The 'Infodemic': Is International Law Ready to Combat Fake News in the Age of Information Disorder?

*Hitoshi Nasu**

1 Introduction

During the COVID-19 pandemic, a variety of false claims have widely been circulated on social media. These include claims about the origins of the virus (for example, claims that the United States military introduced the virus to Wuhan),[1] various health information,[2] and rumours about inefficacy and danger of vaccination.[3] The Vice President of the European Commission for Values and Transparency described this phenomenon a coronavirus 'infodemic', in which false or misleading information has harmed the health of citizens, negatively affected the economy, and undermined the response of public authorities.[4] So-called 'fake news', which emerged as a political issue in modern democracies, has entered a new phase with a far-reaching impact on the general public, extending to areas that are supposedly non-partisan, such as the protection of public health in the fight against the spread of infectious disease.

* Professor of Law, United States Military Academy at West Point; Senior Fellow, Stockton Center for International Law, United States Naval War College.

1 Vanessa Molter and Graham Webster, 'Virality Project (China): Coronavirus Conspiracy Claims', *Internet Observatory* (Blog Post, 31 March 2020) <https://cyber.fsi.stanford.edu/io/news/china-covid19-origin-narrative>.

2 Jack Goodman, 'Coronavirus: Compulsory vaccines in the UK and other rumours fact-checked', *BBC News* (online, 9 May 2020) <https://www.bbc.co.uk/news/52565764>; Philip Howard et al, 'The COVID-19 "infodemic": what does the misinformation landscape look like and how can we respond?' *Oxford Internet Institute* (Blog Post, 15 April 2020) <https://www.oii.ox.ac.uk/blog/the-covid-19-infodemic-what-does-the-misinformation-landscape-look-like-and-how-can-we-respond/>.

3 Richard Horton, 'Offline: Managing the COVID-19 Vaccine Infodemic' (2020) 397(10261) *Lancet* 1474.

4 Věra Jourová, 'Response to disinformation around COVID-19' (Speech, College of Commissioners Meeting, 10 June 2020). See also Ministry of Foreign Affairs of the Republic of Latvia, 'Cross-Regional Statement on "Infodemic" in the Context of COVID-19' *News* (Web Page, 12 June 2020) <https://www.mfa.gov.lv/en/news/latest-news/66117-cross-regional-statement-on-infodemic-in-the-context-of-covid-19>.

The fabrication of information, which 'mimics news media content in form but not in organisational process or intent',[5] has gained asymmetrical influence on the individual perception of real-world events and political choices. This is largely due to the widespread exploitability of information on the internet generally, and social media more specifically. Harmful influences may arise from any false or misleading information ('misinformation') but are of particular concern when such information is generated and circulated with the specific purpose of deceiving people ('disinformation'). This is because the ability to exploit online communication adds to the modern tools of information operations as a means of foreign interference and sabotage.[6] The manipulation of information for deceptive purposes has gained force by taking advantage of the increased ability to disseminate misinformation effectively on social media.

Indeed, the European Union has identified that foreign countries, particularly Russia and China, have engaged in targeted influence operations and disinformation campaigns around COVID-19 to undermine the credibility of the Union and its response to the coronavirus pandemic.[7] Disinformation campaigns conducted during the COVID-19 pandemic, especially those involving Chinese and Russian operatives, have further cultivated the online information environment for the purposes of disruption and destabilisation.[8] The diffused nature of the threat that such hostile information operations pose to national security is likely to test the protective value of international law, as national authorities struggle in developing their regulatory responses to information disorder.

5 David MJ Lazer et al, 'The science of fake news' (2018) 359(6380) *Science* 1094, 1094.

6 See, eg, Rosanna E Guandagno and Karen Guttieri, 'Fake News and Information Warfare: An Examination of the Political and Psychological Processes from the Digital Sphere to the Real World' in Innocent E Chiluwa and Sergei A Samoilenko (eds), *Handbook of Research on Deception, Fake News, and Misinformation Online* (IGI Global, 2019) 167.

