Cyber attacks and cyber (mis)information operations during a pandemic

Article

Published Version

Cyber Attacks and Cyber (Mis)information Operations During a Pandemic

Marko Milanovic* & Michael N. Schmitt**

INTRODUCTION

The COVID-19 pandemic has been accompanied by reprehensible cyber operations directed against medical facilities and capabilities, as well as by a flood of

* Professor of Public International Law, University of Nottingham School of Law. The discussion on misinformation draws on my earlier three part series on *Viral Information and the Freedom of Expression* on EJIL: TALK!, Apr. 13-14, 2020, https://perma.cc/9YLR-YE94.

** Professor of International Law, University of Reading; Francis Lieber Distinguished Scholar, West Point; Strauss Center Distinguished Scholar and Visiting Professor of Law, University of Texas; Charles H. Stockton Distinguished Scholar-in-Residence, U.S. Naval War College.

misinformation. In the Czech Republic, for example, Brno University Hospital was targeted in an as yet unattributed attack that forced the facility to shut down its IT network and that bled over into the affiliated Children's Hospital and the Maternity Hospital. Urgent surgeries had to be postponed, and the hospital could not perform its role as a designated COVID-19 testing center.[1] Similarly, cyber criminals have conducted ransomware attacks targeting medical facilities, including one against Hammersmith Medicines Research, which was on standby in the United Kingdom to test vaccines. Although the primary attack was foiled, patient medical data were exfiltrated and held for ransom.[2] Many other hostile cyber operations that directly interfered with the delivery of care, medical logistics, and the research necessary to effectively fight the virus and its spread have occurred around the world.[3]

So too have hostile cyber operations been directed against public health activities. For instance, one took down the Champaign-Urbana Public Health District's website, on which vital COVID-19 information was being posted. As a result, alternative websites had to be activated to ensure that the information was available to the public.[4] At the national level, the U.S. Department of Health and Human Services was the target of a distributed denial of service attack lasting several hours, although it fortunately failed to significantly affect the agency's systems. A state actor is suspected of having conducted the operation.[5]

And the World Health Organization, which despite politicized claims to the contrary plays a critical role in the global response to the pandemic, was subjected to malicious cyber operations that tried to secure the passwords of its personnel. Although the motives remain unclear, the head of global research and analysis at the Kaspersky cyber security firm noted that "[a]t times like this, any information about cures or tests or vaccines relating to coronavirus would be priceless and the priority of any intelligence organization of an affected country."[6] Cyber criminals have also engaged in phishing attacks impersonating the

1. Catalin Cimpanu, *Czech Hospital Hit by Cyberattack While in the Midst of a COVID-19 Outbreak*, ZDNET (Mar. 13, 2020), https://perma.cc/E4N9-XFHT; Sean Lyngaas, *Czech Republic's Second-Biggest Hospital is Hit by Cyberattack*, CYBERSCOOP (Mar. 13, 2020), https://perma.cc/3QDR-WXDH.

2. Davey Winder, *COVID-19 Vaccine Test Center Hit by Cyber Attack, Stolen Data Posted Online*, FORBES (Mar. 23, 2020), https://perma.cc/E96C-H5R2.

3. Aaron Holmes, *Hackers are Targeting Hospitals Already Stretched Thin from Fighting the Coronavirus—and Experts Say the Worst Cyberattacks May Still Be to Come*, BUS. INSIDER (Apr. 14, 2020), https://perma.cc/LY8C-X49Q; *Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware*, KREBSONSECURITY (May 6, 2020), https://perma.cc/4RAB-XS74; Joseph Marks, *Hospitals Face a Surge of Cyberattacks during the Novel Coronavirus Pandemic*, WASH. POST (Apr. 15, 2020), https://perma.cc/YWX7-C4G8.

4. Debra Pressey, *C-U Public Health District's Website Held Hostage by Ransomware Attack*, NEWS GAZ. (Champaign, IL), Mar. 11, 2020, https://perma.cc/GM7B-TDBL.

5. Shira Stein & Jennifer Jacobs, *Cyber-Attack Hits U.S. Health Agency Amid COVID-19 Outbreak*, BLOOMBERG (Mar. 16, 2020), https://perma.cc/ZC47-AXER.

6. Raphael Satter, Jack Stubbs & Christopher Bing, *Elite Hackers Target WHO as Coronavirus Cyberattacks Spike*, REUTERS (Mar. 23, 2020, 3:08 PM), https://perma.cc/D7NP-9THA.

WHO to gain access to information in personal computers, in one case distributing a fake "My Health e-book" attachment containing a file with malware.[7]

Additionally, the COVID-19 crisis has spawned an epidemic of online misinformation. At times, the claims have been farcical. For instance, individuals in the United Kingdom and the Netherlands have vandalized phone masts in reaction to online conspiracy theories tying the construction of 5G masts to the pandemic.[8] Often the claims are politically motivated, as with suggestions that the virus was created in, and escaped from, a Chinese laboratory. In the United States, the Director of the National Institute of Allergy and Infectious Diseases, Dr. Anthony Fauci, found it necessary to debunk the story, which had been impliedly supported by President Trump during one of his lengthy news conferences.[9] And the scale of the misinformation is truly daunting.[10] According to the British regulator Ofcom, "almost half of UK online adults came across false or misleading information about the coronavirus (COVID-19)" in a single week in early April 2020.[11]

The contemporary power of misinformation and "fake news" to polarize societies and politics is hardly surprising. But the convergence of COVID-19 and viral misinformation is unique in its potential to cause significant societal harm, for the "infodemic" is disrupting the coordinated, medically sound response that is necessary to control the spread of the virus.[12] Tragically, it is even directly causing large-scale loss of human life. Consider Iran, where the government has reported that hundreds died after ingesting methanol or other high-proof alcohol, falsely believing social media claims that doing so would protect them from the virus.[13]

Some states appear to be leveraging the crisis to seek advantage in cyberspace. For example, the Syrian government has allegedly exploited the pandemic to distribute surveillance malware through watering hole attacks and third party app stores.[14] And a report by the State Department's Global Engagement Center, which has not been made public, apparently accuses China, Iran, and Russia of

7. Malwarebytes Labs, *Cybercriminals Impersonate World Health Organization to Distribute Fake Coronavirus E-book* (Mar. 18, 2020), https://perma.cc/5ERJ-78TQ.

8. The theories range from 5G causing COVID-19 to the lockdown measures being imposed as a distraction from the construction of 5G infrastructure and its alleged ill-effects. Jim Waterson & Alex Hern, *At Least 20 UK Phone Masts Vandalised Over False 5G Coronavirus Claims*, GUARDIAN (Apr. 6, 2020), https://perma.cc/FJ34-FTPT; *Dutch Telecommunications Towers Damaged by 5G Protestors: Telegraaf*, REUTERS (Apr. 11, 2020), https://perma.cc/3LC8-25LD.

9. John Haltiwanger, *Dr. Fauci Throws Cold Water on Conspiracy Theory that Coronavirus Was Created in a Chinese Lab*, BUS. INSIDER (Apr. 18, 2020), https://perma.cc/PP8A-HPER.

10. Aaron Holmes, *Roughly Half the Twitter Accounts Pushing to "Reopen America" Are Bots, Researchers Found*, BUS. INSIDER (May 22, 2020), https://perma.cc/3VHL-N3A4.

11. Ofcom, *Half of UK Adults Exposed to False Claims about Coronavirus* (Apr. 9, 2020), https://perma.cc/MWM7-CT74.

12. John Zarocostas, *How to Fight an Infodemic*, LANCET (Feb. 29, 2020); *Coronavirus Myths Explored*, MED. NEWS TODAY (April 6, 2020), https://perma.cc/JZ9Q-FCD2.

13. Bel Trew, *Coronavirus: Hundreds Dead in Iran from Drinking Methanol Amid Fake Reports It Cures Disease*, INDEPENDENT (Mar. 27, 2020), https://perma.cc/257C-CR9G.

14. *Lookout Research: Nation-State Mobile Malware Targets Syrians with COVID-19 Lures*, SECURITY (Apr. 16, 2020), https://perma.cc/RS8J-966L.

exploiting the crisis for propaganda and disinformation purposes against the United States. Those countries have reportedly suggested that COVID-19 is an American bioweapon, that China was not the source of the virus but that instead it was spread by U.S. troops, that the Trump administration's response was flawed while that of China was effective, and that the U.S. economy will be unable to tolerate the crisis. In some cases, state-run media outlets made the allegations, while in others government agencies were the source of the claims. As an example, Russia's defense ministry operates a website that has alleged Bill Gates had a role in creating the virus.[15] While the validity of these assertions, as well as those made against the three countries, may be a matter of contention, it is clear that online sources are being weaponized for political purposes by exploiting the pandemic.

Our goal in this article is to map the various obligations of states under general international law and human rights law with regard to malicious cyber and misinformation operations conducted by state and non-state actors during the pandemic. In Part I we consider cyber operations against health care facilities and capabilities during the COVID-19 pandemic, including public health activities operated by the government, and how such operations, when attributable to a state, can violate the sovereignty of other states, the prohibitions of intervention and the use of force, and the human rights of affected individuals. In Part II we perform a similar analysis with regard to state misinformation operations, especially those that directly or indirectly affect human life and health, whether such misinformation is targeting the state's own population or those of third states. In Part III we turn to the positive obligations states have to protect their populations from hostile cyber and misinformation operations, to the limits human rights law imposes on efforts to combat misinformation, and to protective obligations toward third states and their populations.

I. STATE CYBER OPERATIONS AGAINST HEALTH CARE SYSTEMS DURING THE PANDEMIC

From an international law point of view, it is especially significant that states and state backed hackers appear to be involved in some of the hostile cyber operations against health facilities and capabilities during the COVID-19 pandemic,[16] for international law generally governs the acts of states or those that are attributable to them, pursuant to the law of state responsibility. The lawfulness of cyber operations conducted by non-state actors, such as criminals, hacktivists, or terrorist groups, is generally not assessed by reference to international law. Instead, such activities are subject to the law of any state that enjoys prescriptive jurisdiction over the conduct and is in a position to exercise its enforcement or judicial

15. Betsy Woodruff Swan, *Russian, Chinese and Iranian Disinformation Narratives Echo One Another, Report Says*, POLITICO (Apr. 21, 2020), https://perma.cc/CY3C-TBDB.

16. Dado Ruvic, *U.S., UK Cyber Officials Say State-backed Hackers Taking Advantage of Outbreak*, REUTERS (Mar. 28, 2020), https://perma.cc/RCU7-UPYR.

jurisdiction.[17] Therefore, the first step in analyzing such operations is to determine who conducted them.

To determine whether a state is responsible for violating international law with respect to a cyber operation against a health facility or capability, or public health activity, the operation must be legally attributable to that state, and the act must have violated an international law obligation it owed the target state. In the parlance of the law of state responsibility, the "responsible state" will have committed an "internationally wrongful act" against the "injured state" upon the confluence of these two conditions.[18]

Attribution is clearest when the cyber operation is conducted by organs of the state, like the intelligence services, cyber agency, or armed forces.[19] However, states often turn to non-state groups, such as political hacktivists, terrorist groups, or the private sector to conduct their cyber operations. While there are several situations in which the actions of a non-state actor may be attributed to a state as a matter of law,[20] the most common involves the non-state entity "in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." The International Law Commission confirmed the customary status of this "secondary" rule of international law in its Articles on State Responsibility, a decades-long effort to restate that body of law.[21]

COVID-19-related cyber operations appear to have been committed both by state *de jure* organs and by other entities whose conduct is attributable to a state.[22] The Netherlands announced, for example, that it

> is 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. Not only are these operations highly deplorable examples of irresponsible state behaviour; in many instances, they constitute violations of international law.[23]

17. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS ch. 3 (Michael N. Schmitt gen. ed. 2017) [hereinafter TALLINN MANUAL 2.0].

18. Report of the International Law Commission to the General Assembly, art. 2, U.N. GAOR, 56th Sess., Supp. No. 10, at 32, U.N. Doc. A/56/10 (2001) [hereinafter Articles on State Responsibility].

19. *Id*. art. 4.

20. These include acting as a *de facto* organ of the state, exercising elements of government authority, acting in the absence or default of the official authorities, and engaging in conduct that is acknowledged and adopted by a state as its own. *Id*. arts. 4–5, 9, and 11, respectively.

