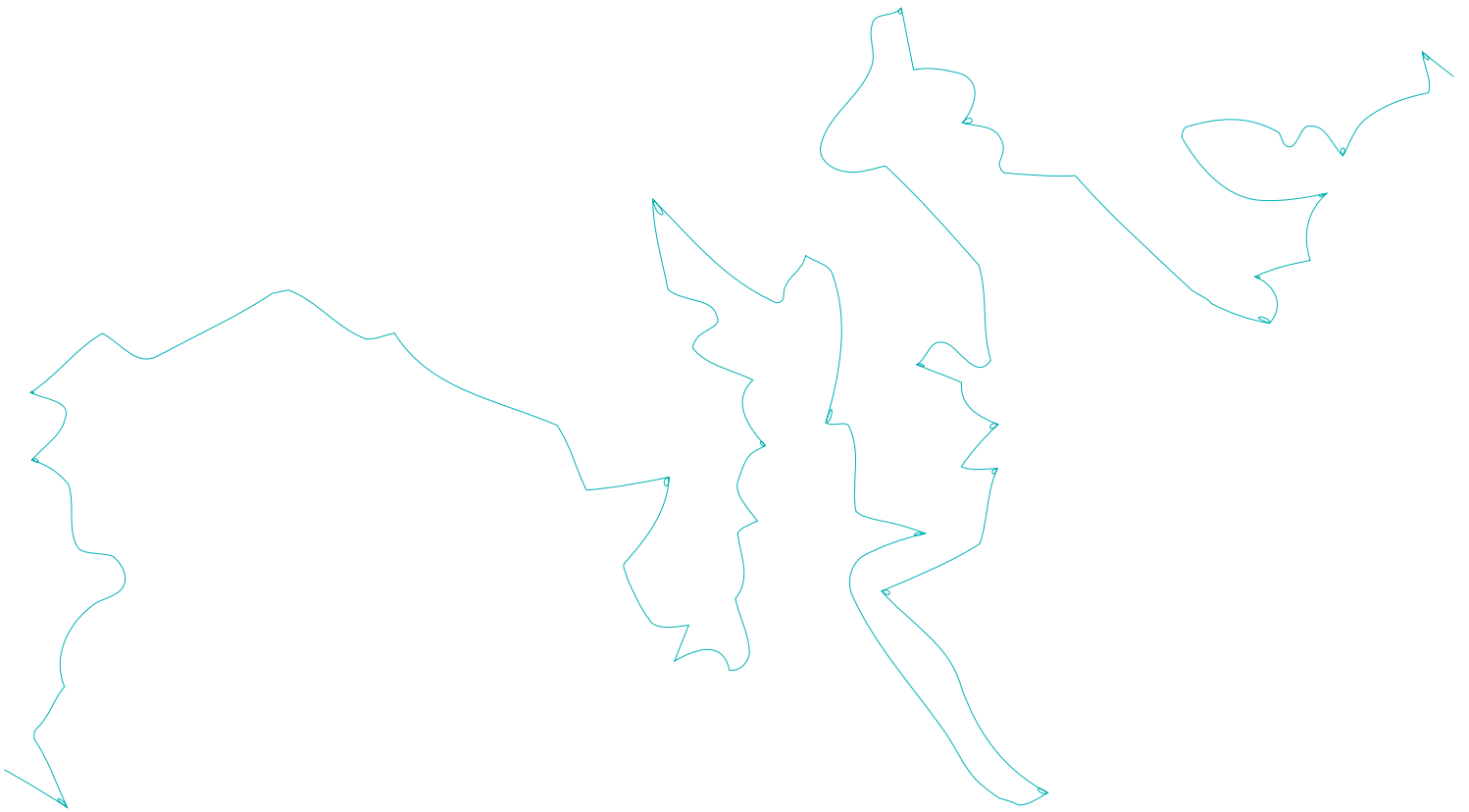
⁴⁹ *State of Cybersecurity & Cyber Threats in Healthcare Organizations*, 7.

⁵⁰ *State of Cybersecurity & Cyber Threats in Healthcare Organizations*, 7.

