Research Paper

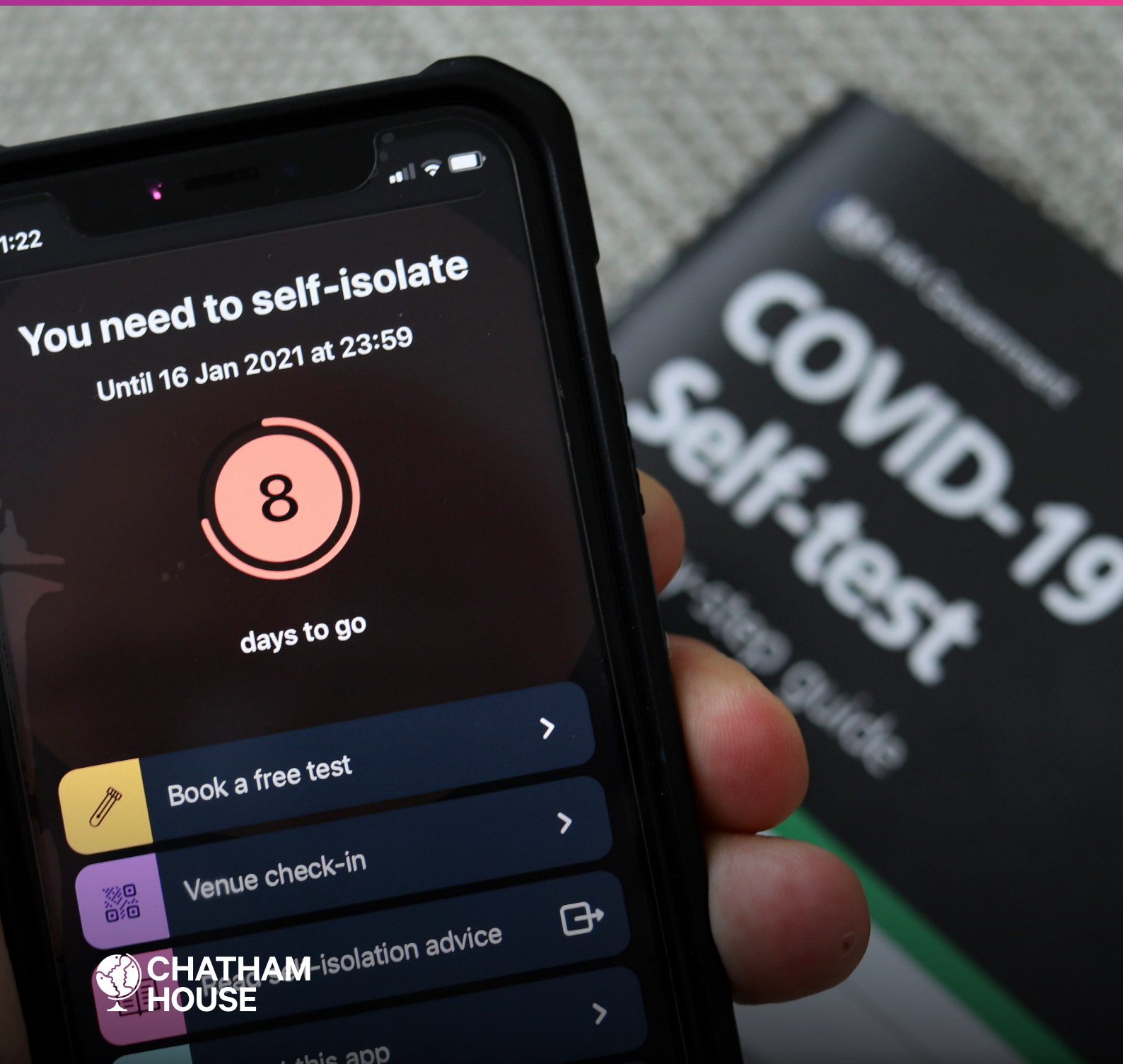
International Security Programme

February 2021

The COVID-19 pandemic and trends in technology

Transformations in governance and society

Joyce Hakmeh, Emily Taylor, Allison Peters and Sophia Ignatidou



CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Summary

- The context of the COVID-19 pandemic has emphasized that, more than ever, governments and businesses have to reinvent themselves through the fuller integration of digital technology in all aspects of their work, and that they must pursue long-term digital transformation in order to compete and operate both nationally and internationally. Otherwise, they risk falling behind, unable to find their place in an altered global landscape.
- The issues encountered during the development of track-and-trace apps as part of the fight against COVID-19 have highlighted significant differences in levels of accountability and transparency between the public and private sectors. This has underlined the areas of tension between corporate power and the authority of democratically elected governments, and the capacity of tech companies not just to deploy 'soft' power in the form of lobbying, but also to block access to essential technologies.
- The fragmented response to the COVID-19 pandemic has brought renewed focus on the lack of internationally agreed technical standards that are both privacy-respecting and secure by design. Such standards could potentially offer interoperability if individuals travel overseas, while at the same time guarding against overreach by some governments.
- It remains to be seen whether the mechanisms and networks that have been established in response to the rise in cybercrime during the pandemic will be leveraged for the long term to sustain progress on cybercrime cooperation. These could prove to be enormously helpful in addressing the challenges that have long impeded effective cooperation on cybercrime between the public and private sectors and criminal justice actors within and across borders.
- As certain countries are now being accused of violating agreed norms during the pandemic, and with the increased blurring of the boundary between state and non-state cyber activity, the gulf between major cyber powers will likely only continue to grow. This could ultimately hinder progress in trying to build some consensus across the international community on the issue of future cyber norms; and, further, could negatively impact practical cooperation across borders on cybercrime and other cyber-related issues.
- The 'infodemic' that has accompanied COVID-19 has made it clear that despite social media companies' efforts to date, problems persist in tackling cyber influence operations and are unlikely to go away unless the platforms radically change their business model – a move that will hurt their bottom line and thus one that they will have every incentive to avoid.

01 Introduction

Technology has been at the forefront of countries' response to COVID-19, but the accelerated digital transformation since 2020 has highlighted some critical risks to individuals and societies.

Joyce Hakmeh

The COVID-19 pandemic – the worst public health crisis in a generation – has been dubbed the 'great accelerator' of digital transformation.[1] For countries around the world, technology has been at the forefront of their response to the crisis. Governments have employed digital technology to provide a health emergency response to their constituents, and businesses have seen an unprecedented rate of digital adoption across their supply chains. From using artificial intelligence (AI) and data modelling to map the spread of infection, to helping tackle and contain it through contact-tracing apps and data analytics, to enabling the remote delivery of critical services and virtual working environments, digital innovations and solutions have focused attention on the potential of technology as well as on the importance of the digital infrastructure and its resilience. There is an increased recognition that, in a post-COVID world, businesses and governments have to reinvent themselves through the further incorporation of digital technology in their ways of working, and that they must pursue long-term digital transformation in order to compete and operate both nationally and internationally. Otherwise they risk falling behind, unable to find their place in an altered global landscape. At the same time, this sharp take-up of digital technology has exposed the widening digital divide not only between businesses themselves, but also between nations. According to the UN, around half of the world's population is offline.[2] For those people who cannot, for example, access essential healthcare information, the digital divide has become a matter of life and death.[3]

---

1 Armano, D. (2020), 'COVID-19 Will Be Remembered As The 'Great Accelerator' Of Digital Transformation', Forbes, 9 September 2020, https://www.forbes.com/sites/davidarmano/2020/09/09/covid-19-will-be-remembered-as-the-great-accelerator-of-digital-transformation/?sh=4f50677c3cb2.
2 United Nations (2019), 'Nearly Half of World's Population Excluded from 'Benefits of Digitalization', Speaker Stresses as Second Committee Debates Information Technology for Development', Press Release, 18 October 2019, https://www.un.org/press/en/2019/gaef3523.doc.htm.
3 United Nations (2020), 'Digital Divide 'a Matter of Life and Death' amid COVID-19 Crisis, Secretary-General Warns Virtual Meeting, Stressing Universal Connectivity Key for Health, Development', Press Release, 11 June 2020, https://www.un.org/press/en/2020/sgsm20118.doc.htm.