21. *Id*. art. 8. Primary rules of international law set forth rights and obligations, whereas secondary rules involve the responsibility of states and remedies such as assurances, guarantees, and reparations.

22. Peter Beaumont, Julian Borger & Daniel Boffey, *Malicious Forces Creating "Perfect Storm" of Coronavirus Disinformation*, GUARDIAN, (Apr. 24, 2020), https://perma.cc/ZA3Q-NH48; Edward Wong, Matthew Rosenberg & Julian E. Barnes, *Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say*, N.Y. TIMES (Apr. 22, 2020), https://perma.cc/33WT-E6FZ.

23. The Kingdom of the Netherlands' Response to the Pre-draft Report of the OEWG [UN Open-Ended Working Group], ¶2 (n.d.), https://perma.cc/9XY5-SFXG.

And the Cyber Security Centre of the Australian Signals Directorate has warned that Advanced Persistent Threat (APT) actors are targeting the nation's health sector and COVID-19 essential services.[24] APT cyber operations are most frequently thought to be conducted by states because of the operational sophistication that is necessary to mount them.

The discussion that follows in this Part and the next will focus on state cyber operations against health care systems during the pandemic, that is, operations that are attributable to a state, irrespective of the precise attribution rule that would be applicable on the given facts. Such state operations can potentially violate several primary obligations under international law. These include (1) sovereignty; (2) the principle of non-intervention; (3) the prohibition on the use of force; and (4) the human rights to life and health.

A. Violation of Sovereignty

The most likely international law obligation to be breached by a state's cyber operation against a health facility or capability, or public health activities, is the obligation to respect the sovereignty of other states. Before discussing the manner in which that obligation might be breached, it must be cautioned that one state—the United Kingdom—has formally taken the position that no such legal rule exists. In its view, sovereignty is but a principle of international law from which primary rules like the prohibition on intervention and that on the use of force emanate, but that it is incapable of being violated on its own.[25]

The United States has wisely refrained from providing complete support in this regard for its closest ally. In a February 2020 speech at the U.S. Cyber Command, Paul Ney, General Counsel of the Department of Defense, observed that

> States have sovereignty over the information and communications technology infrastructure within their territory. The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that *all* infringements on sovereignty in cyberspace *necessarily* involve violations of international law.[26]

Note the hedging, fence-sitting language—not even the staunchest sovereigntist would claim that *all* cyber operations against a state *necessarily* violate its sovereignty. In short, the United States has so far refrained from providing a sufficiently clear articulation of its views on whether sovereignty is a primary

24. CYBER SECURITY CENTRE, AUSTRALIAN SIGNALS DIRECTORATE, ADVISORY 2020-009: ADVANCED PERSISTENT THREAT (APT) ACTORS TARGETING AUSTRALIAN HEALTH SECTOR ORGANISATIONS AND COVID-19 ESSENTIAL SERVICES (n.d.), https://perma.cc/G8QG-M6VM.

25. Jeremy Wright, Attorney General of the UK, Address at Chatham House, Cyber and International Law in the 21st Century (May 23, 2018), https://perma.cc/DWZ3-WNX9.

26. Paul C. Ney, Jr., Dep't Def. Gen. Counsel, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* (Mar. 2, 2020), https://perma.cc/QY33-NEMY (emphasis added).

rule of international law, capable of being violated independently of any other rule.

In reaction to the British position, a growing number of states have publicly acknowledged sovereignty as a binding rule of international law, one that plays an important role with respect to extraterritorial cyber operations conducted by states. The Netherlands, for instance, has stated that "[r]espect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act."[27] In our view, this is the correct legal stance. Moreover, it facilitates international condemnation of cyber operations involving the pandemic as violations of international law, for violation of sovereignty is the easiest legal case to make.

The sovereignty of a state may be breached by cyber operations attributable to another state in two basic ways—by causing effects on the territory of the former or by interfering with its inherently governmental functions, even in the absence of territorial effects.[28] Both types of violations are relevant to the COVID-19-related cyber operations.

With respect to territoriality, relatively broad consensus exists that if a cyber operation is conducted remotely by one state into the territory of another state and causes damage to property or injury in the latter, sovereignty has been breached. [29] It matters not whether the target of the cyber operation is governmental or private in character or whether the individuals affected are public servants or private persons. The essence of the breach is the causation of certain consequences on the territory of the state without that state's consent.[30]

Damage in this context encompasses relatively permanent interference with the functionality of cyber infrastructure.[31] Any cyber operation that renders medical equipment inoperable would qualify. Of greater immediate significance is the fact that the notion of injury extends from cyber operations resulting in death to those merely affecting health in some manner. Thus, by the prevailing view, any of the cyber operations attributable to a state that have negatively affected the health of any individuals on the state's territory, as did those that interfered with the immediate delivery of medical care, violated the sovereignty of that state.

---

27. Letter of July 5, 2019 from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, Appendix: International Law in Cyberspace 2, https://perma.cc/ENU3-DFGV [hereinafter Netherlands MFA Letter]. *See also* France, Ministry of the Armies, International Law Applied to Operations in Cyberspace 6-7 (2019) (English version) [hereinafter Ministry of the Armies Position Paper]; Statements of Austria, Finland, Czech Republic, 2d Substantive Session of OEWG, Feb. 11, 2020, https://perma.cc/J269-SU36.

28. *See* TALLINN MANUAL 2.0, *supra* note 17, r. 4 and accompanying commentary. These two strands of the rule are apparent in the famous 1928 Island of Palmas arbitration decision by Judge Huber: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State." Island of Palmas (Neth. v. US), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

29. TALLINN MANUAL 2.0, *supra* note 17, r. 3.

30. *Id*. at 18.

31. *Id*. at 20–21.

Below the aforementioned threshold of harm, no consensus has crystallized as to when a remotely conducted cyber operation breaches the sovereignty of the state into which it is conducted. For instance, it is unclear whether simply causing cyber infrastructure to operate in a degraded manner or temporarily interfering with its operation qualifies as a breach of sovereignty if the consequences of that action do not involve injury, including illness, or physical damage. The broadest view taken so far is that of France, which has stated that

> [a]ny cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.[32]

For France, every cyber operation disturbing the operation of medical or public health cyber infrastructure on French territory would be considered a violation of its sovereignty. This is so irrespective of whether it directly impacts the health of any individuals. Of course, any negative health outcome would qualify as an "effect."

At the other end of the spectrum, there appears to be consensus that espionage *per se* does not violate the sovereignty of the target state, at least so long as the method used neither causes the requisite effects, as discussed above, nor interferes with inherently governmental functions, as described below.[33] Therefore, even if claims of states accusing others of attempting to steal COVID-19 vaccine and treatment research are accurate, those actions likely would not violate international law, at least so long as the espionage activity consisted solely of the exfiltration of research data without seriously disrupting the research project itself and thereby indirectly causing harm to human life or health, or causing harm to cyber infrastructure.[34]

Cyber operations that do not reach the qualifying threshold for harm to cyber infrastructure, wherever that threshold may lie, will still violate sovereignty should they cause individuals to be unable to secure COVID-19 treatment or preventive measures, and illness or aggravation of illness results. This is because the requisite consequences for breach may be caused directly or *indirectly*. For instance, a denial of service attack against a website providing information on virus testing will violate sovereignty if the upshot of the information's unavailability is an increase in the numbers of infected individuals or exacerbation of the illness's severity due to individuals not having access to timely testing. Ransomware attacks would also constitute a violation of sovereignty if such

32. Ministry of the Armies Position Paper, *supra* note 27, at 7.

33. TALLINN MANUAL 2.0, *supra* note 17, r. 32.

34. David E. Sanger & Nicole Perlroth, *U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks*, N.Y. TIMES, May 13, 2020.

consequences manifested. The key consideration here is the intensity of the causal connection between the cyber operation and some concrete harm.

Whether the consequences of the hostile cyber operation must be foreseeable in order to breach sovereignty remains somewhat unsettled, although the *Tallinn Manual 2.0* International Group of Experts opined that it need not.[35] This issue has little relevance to operations involving health facilities and capabilities, and public health activities, during a pandemic, for the scope and scale of a pandemic is such that almost any interference with the provision of medical care and public health activities would foreseeably impact the health of individuals.

The second means of violating sovereignty is interference with, or usurpation of, an inherently governmental act.[36] The distinction between this form of sovereignty violation and one based on territoriality is that there is no requirement that any particular physical effects manifest on the state's territory. Instead, the basis for finding a violation is the existence of activities that states alone are entitled to perform, the classic examples being the deprivation of liberty and law enforcement more generally. Should one state interfere with the performance of such functions by another state, or if the former engages in activities on the territory of the other state that are reserved to the latter, a violation has occurred.

Although health care is sometimes provided exclusively or primarily by the state, as in the case of the National Health Service in the United Kingdom, this is not universally the case. Because providing medical care is not an inherently governmental function, cyber operations by states that interfere with the provision of health care in another, even if that victim state does provide health care to its own population, do not, on that basis alone, amount to a sovereignty violation.

However, crisis management during an epidemic or a pandemic *is* a governmental responsibility in every state and accordingly an inherently governmental function. Any cyber operation attributable to a state that disrupts another state's crisis management planning and execution during a pandemic, at any level of government, therefore qualifies as a sovereignty violation. This is so irrespective of whether the cyber operation foreseeably places health or life at risk, because it is the mere interference that comprises the violation, not the consequences thereof. To illustrate, a denial of service operation that interferes with the dissemination of COVID-19 information to the public, even temporarily, is unlawful on this basis alone, even in the absence of significant adverse consequences down the causal chain. So is any cyber operation that disrupts the government's coordination of the acquisition, allocation and distribution of essential medical equipment and supplies to the neediest areas of the country.

It is also important to note that the concept of sovereignty is linked to the authority of the state to control its territory and exclusively perform certain functions therein. This bears on the case of cyber operations directed against the World Health Organization. International organizations do not directly enjoy

35. TALLINN MANUAL 2.0, *supra* note 17, at 24.
36. *Id*. at 21–23.

the protections of the rule of sovereignty.[37] Therefore, cyber operations targeting the WHO headquarters in Geneva might qualify as a violation of Swiss territorial sovereignty if they affect cyber infrastructure in Switzerland in a manner that trips over the requisite threshold.[38] But they would not so qualify on the basis of interference in the WHO's operations unless that interference somehow caused the denial of care, or caused illness or aggravation of the virus, to individuals on Swiss territory.

B. Violation of the Prohibition of Intervention

Hostile cyber operations by states during a pandemic can also qualify as intervention into the internal affairs of another state.[39] A breach of the prohibition requires coercive interference into the *domaine réservé* of another state. As noted by the International Court of Justice in the *Nicaragua* judgment, "The element of coercion . . . forms the very essence of prohibited intervention."[40] The Dutch Ministry of Foreign Affairs has explained that although the "precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law, [i]n essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state."[41]

In other words, coercion deprives the injured state of choice regarding an activity it has the right to control.[42] This occurs either by depriving the state of the *ability* to exercise such control or by affecting the state's *will* to such an extent that its choices are no longer free ones.

Domaine réservé denotes an area of activity, often referred to as their internal and external affairs, that is as a general matter left by international law to states.[43] The concept sometimes overlaps with that of inherently governmental function, but there is a difference. Whereas an inherently governmental function is an activity only states perform, the *domaine réservé* can encompass activities

37. Hostile cyber operations against an international organization may, however, be contrary to explicit or implicit obligations of membership that its states parties have freely accepted under the organization's founding treaty.

38. A comparable example would be the attempted cyber operation allegedly committed on Dutch territory by Russian state agents against the headquarters of the Organization for the Prohibition of Chemical Weapons. *See* Netherlands, Ministry of Defence, *Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW* (Oct. 4, 2018), https://perma.cc/86RL-9TKB.

39. *See* TALLINN MANUAL 2.0, *supra* note 17, r. 66 and accompanying commentary.

40. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S), Judgment, 1986 I.C.J. 14, ¶206 (June 27) [hereinafter Nicaragua].

41. Ministry of the Armies Position Paper, *supra* note 27, at 2.

42. Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, prin. 3, G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, U.N. DOC. A/RES/8082 (Oct. 24, 1970). *See also* TALLINN MANUAL 2.0, *supra* note 17, at 317–18.