7 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Tackling COVID-19 Disinformation—Getting the Facts Right', Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions (10 June 2020) JOIN(2020) 8, 3; 'EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic', *EU vs Disinfo* (Blog Post, 1 April 2020) <https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic/>.

8 See, eg, Sascha-Dominik Dov Bachmann, Doowan Lee and Andrew Dowse, 'COVID Information Warfare and the Future of Great Power Competition' (2020) 44(2) *Fletcher Forum of World Affairs* 11.

This article considers the readiness of international law to protect States from information operations that are launched as the means of disrupting government response to the spread of infectious diseases, such as COVID-19. There are relevant rules of international law that impose restrictions on national authorities for their involvement in the dissemination of misinformation and for their response to such activities. However, the unique online information environment, in which various individuals are involved in the decentralised process of creating and disseminating misinformation with or without various degrees of State support, enables hostile actors to work across the traditional boundaries of these rules. A lack of awareness about this complex environment by solely focusing on State-sponsored information operations fails to appreciate the unique challenge that has been posed to national authorities in managing public response to a public health crisis. As such, this article examines both the external- and internal-facing dynamics for international regulation of misinformation, with the focus on the principle of non-intervention as an external regulation of misinformation under general international law and freedom of expression guaranteed under human rights treaties for internal regulation.

2 The Principle of Non-Intervention

States are not prohibited from spreading misinformation under international law, with the exception of a few specific areas. The broadcasting of false information is regulated under the *International Convention Concerning the Use of Broadcasting in the Cause of Peace*, under which a limited number of States Parties have agreed to undertake to prohibit and stop any transmission of false statements when it is 'likely to harm good international understanding'.[9] Under the *International Telecommunication Union's Radio Regulations*, States have an obligation not to send false or misleading signals,[10] but this applies to the identification of its transmitter rather than to the substance of a transmission. The *Convention for the Suppression of Unlawful Acts Against Civil Aviation* merely prescribes criminalising the unlawful and intentional communication

9 *International Convention Concerning the Use of Broadcasting in the Cause of Peace*, opened for signature 23 September 1936, 186 LNTS 301 (entered into force 2 April 1938) art 3(1). Australia, along with France, Netherlands, and the United Kingdom, denounced this treaty in the 1980s. For analysis, see Björnstjern Baade, 'Fake News and International Law' (2018) 29(4) *European Journal of International Law* 1357, 1365–69.

10 *Radio Regulations*, adopted 2 November 2016 (entered into force 1 January 2017) art 18.

of information when it is known to be false and endangers the safety of an aircraft in flight.[11]

Nevertheless, deliberate interference with domestic affairs of another State through the dissemination of misinformation may amount to an intervention prohibited under customary international law. The principle of non-intervention prohibits States from committing an act of intervention, directly or indirectly, in the domestic affairs that fall within the exclusive competence of another State.[12] It remains contentious whether the scope of the exclusive competence is determined by the inherent attributes of sovereignty reserved under international law,[13] or by taking into account various factors as found in the actual practice of States and international organisations.[14] At any rate, within the current framework of international law, there is little doubt that the choice of public health system, and the formulation of regulatory response to infectious diseases, falls within the exclusive competence of the State, considering that it is also reserved as an exception to various treaty commitments.[15]

The relevant question is rather whether the dissemination of misinformation, with a view to or an effect of undermining regulatory efforts to control or contain the spread of virus, amounts to an intervention prohibited under this principle. This is because an element of coercion is considered as the very essence of prohibited intervention,[16] although various views have been expressed in literature about this element from those equating it with forcible measures to the idea that even non-forcible, political influence could amount

11 *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*, opened for signature 23 September 1971, 974 UNTS 177 (entered into force 26 January 1973) art 1(e).

12 *Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations*, GA Res 26/25(XXV), UN Doc A/RES/2625(XXV) (24 October 1970); *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, GA Res 2131(XX), UN Doc A/RES/2131(XX) (21 December 1965).