As our lives continue to be transformed by the experience of the COVID-19 pandemic and by the accelerated digital adoption associated with it, it is all the more urgent that questions concerning the impact of this transformation are now addressed. What is the price that we are paying for innovation and digital take-up, and what issues should we be considering? How can governments and businesses accelerate digital transformation while mitigating the risks that could emanate from it?

It has become evident that the pandemic has brought new opportunities for cybercriminals and for perpetrators of disinformation and 'fake news'. In addition, serious concerns have been raised about the role of surveillance in containing outbreaks; the securitization of the healthcare debate; and the critical challenges of devising new technologies such as contact-tracing apps that are effective in notifying users of potential exposure to infection while also protecting individuals' privacy. Hence, the pandemic has also given rise to a crisis of technology and cybersecurity, and is fuelling what Freedom House has termed a 'crisis for democracy'.[4]

This paper looks at some of the trends that have emerged from this process of rapid and unplanned-for digital adoption. In Chapter 2, Emily Taylor focuses on the relationship between governments and big tech, using the UK's track-and-trace app as a case study. It explores the power imbalances between elected governments and private sector corporations, and the implication of those dynamics in developing and deploying technological solutions – in this case, for public health purposes – that respect individual rights, are robust from a cybersecurity perspective and can achieve epidemiological goals.

In Chapter 3, Allison Peters examines the impact that COVID-19 has had on the cybercrime landscape, exploring the potential for cooperation against cybercrime at national and international levels, and considering whether the awareness that the pandemic has arguably created as to the magnitude of the problem of cybercrime will act as a wake-up call, leading to sustainable policy changes for the long term.

In Chapter 4, Sophia Ignatidou discusses what has been dubbed an 'infodemic' in the context of the COVID-19 crisis, exploring how disinformation has been 'weaponized' and how high-profile political figures, including in liberal democracies, have used the pandemic to manipulate and control the information space. She emphasizes the importance of a 'whole-of-society' approach to curbing this problem, and suggests a number of measures that can be initiated by different stakeholders in order to help address what is an escalating situation.

Each of these three chapters sets its area of focus in the context of developments prior to the pandemic, explores the specific impact of the COVID-19 crisis, and identifies some potential future implications. Looking at these different areas

4 Repucci, S. and Slipowitz, A. (2020), 'Democracy under Lockdown: The Impact of COVID-19 on the Global Struggle for Freedom', October 2020, https://freedomhouse.org/report/special-report/2020/democracy-under-lockdown.

in conjunction, Chapter 5 concludes by stressing the need to restore and build greater public trust in critical measures and policy approaches, and to increase cooperation nationally and internationally.

The paper has been produced as part of a wider Chatham House project, 'Trends in technology: what does the future hold?'. The project aims to help bridge the current 'siloed' approaches in tech policymaking by highlighting common threads and patterns across a number of policy areas, and identifying the best ways to address those in a way that allows digital technology and cyberspace to continue to serve as an engine for social and economic growth for all countries and people around the world.

02
The COVID-19 app: how big tech outwitted the UK government

The development of any health app raises important considerations of human rights, technical and practical challenges, and cybersecurity issues, and – as has been evident during the pandemic – underscores the tensions between governments and tech giants.

Emily Taylor

This chapter incorporates a case study of the UK's COVID-19 track-and-trace app, and what its history reveals about the power dynamics between big tech and elected governments. The app's story reflects trends in both the tech market and in public health in the UK, including the consolidation of mobile operating system and app store markets, the centralization of the UK's public health provision and the impact of successive budget cuts in the decade since 2010, as well as the pitfalls of what has been termed 'tech-solutionism'[5] in the face of complex public health and policy problems.

5 Ada Lovelace Institute (2020), *Exit through the App Store?*, Rapid Evidence Review, 20 April 2020, https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf.

Whatever the merits of the competing design architectures of the first version of the UK's contact-tracing app and the Google–Apple model that was to replace it, the failure of the UK's first app was due to the imposition of a policy decision on a democratically elected government by two unelected, unaccountable tech companies, raising important questions about the legitimacy of the resulting policy. In essence, Apple and Google withheld access to essential technologies until the UK agreed to align its data storage model with that advocated by the tech companies.

This paper also considers the resources dedicated to the app in the context of the UK's wider public health response. Was investment of £11.8m[6] in the first app's development worthwhile, or was policy 'led by technology, rather than the other way around'?[7]

Big tech and public health before COVID-19

Normalization of surveillance, market concentration and political influence

'Google knows more about you and me than the KGB, Stasi or Gestapo ever dreamed of.'[8] So said the German business daily *Handelsblatt* about Google Street View in 2010, three years before Edward Snowden revealed the extent of big tech's data-processing activities. In the private sphere, the free-to-use platforms Google, Facebook, Twitter and, more recently, TikTok have normalized exploitative levels of data collection permitted in their terms of service,[9] termed 'surveillance capitalism' by Shoshana Zuboff[10] and 'extractive industries' by John Naughton.[11]

After a short period of extreme openness and innovation, the online marketplace is now in the hands of a few 'privately controlled industrial behemoths'.[12, 13] Consolidation is evident, both at the application level and within the deeper layers of the internet's architecture,[14] where the same familiar names – Google, Amazon, Facebook, Apple, Microsoft – provide critical infrastructure on which all other services depend.

---

6 Brewis, H. (2020), 'Failed test-and-trace app cost more than £11 million, Government figures show', *Evening Standard*, 19 June 2020, https://www.standard.co.uk/news/uk/test-and-trace-app-cost-uk-government-11million-a4474386.html.
7 Ada Lovelace Institute (2020), *Exit through the App Store?*.
8 Dowling, S. (2010), 'Google Knows More about Us than the KGB, Stasi or Gestapo', *SPIEGEL International*, 19 August 2010, https://www.spiegel.de/international/germany/the-world-from-berlin-google-knows-more-about-us-than-the-kgb-stasi-or-gestapo-a-712680.html.
9 Taylor, E. (2016), 'The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality', Global Commission on Internet Governance, Paper Series: No. 24, January 2016.
10 Zuboff, S. (2015), 'Big other: surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology*, 30(1): pp. 75–89, https://journals.sagepub.com/doi/10.1057/jit.2015.5.
11 Naughton, J. (2016), 'The profits and perils of drilling for crude data', *Guardian*, 1 May 2016, https://www.theguardian.com/commentisfree/2016/may/01/profits-perils-drilling-data-oil-surveillance-online-information.
12 Wu, T. (2010), *The Master Switch: The Rise and Fall of Information Empires*, London: Atlantic Books, Kindle Edition, p. 6.
13 U.S. House of Representatives Judiciary Committee (2020), *Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations*, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, U.S. House of Representatives, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.
14 See Taylor, E. and Hakmeh, J. (eds) (2020), *Journal of Cyber Policy*, 5(1), Special Issue: Consolidation of the Internet, https://www.tandfonline.com/toc/rcyb20/5/1?nav=tocList.

The mobile telephony environment is even more tightly consolidated, with two operating systems accounting for 99.75 per cent of the global market: Google's Android and Apple's iOS,[15] each with their own app store.[16] Apple's App Store is the only means for an app developer to distribute software on iOS devices; and while Google does permit other app stores on Android, Google Play is dominant.[17] Apple's conduct in relation to the App Store has raised antitrust concerns on both sides of the Atlantic,[18] including the denial of third parties' access to key technology in order to gain competitive advantage.[19]

Commercial success has brought political influence to match.[20] In a sector initially shielded from regulation,[21] later attempts by regulators to rein in the market power of big tech have had limited success,[22] and may have had the perverse consequence of entrenching existing market power.[23]

The competitive advantage to be gained from the algorithmic manipulation of big data has engendered a culture of secrecy. A lack of transparency on the part of tech companies makes their processing techniques difficult to assess, critique or regulate.