43. Nationality Decrees Issued in Tunis and Morocco (French Zone), Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 4, at 24 (Feb. 7).

performed by private actors so long as international law allows the state to regulate that activity.

It is unquestionably within the *domaine réservé* of a state to determine how it will handle a health crisis, as is the actual handling of that crisis. The scope of this authority is not limited to actions carried out by government agencies, but instead deals with activities by both government and private health care providers, and any other relevant public health entities. Therefore, if a cyber operation by or attributable to one state obstructs the execution of another state's plan for responding to the pandemic, the former will have engaged in prohibited intervention. This will clearly be the case if the former state *intends* to deprive the victim state of its ability to control its pandemic response (although the intervening state's *motives* may be varied and are legally irrelevant). It is less clear whether this would be the case in the absence of such an intent, when the cyber operation only has as its *effect* the loss of the victim state's ability to control its pandemic response.[44]

For example, if attributable to a state, the attack against the Czech medical hospital that rendered it unable to perform its designated function as a COVID-19 testing facility pursuant to the Czech government's plan was coercive. Assuming attribution for the sake of illustration, so too was the interference with the British vaccine testing laboratory, as it was chosen as a facility for that purpose in the United Kingdom's crisis management plan. The key to both incidents is that the state was unable to execute its public health crisis response as planned.

By contrast, consider the 2017 WannaCry Ransomware attack that exploited a vulnerability in an outdated version of Microsoft Windows to infect over 200,000 computers in more than 150 countries by encrypting computer files and demanding $300 in crypto currency to restore access. The attack impacted companies ranging from FedEx and Renault to Telefonica and Deutsche Bahn. However, National Health Service England was hardest hit. The impact was widespread and immediate. For instance, medical personnel were unable to access patient records, and medical equipment was locked. As a result, appointments and procedures had to be cancelled and patients diverted to health care unaffected facilities.[45] North Korea is widely believed to have conducted the operation.[46]

The following year, the British Attorney General noted, in the same speech in which he disputed the existence of a rule of sovereignty, that "[a]cts like the targeting of essential medical services are no less prohibited interventions, or even

44. *See* TALLINN MANUAL 2.0, *supra* note 17, at 318.

45. Michael N. Schmitt & Sean Fahey, *WannaCry and the International Law of Cyberspace*, JUST SEC. (Dec. 22, 2017), https://perma.cc/XPR8-438R.

46. *See, e.g.*, David E. Sanger, *U.S. Accuses North Korea of Mounting WannaCry Cyberattack*, N.Y. TIMES (Dec. 18, 2017), https://perma.cc/JN3Z-BXHR; Wright, *supra* note 25; JAPAN, MINISTRY OF FOREIGN AFFAIRS, *Press Conference by Foreign Press Secretary Norio Maruyama* (Dec. 20, 2017), https://perma.cc/ANP5-DMG6.

armed attacks, when they are committed by cyber means."[47] Since WannaCry directly affected the physical well-being of individuals in the United Kingdom, it clearly amounted to a violation of sovereignty on that basis for those who, unlike the UK, support a rule of sovereignty. Yet, it is less clear that the operation amounted to prohibited intervention.

Although the attack was coercive in fact, WannaCry was not coercive vis-à-vis the *domaine réservé* of health care. Rather, the operation was designed to secure a ransom payment; albeit highly disruptive, it did not deprive the United Kingdom of the ability to exercise control over health care in the country, nor did it affect its will with regard to health care choices that North Korea wished to impose on the United Kingdom. In that sense, it differed from the COVID-19 operations, which dispossessed the Czech Republic and the United Kingdom of the ability to execute specific elements of their crisis management plans to deal with the pandemic, and were designed to do so.

As this example illustrates, the prohibition on intervention does not suffice to fully compensate for the United Kingdom's claimed lack of a rule of sovereignty.[48] The prohibition of intervention is, at least under the mainstream view of the rule, bound up in considerations of the intervening state's intent, which the mere production of adverse effects on health care or any other matter might not trigger.

C. Violation of the Prohibition on the Use of Force

A third possible internationally wrongful act with respect to state cyber operations targeting medical and public health activities, facilities and capabilities in another state during the pandemic is the unlawful use of force in violation of Article 2(4) of the U.N. Charter and its customary international law counterpart.[49] In the cyber context, the troublesome issue has always been determining the criteria for characterizing a cyber operation as a use of force.[50] Yet, general consensus exists that cyber operations causing significant damage, destruction, injury, or death qualify.[51] Therefore, any cyber operations attributable to a state mounted into another state that can be causally linked directly to multiple deaths or lead to a significant increase in COVID-19 infection rates would likely be considered a use of force. Of course, at a certain point the causal nexus would be too attenuated

47. Wright, *supra* note 25. Wright cited Article 2(7) of the UN Charter as a basis for the prohibition on intervention. It is not, for the article deals with intervention by the United Nations, not by states. The prohibition on intervention as it applies to states is grounded in customary international law.

48. On the relationship between sovereignty and intervention, *see* Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, CHATHAM HOUSE, 48-52 (Dec. 2019), https://perma.cc/L5WA-FWYS.

49. U.N. Charter art. 2(4).

50. *See generally* Michael N. Schmitt, *The Use of Cyber Force and International Law*, in OXFORD HANDBOOK ON THE USE OF FORCE IN INTERNATIONAL LAW 1110 (Marc Weller ed. 2015).

51. *See, e.g.*, Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2002), *reprinted in* 54 HARV. INT'L L.J. ONLINE 1, 4 (2012).

to amount to a breach. But any cyber operation in which these consequences are the foreseeable effect of the cyber operation would rise to the level of a use of force.

At the extreme end of the harmful effects spectrum, such a cyber operation could qualify not only as a use of force but also as an "armed attack" in the sense of Article 51 of the Charter, which the International Court of Justice has labeled the "gravest form" of use of force, one that entitles the victim state to self-defense.[52] The Court's position is the mainstream view in the, majority view in the legal literature. Importantly, however, the United States has argued that there is no difference between a wrongful use of force and an armed attack. Therefore, it reserves the right to use cyber or kinetic force in response to any cyber operation against the health sector that qualifies as a use of force.[53]

Two possible objections could be envisaged against this line of argument. First, it could be asserted that the Article 2(4) prohibition on the use of force is subject to a *de minimis* gravity threshold of the kind that applies, in the estimation of most states and scholars, to the Article 51 notion of armed attack, if at a lower level of intensity. Thus, for example, it has been disputed in the literature whether smaller scale incidents, including the targeted killings by states of single (private) individuals, qualify as uses of force.[54] A prominent recent example in that regard was the 2018 attempted assassination of Sergei and Yulia Skripal, allegedly by Russian state agents using a potent nerve agent, in Salisbury, England. That incident was, in fact, qualified by the British Prime Minister as a use of force by Russia against the UK (although she did not qualify it as an armed attack).[55] In our view, setting a *de minimis* threshold for Article 2(4) would be problematic and difficult to do in a non-arbitrary fashion.[56] And even if such a threshold existed, a cyber operation that directly led to multiple deaths would almost certainly cross it.

The second objection is more conceptual, even philosophical—that the relevant cyber operation was not a use of force because *it* did not *cause* any deaths. The cause of the deaths was the virus, which the state using the cyber operation did not introduce into the community. What that state did was simply to prevent

52. U.N. Charter art. 51; Nicaragua, *supra* note 40, at ¶191.

53. U.S. DEP'T OF DEFENSE, OFFICE OF THE GEN. COUNSEL, LAW OF WAR MANUAL §16.3.3.1. *See also* Abraham D. Sofaer, *International Law and the Use of Force*, 82 AM. SOC'Y INT'L L. PROC. 420, 422 (1988); Koh, *supra* note 51, at 4.

54. *See, e.g.*, OLIVIER CORTEN, THE LAW AGAINST WAR 52 (2010); Independent International Fact-Finding Mission on the Conflict in Georgia, Report, Vol. II, at 242, fn. 49 (2009), https://perma.cc/6KEU-UB7M.

55. *See* Theresa May, Prime Minister, United Kingdom, Commons Statement on Salisbury Incident (Mar. 12, 2018), https://perma.cc/76L5-5CVP. *See also* Tom Ruys, *"License to Kill" in Salisbury: State-Sponsored Assassinations and the Jus ad Bellum*, JUST SEC. (Mar. 15, 2018), https://perma.cc/KHL6-MHJV; Dapo Akande, *The Use of Nerve Agents in Salisbury: Why does it Matter Whether it Amounts to a Use of Force in International Law?*, EJIL: TALK! (Mar. 17, 2018), https://perma.cc/QM2Z-AQTQ.

56. *See generally* Tom Ruys, *The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?*, 108 AM. J. INT'L L. 159 (2014).

the victim state from managing the effects of the epidemic on its territory. And it is difficult, if not impossible, to prove that absent the cyber operation the territorial state would in fact have prevented infections or that any specific person would have survived COVID-19.

There is some force to this objection—preventing a state from managing an infectious disease on its territory is not exactly equivalent to introducing such a disease to that territory. But while the effects of the cyber operation on deaths and health might be difficult to establish with precision, if they are of a significant magnitude or if a malicious intent on the part of the state engaging in the cyber operation can be inferred, the causality concerns would not, in our view, be such to exclude the possibility that there was a use of force prohibited by Article 2 (4).[57]

Even if a cyber operation does not directly contribute to an increased incidence in COVID-19 infections and deaths, it could still potentially qualify as a use of force. As with a violation of sovereignty, relatively permanent interferences with the functioning of cyberinfrastructure and equipment upon which it depends is generally considered damage for the purpose of the prohibition on the use of force, since the "effect" is comparable to that which would be considered a use of force if caused by non-cyber means.[58] For instance, a cyber operation that required the replacement of a significant amount of medical equipment would qualify on that basis, even if no significant harm befell individuals who relied upon the equipment for treatment and care, thanks to redundant systems that the territorial state had in place.

As with the obligation to respect the sovereignty of other states, the precise threshold at which a cyber operation that does not result in significant damage, destruction, injury, or death reaches the level of a use of force remains unsettled in international law. The emerging approach seems to consider a variety of factors in making that assessment. They include, *inter alia*, the severity of the consequences, the invasiveness of the operation, the measurability of the effects, the causal directness of the operation, and the entity that mounted the operation.[59]

---

57. To use a criminal law analogy, if person *A* sees person *B* drowning and reaching for a lifebelt, and *A* then kicks the lifebelt away with the intention that *B* shall die, we would have no problem in saying that *A* murdered *B* even if he did not put *B* in that life-jeopardizing situation in the first place. We are grateful to Di Birch, Paul Roberts, and Matt Thomason for a discussion on this point.

58. TALLINN MANUAL 2.0, *supra* note 17, at 7; Netherlands MFA Letter Appendix, *supra* note 27, at 3-4.

59. *See, e.g.*, Ministry of the Armies Position Paper, *supra* note 27, at 7 ("In the absence of physical damage, a cyberoperation may be deemed a use of force against the yardstick of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target."); Netherlands MFA Letter Appendix, *supra* note 27, at 29 ("It is necessary . . . to examine both qualitative and quantitative factors. The Tallinn Manual 2.0 refers to a number of factors that could play a role in this regard, including how serious and far-reaching the cyber operation's consequences are, whether the operation is military in nature and whether it is carried out by a state."); and Koh, *supra* note 51, at 4 ("In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor

Given the scale and effects of the pandemic, it is likely that states will look favorably on characterizing cyber operations against the health sector as uses of force even if those operations fall short of causing death or aggravation of illness on a widespread scale. For instance, an operation that shut down a large hospital or that interfered in a significant and direct manner with the distribution of essential public health information could well be styled by states as a use of force, even if it did not cause direct harm to human lives or health or permanently interfere with infrastructure or equipment.

D. Violation of Human Rights

The violations of the rules of general international law that we have examined above conceptualize the malicious state cyber operation as a violation of the rights of the victim *state*. But such operations also potentially implicate the rights that individuals hold directly under international law, without state mediation. After all, the primary harm that such operations cause is to human life and health, even if the violation is legally cast as an infringement on state sovereignty, or as a breach of the prohibitions of intervention or the use of force. It is appropriate to examine such operations from the standpoint of international human rights law because "the same rights that people have offline must also be protected online."[60]

The human rights to life and health are protected by numerous universal and regional human rights treaties; importantly, the right to life is non-derogable.[61] Under Article 6 of the International Covenant on Civil and Political Rights (ICCPR), "Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life."[62] Similarly, under Article 12(1) of the International Covenant on Economic, Social and Cultural Rights (ICESCR), "The States Parties to the present Covenant recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health."[63] Not only do these treaties enjoy widespread acceptance, but the rights to life and health have also been authoritatively held to form part of customary international law.[64]

---

perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues.). *See also* TALLINN MANUAL 2.0, *supra* note 17, r. 69, and accompanying commentary.