⁵¹ *Tham, Irene. 2019. "Probe Report on SingHealth Data Breach Points to Basic Failings." The Straits Times, 10 January. (<https://www.straitstimes.com/singapore/probe-report-on-singhealth-data-breach-points-to-basic-failings>).*

and interoperable technology may be a boon in one sense, it also increases the threat surface and points of access for malicious cyber actors.⁵² Hence, hospitals, while adopting the Internet-of-Things (“IoT”) to connect diverse systems, including printers, scanners, medical devices and so on, should be aware of this issue and plan accordingly for networked cybersecurity and cyber resilience while evolving their systems. In the same vein, the medical industry is also heavily reliant on legacy systems that are outdated and no longer supported with security updates. Needless to say, these systems need to be overhauled.

These are some last-mile, but extremely important, measures that individual hospitals and healthcare facilities will need to implement to achieve defensible cybersecurity. ■



⁵² *State of Cybersecurity & Cyber Threats in Healthcare Organizations*, 8.

Healthcare and medical care facilities arguably perform the most essential of services to society, more so currently than ever. It is a mark of recognition of this important fact that the Bio-Cyber Norm is slowly emerging in the otherwise highly contested arena of cyber norms. That states have become cognisant of and are training their guns on this issue is encouraging, given how disheartening it is that malicious cyber actors are sparing not even these essential services in their quest to use the cyberspace for strategic or monetary advantages. To be sure, there is a long way to go, but with time and concerted effort from states, there is currently every hope that the Bio-Cyber Norm will carve out a much-needed special place of protection for medical and healthcare personnel and facilities in cyberspace. The norm already has multi-stakeholder support in the form of academics and non-state organisations calling for its adoption through the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector.⁵³

However, India and other Asian countries should not wait for any obligation to crystallise in international law before taking action. As the paper has discussed, states should:

- 1/ Articulate a strong and clear national cybersecurity strategy or a comparable document setting out broad policy goals and objectives in accordance with the given country's strengths and weaknesses;
- 2/ Articulate a sector-specific cybersecurity strategy for the medical and healthcare sector, taking into account relevant medical expertise;
- 3/ Require hospitals and other facilities to each draw up a cybersecurity strategy or management plan while simultaneously training staff (both technical and non-technical) in cyber hygiene, thereby ensuring the capability to enforce it.

⁵³ Oxford Institute for Ethics, Law and Armed Conflict. 2020. "The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector." (<https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea>).

The Authors

Sarvjeet Singh is a Fellow at National Law University Delhi.

Sharngan Aravindakshan is a Programme Officer at the Centre for Communication Governance at National Law University Delhi.

The authors are grateful to Smitha Krishna Prasad for her help with the initial abstract and continued discussions while writing the draft.

References

ASEAN. 2010. "2010 Master Plan on ASEAN Connectivity: One Vision, One Identity, One Community."
(<https://cil.nus.edu.sg/wp-content/uploads/formidable/18/2010-Master-Plan-on-ASEAN-Connectivity.pdf>).

Barnes, Julian E., and David E. Sanger. 2020. "Russian Intelligence Agencies Push Disinformation on Pandemic." *The New York Times*, 28 July.
(<https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html>).

Centre for Communication Governance. 2020. "Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020." New Delhi, National Law University Delhi.

Cristiano, Fabio. 2020. "The Road Toward Agonistic Pluralism for International Cyber Norms". Council on Foreign Relations, 6 July.
(<https://www.cfr.org/blog/road-toward-agonistic-pluralism-international-cyber-norms>).

Datta, Saikat. 2016. "Defending India's Critical Information Infrastructure – The Development and Role of the National Critical Information Infrastructure Protection Centre (NCIIPC)." Internet Democracy Project 2.
(<https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf>).

De Tomas Colatin, Samuele. 2018. "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace." NATO CCDCOE.
(<https://ccdcoe.org/incyber-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/>).

Dig.watch. 2020. "UN GGE and OEWG."
(<https://dig.watch/processes/un-gge>).

D'Incau, Fosca and Stefan Soesanto. 2017. "The UN GGE Is Dead: Time to Fall Forward." European Council on Foreign Relations, 15 August.
(https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance).

Government of India, Department of Electronics and Information Technology. 2014. "Notification."
(<https://www.meity.gov.in/>).