The EU's flagship privacy regulation, the General Data Protection Regulation 2016/679 (GDPR), was 'one of the most lobbied pieces of European legislation in European Union history'.[24] While the GDPR has required enterprises to make substantial adjustments in the way they handle personal data, it has barely impacted the core business model of targeted advertising, enabled by the storage and processing of enormous data troves.

---

15 Statcounter GlobalStats (1999–2020), 'Mobile Operating System Market Share United Kingdom', https://gs.statcounter.com/os-market-share/mobile/united-kingdom (accessed 8 Oct. 2020); The Netherlands Authority for Consumers & Markets (2019), *Market study into mobile app stores*, 11 April 2019, https://www.acm.nl/sites/default/files/documents/market-study-into-mobile-app-stores.pdf.
16 For an introduction to the world of apps and app stores, see U.S. House of Representatives Judiciary Committee (2020), *Investigation of Competition in Digital Markets*, Section IV, D, pp. 93 ff.
17 The Netherlands Authority for Consumers & Markets (2019), *Market study into mobile app stores*, p. 50; U.S. House of Representatives Judiciary Committee (2020), *Investigation of Competition in Digital Markets*, p. 95.
18 See U.S. House of Representatives Judiciary Committee (2020), *Investigation of Competition in Digital Markets*, pp. 340 ff., and European Commission (2020), *Competition policy for the digital era*, p. 34, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.
19 The European Commission opened an investigation in June 2020 in relation to 'Apple's limitation of access to the Near Field Communication (NFC) functionality ("tap and go") on iPhones for payments in stores […]'. See European Commission (2020), 'Antitrust: Commission opens investigation into Apple practices regarding Apple Pay', Press Release, 16 June 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1075.
20 Public Citizen (2014), *Mission Creep-y: Google Is Quietly Becoming One of the Nation's Most Powerful Political Forces While Expanding Its Information-Collection Empire*, Washington, DC: Public Citizen's Congress Watch, https://www.citizen.org/wp-content/uploads/google-political-spending-mission-creepy.pdf.
21 Tech platforms benefit from statutory protection against liability for content as 'intermediaries' (47 U.S.C. s230 Communications Decency Act 1996, https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)) and as 'mere conduit' (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031)).
22 Jones, K. (2020), 'Regulating Big Tech: Lessons from COVID-19', Chatham House Expert Comment, 10 June 2020, https://www.chathamhouse.org/2020/06/regulating-big-tech-lessons-covid-19.
23 See for example Batikas, M. et al. (2020), 'European Privacy Law and Global Markets for Data', Centre for Economic Policy Research Discussion Paper No. DP14475, 6 March 2020.
24 Long, W. (2014), 'Significant Impact of New EU Data Protection Regulation on Financial Services', *Global Banking & Finance Review*, 18 April 2014, pp. 1–3.

The competitive advantage to be gained from the algorithmic manipulation of big data has engendered a culture of secrecy. A lack of transparency on the part of tech companies makes their processing techniques difficult to assess, critique or regulate, whether by governments, academics, civil society or even by other parts of the tech industry. As a result, 'dominant platforms exploit their gatekeeper power to dictate terms and extract concessions that no one would reasonably consent to in a competitive market'.[25] A policy vacuum has been created by Western governments 'declining to regulate or ducking contemporary challenges'.[26]

Whatever else the past two decades have brought us, they have not delivered a blueprint for sound technological governance.

UK public health 2010–20: centralization, defunding, and marginalization of local expertise

Track and trace – done by humans – is a basic task of public health authorities, having long been deployed to mitigate outbreaks of infectious diseases.[27] Contact tracing is a skilled job and requires local knowledge. Through interviews, a public health official can help people piece together their movements over a relevant period, jogging their memory while looking out for anomalies or 'red flags' (such as '… and then I went to visit my mother, who's in a care home').[28] The contacts thus identified are then followed up by the team.

A local public health team 'has deep knowledge of the characteristics of [their] patch that make its health inequalities so stark and its residents so vulnerable'.[29]

A decade of austerity in the UK, from 2010, led to substantial cuts in public health provision. To take the example of England, the elimination of its regional health authorities[30] left most local public health teams having to coordinate with local authorities (numbering in the hundreds) in the absence of the much larger regional bodies (numbering eight to 10) that had previously coordinated between central and local government on policy and service provision. A 'huge disconnect' thus developed between public health and different branches of government. Functions such as environmental health, community and neighbourhood teams, and youth services workers were lost, 'the kind of staff […] used during 2009 swine flu to work closely with the NHS'.[31] In the place of local public health teams emerged a centralized provision, often outsourced to private companies.[32]

---

25 U.S. House of Representatives Judiciary Committee (2020), *Investigation of Competition in Digital Markets*, p. 11.
26 Jones (2020), 'Regulating Big Tech'.
27 Mears, J. et al. (2014), 'Prospective evaluation of a complex public health intervention: lessons from an initial and follow-up cross-sectional survey of the tuberculosis strain typing service in England', *BMC Public Health*, 14(1023), doi:10.1186/1471-2458-14-1023; Lawrence, F., Garside, J., Pegg, D., Conn, D., Carrell, S. and Davies, H. (2020), 'How a decade of privatisation and cuts exposed England to coronavirus', *Guardian*, 31 May 2020, https://www.theguardian.com/world/2020/may/31/how-a-decade-of-privatisation-and-cuts-exposed-england-to-coronavirus.
28 Author interview with Dr Nick Cavell, 3 September 2020.
29 Lawrence et al. (2020), 'How a decade of privatisation and cuts exposed England to coronavirus'.
30 Scally, G. (2020), 'England's ravaged public health system just can't cope with the coronavirus', *Guardian*, 30 March 2020, https://www.theguardian.com/commentisfree/2020/mar/30/england-public-health-coronavirus-cuts-regional.
31 Lawrence et al. (2020), 'How a decade of privatisation and cuts exposed England to coronavirus'.
32 Ibid.

COVID-19 trends

The outbreak of a new coronavirus, SARS-Cov-2 or the COVID-19 virus, thought to have originated in Wuhan, China, rapidly developed into a global pandemic during the first half of 2020. As the disease spread remorselessly throughout the world, several national governments announced that a track-and-trace app would form part of their public health response to the pandemic: these included Singapore,[33] South Korea,[34] Germany, Switzerland and Ireland.[35] In brief, such apps work by tracking an individual's movements, using Bluetooth Low Energy technology to detect and identify the phones of other app users, while collecting data about interactions with others (how close, and for how long). If an app user develops symptoms of COVID-19, the app notifies all those who have come into contact with that user during a predefined period. Individuals are then able to self-isolate or take other measures to safeguard their health.

The development of any health app raises considerations of human rights, technical and practical challenges, and cybersecurity issues.

Human rights: the three key threats

Data relating to an individual's health is protected by Article 8 of the European Convention on Human Rights, and is a special category of personal data under the GDPR,[36] attracting higher levels of protection than other data. The serious cross-border threat to public health of an ongoing pandemic is a justifiable ground for some limitations on individuals' right to privacy, but such limitations may not remain justifiable once the current pandemic has been brought under control.