60. U.N. Human Rights Council, Resolution 32/13 (The promotion, protection and enjoyment of human rights on the Internet), ¶1, U.N. Doc. A/HRC/RES/32/13 (July 18, 2016).

61. International Covenant on Civil and Political Rights art. 4, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]. On derogations from the ICCPR, see Human Rights Committee, Statement on Derogations from the Covenant in Connection with the COVID-19 Pandemic, U.N. Doc. CCPR/C/128/2 (Apr. 24, 2020).

62. ICCPR, *supra* note 61, art. 6.

63. International Covenant on Economic, Social and Cultural Rights, art. 12(1), Dec. 16, 1966, 993 U.N.T.S. 3.

64. *See, e.g.*, Human Rights Comm., General Comment No. 24, ¶8, U.N. Doc. CCPR/C/21/Rev.1/Add.6, P 17 (Nov. 4, 1994); *see also* Christof Heyns, Dapo Akande, Lawrence Hill-Cawthorne, & Thompson Chengeta, *The International Legal Framework Regulating Armed Drones*, 65 INT'L COMP. L. Q. 791, 819 (2016).

States have an array of negative and positive obligations under both rights. In particular, they have the negative obligation to *respect* the rights, which is an obligation of restraint, that is, it means that states should not, without adequate justification, engage in activities that adversely affect them. In the right-to-life context, the negative obligation has traditionally revolved around the prohibition of an *arbitrary deprivation of life*, specifically through the use of lethal or potentially lethal force by state agents, as in the policing context.

That context is not directly comparable to hostile cyber operations that increase the risk of exposure to the virus during the pandemic or that decrease the availability of treatment. There is to our knowledge no exact analogue to this scenario in existing human rights jurisprudence, particularly with regard to the question of whether such an operation can entail a *deprivation* of life, a concept that implicitly includes various considerations of causality. On the one hand, it would seem manifest that if a state deliberately infected an individual with a potentially lethal virus, that would count as a deprivation of life—just as if it poisoned that individual with a potentially (but not inevitably) lethal nerve agent, as in the Skripal incident. On the other, if a state, through a hostile cyber operation, knowingly and intentionally increased the risk that a population would be exposed to infection, or denied them effective treatment, we see no material legal or moral difference to the deliberate-infection scenario.

The Human Rights Committee, the treaty body established by the ICCPR, has consistently held that the right to life "should not be interpreted narrowly."[65] It has also held that a "[d]eprivation of life involves an intentional or otherwise foreseeable and preventable life-terminating harm or injury, caused by an act or omission. It goes beyond injury to bodily or mental integrity or threat thereto."[66] While acknowledging the absence of examples in existing jurisprudence that are precisely analogous to a cyber operation that affects a state's ability to combat a pandemic, we do not consider it to be too much of a stretch to suggest that such operations may constitute deprivations of life, even if the immediately proximate cause of any death would be the coronavirus and not the cyber operation itself. Moreover, such deprivations of life would necessarily be arbitrary, for there is no conceivable legitimate justification that a state could offer for causing them.

The foregoing analysis applies even more readily to the human right to health. The obligation to *respect* that right "requires States to refrain from interfering directly or indirectly with the enjoyment of the right to health."[67] Hostile cyber operations that disrupt individuals' access to health care, or more generally a state's ability to mitigate the effects of a pandemic, would easily run afoul of that prohibition, which contains no threshold criterion such as the *deprivation* of life.

65. Human Rights Comm., General Comment No. 6, ¶1, U.N. Doc. CCPR: 30/04/1982 (Apr. 30, 1982); Human Rights Comm., General Comment No. 36, ¶3, CCPR/C/GC/36 (Oct. 30, 2018).

66. Human Rights Comm., General Comment No. 36, ¶6, CCPR/C/GC/36 (Oct. 30, 2018).

67. Comm. on Econ., Soc. & Cultural Rights, General Comment No. 14, ¶33, U.N. Doc. E/C.12/2000/4 (2000) [hereinafter CESCR General Comment No. 14].

However, a controversial threshold issue when asserting that such state cyber operations constitute a violation of human rights is extraterritoriality. The question is whether states owe human rights obligations to individuals located outside their sovereign territory, and, if so, in what circumstances.[68] This issue has been particularly contentious with respect to kinetic and detention operations during armed conflict, with some states, foremost among them the United States, resisting any attempts at the extraterritorial application of human rights treaties (consider drone strikes or the preventive detention of terrorists in Guantánamo).[69] And it is one that has direct bearing on whether the cyber operations attributable to states that have targeted health facilities and capabilities, and public health activities, in other states violate the human rights of affected individuals at all.

Many human rights treaties, among them the ICCPR, use the notion of state jurisdiction to delineate their scope of application.[70] Human rights courts and treaty bodies have interpreted that notion in two basic ways—as state control over a *territory* in which the victim of the human rights violation is located (the spatial conception or model of jurisdiction), or as state authority, power or control over the *victim* directly, exercised by one of the state's agents (the personal conception or model of jurisdiction).[71] Yet some treaties, like the ICESCR, contain no such jurisdiction clause. It is even less clear how *customary* human rights law applies extraterritorially, although arguably "[i]n its customary form, at least the negative obligation not arbitrarily to deprive someone of their life appears not to be limited to application *within* a State's territory."[72]

One of us (Milanovic) has long advocated for an expansive and factual approach to the extraterritorial application of human rights treaties, arguing in particular that the *negative* obligation to respect human rights should be territorially unrestricted.[73] Thus, for example, even in the cyber surveillance context involving no direct harm to life or health, the right to privacy would apply extraterritorially,

68. In support of extraterritorial applicability, see Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) 2004 ICJ 136, ¶111 (ICCPR) and ¶112 (ICESCR); Human Rights Comm., General Comment No. 31, ¶10, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (May 26, 2004); Comm. on Econ., Soc. & Cultural Rights, General Comment No. 24, ¶27, U.N. Doc. E/C.12/GC/24 (2017).

69. U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations of the Human Rights Committee: United States of America, ¶10, U.N. Doc. CCPR/C/USA/CO/3/Rev.1 (Dec. 18, 2006).

70. Thus, under Article 2(1) of the ICCPR, "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant," while under Article 1 ECHR "[t]he High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention." European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 1, 213 U.N.T.S. 221 (1953) [hereinafter ECHR].

71. *See generally* MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES 127-208 (2011). The jurisprudence of the European Court of Human Rights is both the most varied and the most restrictive in its approach to extraterritorial application, whereas the case law of other human rights bodies tends to be more generous.

72. Heyns et al., *supra* note 64, at 823.

73. MILANOVIC, *supra* note 71, at 209 *et seq*.

and the state engaging in such operations would need to justify any interferences with privacy.[74] The other (Schmitt) concurs with the approach when applied to customary human rights obligations, but is somewhat hesitant to apply it to human rights treaties, preferring a case-by-case approach to their extraterritorial application. Both of us agree, however, that an expansive view of the extraterritorial application of human rights obligations is both desirable and sensible.

Of course, it is possible to hold reasonably different views about how jurisdiction clauses in human rights treaties are to be interpreted, and more so about the extraterritorial applicability of customary human rights law.[75] That said, it is worth briefly considering how human rights bodies would apply existing extraterritoriality case law to malicious cyber operations against health care systems in other countries.

Beginning with the most restrictive approach, the European Court of Human Rights (ECtHR) held in *Bankovic* that even dropping a *bomb* on an individual in an area outside a state's control is insufficient to create a jurisdictional link for the purpose of the right to life.[76] By that logic, a cyber operation that directly (let alone indirectly) resulted in death would not suffice to create such a link.[77] Thus, if a case were litigated against a European Convention on Human Rights (ECHR) state party on a claim of malicious extraterritorial cyber operation targeting the health sector, the Court would have to radically depart from some of its existing case law to find that the operation falls within the Convention's scope.[78]

The Human Rights Committee has not been as restrictive as the ECtHR. In its recent General Comment No. 36 on the right to life, it embraced a very broad, functional theory of the extraterritorial application of the right.[79] The Committee thus held that the notion of state jurisdiction in Article 2(1) ICCPR encompasses "all persons over whose *enjoyment* of the right to life [the state] exercises power or effective control. This includes persons located outside any territory effectively controlled by the State, whose right to life is *nonetheless impacted* by its

74. *See* Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81 (2015).

75. *See, e.g.*, Ryan Goodman, *The United States' Long (and Proud) Tradition in Support of the Extraterritorial Application of International Human Rights Law*, JUST SEC. (Mar. 10, 2014), https://perma.cc/3LA8-BBBE.

76. Bankovic v. Belgium, 2001-XII Eur. Ct. H.R. ¶¶74-82.

77. *See* U.K. Investigatory Powers Trib., Human Rights Watch Inc. & Ors v. Secretary of State for the Foreign & Commonwealth Office & Ors, [2016] UKIP Trib 15_165-CH (16 May 2016) (ruling that the ECHR did not apply to electronic surveillance activities of the UK government abroad, and expressly relying on an analogy to *Bankovic* in doing so).

78. The Court's current leading case on extraterritoriality is Al-Skeini and Others v. United Kingdom, App. No. 55721/07, 2011-IV Eur. Ct. H.R., in which the Court partly departed from *Bankovic* without overruling it, and in which it affirmed the spatial and personal conceptions of jurisdiction. The Court most recently affirmed *Bankovic* in M.N. & Others v. Belgium, App. No. 3599/18, 2020-V Eur. Ct. H.R. The Court has yet to rule directly in a case that concerns the extraterritorial applicability of the ECHR to electronic surveillance or cyber operations; in its most recent surveillance cases that issue was raised, but the Court managed to avoid it. *See* Big Brother Watch and Others v. the United Kingdom, App. No. 58170/13, 2018-IX Eur. Ct. H.R.

79. *See also* Heyns et al, *supra* note 64, at 823-25.

military or *other activities* in a *direct and reasonably foreseeable manner*."[80] The Committee thus moved away from a jurisdictional paradigm of state control over the victim to that of state control over the victim's *enjoyment* of their rights. It seems reasonably clear that a hostile cyber operation against health care systems during the pandemic could be an exercise of *power* over the affected individuals' enjoyment of the right to life, and that such operations would adversely impact the exercise of the right to life in a direct and reasonably foreseeable manner.

As for the Committee on Economic, Social and Cultural Rights, in 2000 it opined that "States parties have to respect the enjoyment of the right to health in other countries."[81] Nearly two decades later, the Committee further explained that because the ICESCR lacks a clause limiting its extraterritorial application, its provisions are not subject to any such kind of threshold restriction, jurisdictional or otherwise.[82] In particular, the Committee's position is that:

> The extraterritorial obligation to respect requires States parties to refrain from interfering directly or indirectly with the enjoyment of the Covenant rights by persons outside their territories. As part of that obligation, States parties must ensure that they do not obstruct another State from complying with its obligations under the Covenant.[83]

Again, if this is the relevant legal standard—which is tantamount to arguing that negative obligations under the ICESCR are not subject to any territorial limitation—then any hostile cyber operation by a state that adversely affects the health of individuals in another state during the pandemic would be within the scope of the treaty,[84] and would almost inevitably violate it.

To conclude, in our estimation state cyber operations that directly or indirectly harm human life and health can properly be characterized as violations of treaty and customary international human rights law. This should be an uncontroversial proposition for operations affecting individuals within the state's own territory, but it is a more complex one when such operations are deployed extraterritorially. Normatively, it is hard to understand why a state's negative obligation to respect the rights to life and health should not apply outside that state's territory. As the Human Rights Committee put it, "it would be unconscionable to so interpret the responsibility under article 2 of the Covenant as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory."[85] The relevance of human rights,

80. HRC General Comment No. 36, *supra* note 65, ¶63 (emphasis added).

81. CESCR General Comment No. 14, *supra* note 67, ¶39.

82. CESCR General Comment No. 24, *supra* note 68, ¶27.

83. *Id.* ¶29.