13 See *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States of America*) (*Merits*) [1986] ICJ Rep 14, 108 [205] ('*Nicaragua*'): holding that a prohibited intervention must 'be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely'.

14 See *Nationality Decrees Issued in Tunis and Morocco* (*Advisory Opinion*) [1923] PCIJ (ser B) No 4, 24: observing that the scope of the exclusive competence of the State is 'an essentially relative question' and 'depends on the development of international relations.'

15 See, eg, *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) arts 12(3), 19(3), 21, 22(2) ('ICCPR').

16 *Nicaragua* (n 13) 108 [205].

to an intervention.[17] Depending on the substantive standard applied to assess coerciveness, the disruption of a public health system with the dissemination of misinformation could amount to an intervention in cases where such an operation is attributable to the State.

Of particular relevance is General Assembly Resolution 36/103, which lists a wide range of interferences as constituting an intervention. It relevantly refers to the duty of a State to 'abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States'.[18] It also enjoins States to refrain from the exploitation and distortion of human rights issues as a means of interference, exerting pressure on other States or creating distrust and disorder within and among States.[19] Although this resolution was adopted by majority, its status under customary international law has been in doubt due to the objection of many Western States.[20] Indeed, various forms of non-forcible interference ranging from lobbying, propaganda broadcasting, and the dissemination of false information have been commonplace in state practice. This was particularly the case during the Cold War when the superpowers were competing with attempts to exert transnational political influence in different parts of the world.[21]

However, with the increased vulnerability to hostile cyber operations and associated exploitation of social media, there are indications that Western States are becoming more amenable to lowering the bar for the assessment of coerciveness as the requisite element of intervention.[22] While acknowledging that there is no consensus among States on the precise boundaries of this principle, Jeremy Wright, the former Attorney-General of the United Kingdom, referred to the manipulation of the electoral system to alter the results of an election in another country, intervention in the fundamental operation of

17 See, eg, Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention' (2015) 14 *Baltic Yearbook of International Law* 137, 146–9; Maziar Jamnejad and Michael Wood, 'The Principle of Non-intervention' (2009) 22(2) *Leiden Journal of International Law* 345, 368–77; Lori Fisler Damrosch, 'Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs' (1989) 83(1) *American Journal of International Law* 1, 3–4.

18 *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, GA Res 36/103, UN Doc A/RES/36/103 (9 December 1981) [II(j)].

19 Ibid [II(l)].

20 Adopted by 120 to 22, with 6 abstentions.

21 See, eg, Calder Walton, 'Spies, Election Meddling, and Disinformation: Past and Present' (2019) 26(1) *Brown Journal of World Affairs* 107.

22 Cf Henning Lahmann, 'Information Operations and the Question of Illegitimate Interference under International Law' (2020) 53(2) *Israel Law Review* 189, 209–12.

Parliament or in the stability of a financial system as practical examples of prohibited intervention.[23] Likewise, in the United States, the General Counsel of the Department of Defense Paul Ney has labelled a cyber operation that interferes with another country's ability to hold an election or that tampers with another country's election results as clear examples of prohibited intervention,[24] drawing verbatim from the remarks made by Brian Egan as Legal Adviser to the Department of State.[25] It is nevertheless plausible to envisage situations where these hostile operations are conducted simply as malicious acts that are designed to disrupt the political or economic system of another country, without a particular intention to cause the target State to change its policy or decision.[26]

The Australian Government has interpreted coercive means as interferences that 'effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature'.[27] According to this position, the intention to change the target State's policy or decision is not material to its assessment of foreign interference under the principle of non-intervention. Instead, the mere fact that the State has lost control over an inherently governmental function would be sufficient to satisfy the standard of coerciveness. It reflects the growing concern among political circles about increasingly sophisticated attempts by foreign powers to influence domestic political processes, which resulted in the enactment of the *National Security Legislation Amendment* (*Espionage and Foreign Interference*) *Act 2018* (Cth).[28]

The standard may even be further relaxed to extend the reach of this principle to the dissemination of misinformation that generates dissent or

23 Jeremy Wright, 'Cyber and International Law in the 21st Century' (Speech, Chatham House Royal Institute, 23 May 2018).