The law encourages the anonymization of data, and, appropriately handled, this can be a way of reducing the risks associated with data processing. Yet numerous studies have shown the ease with which data can be deanonymized.[37,38]

Human rights experts advise that a COVID app would raise three key risks of interference with Article 8:

— **Centralized data collection.** Should the data generated by the app's use be stored centrally, in a single database, or should it be decentralized, with the majority of data processing and storage occurring at the level of the user's handset? A centralized data collection system would require substantial safeguards to avoid potential abuse by the data controller (whether government or private sector). Technical and human rights experts favoured a decentralized

---

33 Vaswani, K. (2020), 'Coronavirus: The detectives racing to contain the virus in Singapore', BBC News, 19 March 2020, https://www.bbc.co.uk/news/world-asia-51866102.
34 Smith, J., Shin, H. and Cha, S. (2020), 'Ahead of the curve: South Korea's evolving strategy to prevent a coronavirus resurgence', Reuters, 15 April 2020, https://uk.reuters.com/article/uk-health-coronavirus-south korea-respons/ahead-of-the-curve-south-koreas-evolving-strategy-to-prevent-a-coronavirus-resurgence-idUK KCN21X0N2.
35 Jee, C. (2020), 'Is a successful contact tracing app possible? These countries think so.', *MIT Technology Review*, 10 August 2020, https://www.technologyreview.com/2020/08/10/1006174/covid-contract-tracing-app-germany-ireland-success/amp.
36 Article 9. Note that 9(2)(i) exempts the processing of health data 'necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health'.
37 Schneier, B. (2015), *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York: W. W. Norton & Co.
38 Sweeney, L. (2000), *Simple Demographics Often Identify People Uniquely*, Pittsburgh: Carnegie Mellon University, https://dataprivacylab.org/projects/identifiability/paper1.pdf.

model for apps: one in which the data is stored on the user's device.[39] This avoids the privacy risks of a centralized system, while delivering essential health information to individuals.

— **Mandatory app use.** Matrix Chambers considered a combination of a mandatory and centralized design to comprise a 'wholly unprecedented level of granular data about the social network of the majority of the population'.[40] Some employers are already reported to be insisting that staff use the app,[41] a predictable development that would impact on a state's human rights obligations to individuals.

— **Immunity passports.** If the app were used to generate immunity passports 'on the basis of […] location or immigration status, it might give rise to stigmatisation and indirect discrimination'.[42] Discrimination on the basis of age or race could occur where mass statistical data fails to take adequate account of personal characteristics.

The public health advantages of centralized data storage

The primary function of a COVID app is to inform individuals about their potential exposure to the virus. Either a centralized or decentralized model would achieve this objective. In addition to the primary function, the app could potentially serve as a public health intervention to suppress the pandemic, offering health officials a view of the entire country's level of infection, identifying virus 'hotspots' and enabling the swift mobilization of resources. According to one epidemiologist: 'One of the advantages is that it's easier to audit the system and adapt it more quickly as scientific evidence accumulates.'[43] To perform this function, the app would require centralized storage of data[44] and would need to be downloaded by a substantial proportion of the population. In interviews conducted as part of the research for this paper, public health experts described a centralized model as prioritizing the collective good (control of the pandemic) over an individualistic/libertarian approach[45] – a tension that is also apparent in other contexts such as the wearing of masks in public places.

Technical and practical challenges – getting the app to work

Any successful app would need to provide 'proximity event logging', detecting other devices running the app via Bluetooth at frequent enough intervals to measure the duration of encounters between people and at a near-enough range

---

39 See for example Troncoso, C. et al. (2020), 'Decentralized Privacy-Preserving Proximity Tracing', GitHub, version 25 May 2020, https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf; see also Open Rights Group (n.d.), 'NHSX scraps centralised model for COVID-19 app', https://www.openrightsgroup.org/campaign/protecting-digital-rights-during-covid-19.
40 Ryder, M. et al. (2020), *COVID-19 & Tech responses: Legal opinion*, Matrix Chambers, 30 April 2020, para. 67, https://www.matrixlaw.co.uk/wp-content/uploads/2020/05/Covid-19-tech-responses-opinion-30-April-2020.pdf.
41 Leswing, K. (2020), 'Companies could require employees to install coronavirus-tracing apps like this one from PwC before coming back to work', CNBC, 6 May 2020, https://www.cnbc.com/2020/05/06/pwc-is-building-coronavirus-contact-tracing-software-for-companies.html.
42 Ryder et al. (2020), *COVID-19 & Tech responses: Legal opinion*, para. 85.
43 Professor Christophe Fraser, epidemiologist advising NHSX, quoted in Kellion, L. (2020), 'NHS rejects Apple-Google coronavirus app plan', BBC News, 27 April 2020, https://www.bbc.co.uk/news/technology-52441428.
44 See Levy, I. (2020), 'The security behind the NHS contact tracing app', National Cyber Security Centre Events and initiatives blog, 4 May 2020, https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app.
45 Author interview with William Buckland, 1 September 2020.

to capture encounters at risk of transmitting the virus, without draining a device's battery. The app must work while a device is locked.[46]

Working with Bluetooth creates technical challenges, particularly in detecting proximity within the 2–4 metre range.[47] Bluetooth has a history of security breaches that have been comprehensively reported and studied.[48] Security-conscious smartphone users are often advised to turn off Bluetooth when it is not needed.

To work, COVID-19 apps need users to keep Bluetooth running – particularly when they are in public places – which holds the potential to expose users to attack or surveillance.

To work, COVID-19 apps need users to keep Bluetooth running – particularly when they are in public places – which holds the potential to expose users to attack or surveillance. Cooperation with the two biggest mobile operating system platforms, Google's Android and Apple's iOS, was essential so that the app would be authorized for inclusion in their respective app stores.

Cybersecurity challenges

A centralized contact-tracing system would require high levels of competence and planning to mitigate the risk of unauthorized access, particularly if the data were to be stored centrally.[49] Cybersecurity risk mitigation should also seek to reduce the impact of eavesdropping or fake exposure events.[50] A bad actor could target specific populations, using a powerful antenna (for example, outside a police station or healthcare facility), and submitting (via the bad actor's app) a false report of infection.[51] This could result in the needless quarantining of key workers.

Case study: Google–Apple and the UK app

The 'Google–Apple' model

In April 2020, after several national governments had already deployed their own track-and-trace apps, Apple and Google entered the market.[52] The two

---

46 Levy (2020), 'The security behind the NHS contact tracing app'.
47 Biddle, S. (2020), 'The inventors of Bluetooth say there could be problems using their tech for coronavirus contact tracing', The Intercept, 5 May 2020, https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing.
48 See for example Greenberg, A. (2020), 'Does COVID-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered', *Wired*, 17 April 2020, https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses.
49 For example, an attack by hackers on the US Office of Personnel Management in 2015, alleged to have been perpetrated by China, resulted in a data breach compromising 22.1 million records. See Adams, M. (2016), 'Why the OPM Hack Is Far Worse Than You Imagine', Lawfare blog, 11 March 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.
50 Privacy and security risk evaluation of digital proximity tracing systems, The DP-3T project, 21 April 2020.
51 See Levy, I. (2020), *High level privacy and security design for NHS COVID-19 Contact Tracing App*, London: National Cyber Security Centre, Version 0.1, 3 May 2020, p. 10, https://www.ncsc.gov.uk/files/NHS-app-security-paper%20V0.1.pdf.
52 Apple Newsroom (2020), 'Apple and Google partner on COVID-19 contact tracing technology', 10 April 2020, https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology.

companies announced that they were developing a functionality, to be built into their mobile operating systems, that would allow governments to build apps. Based on a decentralized model, central servers would not contain information regarding who may have been infected with coronavirus from whom.

Neither Apple or Google was prepared to permit apps to run Bluetooth contact-monitoring technology in the background of their operating systems in a way that could allow governments to collect an anonymized overview of contacts that were taking place. The companies stated that this would set an undesirable precedent, allowing governments to track their populations for potentially malicious purposes. 'If [public health authorities] create an app, it must meet specific criteria around privacy, security and data control.'[53] These criteria were set by Apple and Google.

The UK's COVID-19 app, version 1.0

Since early March 2020, the UK government had been developing its own app. The UK initially opted to use a centralized data storage model for epidemiological reasons, while incorporating numerous privacy and cybersecurity protections.[54] The first version of the app was developed by the National Health Service's specialist unit for technology, digital and data (NHSX), in close consultation with cybersecurity experts at the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO).