84. *See also* Olivier De Schutter et al., *Commentary to the Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights*, 34 HUM. RGTS. Q. 1084, 1126-31 (2012).

85. Lopez Burgos v. Uruguay, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40) at 176 (1981), ¶12.3.

both symbolic and practical, should not be underplayed in situations in which a state is causing harm primarily to human beings, as opposed to other states as abstract entities. Human rights law is in many ways normatively a better fit for describing the nature of the wrongdoing in question than are the state-oriented rules on sovereignty, non-intervention, or use of force.[86]

II. STATE MISINFORMATION DURING THE PANDEMIC

The COVID-19 pandemic has been accompanied by extensive misinformation[87] produced by both states and non-state actors—a veritable infodemic that spreads infectiously over social media. This has ranged widely. For instance, misinformation during the pandemic has included attempts to minimize the infectivity or virulence of the disease, the promotion of false and potentially even lethal "cures" for the virus, and conspiracy theories about the origins of the virus and its (nonexistent) relationship with 5G phone masts.[88]

Our focus in this Part will be on evaluating *state* misinformation during the pandemic, that is, misinformation that originated with and/or is being spread by persons whose conduct is attributable to the state. We will deal with misinformation by non-state actors in Part III. It is of course perfectly possible—and commonplace—for misinformation to originate with private individuals or organized non-state actors, but then be picked up and amplified by state actors (and vice versa). For example, the 5G conspiracy theories appear to have originated organically or spontaneously, only to be amplified by state actors (and some unfortunate celebrities).[89] Such state-amplified misinformation is legally no different from misinformation that originated with the state.

With regard to its target audience, state misinformation can be projected *internally* against the state's own population or *externally* against the population of another state, or both. Its purposes can be wide-ranging. For example, a state might conduct extraterritorial disinformation operations targeting an adversary to sow discontent and dissent, as was described above, while misinformation appears to have been deployed internally during the COVID-19 crisis by governments to project a sense of power, authority, and competence; to blame some other actor for the state's missteps in addressing the pandemic; or simply as a

86. Marko Milanovic, *The Salisbury Attack: Don't Forget Human Rights*, EJIL: TALK!, (Mar. 15, 2018), https://perma.cc/C7XE-QTYF.

87. We define misinformation as any false item of information that is directly or indirectly relevant to the pandemic. One can also speak of disinformation, a term that implies intentionality on the part of the originator or the spreader of false information. We prefer to use misinformation as a broader term, and will discuss the intentional spreading of misinformation in due course.

88. For a comprehensive overview, *see List of Known Misinformation and Disinformation Regarding Corona Virus in Social Media*, CTR FOR INFORMED DEMOCRACY & SOCIAL-CYBERSECURITY, (2020), https://perma.cc/92K9-PT9H.

89. *See* Ryan Gallagher, *5G Virus Conspiracy Theory Fueled by Coordinated Effort*, BLOOMBERG (Apr. 9, 2020, 7:04 AM), https://perma.cc/9F4A-GE49; James Temperton, *How the 5G Coronavirus Conspiracy Theory Tore Through the Internet*, WIRED (Apr. 6, 2020), https://perma.cc/N648-EWTD.

convenient distraction.[90] And states can complement misinformation with direct and indirect forms of censorship to hinder efforts to correct the state's false narratives. This is a well-worn playbook for authoritarian regimes.

State misinformation can be analysed from three perspectives: 1) as a violation of human rights law when directed against a state's own population; 2) as a violation of human rights law when directed against the populations of other states; and 3) as a violation of sovereignty and the prohibition of intervention when directed against other states. We will address each in turn.

A. Violation of Human Rights Law When Directed Against A State's Own Population

State misinformation directed against its own population can be especially damaging during a pandemic. It inherently attracts more attention, and its impact is inevitably amplified by the media. Such misinformation damages the information ecosystem as a whole and destroys the public trust necessary for combatting the pandemic. When employing direct and indirect forms of censorship in parallel, state actors can construct, promote, and entrench entire false narratives by simultaneously spreading misinformation and suppressing accurate information.

Because managing the coronavirus epidemic requires the population at large to willingly adopt measures such as handwashing and social distancing, state misinformation that minimizes the threat posed by the virus is particularly harmful. Examples range from downplaying the virulence or danger of COVID-19, as has occurred in Brazil,[91] to Nicaragua and Turkmenistan's denials that the virus is even present (or at least not being transmitted).[92] The spread by state agents of misinformation about specific medicines and treatments, for instance by promoting ineffective or unproven treatments, is likewise dangerous.[93] It is especially problematic when coupled with the suppression of accurate information.[94] There is no question that such misinformation can directly place lives and health at risk.

---

90. *See e.g.*, Julian Borger, *Trump Scapegoating of WHO Obscures its Key Role in Tackling Pandemic*, THE GUARDIAN (Apr. 8, 2020, 18:53), https://perma.cc/ZBM4-FHBJ; Lily Kuo, *"American coronavirus": China Pushes Propaganda Casting Doubt on Virus Origin*, THE GUARDIAN (Mar. 12, 2020, 20:59), https://perma.cc/29S6-SEMP.

91. Ernesto Londoño, Manuela Andreoni & Letícia Casado, *Bolsonaro, Isolated and Defiant, Dismisses Coronavirus Threat to Brazil*, N.Y. TIMES (June 18, 2020), https://perma.cc/BNT7-DP8C; Ishaan Tharoor, *Brazil's Bolsonaro Sits on a Ticking Coronavirus Time Bomb*, WASH. POST (May 1, 2020, 12:00 AM), https://perma.cc/WMK4-6T9Y.

92. Abdujalil Abdurasulov, *Coronavirus: Why has Turkmenistan Reported no Cases*?, BBC NEWS (Apr. 7, 2020), https://perma.cc/CSA3-6QWR; Wilfredo Miranda & Tom Phillips, *President Nowhere To Be Seen as Nicaragua Shuns Coronavirus Curbs*, THE GUARDIAN (Apr. 8, 2020, 12:17 EDT), https://perma.cc/8WFW-QNMM.

93. For example, a herbal tonic being actively promoted by the president of Madagascar. Bukola Adebayo, *Amid WHO Warnings and with No Proof, Some African Nations Turn to Herbal Tonic to Try to Treat Covid-19*, CNN (May 15, 2020, 15:41 GMT), https://perma.cc/BQU7-G7LD.

94. Misinformation can come from local or regional authorities and still be attributable to the state as a matter of international law; it need not emanate from central authorities or with their blessing. In that regard, *see* Andrew Higgins, *In Pandemic, a Remote Russian Region Orders a Lockdown on Information*, N.Y. TIMES (Apr. 23, 2020), https://perma.cc/WH4K-DJBR (discussing the efforts of local

From the international human rights law perspective, the characterization of state misinformation depends primarily on the nature and magnitude of the social harm that it causes, the directness of the causal nexus between the state's information and the harm, and the objectives of the relevant state agents who spread the misinformation. Analysis is always highly contextual, but two broad conclusions are possible.

First, state agents who systematically disseminate falsehoods may be denying individuals' right to seek and receive information by hindering their ability to access accurate information, especially when states simultaneously suppress accurate information. The right to seek and receive information is part and parcel of the freedom of expression in international human rights law.[95]

Second, state agents who spread misinformation online that directly affects health or exposes individuals to significantly elevated risks violate their state's obligations to respect and protect the rights to life and health, as guaranteed by international human rights instruments. It is clear that the right to life extends to "general conditions in society that may give rise to direct threats to life . . . [including] the prevalence of life threatening diseases."[96] There is also no doubt that in order to respect the right to health, states have to refrain "from censoring, withholding or intentionally misrepresenting health-related information," "take measures to prevent, treat and control epidemic and endemic diseases," and "provide education and access to information concerning the main health problems in the community."[97] The U.N. Committee on Economic, Social, and Cultural Rights rightly observes that the "deliberate withholding or *misrepresentation* of information vital to health protection or treatment" violates a state's duty to respect the right to health.[98]

In sum, state agents have a negative duty under human rights law to refrain from spreading misinformation that harms human health. Such a duty will clearly apply if the misinformation is being spread knowingly or deliberately.

B. Violation of Human Rights Law When Directed Against Individuals in Other States

The foregoing analysis would apply with equal force to misinformation spread by the state *externally* against the populations of other states. "The right to freedom of expression, which includes the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any media, applies to

---

authorities in a Russian region to spread misinformation and suppress accurate information, with a local activist being quoted as saying that "Putin is not sitting in a bunker telling everyone to hide the truth. . . . Local officials lie because this is what they have always done. It is a habit.").

95. ICCPR, *supra* note 61, art. 19; Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 10, E.T.S. No. 5.

96. HRC General Comment No. 36, *supra* note 65, ¶26.

97. CESCR General Comment No. 14, *supra* note 67, ¶¶34, 44.

98. *Id*. ¶50 (emphasis added).

everyone, everywhere."[99] Polluting the information space in another state is not meaningfully different, either legally or morally, from doing the same thing on one's own territory. The same is true with respect to more direct harm to human lives and health.

The difficulty that arises, however, is the issue of extraterritoriality examined above. That analysis applies *mutatis mutandis* here. To the extent that the obligations implicated are negative duties of restraint, it matters not whether the harm to human lives and health is caused by a cyber operation that, say, physically makes COVID-19 testing impossible, or by a misinformation campaign that fatally undermines public confidence in, and willingness to partake of, testing. The extraterritoriality analysis is the same—if the former scenario falls within the scope of application of human rights treaties, then so too does the latter. Simply put, what matters is the extent of the misinformation operation's causal contribution to the harm.

C. Violation of General International Law When Directed Against Other States

Finally, state misinformation operations directed against other states can also violate the rules of general international law examined above. For instance, seemingly reliable misinformation intended to convince individuals to prophylactically consume substances that make them ill or risk death would violate the sovereignty of the state in which those effects manifested. Depending on the scale of the sickness or death caused and the directness of the causal connection, a cyber misinformation operation even could rise to the level of a use of force.

Somewhat less clear cut is the application of the principle of non-intervention to misinformation attributable to a state. If misinformation directly causes part of the target state's crisis management plan to fail and was designed to do so, as in falsely announcing that a particular hospital is no longer receiving COVID-19 patients or that testing at a certain location has ended, our view is that the coerciveness requirement is satisfied. Such actions would be analogous to undisputed examples of intervention, like manipulating election machinery or altering a vote count. They block a state's ability to execute a plan with respect to its *domaine réservé*.

But when the misinformation does not substantially deprive the target state of the ability to manage the epidemic, it is less clear the action is coercive, as distinct from merely serving to influence the population. This is so even if the misinformation proves harmful. An example would be the dissemination of false or misleading information about testing statistics or claims that public health measures should be relaxed. Such actions would be analogous to Russia's hacking of databases and the release to Wikileaks of emails of Hillary Clinton and others involved in her campaign, and the spreading of false or misleading information

99. David Kaye, Harlem Désir & Edison Lanza, *COVID-19: Governments Must Promote and Protect Access to and Free Flow of Information During Pandemic – International Expert*s, U.N. HUMAN RIGHTS OFFICE OF THE HIGH COMM'R (Mar. 19, 2020), https://perma.cc/3SSU-8657.

about her during the 2016 U.S. presidential elections. As noted, the point at which influence becomes coercion remains unsettled in international law, but some acts of misinformation would unambiguously qualify as prohibited intervention. Even when they do not, it must be remembered that the misinformation might violate the target state's sovereignty on the basis of interfering with an inherently governmental act.

III. STATE OBLIGATIONS REGARDING CYBER OPERATIONS AND MISINFORMATION BY NON-STATE ACTORS AND THIRD STATES DURING THE PANDEMIC

Parts I and II examined how cyber and misinformation operations attributable to a state can violate various rules of general international law and human rights law. These were mainly negative obligations of restraint. In this Part, analysis turns to the *positive* obligations that states have with regard to COVID-19-related cyber and misinformation operations conducted by non-state actors and third states. It focuses on three related issues: a state's positive due diligence obligation under human rights law to protect its own population against hostile operations; the limits that international law imposes on such protective measures, particularly with regard to the freedom of expression; and the positive due diligence obligations under general international law and human rights law to stop hostile operations against third states and their populations when such operations are emanating from the state's territory.