24 Paul C Ney Jr, 'DoD General Counsel Remarks at the US Cyber Command Legal Conference' (Speech, US Cyber Command Legal Conference, 2 March 2020).

25 Brian J Egan, 'Remarks on International Law and Stability in Cyberspace' (Speech, Berkeley Law School, 10 November 2016).

26 Michael Schmitt, 'The Defense Department's Measured Take on International Law in Cyberspace', *Just Security* (Blog Post, 11 March 2020) <https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/>. See also Jens David Ohlin, *Election Interference: International Law and the Future of Democracy* (Cambridge University Press, 2020) 82–5.

27 Department of Foreign Affairs and Trade, *Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace* (Report, 2019) <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html>.

28 Nigel Brew, 'Foreign interference—neither new nor limited to China' (Research Paper, Parliamentary Library, Parliament of Australia, 11 September 2019).

encourages insurgency.[29] However, given the diffused nature of threats posed by misinformation, the causal nexus between information operations and their coercive effect inevitably becomes tenuous. Although it is widely accepted that the principle applies to indirect means of intervention,[30] there are practical difficulties in establishing the coercive nature of information operations because indirect causation necessarily moves such activities in the direction of permissible interference and away from intervention.[31] It remains to be seen if the general practice among States evolves to extend the scope of prohibition to information operations, which are not intended to change the target State's policy or to deprive it of the ability to function but rather to reduce its effectiveness, for example, by subverting public health measures to protect the population against the spread of infectious diseases.

Information operations could amount to an intervention only if such an operation is attributable to a State. When there is no clear evidence of attribution, the question might nonetheless arise whether the State has an obligation of due diligence to ensure that its territory is not knowingly used as a base, by a non-state actor or another State, for violations of international law.[32] This means that States might be required to take feasible measures against those who are disseminating misinformation in a manner which would disrupt the operation of a public health system of another State in combating the spread of infectious diseases. There are reports suggesting that State-sponsored media outlets from China, Iran, Russia and Turkey have been generating and disseminating misinformation in European languages.[33] There could be a potential ground for claiming State responsibility, in cases where such information operations amount to an infringement upon another State's sovereignty

29 See Jamnejad and Wood (n 17) 374. See also Nicholas Tsagourisas, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace', *EJIL:Talk!* (Blog Post, 26 August 2019) <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/>: considering interference in the process of the formation of sovereign authority as coercive. But see Ohlin (n 26) 103–4.

30 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) r 66 [24] ('*Tallinn Manual 2.0*').

31 Michael N Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19(1) *Chicago Journal of International Law* 30, 51–2.

32 *Tallinn Manual 2.0* (n 30) r 6 [27].

33 Katarina Rebello et al, 'Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users', *COMPROP Data Memo* (29 June 2020) <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2020/06/Covid-19-Misinfo-Targeting-French-German-and-Spanish-Social-Media-Users-Final.pdf>.

or to an intervention by causing sustained disruption of the latter's public health system.

It is even possible to envisage situations where a State may assert a breach of the principle of non-use of force when a foreign military force engages in disinformation campaigns with the intention to cause a greater number of deaths resulting from the uncontrollable spread of infectious diseases. Indeed, multiple States have adopted the view that hostile activities by non-traditional means, such as cyber operations, can constitute a use of force when the scale and effects of such activities are comparable to those of a conventional act of violence covered by the prohibition.[34] However, the causal link between the dissemination of misinformation and physical harm is rather tenuous, which could make States reluctant to accept such characterisation.