Shortly after the UK app launched, it was reported that it was failing to discover iPhones where devices were locked.[55] The UK government undermined its own arguments about safeguards protecting the identity of individuals in a centralized system after advice to ministers was leaked suggesting that they could be given the ability to deanonymize the data gathered by the app.[56]

Despite extensive negotiations with a number of governments, Apple was not willing to shift its position on allowing Bluetooth to operate in the background for apps not using their decentralized infrastructure. In response, several countries that had originally pursued a centralized model – among them Germany, Italy, Denmark and Singapore – made the decision to switch to the Google–Apple model.

The political influence of the tech companies became apparent as they teamed up with privacy campaigners and often 'play[ed] hardball with politicians'.[57] Those familiar with the development of the UK app describe how the US tech giants worked

---

53 Apple and Google (2020), *Exposure Notifications: Frequently Asked Questions*, September 2020, v1.2, Question 6, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf (accessed 11 Oct. 2020).
54 National Cyber Security Centre blogs and papers around launch: Levy (2020), 'The security behind the NHS contact tracing app'; technical paper, Levy (2020), *High level privacy and security design for NHS COVID-19 Contact Tracing App*; Gould, M. and Lewis, G. (2020), 'Digital contact tracing: protecting the NHS and saving lives', GOV.UK Department of Health and Social Care, Technology in the NHS blog, 24 April 2020, https://healthtech.blog.gov.uk/2020/04/24/digital-contact-tracing-protecting-the-nhs-and-saving-lives.
55 Redpath, L. (2020), 'Discovery fails when both devices are locked #2', Github, NHSX/Covid-19-app-iOS-BETA, 7 May 2020, https://github.com/nhsx/COVID-19-app-iOS-BETA/issues/2.
56 Pegg, D. and Lewis, P. (2020), 'NHS coronavirus app: memo discussed giving ministers power to 'de-anonymise' users', *Guardian*, 13 April 2020, https://www.theguardian.com/world/2020/apr/13/nhs-coronavirus-app-memo-discussed-giving-ministers-power-to-de-anonymise-users?utm_term=RWRpdG9yaWFsX0d1YXJkaWFuVG9kYXlVS19XZWVrZGF5cy0yMDA0MTQ%3D&utm_source=esp&utm_medium=Email&CMP=GTUK_email&utm_campaign=GuardianTodayUK.
57 Scott, M. et al. (2020), 'How Google and Apple outflanked governments in the race to build coronavirus apps', Politico, 15 May 2020, https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany.

behind the scenes to persuade elected decision-makers across several countries to reject 'home-grown' apps in favour of the Google–Apple model – in some cases, just prior to the planned launch.

Having tried and failed to craft its own app, the UK announced that it was shifting to the Google–Apple decentralized model, combined with a QR code-based check-in to pubs and other public venues. Version 2.0 of the UK app was launched on 24 September 2020.[58] By the end of October it had been downloaded 19 million times.[59] Shortly after the launch, there were reports of ghost 'possible exposure' messages, which security researchers attribute to competing risk algorithms being run both in the Google–Apple back end and the UK's front end, developed by NHSX.[60]

What can we learn from the UK app story?

Tech platforms impose policy on governments

The story of the UK's track-and-trace app demonstrates the influence exerted by Google and Apple over elected policymakers. In June 2020 Health Secretary Matt Hancock accused Apple of being 'intransigent' and of not doing enough to work with 'democratically elected governments', adding that '… Apple wouldn't make the change to allow [the UK app] to work on Apple'.[61]

However it was accomplished, the outcome was that two companies withheld access to essential technologies on the basis of their own preferred policy solution: decentralized data storage. While this may have been the option that human rights activists and technologists would have championed, it does not achieve the epidemiological benefits of the initial NHSX app design. It raises questions over the legitimacy of the policy outcome, as tech companies imposed an individualistic ideology on the technical solution over one that prioritized collective public health.

The episode highlights the power imbalances between elected governments and private sector corporations. There are significant differences in levels of accountability and transparency between the public and private sectors. It underlines the realpolitik of corporate power over that of democratically elected governments, and the willingness to block access to essential technologies and deploy soft power in the form of lobbying. It is ironic that Google, itself a voracious collector of centralized data even where this is unnecessary to perform the relevant contract or service,[62] could participate in barring democratic governments from adopting centralized architecture for a health app during a pandemic, on the grounds of privacy – a case of 'do as I say, not as I do'.

---

58 O'Halloran, J. (2020), 'NHS COVID-19 contact-tracing app to launch in England and Wales on 24 September', Computer Weekly, 11 September 2020, https://www.computerweekly.com/news/252488930/NHS-Covid-19-contact-tracing-app-to-launch-in-England-and-Wales-on-24-September.
59 Cook, J. (2020), 'NHS COVID-19 app: how does track and trace work, and what does the 'possible exposure' message mean?', *Telegraph*, 30 October 2020, https://www.telegraph.co.uk/technology/0/nhs-covid-19-app-track-trace-how-work-download-now-phone.
60 Author interview with Luke Redpath, 5 October 2020.
61 Merrick, J. (2020), 'Matt Hancock accuses Apple of 'intransigence' in working with governments after u-turn over tracking app', inews, 21 June 2020, https://inews.co.uk/news/politics/matt-hancock-apple-intransigence-working-governments-u-turn-tracking-app-452028.
62 See analysis of platforms' terms of service in Taylor (2016), 'The Privatization of Human Rights'.

The lack of international technical standards for COVID-19 apps

Healthcare interventions typically need to conform to the highest standards of safety and efficacy, and are covered by international human rights laws.[63] COVID-19 smartphone apps constitute a healthcare intervention, and yet, despite the pandemic's global reach, countries are developing apps independently, and there are no internationally agreed technical standards that are both privacy-respecting and secure by design, which could guide the development of track-and-trace apps in the UK and elsewhere. Such standards could potentially offer interoperability if individuals travel overseas, and at the same time protect against overreach by governments, some of which are reported to be using a COVID-19 app to record data including names, addresses, sex, gender, age, location, disease symptoms and test results.

Was the UK app really a threat to privacy and security?

By the time the UK announced its planned transition to the Google–Apple model, the development of the original app had cost approximately £11.8m.[64]

The UK's decision to pursue a centralized model for its app was criticized on human rights grounds. However, the public health professionals interviewed for this paper were unanimous in their opinion that centralized data is essential for epidemiological purposes. While the UK government admitted that it failed to fulfil its GDPR requirements – by deploying the app without a Data Protection Impact assessment[65] – its other choices in creating the app showed a high level of respect for individual privacy and security by design, contrasting with the 'surveillance capitalism' of big tech.

In theory, the Google–Apple app should not collect location data.[66] In practice, concerns have been raised about Google's collection of data associated with app use through the software that powers its app distribution service Google Play. Despite location data not being collected in Ireland's track-and-trace app, for example, it appears that Android users suffer a degradation in service if they do not enable data sharing at a low level in the platform.[67]

Additionally, there are concerns over the issues that may arise in the longer term if Google and Apple monetize these services in the future. This infrastructure could, in theory, allow the development of large-scale, multinational contact maps that could enable the capture of significant amounts of network information. It is unclear how domestic or international regulation could prevent this. Moreover, third parties – for example health insurers – might in the future produce their

---

63 UN General Assembly (1966), International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, 999: Article 17, available at: https://www.refworld.org/docid/3ae6b3aa0.html.
64 UK Parliament Hansard (2020), 'COVID-19: Test and Trace App', Privacy Notice Question, House of Lords, Volume 804, 22 June 2020, https://hansard.parliament.uk/Lords/2020-06-22/debates/69F28101-5695-4379-B23A-5E2CE7278BFF/Covid-19TestAndTraceApp.
65 Open Rights Group (2020), 'Government Admits Test and Trace Unlawful', Press Release, 20 July 2020, https://www.openrightsgroup.org/press-releases/government-admits-test-and-trace-unlawful.
66 Google (2020), 'Privacy-safe contact tracing using Bluetooth Low Energy', blog post, https://www.blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf.
67 O'Brien, C. (2020), 'COVID Tracker app throws spotlight on Google data harvesting', *Irish Times*, 30 July 2020, https://www.irishtimes.com/business/technology/covid-tracker-app-throws-spotlight-on-google-data-harvesting-1.4315739.

own apps that use the Google–Apple back end (through the published API[68]), but that collect additional data with user consent. Although under the decentralized model proposed by Google and Apple identifiable data are not uploaded to a central server, there do appear to be methods for harvesting data that the Irish app, for example, has used to report on its effectiveness.[69] The Irish app invites users to give consent for the collection of some data.