Government of India, National Critical Information Infrastructure Protection Centre. 2013. "Guidelines for the Protection of Critical Information Infrastructure, Version 1.0."
(<https://www.cii.in/uploads/1Guidelines%20for%20Protection%20of%20NCII-CoverPage599.pdf>).

Government of India, National Critical Information Infrastructure Protection Centre. 2015. "Guidelines for the Protection of Critical Information Infrastructure, Version 2.0."
(https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf).

Ghosh, Abantika. 2019. "Stack and Blueprint – Building Digital Infrastructure for National Health Database." The Indian Express, 5 November.
(<https://indianexpress.com/article/explained/explained-stack-and-blueprint-building-digital-infrastructure-for-national-health-database-6103245/>).

International Telecommunication Union. 2018. "Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity."
(https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018).

Kwang, Kevin. 2018. "Singapore Health System Hit by ,Most Serious Breach of Personal Data' in Cyberattack; PM Lee's Data Targeted." CNA, 18 October.
(<https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318>).

Le Bris, Aurore and Walid El Asri. 2017. "State of Cybersecurity & Cyber Threats in Healthcare Organizations – Applied Cybersecurity Strategy for Managers." Essec Business School Strategic Report.
(<http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf>).

Ministry of Health and Family Welfare, Government of India. 2017.

"National Health Policy 2017."

(https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf).

NATO Cooperative Cyber Defence Centre for Excellence. 2013.

"National Cyber Security Strategy Guidelines."

(https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf).

Niti Aayog, Government of India. 2020. "National Health Stack-Strategy and Approach."

(https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf).

Oxford Institute for Ethics, Law and Armed Conflict. 2020. "The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector."

(<https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.>).

Porter, Sophie. 2020. "Cyberattack on Czech Hospital Forces Tech Shutdown during Coronavirus Outbreak." Healthcare IT News, 3 April.

(<https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak>).

Secretary of Defence. 2016. "Principles Related to the Protection of Medical Care Provided by Impartial Humanitarian Organizations During Armed Conflict." Washington: Pentagon.

(<https://dod.defense.gov/Portals/1/Documents/pubs/Principle-Promulgation-Memo.pdf>).

Staff Reporter. 2020. "German Hospital Hacked, Patient Taken to Another City Dies." Associated Press, 17 September.

(<https://apnews.com/cf8f8eee1adcec69bcc864f2c4308c94>).

Tham, Irene. 2019. "Probe Report on SingHealth Data Breach Points to Basic Failings." The Straits Times, 10 January.

(<https://www.straitstimes.com/singapore/probe-report-on-singhealth-data-breach-points-to-basic-failings>).

United Nations General Assembly. 2013. "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures."

A/RES/58/199 2004, 23 December 2013.

(<https://digitallibrary.un.org/record/509571?ln=en>).

United Nations General Assembly. 2015. "Developments in the Field of Information and Telecommunications in the Context of International Security." A/RES/70/237, 23 December.
(<https://undocs.org/A/RES/70/237>).

United Nations Group of Governmental Experts. 2010. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security."
(<https://doi.org/https://undocs.org/A/65/201>).

United Nations Group of Governmental Experts. 2013. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security."
(<https://undocs.org/A/68/98>).