A. Positive Due Diligence Obligation under Human Rights Law to Protect the State's Own Population Against Hostile Operations by Other States and by Non-State Actors

International human rights law requires states to protect (secure, ensure) the human rights that individuals on their territory, or otherwise within their jurisdiction, enjoy, a principle set out, *inter alia*, in Article 2(1) ICCPR."[100] The obligation to protect is one of due diligence, a duty of conduct, not of result. It does not require states to prevent or stop all possible harm to life or health, but only to take all feasible measures reasonably at their disposal.[101] That duty extends to harm caused by natural disasters, therefore, in the context of the pandemic, it requires states to take feasible measures to protect their populations from the virus.[102]

---

100. ICCPR, *supra note* 61, art. 2(1).

101. *See* Antonio Coco & Talita de Souza Dias, *Part I: Due Diligence and COVID-19: States' Duties to Prevent and Halt the Coronavirus Outbreak*, EJIL: TALK! (Mar. 24, 2020), https://perma.cc/HQ3B-EXST.

102. *See, e.g.*, Öneryıldız v. Turkey, App. No. 48939/99, 2004-XI Eur. Ct. H.R., ¶¶89-90, 97-110 (holding Turkey responsible for failing to protect the right to life because its state officials did not do everything within their power to protect the inhabitants of a slum from the immediate and known risks to which they were exposed as the result of an unsafe municipal garbage dump that suffered a methane explosion, killing or injuring many individuals); M. Özel & Others v. Turkey, App. No. 14350/05, 2015-XI Eur. Ct. H.R., ¶¶173-174 (duty to protect life exists even with regard to unexpected natural disasters outside the state's control, such as earthquakes).

But the duty also applies to harm directly caused by third parties.[103] As explained by the Human Rights Committee,

> the positive obligations on States Parties to ensure Covenant rights will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities. There may be circumstances in which a failure to ensure Covenant rights as required by article 2 would give rise to violations by States Parties of those rights, as a result of States Parties' permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities.[104]

Thus, the fact that the hostile cyber operations targeting medical facilities and capabilities or public health activities may have been conducted by non-state actors operating independently does not relieve states of the burden of taking action to prevent them from placing individuals at risk, so long as the cyber operation in question affects a specific human right, such as the right to life or the right to health. The same is true with respect to misinformation campaigns having comparable effects.

The Human Rights Committee has applied this approach in the health context. For instance, in its 2018 General Comment No. 36, the Committee noted that the obligation to take measures to safeguard the right to life can require states to take "appropriate measures to address the general conditions in society that may give rise to direct threats to life," including "life-threatening diseases."[105] Over three decades earlier, it similarly had observed,

> the right to life has been too often narrowly interpreted. The expression "inherent right to life" cannot properly be understood in a restrictive manner, and the protection of this right requires that States adopt positive measures. In this connection, the Committee considers that it would be desirable for States parties to take all possible measures to . . . adopt measures to eliminate . . . *epidemics*.[106]

By this interpretation, with which we agree, states must, as a matter of law, take all feasible measures, including by cyber means, to prevent and respond to cyber operations that risk diminishing the ability of private or public health care

---

103. *See, e.g.*, Velásquez Rodríguez v. Honduras, Inter-Am. Ct. H.R. (Ser. C) No. 4 (1988), Inter-American Court of Human Rights (IACtHR), 29 July 1988, ¶¶172-173 (the very first judgment of the Inter-American Court, which for the first time in human rights jurisprudence elucidated the protective due diligence obligation with regard to violations of the right to life perpetrated by third parties).

104. HRC General Comment No. 31, *supra* note 68, ¶8.

105. HRC General Comment No. 36, *supra* note 65, ¶26.

106. HRC General Comment No. 6, *supra* note 65, ¶5.

facilities to treat COVID-19 patients, so long as such hostile operations are reasonably foreseeable.[107] This obligation arguably extends beyond those attacks that directly interfere with the delivery of health care, as in a cyber operation that obstructs the operation of ventilators or other critical medical equipment, to those that hinder public health measures to fight the pandemic, like disruption of virus testing. It must be emphasized that the obligation to protect the rights of individuals to whom the state owes human rights obligations also encompasses cyber operations that are conducted by third states (and not just non-state actors) against medical facilities and capabilities and public health activities.[108]

Overarching positive obligations also exist with regard to the right to health and the freedom of expression. Thus, for example, the Committee on Economic, Social and Cultural Rights has held that states violate their positive obligation to protect the right to health if they fail "to take all necessary measures to safeguard persons within their jurisdiction from infringements of the right to health by third parties."[109]

Cumulatively, in the context of the pandemic, the positive duty to protect the rights to life, health, and the freedom of expression entails the following concrete steps, in addition to measures that states are taking to combat the virus itself:

- First, states must take all feasible measures to prevent hostile cyber operations adversely affecting their health care systems and capacities when such operations are capable of causing harm to human life or health or disrupting the state's response to the pandemic. It is irrelevant whether the malicious cyber operation is emanating from a non-state actor or from another state.
- Second, states must take all feasible steps to promote *accurate* COVID-19-related information and facilitate access to such information.
- Third, in a very narrow category of cases—those with a clear causal link to substantial harm or risk to human life or health—states have a *duty* to suppress COVID-19-related misinformation, strictly subject to necessity and proportionality requirements for lawfully limiting the freedom of expression. For example, the state would have the duty to suppress speech that claims ingesting methanol is a cure

107. HRC General Comment No. 36, *supra* note 65, ¶¶7, 18, 21. *See also* Tagayeva & Others v. Russia, App. No. 26562/07, 2017-IV Eur. Ct. H.R., ¶¶481-493 (holding Russia responsible for its breach of the positive obligation to protect life with regard to the terrorist attack against a school in Beslan, because Russian authorities had sufficiently specific information about the planned attack and failed to take measures to prevent or mitigate the risk of the attack).

108. HRC General Comment No. 36, *supra* note 65, ¶22. *See also* El-Masri v. Former Yugoslav Republic of Macedonia, App. No. 39630/09, 2012-XII Eur. Ct. H.R. (holding Macedonia responsible for failing to prevent, and for being complicit in, human rights violations perpetrated by U.S. agents on its territory during an "extraordinary rendition" operation).

109. CESCR General Comment No. 14, *supra* note 67, ¶51.

for COVID-19. And in a somewhat wider set of cases, states would be *permitted* to suppress such misinformation (see discussion below).

- Fourth, in that regard, states must take reasonable steps to regulate and cooperate with corporate actors that manage digital platforms, like social media companies, which host the vast bulk of online expression by private individuals.

Indeed, even without state regulation, private actors such as social media platforms are aggressively taking measures to curb COVID-19 misinformation, far more so than with regard to political misinformation.[110] Responses have ranged from the promotion of accurate information from authoritative sources and notices flagging suspicious content, to taking down content or relegating it in search results. The relevant policies of digital platforms are constantly evolving[111] and their moderation decisions have been quite granular. For example, YouTube is removing videos promoting conspiracy theories about 5G networks and the coronavirus, but it is not taking down videos promoting other 5G conspiracies, choosing instead not to include these in search results.[112] Even WhatsApp, which employs end-to-end encryption and thus cannot moderate content as such, has introduced measures to slow down the spread of misinformation, such as limits on the number of times a message can be forwarded.[113] Analogously with efforts to slow the spread of the pandemic, WhatsApp is trying to reduce the R_0, or the basic reproduction number, of the infodemic.

Although private entities are generally not directly bound by international human rights law, through the acceptance of various soft initiatives such as the Ruggie Principles,[114] as well as in response to work by the U.N. Special Rapporteur on the Freedom of Expression (among others),[115] a number of digital platforms have acknowledged the need for more rigorous and transparent self-regulation and a degree of state intervention. Crucially, they are increasingly

110. Evelyn Douek, *COVID-19 and Social Media Content Moderation*, LAWFARE (Mar. 25, 2020, 1:10 PM), https://perma.cc/TYJ6-8AZ2.

111. *See, e.g.*, Yoel Roth & Nick Pickles, *Updating our Approach to Misleading Information* (May 11, 2020), https://perma.cc/87ST-JV3S (explaining the newest iteration of Twitter's approach to misinformation).

112. Alex Hern, *YouTube Moves to Limit Spread of False Coronavirus 5G Theory*, THE GUARDIAN (Apr. 5, 2020, 10:57 EDT), https://perma.cc/2K5M-L4EG.

113. Alex Hern, *WhatsApp to Impose New Limit on Forwarding to Fight Fake News*, THE GUARDIAN (Apr. 7, 2020, 3:00 EDT), https://perma.cc/6ZZR-3LMM.

114. John G. Ruggie, Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011).

115. David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Online Content Regulation)*, U.N. Doc. A/HRC/38/35 (Apr. 6, 2018).

adopting international human rights law as a universal regulatory framework. Facebook, for example, has done so explicitly.[116]

However, states shoulder a positive obligation under human rights law to ensure that the companies' approaches to online speech are appropriate, and that the restrictions they impose on expression are not excessive. Major regulatory decisions that potentially involve balancing competing human rights need to be made by states, and subjected to public scrutiny. As the U.N. Special Rapporteur, David Kaye, has explained, "the rules of speech for public space, in theory, should be made by relevant political communities, not private companies that lack democratic accountability and oversight."[117] In the wake of waves of misinformation affecting everything from elections to pandemic response, the increasing regulatory activity of states is both inevitable and appropriate. For example, Google, Facebook, Microsoft, and Twitter have signed up to a recent EU regulatory regime.[118] The private sector will therefore be increasingly guided by human rights principles, including those set forth above, when determining how to respond to the infodemic of COVID-19 misinformation.[119]

B. Constraints under Human Rights Law When Combatting Hostile Cyber Operations and Misinformation

When taking measures to protect their populations from hostile cyber operations and misinformation, states must not unduly infringe on human rights, particularly the freedom of expression. They must, in other words, strike the right balance between potentially competing rights and interests—a common occurrence within human rights law.[120]

Nevertheless, it would be a categorical error to view the freedom of expression simply as a restriction on a state's measures designed to protect its population during the pandemic. Rather, the freedom of expression is essential for effectively combating the pandemic. Unjustified suppression of speech can, like the untrammeled dissemination of viral misinformation, lead to more deaths in the long run. Recall the Chinese government's censorship of the doctor who warned

116. Monika Bickert (Facebook), *Charting a Way Forward: Online Content Regulation* (Feb. 2020), https://perma.cc/75XS-LVWU; *Sejal Parmar, Facebook's Oversight Board: A Meaningful Turn Towards International Human Rights Standards*?, JUST SEC. (May 20, 2020), https://perma.cc/JBP6-XUJU.

117. David Kaye, *A New Constitution for Content Moderation*, ONEZERO (June 25, 2019), https://perma.cc/W3F4-M97Y.

118. *See* the Code of Practice on Disinformation, which, *inter alia*, involves a self-reporting obligation. *Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019*, EUROPEAN COMM'N, (Oct. 29, 2019), https://perma.cc/HSD3-FG3D.

119. Kate Jones, *Online Disinformation and Political Discourse Applying a Human Rights Framework*, CHATHAM HOUSE REPORT (Nov. 2019) https://perma.cc/K6A9-G78V.

120. Consider, for example, the need to strike a balance between protecting the freedom of expression, on the one hand, and reputations, on the other, in the defamation context. *See, e.g.*, Von Hannover v. Germany, App. No. 59320/00, 2004-VI Eur. Ct. H.R. (finding that Germany had overprotected the freedom of expression of the press while underprotecting the right to the private life of the applicant).

of the virus' spread[121] and the imposition by the UK National Health Service of a ban on NHS health professionals speaking out about workplace conditions.[122] Such measures have only exacerbated the situation. And in countries around the world, the important role of journalists and civil society as public watchdogs is being demonstrated daily as government misinformation, errors, and lack of resources in the health systems are exposed, not for the purpose of assigning blame, but to ensure that they are rectified as quickly as possible.[123]

In short, when state efforts to combat pandemic-related hostile cyber operations or misinformation limit human rights, they must comply with the requirements of the relevant treaties, such as those found in Article 19 of the ICCPR and Article 10 of the ECHR. The measures have to be prescribed by law, necessary to pursue a specific legitimate aim, and be proportionate to that aim.[124] Public health is irrefutably one such aim.[125] Specifically, suppression of misinformation can in principle qualify as necessary for the protection of public health when the social harm caused by untruthful speech cannot be effectively remedied by more truthful speech. Clearly, that is sometimes the case with respect to the pandemic, for the misinformation is proving highly effective and the propagation of accurate information has at times been unable to mitigate the harm. Finally, limitations must always be proportionate in the sense of avoiding, to the extent possible, the potential harm that they could cause.