Was the app the correct public health response?

In June 2020 Australia's deputy chief medical officer Nick Coatsworth criticized the Google–Apple app model thus: 'It fundamentally changes the locus of control and takes out the middle person and the middle person is the contact tracer, the people who have kept us safe.'[70] Dr Coatsworth's remarks emphasize the critical role of the human contact tracer.

A feature of the UK coronavirus response to date is how little it has leveraged the expertise and resources of its local public health teams.

A feature of the UK coronavirus response to date is how little it has leveraged the expertise and resources of its local public health teams. Even when the UK switched to a human-first track-and-trace response in June 2020, it bypassed local public health teams, preferring to recruit centrally through private sector-led initiatives contracted out to private service providers Sitel and Serco. There have been repeated criticisms that the UK's human track-and-trace efforts failed to make efficient use of the available skills and resources.[71] One of the early recruits to be a Tier 2 contact tracer, Dr Nick Cavill (who holds a PhD in public health), was interviewed as part of the research for this paper. Dr Cavill completed his training in April 2020, but by the time of our interview, in September, had not received a single assignment. It is unknown whether Dr Cavill's experience of the track-and-trace effort during this period reflected a lack of testing, lack of budget or other factors.

Apps are better than humans at 'remembering', but humans are better at understanding the significance of details, such as whether two people in contact were wearing masks, were behind protective screens, or were separated by the thin walls of adjoining flats and never in contact at all.

As a whole, the UK's pandemic response has been criticized for being too centralized. The erosion of the public health function over the past decade, coupled with the poor use of the skilled resources that remain in place at the local level, has created a gap that even the best app could only partly fill.

---

68 Application programming interface.
69 Cellan-Jones, R. and Kelion, L. (2020), 'Coronavirus: The great contact-tracing apps mystery', BBC News, 21 July 2020, https://www.bbc.co.uk/news/technology-53485569.
70 Grubb, B. (2020), "There's no way we're shifting': Australia rules out Apple-Google coronavirus tracing method', *Sydney Morning Herald*, 29 June 2020, https://www.smh.com.au/technology/there-s-no-way-we-re-shifting-australia-rules-out-apple-google-coronavirus-tracing-method-20200629-p5573s.html.
71 See for example McKee, M. (2020), '"NHS" Test and Trace under fire–a system flawed by design', BMJ Opinion, 11 December 2020, https://blogs.bmj.com/bmj/2020/12/11/martin-mckee-nhs-test-and-trace-under-fire-a-system-flawed-by-design.

Conclusion: who should make the policy decisions – tech or government?

The COVID-19 app in the UK has become emblematic of a troubling power imbalance between technology firms and elected governments. Google and Apple withheld access to essential technologies and their app stores, and deployed their lobbying power to impose an ideology that championed individual rights over collective public health. Both outcomes have merit, and it is clear that a successful solution should simultaneously be both respectful of individual rights and robust from a cybersecurity perspective, while also effectively serving essential epidemiological goals.

The episode also highlights double standards in the accountability of government versus that of the private sector. Privacy advocates rightly called for accountability and transparency from the UK government over its plans to develop a COVID-19 track-and-trace app, and they were given it – with publication of the source code and of extensive detail on how the GDPR's data minimization principle would be respected, information security risks would be mitigated and data protection authorities involved in the design. When the UK failed in its obligation to conduct a Data Protection Impact assessment, it was rightly held to account.

In the case of Google at least, the big tech track record on data privacy is poor. Google's terms of service expose an exploitative level of data processing, and the impact on individuals' privacy is amplified when combined with the platform's many popular services – resulting in a firehose of data from search queries, mapping, DNS[72] queries, Gmail and video consumption on YouTube, not to mention the incidental collection of location, device details and IP addresses.

The story of the UK app can also be seen as an example of 'tech-solutionism', rather than a response to a well-evidenced need. The insistence on a decentralized solution placed the app primarily in the hands of individuals, rather than in those of local public health teams for whom it could have served as an additional resource.

The app story has highlighted the impact of concentration in the mobile operating platforms; the pivotal role of the app stores in enabling access to markets; the lobbying power of big tech companies, which themselves lack accountability, and their ability to withhold access to essential technologies until their preferred policy solution was adopted. Simply put, governments had no choice but to comply.

72 Domain name system.

03
Is COVID-19 changing the cybercrime landscape?

COVID-19-related cybercrime, including malicious activity targeting medical facilities and research centres, may have lasting implications for global cooperation to tackle cybercrime, and for internet governance more broadly.

Allison Peters

On 10 September 2020, in Germany, more than 30 internal servers of the University Hospital of Düsseldorf were hit by a cyberattack, which crippled the hospital's systems and caused emergency patients to be turned away.[73] In the midst of the global crisis arising from the COVID-19 pandemic, the hospital was forced to route patients to other facilities for care. German authorities subsequently launched an investigation to determine whether the death of a re-routed patient had resulted from delays to her treatment because of the cyberattack;[74] if this was found to be the case, the death of the patient would be the first known fatality directly caused by a ransomware attack. This attack was not an isolated incident. During the pandemic, malicious cyber actors are also known to have targeted

73 Eddy, M. and Perlroth, N. (2020), 'Cyber Attack Suspected in German Woman's Death', *New York Times*, 18 September 2020, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.
74 Cimpanu, C. (2020), 'First death reported following a ransomware attack on a German hospital', ZD Net, 17 September 2020, https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital.

the Paris hospital system; medical clinics and healthcare agencies in the US; the World Health Organization (WHO); COVID-19 treatment and vaccine research institutions; and other healthcare entities.[75]

Such incidents are reminders of the constant threat that cybercrime and other malicious cyber activity presents to countries' national, economic and human security. And these threats are nothing new. Cybercrime was already accelerating rapidly and evolving in most parts of the world before the COVID-19 pandemic, and the virus has only served to provide perpetrators with new opportunities and vulnerabilities to exploit for a variety of motivations. The stakes are perhaps higher now, in terms of how such crimes will impact national governments as they struggle to blunt the spread of both a deadly infectious disease and its resulting economic effects. Thus, cybercrime has been thrust into the spotlight as a threat to which more attention needs to be paid, across all sectors in all societies. In the long term, there are a number of questions about how the rise of cybercrime linked to the pandemic will impact developments that were already under way before the onset of the pandemic. In particular, COVID-19-related cybercrime, and the global attention being paid to it, may have lasting implications for global cybercrime cooperation and for internet governance more broadly.