3 Freedom of Expression

Domestically, regulatory responses to misinformation are likely to cause tension with individual freedom of expression, in cases where there are relevant human rights obligations under international law, such as the International Covenant on Civil and Political Rights (ICCPR),[35] or under municipal law, such as the First Amendment of the United States Constitution.[36] Such obligations

34 See, eg, Department of Foreign Affairs and Trade, *Australia's Position on the Application of International Law to State Conduct in Cyberspace* (Report, 2017) s 1 <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html#Annex-A>; Letter from the Minister of Foreign Affairs of the Government of the Netherlands to the President of the House of Representatives of the Government of the Netherlands, 5 July 2019 (5 July 2019) Appendix, 3; Ministère des Armées, 'Droit international appliqué aux opérations dans le cyberespace' (Report, 2019) 7 [1.1.2]; Wright (n 23); Ney (n 24); Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 *Harvard International Law Journal* 1, 3–4.

35 ICCPR (n 15) arts 2(1), 19(2). See also *Arab Charter on Human Rights*, adopted 23 May 2004 (entered into force 15 March 2008), reprinted in (2005) 12 International Human Rights Reports 893, art 32; *African Charter on Human and Peoples' Rights*, opened for signature 27 June 1981, 1520 UNTS 217 (entered into force 21 October 1986) art 9(2); *American Convention on Human Rights*, opened for signature 22 November 1969, 1144 UNTS 123 (entered into force 18 July 1978) art 13; *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) art 10.

36 It reads: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.'

impose legal constraints upon the ability of national authorities to suppress or prevent the spread of misinformation. However, freedom of expression is not guaranteed without any qualification or exceptions. National authorities are generally allowed to restrict freedom of expression when requisite requirements are met.[37] Moreover, the ICCPR specifically proscribes any propaganda for war and advocacy of national, racial or religious hatred inciting discrimination, hostility or violence.[38]

With the global outbreak of COVID-19, numerous criminal prosecutions have been launched to combat misinformation in different jurisdictions. On 15 March 2020, Elijah Muthui Kitonyo was arrested in Kenya for publishing false information regarding COVID-19 on his Twitter account.[39] In Mauritius, Jahmeel Peerally was arrested on 25 March 2020 for falsely claiming that riots had erupted after the Prime Minister announced the closure of supermarkets and shops as a response to COVID-19.[40] In the same country, Rachna Seenauth was arrested on 15 April 2020 for fabricating 'breaking news' regarding a conference call to discuss the 'miracle treatment' for COVID-19.[41] In South Africa, several people have been charged for spreading false information regarding COVID-19.[42] There are also numerous counts of misinformation removed or blocked on social media and other corrective measures in an attempt to suppress the impact of misinformation.

The legality of these measures depends on whether such restrictions on freedom of expression are justifiable on legitimate grounds as provided in the relevant treaty instrument or under domestic law. There are certain requirements that are commonly observed across different jurisdictions, such as the tests of necessity and proportionality. However, the specific legal requirements

37 For detailed analysis, see RK Helm and H Nasu, 'Regulatory Responses to "Fake News" and Freedom of Expression: Normative and Empirical Evaluation' (2021) 21(2) *Human Rights Law Review* 302.

38 ICCPR (n 15) art 20. See generally M G Kearney, *The Prohibition of Propaganda for War in International Law* (2007).

39 B Senne, 'Kenyan Man Arrested for Spreading Fake News on Coronavirus', *Times Live* (online, 16 March 2020) <https://www.timeslive.co.za/news/africa/2020-03-16-kenyan-man-arrested-for-spreading-fake-news-on-coronavirus/>.

40 L Sophie, 'Fake News: Jahmeel Peerally arrêté', *Soutenex Lexpress.mu* (Web Page, 25 March 2020) <https://www.lexpress.mu/article/373277/fake-news-jahmeel-peerally-arrete>.

41 T Mendel, 'Mauritius: "Fake News" Arrest for Political Satire Not Legitimate' *Centre for Law and Democracy* (Web Page, 17 April 2020) <https://www.law-democracy.org/live/mauritius-fake-news-arrest-for-political-satire-not-legitimate/>.