Three points are essential in this regard. First, and critically, untruthfulness is not in itself a ground for suppressing expression. To be limitable, misinformation has to directly contribute to social harm, which has to be of such magnitude that there is a "pressing social need" (to use the parlance of the European Court) to restrict such expression.[126] The engagement of human rights bodies with so-called "memory laws," which can range from criminalizing the denial of specific historical facts or atrocities, like the Holocaust, to punishing any negation of an overarching historical narrative, is instructive.[127] Painting with a very broad brush, human rights bodies have accepted such measures *only* if the

121. *Li Wenliang: Coronavirus Kills Chinese Whistleblower Doctor*, BBC NEWS (Feb. 7, 2020), https://perma.cc/6UNX-5ZF2. Such censorship appears to be continuing. Stephanie Kirchgaessner, Emma Graham-Harrison & Lily Kuo, *China Clamping Down on Coronavirus Research, Deleted Pages Suggest*, THE GUARDIAN (Apr. 11, 2020, 8:33), https://perma.cc/3P5V-BXME.

122. Sarah Johnson, *NHS Staff Forbidden from Speaking out Publicly about Coronavirus*, THE GUARDIAN (Apr. 9, 2020, 3:56 EDT), https://perma.cc/KB9W-TLY8.

123. Yasmeen Abutaleb, Josh Dawsey, Ellen Nakashima & Greg Miller, *The U.S. was Beset by Denial and Dysfunction as the Coronavirus Raged*, WASH. POST (Apr. 4, 2020), https://perma.cc/ZNS9-N53T.

124. ICCPR, *supra* note 61, art. 19(3); ECHR, *supra* note 70, art. 10(2). *See also* TALLINN MANUAL 2.0, *supra* note 17, r. 37, and accompanying commentary.

125. *See* ICCPR, *supra* note 61, art. 19(3), and ECHR, *supra* note 70, art. 10(2).

126. *See, e.g.*, Lingens v. Austria, 103 Eur. Ct. H.R. (ser. A), ¶39 (1986).

127. Alina Cherviatsova, *Gravity of the Past: Polish-Ukrainian Memory War and Freedom of Speech*, EJIL: TALK! (Feb. 22, 2018), https://perma.cc/4D85-678E; Gleb Bogush & Ilya Nuzov, *Russia's Supreme Court Rewrites History of the Second World War*, EJIL: TALK! (Oct. 28, 2016), https://perma.cc/AK77-WK69.

misinformation, interpreted in its context, also constituted incitement to hatred or intolerance.

For example, in the *Faurisson* case, the Human Rights Committee accepted the justifiability of the applicant's criminal prosecution for denying the existence of gas chambers in Auschwitz, but did so solely because in the French context the denial amounted to a "coded" expression of anti-Semitism.[128] In General Comment No. 34, the Committee added:

> Laws that penalize the expression of opinions about historical facts are incompatible with the obligations that the Covenant imposes on States parties in relation to the respect for freedom of opinion and expression. The Covenant does not permit general prohibition of expressions of an erroneous opinion or an incorrect interpretation of past events.[129]

In short, human rights bodies demand substantial potential harm well beyond mere untruthfulness to justify a state's limitation of expression.

Second, even when limitations on false speech are necessary and proportionate in principle in order to achieve a lawful end such as health, they must be calibrated to minimize any chilling effect on potentially beneficial speech.[130] In the context of the pandemic, such effects can be especially problematic vis-à-vis medical matters regarding which expert consensus is divided, tentative, or lacking. Recall how healthcare professionals initially were nearly unanimous in advising against the personal use of face masks, only to reverse themselves in light of new information.[131] It is particularly important that restrictions on the dissemination of false information not impede such adjustments, as the health community's understanding of a health threat and adequate responses thereto evolve.

Third, while "political" speech enjoys heightened protection, that category is analytically imprecise. Yes, it is clear that under human rights case law "there is little scope . . . for restrictions on political speech or on debate of questions of public interest."[132] However, as illustrated by the divisiveness over the need to social distance, originally apolitical issues can easily become politicized. This has even occurred with regard to ostensibly technical matters like the figures for individuals tested, available hospital beds or ventilators, and individuals who are afflicted with the virus or have died as a result of contracting it.[133] The mere fact

128. Communication No. 550/1993: France (Jurisprudence), U.N. Doc. CCPR/C/58/D/550/1993 (1996) (Robert Faurisson v. France), ¶¶9.3-9.7, and separate opinion by Elizabeth Evatt, David Kretzmer, and Eckart Klein.

129. Human Rights Comm., General Comment No. 34, ¶49, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011).

130. *Id.* ¶47.

131. *Recommendation Regarding the Use of Cloth Face Coverings, Especially in Areas of Significant Community-Based Transmission*, CTRS. FOR DISEASE CONTROL & PREVENTION (Apr. 3, 2020 date last reviewed), https://perma.cc/A6QH-U35S.

132. Wingrove v. United Kingdom, 5 Eur. Ct. H.R., ¶58 (1996).

133. *See, e.g.*, *Trump's Claim That U.S. Tested More Than All Countries Combined Is 'Pants On Fire' Wrong*, KAISER HEALTH NEWS (May 1, 2020), https://perma.cc/JG9D-3JLR.

that it is a *politician* who engages in COVID-19 misinformation, offline or online, does not mean that such speech can never be limited. Unlike First Amendment doctrine,[134] international human rights law does not categorically ban content or viewpoint-based restrictions on political speech.

Given the aforementioned limitations on a state's ability to ban COVID-19 misinformation, the question becomes what states may lawfully do to address the infodemic. Some have adopted new legislation, repurposed old legislation, or implemented other measures to combat the spread of misinformation in general.[135] In the face of the pandemic, some states are applying these pre-existing measures to COVID-19-related misinformation. Others, however, have adopted sweeping solutions that have been criticized for their over-breadth.[136] The Council of Europe's Commissioner on Human Rights has thus felt compelled to urge member states "to preserve press and media freedom and ensure that measures to combat disinformation are necessary, proportionate and subject to regular oversight, including by Parliament and national human rights institutions."[137] To that caution we can add several broad conclusions.

First, laws that contain blanket bans on misinformation or untruthful speech that are not narrowly tailored to achieve a particular legitimate aim fail the necessity and proportionality tests under human rights law, and accordingly unduly infringe on the freedom of expression. As noted in the 2017 Joint Declaration of Special Mandates on the Freedom of Expression, "[g]eneral prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information,' are incompatible with international standards for restrictions on freedom of expression . . . and should be abolished."[138]

Second, since the impact of pandemic misinformation varies from country to country, the permissible restrictions on expression under international human rights law will equally be context-specific. Where misinformation is proving effective, greater expression-restricting measures may be justified. By contrast, in a state with robust online and offline sources of information, it might be possible

134. Frederick Schauer, *The Exceptional First Amendment*, HARVARD UNIV., HARVARD KENNEDY SCHOOL OF GOVERNMENT, FACULTY RESEARCH WORKING PAPER SERIES (Feb. 2005), https://perma.cc/UR7F-W2AG.

135. *See, e.g., Singapore invokes 'fake news' law for first time over Facebook post*, THE GUARDIAN (Nov. 25, 2019, 4:50 EST), https://perma.cc/5Y28-85NC.

136. *See, e.g.*, Mu Sochua, *Coronavirus 'Fake News' Arrests Are Quieting Critics*, FOREIGN POLICY (May 22, 2020, 9:23 AM), https://perma.cc/95JS-PV2A.

137. *Press Freedom must not be Undermined by Measures to Counter Disinformation about COVID-19*, COMM'R FOR HUMAN RIGHTS OF THE COUNCIL OF EUROPE, (Apr. 3, 2020), https://perma.cc/64YG-FU45.

138. The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda*, ¶2A (Mar. 3, 2017), https://perma.cc/4MGV-VWCE.

to counter misinformation by other methods, especially through the efforts of the government and other authoritative institutions that can promote accurate information, without imposing significant restrictions.

Third, the imposition of criminal penalties on those who engage in the spreading of misinformation, online or offline, is unlikely to satisfy the proportionality test if the state failed to carefully adopt measures calibrated to its own context and the threat it is facing, and where less restrictive measures were available but not tested. Such penalties could suggest that their purpose was not to combat the virus, but rather to silence criticism of the government more generally, as has been the case with a number of authoritarian regimes.[139]

Therefore, penalties of this nature are *per se* illegitimate under human rights law because they are not actually pursuing the legitimate aim of protecting public health. Criminalization of misinformation is only appropriate in the most exceptional of cases, through laws that contain a precise definition of the social harm caused by untruthful speech and require proof of a high standard of *mens rea*. An example would be criminalizing the dissemination of misinformation about methanol or other substances as a cure for COVID-19 knowing that the information is false and knowing the health risks of ingesting the substance. The more repressive a measure is, the more it needs to be used surgically, and only when a less restrictive measure would be ineffective.[140]

The same analysis would apply to a state's shutdown of internet services.[141] In particular, the harm caused by a shutdown would almost certainly be disproportionate, for it would impede the freedom of online expression completely in the targeted areas. It is difficult to fashion a scenario in which such an action would be justified for the purpose of combating COVID-19 misinformation, for access to online information is essential to combating, and recovering from, the pandemic. Consider, as an example, the adverse effects that the ban on high-speed Internet access that the Indian government has imposed in Kashmir has had on the availability of COVID-19 information.[142] Freedom of expression necessarily

139. Florian Bieber, *Authoritarianism in the Time of the Coronavirus*, FOREIGN POLICY (Mar. 30, 2020, 10:30 AM), https://perma.cc/HDZ3-GVPC; Csaba Győry, *Fighting Fake News or Fighting Inconvenient Truths*?, VERFASSUNGSBLOG (Apr. 11, 2020), https://perma.cc/92H5-FYF5; Todd Prince, *Russian Activist Says She's Hit By First Investigation Under 'Fake' Coronavirus News Law*, RADIO FREE EUROPE (Apr. 05, 2020 7:12 GMT), https://perma.cc/TF9B-3LGX.

140. A reasonably tailored example of a criminal law that could satisfy the necessity and proportionality tests – depending on how it is applied in practice – is the penal legislation adopted by South Africa that criminalizes publishing a statement through any medium with the *intention to deceive* about Covid-19, anyone's Covid-19 infection status or government measures to address the pandemic. The "intention to deceive" *mens rea* standard is an appropriately high one. *See* Dario Milo & Johan Thiel, *South Africa: Fake News About Covid-19 Now a Criminal Offence*, INFORRM'S BLOG (Mar. 22, 2020), https://perma.cc/WS5G-XAL4.

141. David Kaye, *Report of the Special Rapporteur to the Human Rights Council on Disease Pandemics and the Freedom of Opinion and Expression*, U.N. Doc. A/HRC/44/49 (Apr. 23, 2020), ¶¶24-29.

142. Niala Mohammad, *High-Speed Internet Ban Keeps Kashmir in Dark, Journalists Say*, VOICE OF AMERICA (May 13, 2020, 6:11 PM), https://perma.cc/Y3YG-Z7AZ; Ahmer Khan & Billy Perrigo, *What*

includes the right to access the Internet as a general matter, so long as such access is available.[143]

Finally, it is interesting to observe how some digital platforms have assumed the role of human rights protectors against *state* misinformation. For instance, Facebook and Twitter have taken down posts by national leaders that disseminate certain misinformation, such as the uncritical promotion of the use of hydroxychloroquine.[144] In doing so, companies can rely on international human rights law to resist unjustified state demands to remove content. As noted by U.N. Special Rapporteur on the Freedom of Expression David Kaye, "[i]t is much less convincing to say to authoritarians, 'We cannot take down that content because that would be inconsistent with our rules,' than it is to say, 'Taking down that content would be inconsistent with the international human rights our users enjoy and []which your government is obligated to uphold.'"[145]

C. Positive Due Diligence Obligation under General International Law and Human Rights Law to Stop Hostile Operations Against Other States

The discussion has thus far examined the state's duty of protection against malicious cyber and misinformation operations that target its own population. But the question remains whether such a protective duty can also arise when such operations are emanating from or transiting through a state's territory while affecting third states. We submit that the answer is Yes on two bases. First, such a due diligence obligation arises under general international law. Second, and more contestably, it may also arise under human rights law.