Cybercrime in the pre-COVID period

Cybercrime was a persistent and often transnational threat before the COVID-19 pandemic hit. The ubiquity of technology and the growing rates of internet connectivity, coupled with the continued development of new technologies that allow for anonymity, have made cybercrime a low-risk, high-reward venture for a wide spectrum of state and non-state actors.[76] Legacy technology used by critical infrastructure and a lack of adequate investments in cybersecurity in certain parts of the world have also exacerbated the problem.[77] The professional services firm Accenture found that the average cost of cybercrime for companies (across 11 different countries and 16 different industry sectors) increased by some 12 per cent in 2018, to a new high of $13 million, from $11.7 million in 2017.[78] The same study also estimated that the total economic value at risk from cybercrime around the globe may be as high as $5.2 trillion in the five-year period 2019–23.[79] It found that the techniques used by non-state and nation-state actors to commit cybercrimes were evolving, with perpetrators increasingly using 'people-based

---

75 Burt, T. (2020), 'Protecting healthcare and human rights organizations from cyberattacks', Microsoft On the Issues blog, 14 April 2020, https://blogs.microsoft.com/on-the-issues/2020/04/14/accountguard-cyber attacks-healthcare-covid-19; https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus.
76 Peters, A. and Jordan, A. (2020), 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime', *Journal of National Security Law & Policy*, 10(3), pp. 490–2, https://jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf.
77 Booth, A. et al. (2019), 'Critical infrastructure companies and the global cybersecurity threat', McKinsey & Company, 11 April 2019, https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat; European Court of Auditors (2019), *Challenges to effective EU cybersecurity policy*, Briefing Paper, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.
78 Accenture Security and Ponemon Institute LLC (2019), *The Cost of Cybercrime. Ninth Annual Cost of Cybercrime Study: Unlocking the value of improved cybersecurity protection*, p. 11, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50.
79 Ibid, p. 14.

attacks' such as phishing or other forms of social engineering attacks.[80] The boundary between state actors and non-state cybercriminals was also increasingly blurring, as states abetted and in some instances directly employed non-state cybercriminals and/or their tools to advance their objectives.[81]

Law enforcement has struggled to keep up with this dynamic threat, resulting in a significant global cyber enforcement gap that allows cybercriminals to operate with near impunity. For example, the think-tank Third Way estimated in 2018 that only three in 1,000 reported cyber incidents in the US saw the arrest of one or more perpetrators.[82] While the extent of the entire global enforcement gap is unknown, the rates of arrest are not much better in a broad range of countries. There are numerous technical, operational and strategic challenges that have contributed to this gap,[83] including significant hurdles related to the collection, handling and transfer of electronic evidence.[84] The fact that cybercrime investigations often require intensive cooperation within and across borders presents particularly thorny challenges. This gap has resulted in a perception among certain publics that, while governments have the legal authority to bring malicious cyber actors to justice, law enforcement will rarely be able, or willing, to try to do so. This may be, in part, due to the lack of capacity and capability among criminal justice actors on cybercrime and digital evidence. This leads to decreased public trust in the ability of law enforcers to secure justice for victims, which can hinder reporting.[85]

Cybercrime during COVID-19

While cybercrime was continuing to increase and transform before the COVID-19 crisis, some data now indicate that the pandemic has only made things worse, at least at certain points. Europol (the European Union Agency for Law Enforcement Cooperation) noted that with a record number of people staying in their homes and relying even more on the internet for daily activities including work, education and leisure, 'the ways for cybercriminals seeking to exploit emerging opportunities and vulnerabilities have multiplied'.[86] According to one study published in March 2020, 88 per cent of US organizations had encouraged or required employees

80 Ibid, p. 13; Cybersecurity & Infrastructure Security Agency (2020), 'Avoiding Social Engineering and Phishing Attacks', Security Tip (ST04-014), last revised 25 August 2020, https://us-cert.cisa.gov/ncas/tips/ST04-014.
81 Public-Private Analytic Exchange Program (2019), *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*, pp. 4–5, https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf; Healey, J. (2012), *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Washington, DC: Atlantic Council, https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.
82 Eoyang, M. et al. (2018), 'To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors', Third Way, 29 October 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.
83 Peters and Jordan (2020), 'Countering the Cyber Enforcement Gap', pp. 491–8.
84 Ibid, pp. 514–5.
85 Button, M. et al. (2020), *Victims of Computer Misuse*, Executive Summary, University of Portsmouth, April 2020, p. 7, https://researchportal.port.ac.uk/portal/files/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf,page.
86 Europol (2020), *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, 3 April 2020, p. 3, https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf.

to work remotely.[87] In addition, social media usage rates have spiked.[88] Such shifts have created a large pool of individuals, businesses and even public officials who are increasingly using online communication, often with less stringent cybersecurity measures in place than would be employed in an office environment. This provides cybercriminals with an unprecedented number of victims to target.[89,90]

While cybercrime was continuing to increase and transform before the COVID-19 crisis, some data now indicate that the pandemic has only made things worse, at least at certain points.

As well as having a growing number of potential targets, cybercriminals have customized their tactics, techniques and procedures (TTP) to the COVID-19 crisis, often exploiting people's fears about the pandemic to their advantage. INTERPOL (the International Criminal Police Organization) found an increase in the detected number, reported by global law enforcement entities, of malware and ransomware campaigns using the COVID-19 pandemic to access and infect computers.[91] Among the many examples of how cybercriminals are exploiting fears about the virus to conduct business are phishing campaigns or malware distribution through websites that have the appearance of being legitimate sources of information about COVID-19.[92]

Social engineering has been key to the success of many cybercriminals seeking to exploit the pandemic. While this was already a technique used by cybercriminals before COVID-19, the cybersecurity company FireEye found that: 'COVID-19 is being adopted broadly in social engineering approaches because it has widespread, generic appeal, and there is a genuine thirst for information on the subject that encourages users to take actions when they might otherwise have been circumspect.'[93] Business email compromise (BEC) attacks, in particular, are expected to continue to increase in frequency during the current crisis. These are a type of fraud that typically targets

---

87 Gartner (2020), 'Gartner HR Survey Reveals 88% of Organizations Have Encouraged or Required Employees to Work From Home Due to Coronavirus', Press Release, 19 March 2020, https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88--of-organizations-have-e; Hawdon, J., Parti, K. and Dearden, T. E. (2020), 'Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment', *American Journal of Criminal Justice*, 45, pp. 546–62, 10 June 2020, https://link.springer.com/article/10.1007/s12103-020-09534-4#ref-CR16.
88 Samet, A. (2020), '2020 US Social Media Usage: How the Coronavirus is Changing Consumer Behavior', Business Insider, 9 June 2020, https://www.businessinsider.com/2020-us-social-media-usage-report.
89 United Nations Office on Drugs and Crime (2020), *Cybercrime and COVID19: Risks and Responses, Vienna: UNODC Cybercrime and Anti-Money Laundering Section*, p. 1, https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf.
90 Joyce, S. (2020), 'Limited Shifts in the Cyber Threat Landscape Driven by COVID-19', FireEye, Threat Research blog, 8 April 2020, https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html; Europol (2020), 'Make Your Home a Cyber Safe Stronghold', Public awareness and prevention guide, https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold.
91 INTERPOL (2020), *COVID-19 Pandemic: Guidelines for Law Enforcement*, 26 March 2020, p. 18, https://www.interpol.int/content/download/15014/file/COVID19_LE_Guidelines_PUBLIC_26mar2020.pdf.
92 Council of Europe (2020), 'Cybercrime and COVID-19', Council of Europe Portal, Cybercrime News, 27 March 2020, https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19; Pazzanese, C. (2020), 'Battling the 'pandemic of misinformation'', *The Harvard Gazette*, 8 May 2020, https://news.harvard.edu/gazette/story/2020/05/social-media-used-to-spread-create-covid-19-falsehoods.
93 Joyce (2020), 'Limited Shifts in the Cyber Threat Landscape Driven by COVID-19'.

anyone who performs legitimate fund transfers. In April 2020 the US Federal Bureau of Investigation (FBI) noted that there had been an increase in BEC targeting municipalities purchasing COVID-19-related equipment and medical supplies.[94]

The above factors are reported to have resulted in an overall acceleration of cybercrime as the COVID-19 crisis took hold. As early as April 2020, the FBI reported that complaints of cybercrime had increased up to fourfold compared with the months prior to the pandemic.[95] By mid-2020, the US Secret Service estimated that $30 billion in COVID-19 relief funds would be lost to cybercrime.[96] The UN Under-Secretary-General and High Representative for Disarmament Affairs told an informal meeting of the UN's Security Council that there had been a 600 per cent increase in 'malicious emails' during the crisis.[97] In addition, the member states of Europol reported an increase in the number of attempts to access illegal websites featuring child sexual exploitation material.[98] However, some data indicate that the dramatic spikes in cybercrime recorded at the beginning of the COVID-19 crisis may be starting to level off.[99]