42 A Nyathi, R Thaw and K Palm, 'Cele: 8 People Arrested for Spreading Fake News on COVID-19', *Eyewitness News* (online, 7 April 2020) <https://ewn.co.za/2020/04/07/cele-8-people-arrested-for-spreading-fake-news-on-covid-19>.

for restriction or standards to be applied in evaluating the lawfulness of restriction vary in each jurisdiction. Therefore, any categorical denial of regulatory measures, such as the UN Special Rapporteur's statement that 'the penalization of disinformation is disproportionate',[43] is misleading and does not help guide national authorities in finding an appropriate balance between combating misinformation and respecting freedom of expression in the course of developing regulatory responses that are both effective and norm compliant.

The extent to which, and circumstances in which, restrictions on the dissemination of misinformation are justifiable depends on the construction of a particular provision in which freedom of expression is guaranteed. Under the ICCPR, for example, contracting parties are allowed to impose restrictions on any form of expression or means of its dissemination, including systems to support such communication, such as Internet service providers or search engines, to the extent necessary for the protection of national security, public order, public health or morals.[44] It is thus conceivable that restrictions on misinformation regarding health-threatening activities are deemed necessary and justifiable on public health grounds.[45] The European Court of Human Rights has, on the other hand, granted contracting parties a margin of appreciation in determining what is necessary to protect the competing interests identified as the permissible grounds for restricting freedom of expression, especially in cases where there is no European consensus on how to regulate an emerging or divisive problem.[46]

States may also be entitled to declare a public emergency to derogate from certain obligations to protect human rights, as many countries did during the COVID-19 pandemic. The declarations of derogation made during the pandemic

43 David Kaye, *Disease Pandemics and the Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HRC/44/49 (23 April 2020) [42].

44 Human Rights Committee, *General Comment No 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [43]. See generally K Jakubowicz, 'Early Days: The UN, ICTs and Freedom of Expression' in T McGonagle and Y Donders (eds), *The United Nations and Freedom of Expression and Information: Critical Perspectives* (Cambridge University Press, 2015) 304; Andrew Puddephatt, 'Freedom of Expression Rights in the Digital Age' (Reference Series No 6, Open Society Foundation, April 2011) 6.

45 See Paul M Taylor, *A Commentary on the International Covenant on Civil and Political Rights* (2020) at 574; William A Schabas, *Nowak's CCPR Commentary* (3rd ed 2019) at 572.

46 See, eg, *Animal Defenders International v United Kingdom* (2013) 57 Eur Court HR 362, [123]; *TV Vest AS v Norway* [2008] V Eur Court HR 265, 291 [67]; *Handyside v United Kingdom* (1976) 1 Eur Court HR 737, [57]. See generally Bychawska-Siniarska, *Protecting the Right to Freedom of Expression under the European Convention on Human Rights* (Council of Europe, 2017) 44–62.

have mainly focused on the right to liberty, freedom of movement and freedom of assembly to justify lockdown measures.[47] In its statement issued on 30 April 2020, the Human Rights Committee urged States Parties not to rely on derogation, where their public health or other public policy objectives can be attained by restricting the rights or introducing reasonable limitations in conformity with the provisions for such restrictions and limitations set out in the ICCPR.[48] This statement suggests that even during a public emergency, the Committee is of the view that States should, in the first place, make use of the restrictions available under each provision, while acknowledging that freedom of expression and information constitutes important safeguards for ensuring compliance with their obligations under the ICCPR in the exercise of emergency powers.[49]

However, various restrictive measures to prevent and suppress the dissemination of misinformation are not completely effective due to practical constraints. There are technical difficulties with policing all the communications on social media platforms. A threat of sanctions or blocking of communication does not deter everyone from spreading misinformation or engaging in disinformation campaigns. This is especially the case when those responsible for generating or disseminating misinformation are operating from foreign jurisdictions. The criminal law approach therefore has its limit in the absence of international legal mechanisms for mutual cooperation in law enforcement between relevant countries. Because of this limitation, some States may resort to extraterritorial suppressive measures by engaging in cyber operations to disrupt disinformation campaigns at their sources, as the United States and the United Kingdom did against the so-called Islamic State,[50] to the extent that it does not amount to an infringement upon the sovereignty of another State,[51] or to a prohibited intervention as discussed earlier.