With regard to the former, states are bound in our view by the obligation of due diligence to terminate cyber operations launched from or through their territory that have serious adverse consequences with respect to the rights under international law of other states.[146] This obligation extends to taking action to stop such cyber operations, whether conducted by states or non-state actors. To the extent that the hostile cyber operation in question would have constituted an internationally wrongful act (such as violation of sovereignty, intervention, or a use of force)

Life Is Like Inside the World's Longest Lockdown, TIME (May 5, 2020, 10:30 PM EDT), https://perma.cc/67CA-QAJT.

143. Kaye, Désir & Lanza, *supra* note 99.

144. *Coronavirus: World Leaders' Posts Deleted Over Fake News*, BBC NEWS (Mar. 31, 2020), https://perma.cc/H55Q-NAGX.

145. Kaye, A New Constitution, *supra* note 117.

146. *See* TALLINN MANUAL 2.0, *supra* note 17, ch. 2. *See also* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7); Island of Palmas (Neth. v. US), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928); Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, at 22 (Apr. 9). Although it has not confirmed its acceptance of due diligence as a binding rule of law yet, Australia has highlighted the conditions for its applicability: "To the extent that a state enjoys . . . sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure [they] are not used to harm other states . . . .[It] may not be reasonable to expect (or even possible for) a state to prevent all malicious use of ICT infrastructure . . . . However, . . . if a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law." Australia, *International Cyber Engagement Strategy* 91 (2017).

had the territorial state conducted it, that state must take feasible measures to put an end to any ongoing operations from or through cyber infrastructure on its territory targeting activities addressing the crisis in other states.

There is no reason to exclude application of the rule to hostile cyber operations against medical facilities or capabilities, or public health activities. Before the obligation attaches, however, the hostile cyber operation must have serious consequences vis-à-vis a right under international law of the state in question—as discussed above, cyber operations risking harm to human life and health would certainly qualify, as, *inter alia*, a potential breach of sovereignty, as would those that interfered with a state's public health operations.

This obligation is simply the cyber application of a wide-ranging due diligence positive obligation under general international law requiring a state to stop harm to the rights of other states emanating from its territory. It is nothing more than a corollary of the sovereignty that the state enjoys over its territory, which is a bundle not only of rights, but also of duties. However, it must be cautioned that not all states have publicly commented in the cyber context on whether the due diligence obligation is a binding rule of international law, although there does appear to be international consensus that it is at least a voluntary non-binding norm applicable to cyber operations.[147] That said, a number of states have recently confirmed their acceptance of such a rule as a matter of customary international law, joining the "International Group of Experts" that authored the *Tallinn Manual on the International Law Application to Cyber Operations*.[148] The French position is representative:

> In accordance with the due diligence principle, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" [information and communications technology], including acts that infringe the territorial integrity or sovereignty of another State. In addition, States must ensure that non-state actors do not use their territory to carry on such activities, and not use proxies to commit internationally wrongful acts using ICTs.[149]

The COVID-19 pandemic is likely to strengthen the willingness of states to support characterization of due diligence as a binding obligation.[150] After all,

147. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*, ¶23 (June 24, 2013) ("States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."); Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174, ¶28(f) (July 22, 2015) ("States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.").

148. TALLINN MANUAL 2.0, *supra* note 17, r. 6.

149. Ministry of the Armies Position Paper, *supra* note 27, at 10. *See also, e.g.*, Netherlands MFA Letter, *supra* note 27, at 4-5; Finland, Statement at 2d Substantive Session of OEWG (Feb. 10-14, 2020), https://perma.cc/5RQ8-VUMD.

150. Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic, EUROPEAN COUNCIL OF THE

why would any responsible state not take feasible measures to put an end to such activity?

This raises the question of whether a positive protective obligation to prevent transboundary harm to human life and health exists under international human rights law. As we have explained, the existence of a protective obligation is not controversial. What *is* controversial is its (extra)territorial scope of application. If a state exercises spatial jurisdiction (control of territory) beyond those areas over which it has sovereignty, for example as a belligerent occupier, the protective duty certainly would apply. Russia, for instance, has the obligation to secure or ensure the human rights of people in Crimea, even though it lacks sovereignty over Crimea.

A more difficult question is whether a protective duty would apply in the absence of territorial control. For instance, would Russia have such an obligation vis-à-vis pandemic-related cyberattacks or misinformation emanating from its territory and affecting individuals in, say, Germany or the UK. One of us has previously argued that no such obligation would exist without territorial control.[151] It is difficult, for example, to see how the jurisprudence of the European Court in particular could sustain such an obligation.

However, in recent years a number of other human rights bodies have put forward much more expansive interpretations, mainly with regard to transboundary harm caused by *corporate* entities domiciled within or operating from a state's territory. Thus, for example, both the Committee on Economic, Social and Cultural Rights[152] and the Human Rights Committee[153] have held that an extraterritorial protective obligation would exist in such circumstances under the ICESCR and the ICCPR. So has the Inter-American Court of Human Rights, which has held that an extraterritorial protective obligation would arise with respect to transboundary environmental harm affecting the right to life, even when such harm is caused by private actors.[154]

EUROPEAN UNION (Apr. 30, 2020 13:00), https://perma.cc/QAN8-NLR6 ("The European Union and its Member States call 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 consensus reports of the United Nations Groups of Governmental Experts (UNGGEs) in the field of Information and Telecommunications in the Context of International Security.").

151. Milanovic, *supra* note 71, at 210.

152. CESCR General Comment No. 24, *supra* note 68, ¶¶30-35.

153. HRC General Comment No. 36, *supra* note 65, at ¶22 ("[States] must also take appropriate legislative and other measures to ensure that all activities taking place in whole or in part within their territory and in other places subject to their jurisdiction, but having a direct and reasonably foreseeable impact on the right to life of individuals outside their territory, including activities taken by corporate entities based in their territory or subject to their jurisdiction, are consistent with article 6.").

154. The Environment and Human Rights, Advisory Opinion OC-23/17 Requested by the Republic of Colombia, Inter-Am. Ct. H. R. (Nov. 15, 2017), ¶¶ 101-104, esp. ¶ 102 ("In cases of transboundary damage, the exercise of jurisdiction by a State of origin is based on the understanding that it is the State in whose territory or under whose jurisdiction the activities were carried out that has the effective control over them and is in a position to prevent them from causing transboundary harm that impacts the enjoyment of human rights of persons outside its territory. The potential victims of the negative consequences of such activities are under the jurisdiction of the State of origin for the purposes of the

If this jurisprudence is taken as a starting point, it would appear a reasonably straightforward analogy to say that states have a duty to prevent transboundary harm to life and health caused by cyber and misinformation operations emanating from their territory. Such an obligation would apply regardless of the identity of the immediate perpetrator of the harm—which could be a corporate entity, a hacker group, an armed group, or even a third state. We can see no reason why these human rights bodies (with the exception of the European Court) would not apply the same reasoning to cyber harm during the pandemic. That said, it must be acknowledged that the existence of such a positive obligation is more controversial than that of a negative obligation for the state itself not to cause transboundary harm, which we examined above.

On a final note, if a due diligence obligation to stop hostile cyber operations and misinformation harmful to human life and health emanating from a state's own territory and affecting another state already exists under general international law, why should it matter whether a similar obligation would also exist under human rights law? That obligation would not be redundant for three reasons. First, a protective human rights obligation would be owed not (just) to other states, but also directly to affected individuals. Second, these individuals would have certain remedies available to them, such as litigation before domestic courts and international human rights bodies. Third, substantively the positive human rights obligations might be more demanding than the general international law one. Human rights jurisprudence has frequently incorporated more systemic and preventive duties into protective obligations,[155] unlike, arguably, the due diligence obligation under general international law.[156] Normatively, the greater intensity of the preventive obligation under human rights law would be justified by the importance of the interests at stake, that is, the direct adverse consequences to human life and health.

CONCLUSION

International law can play a robust role in addressing the COVID-19 pandemic. As discussed above, and as recently noted by the Dutch government,

> . . . malicious cyber operations targeting healthcare systems or facilities could, depending on the specific circumstances, be qualified as a violation of international law. Equally, cyber enabled information operations that intervene with, for example national crisis response mechanisms during a health crisis, could, depending on the circumstances, be qualified as violation of international law.[157]

---

possible responsibility of that State for failing to comply with its obligation to prevent transboundary damage."). *See also* Antal Berkes, *A New Extraterritorial Jurisdictional Link Recognised by the IACtHR*, EJIL: TALK! (Mar. 28, 2018), https://perma.cc/988T-A4RE.

155. *See* CESCR General Comment No. 24, *supra* note 68, ¶33.

156. TALLINN MANUAL 2.0, *supra* note 17, rr. 6-7 and accompanying commentary.

157. Netherlands, Pre-draft Report, *supra* note 23, ¶18.

A state's COVID-19-related cyber operations can violate the sovereignty of the state into which they are conducted, intervene in that state's internal affairs, or even amount to a wrongful use of force against it. They may also violate the human rights of individuals on the state's own territory and beyond.

Further, states have a duty under human rights law to combat certain cyber operations related to the pandemic, including misinformation by states and non-state actors, in order to protect the human rights to life and health of those on its territory. Arguably, they shoulder the same obligation when cyber operations affecting the human rights of individuals beyond their borders are launched from or through their territory. In doing so, however, states must not unduly infringe upon other human rights, such as the freedom of expression. The pandemic must not be used opportunistically as a pretext for state censorship of criticism and dissent, whether online or offline. This is especially so because the "freedom of opinion and expression goes hand-in-glove with public health."[158] Finally, in our estimation, states must, pursuant to the general international law due diligence obligation, take feasible measures to put an end to hostile cyber operations launched from their territories by another state or a non-state actor that are related to the COVID-19 pandemic if they cause serious adverse consequences with respect to the rights of other states, the most likely such right being respect for its sovereignty.

However, as should be clear, some aspects of the law are far from settled. For instance, at least one state, wrongly in our view, rejects the existence of the general international law rule most likely to be breached by COVID-19-related cyber operations, sovereignty. In doing so, it has denied itself the opportunity to condemn other states that launch harmful cyber operations during this pandemic, as well as the right to respond with countermeasures under the law of state responsibility. And many other aspects of the relevant law are the subject of normative uncertainty, such as the extraterritorial application of human rights obligations to respect and protect.

It is difficult to find anything positive about this horrific global pandemic. However, it can help draw attention to the criticality of moving the international cyber law discourse among states forward much more quickly than has been the case to date. Many states have been cautious about proffering their interpretation of the applicable law, and to some extent rightfully so, but caution has consequences. It can leave us normatively ill-prepared for the next crisis. Some states have condemned the COVID-19-related cyber operations, although seldom on the basis of international law, as distinct from political norms of responsible state

158. Kaye, *supra* note 141, ¶10.

behavior.[159] Hopefully, they will add legal granularity to future statements. But all states, human rights courts, human rights monitoring bodies, the academy, the private sector, and NGOs must take up the challenge presented by this tragic pandemic to move the law governing cyberspace in the right direction.[160]

159. *See* Statements by Australia, China, Czech Republic, Republic of Korea, Netherlands, United Kingdom, United States, and the Council of the European Union *in* Kubo Mačák, Laurent Gisel & Tilman Rodenhäuser, *International Law Protections against Malicious Cyber Operations, Background Paper for Virtual Workshop, Applying International Law in Cyberspace: Protections and Preventions*, Oxford Institute for Ethics, Law and Armed Conflict, May 16, 2020 (on file with the authors).

160. *See, e.g.*, Dapo Akande, Dubcan B. Hollis, Harold Hongju Koh, & James O'Brien, *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector*, JUST SEC. (May 21, 2020), https://perma.cc/8DET-VAYK; *World Leaders Call on Governments to Stop Cyberattacks Plaguing Healthcare Systems*, CYBER PEACE INSTITUTE (May 26, 2020), https://perma.cc/XLS9-RCQ3.