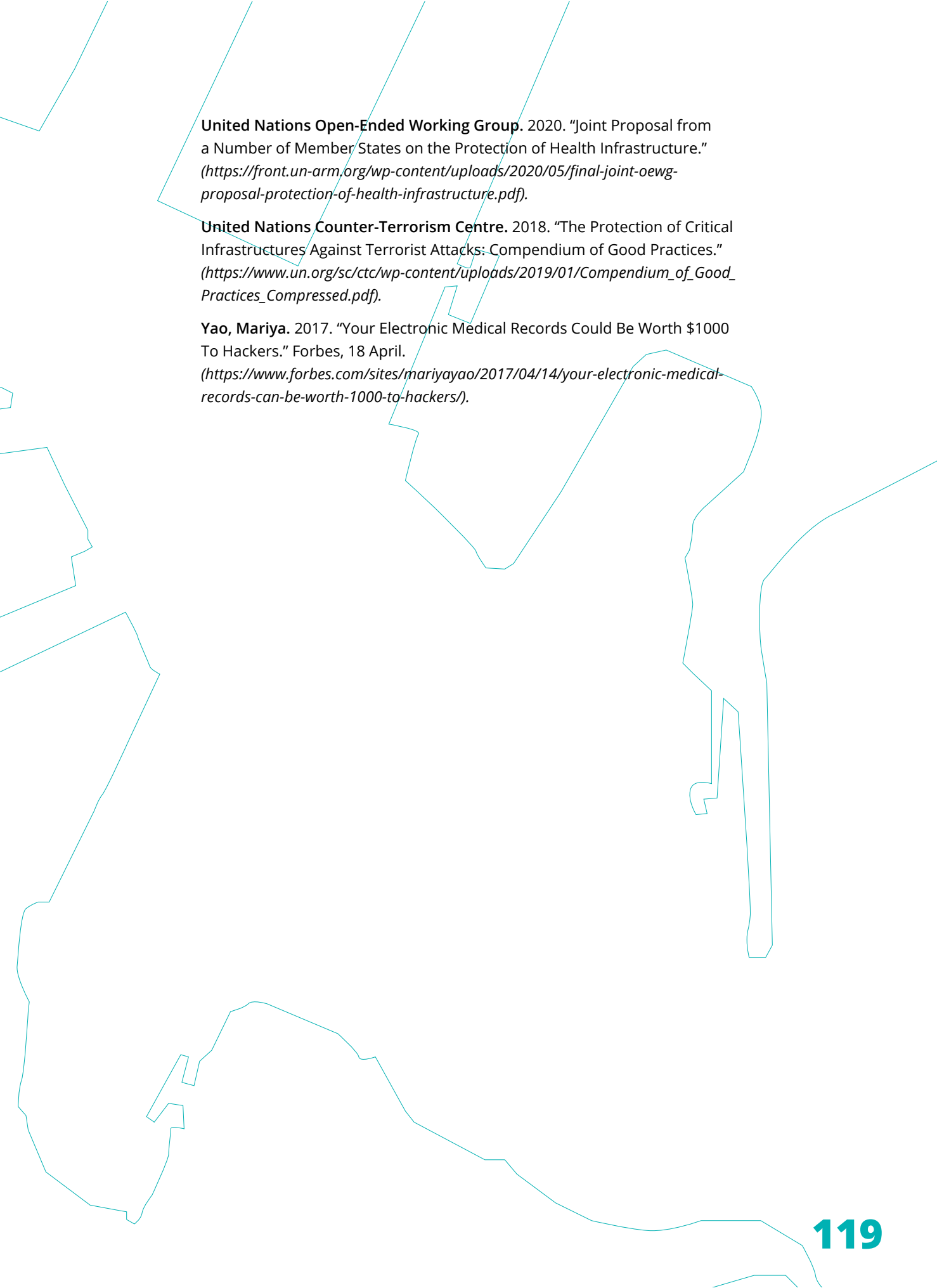
United Nations Group of Governmental Experts. 2015. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security."
(<https://dig.watch/sites/default/files/UN%20GGE%20Report%202015%20%28A-70-174%29.pdf>).

United Nations Open-Ended Working Group. 2020. "Comments by the International Committee of the Red Cross on the Initial 'Predraft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security."
(<https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-icrc-on-initial-pre-draft-report-of-oewg.pdf>).

United Nations Open-Ended Working Group. 2020. "Comments Submitted by the Czech Republic in Reaction to the Initial 'Pre-Draft' Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security."
(<https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf>).

United Nations Open-Ended Working Group. 2020. "France's Response to the Pre-Draft Report from the OEWG Chair."
(<https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf>);

United Nations Open-Ended Working Group. 2020. "The Kingdom of the Netherlands' Response to the Pre-Draft Report Of the OEWG."
(<https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf>).



United Nations Open-Ended Working Group. 2020. "Joint Proposal from a Number of Member States on the Protection of Health Infrastructure." (<https://front.un-arm.org/wp-content/uploads/2020/05/final-joint-owg-proposal-protection-of-health-infrastructure.pdf>).

United Nations Counter-Terrorism Centre. 2018. "The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium of Good Practices." (https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf).

Yao, Mariya. 2017. "Your Electronic Medical Records Could Be Worth \$1000 To Hackers." *Forbes*, 18 April. (<https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/>).