---

47 ICCPR (n 15) arts 9, 12 and 21 respectively.

48 'Statement on Derogations from the Covenant in connection with the COVID-19 Pandemic', UN Doc CCPR/C/128/2 (30 April 2020) [2(c)].

49 Ibid [2(f)].

50 'UK Targeted ISIS Drones and Online Servers in Cyber Attack', *Financial Times* (online, 7 February 2021), <https://www.ft.com/content/360a8e1c-b241-40f7-b944-45a4f8854ac5>; 'UK Launched Cyber-Attack on Islamic State', *BBC News* (online, 12 April 2018) <https://www.bbc.co.uk/news/technology-43738953>.

51 For debate regarding the respect for sovereignty as a rule of international law applicable in cyberspace, see Geoffrey P Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 *American Journal International Law Unbound* 207–12; Michael N Schmitt and Liis Vihul, 'Sovereignty in Cyberspace: *Lex Lata Vel Non*?' (2017) 111 *American Journal of International Law Unbound* 213–8; Michael N Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95(7) *Texas Law Review* 1639.

4 Conclusion

Within the existing framework of international law, States are not prohibited from disseminating misinformation in another State unless it amounts to an intervention due to the coercive nature of interference with the domestic affairs of the latter State. There are indications in State practice that the substantive standard for coerciveness might be shifting towards extending the reach of this principle to the dissemination of misinformation that generates dissent or encourages insurgency. However, because of the unique online information environment where threats posed by misinformation are diffused in nature, there are technical difficulties in establishing the causal nexus between information operations and their coercive effect or clear evidence for attribution of these operations to a State. There is also a question as to whether the State has an obligation of due diligence to ensure that its territory is not knowingly used as a base, by a non-state actor or another State, for violations of international law through the dissemination of misinformation.

On the domestic front, States reserve the sovereign right to develop and employ any effective means of combating misinformation within their own jurisdiction, to the extent that associated restrictions on freedom of expression are tailored and justifiable under the applicable rules of international or domestic human rights law. Nevertheless, the emergence of the 'infodemic' disrupting government response to the spread of coronavirus has shown that many national authorities are yet to develop an effective and norm-compliant system to suppress or eliminate the harmful impact of misinformation. There is also a limit to the criminal law approach in combating information operations originating from foreign jurisdictions, in the absence of international legal mechanisms for mutual cooperation in law enforcement.

Between these two possible legal solutions lies a swath of unregulated space in which hostile actors can launch information operations by disseminating misinformation without assuming any legal liability. This space will remain wide open for exploitation as long as the strict standard is maintained for assessing coerciveness of foreign interference as the requisite element of intervention prohibited under customary international law or by worshipping freedom of expression with the categorical denial of regulatory measures to suppress misinformation. The traditional framework of international law, which has been built upon the premise that the free flow of information helps sustain and promote liberalism, does not provide adequate protection against the rise of information disorder disrupting government response to a public health crisis.

Equally concerning is the exploitability of misinformation when it is employed as part of hybrid threats, combined with military operations such as cyberattacks, to disrupt the regulatory system that the target State has in place for responding to a public health crisis. Such hybrid threats may exploit a legal 'grey zone', where it is unclear how the conduct should be legally characterised due to the lack of a clear and shared understanding of what constitutes an intervention and the circumstances in which States are required to exercise due diligence under general international law. In such situations, the defending State is left with difficult choice between the pursuit of peaceful solutions,[52] and, taking risks of legal uncertainty, the adoption of unilateral remedial measures such as extra-territorial suppressive measures through cyber operations to disrupt disinformation campaigns at their sources.

Acknowledgments

The author is grateful to Associate Professor Aurel Sari for helpful comments on an earlier draft. The thoughts and opinions expressed are those of the author and do not necessarily represent those of the US Government, the US Department of the Navy, the US Military Academy, or the US Naval War College.

52 Cf The White House President Barack Obama, 'Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference' (Web Page, 25 September 2015) <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint> (in relation to cyber espionage).