Broadly speaking, the types of threat actors that are conducting malicious cyber activity in the COVID-19 era are thought to be similar to those conducting such activity before the outbreak of the virus. Criminals, criminal organizations, nation states and state-backed actors are perpetrating malicious cyber activity with a variety of motivations during this crisis.[100] For many non-state criminals and criminal organizations, the proliferation of potential victims has been a boon for their financially motivated cybercrime businesses. For states and state-backed actors, the motivations are often quite different. Advanced persistent threat groups (APTs) receiving direction and/or support from states are targeting critical infrastructure, including hospitals and vaccine development labs. It is widely suspected that they are motivated by a desire to gain access to valuable information about COVID-19 response efforts and research.[101] WHO reported in April 2020 that it had seen a fivefold increase in cyberattacks, with at least some of these incidents believed to be linked to hackers connected to the Iranian government.[102] The UK, the US and Canada have publicly accused APTs associated with the Russian government

---

94 FBI News (2020), 'FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic', Press Release, 6 April 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.
95 Aspen Institute (2020), 'Fight Back: How to Stop Cyber Criminals During the Pandemic', Aspen Digital Webinar, 16 April 2020, https://www.aspeninstitute.org/events/fight-back-how-to-stop-cyber-criminals-during-the-pandemic.
96 Miller, M. (2020), 'Senior official estimates $30 billion in stimulus funds will be stolen through coronavirus scams', The Hill, 9 June 2020, https://thehill.com/policy/cybersecurity/501936-senior-official-estimates-30-billion-in-stimulus-funds-will-be-stolen.
97 Associated Press via ABC news (2020), 'The Latest: UN warns cybercrime on rise during pandemic', 23 May 2020, https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542.
98 Europol (2020), *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, pp. 7–9.
99 See for example Scroxton, A. (2020), 'Coronavirus: Cyber crime landscape evolving as lockdown eases', Computer Weekly, 26 June 2020, https://www.computerweekly.com/news/252485257/Coronavirus-Cyber-crime-landscape-evolving-as-lockdown-eases.
100 The motivation for child sexual exploitation material (CSEM) is obviously quite different. Europol (2020), *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*.
101 United Nations Office on Drugs and Crime (2020), *Cybercrime and COVID19: Risks and Responses*, p. 2.
102 World Health Organization (2020), 'WHO reports fivefold increase in cyber attacks, urges vigilance', News Release, 23 April 2020, https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance; Menn, J. et al. (2020), 'Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus – sources', Reuters, 2 April 2020, https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC.

of targeting vaccine research and development organizations.[103] Similarly, US authorities have accused actors affiliated with the Chinese government of being behind cybercrime and other forms of malicious cyber activity perpetrated against organizations conducting research related to COVID-19.[104]

While the threat actors remain largely the same, the risks posed to certain sectors during the COVID-19 crisis by a cybercrime incident or cyberattacks may be even greater. In particular, although the healthcare sector was already a major target for cybercrime before the pandemic – particularly through ransomware attacks, where victims' data or systems are held hostage until victims pay a ransom, as happened in the 2017 WannaCry attack on the UK's National Health Service[105] – a disruption or complete shutdown of a hospital treating patients, or of a research institution working to find a vaccine and treatments, could be tremendously destabilizing to entities already under unprecedented strain.[106] For a hospital, a successful attack could mean days or even weeks of being offline, and there is a risk that recovery efforts could inhibit a medical facility's ability to provide rapid, life-saving care to patients, as already demonstrated in the case of the attack on the University Hospital of Düsseldorf in March 2020.[107] INTERPOL has already reported a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response.[108] Cybercriminals are striking at healthcare providers and medical facilities as a means of targeting a sector that has lagged behind in its cybersecurity capacity – at a time when an institution may be most willing to pay a ransom in order to recover quickly from an attack. In addition, insurance companies have, in some cases, been reported as having advised entities in the healthcare sector to pay a ransom instead of incurring the substantial recovery costs in the event of an attack, despite law enforcement guidance in certain countries against doing precisely that.[109] While targeting the healthcare sector is not a novel approach for cybercriminals, the stakes for such attacks may be significantly higher in the context of the current pandemic.[110]

---

103 Cohen, Z., McGee, L. and Marquardt, A. (2020), 'UK, US and Canada allege Russian cyberattacks on COVID-19 research centers', CNN, 17 July 2020, https://www.cnn.com/2020/07/16/politics/russia-cyberattack-covid-vaccine-research/index.html.
104 FBI & CISA (2020), 'People's Republic of China (PRC) Targeting of COVID-19 Research Organizations', Public Service Announcement, 13 May 2020, https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.
105 Ghafur, S. et al. (2019), 'A retrospective impact analysis of the WannaCry cyberattack on the NHS', *npj Digital Medicine*, 2(98), https://www.nature.com/articles/s41746-019-0161-6.
106 Europol (2020), *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*; Mathews, L. (2020), 'Ransomware Damage To U.S. Healthcare Industry Passes $150 Million In Four Years', *Forbes*, 16 February 2020, https://www.forbes.com/sites/leemathews/2020/02/16/ransomware-damage-to-us-healthcare-industry-passes-150-million-in-four-years/#a6d79f06d7e0.
107 Peters, A. and Mehta, I. (2020), 'This is not the time to leave our hospitals unprotected against cyberattacks', *Washington Post*, 19 March 2020, https://www.washingtonpost.com/opinions/2020/03/19/this-is-not-time-leave-our-hospitals-unprotected-against-cyberattacks.
108 INTERPOL (2020), 'Cybercriminals targeting critical healthcare institutions with ransomware', 4 April 2020, https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.
109 Jalali, M. and Kaiser, J. (2018), 'Cybersecurity in Hospitals: A Systematic, Organizational Perspective', *Journal of Medical Internet Research*, 20(5): e10059, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174; Gallagher, R. and Bloomberg (2020), 'Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus', *Fortune*, 1 April 2020, https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus; Dudley, R. (2019), 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks', ProPublica, 27 August 2019, https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.
110 Joyce (2020), 'Limited Shifts in the Cyber Threat Landscape Driven by COVID-19'.

Taken together, these factors have put cybercrime in the spotlight during the COVID-19 crisis as a threat impacting countries and their people around the world. Combating this threat will require strong cooperation within and across borders. Already, a number of cooperation mechanisms have been set up since the outbreak of the coronavirus in order to deal with the rising cybercrime challenge that transcends national borders. For example, the COVID-19 Cyber Threat Coalition was established to bring together cybersecurity practitioners who have volunteered their time to share cyberthreat intelligence.[111] Another entity, the CTI League, connects the cybersecurity community to law enforcement agencies, with the particular purpose of protecting life-saving sectors from cyberattacks during the course of the COVID-19 crisis. The League produces intelligence feeds, analyses attacks, and works with relevant agencies to 'take down' cybercriminals.[112] Governments are also enhancing and establishing new mechanisms to boost cooperation between criminal justice actors. In the US, the FBI established a COVID-19 Working Group in March 2020; this comprises hundreds of personnel, and is dedicated to boosting the investigation of and response to COVID-19-related crime.[113] In June, Europol announced the launch of the European Financial and Economic Crime Centre (EFECC) to support EU member states and EU institutions on issues related to financial and economic crime, noting that law enforcement authorities would need more support to follow the 'money trail' as part of their investigations into cybercrime and other forms of crime.[114] Multilateral organizations such as INTERPOL and the UN are also boosting their efforts to educate participating countries on COVID-19-related cybercrime.[115]

The long-term impacts of COVID-19-related cybercrime

While the long-term impact of the COVID-19 crisis on the evolving threat of cybercrime cannot yet be assessed, there are several pressing questions about how the developments seen during the pandemic will affect global cooperation on cybercrime, on a number of levels. Policymakers, practitioners and advocates will need to pay close attention to these issues in the near future.

First, will the mechanisms and networks that have been established in response to the rise in cybercrime be leveraged and institutionalized in the long term to sustain progress on cybercrime cooperation? While governments are rightly focused on trying to slow the spread of the coronavirus and blunt the pandemic's economic impact (and as law enforcement authorities themselves are directly

---

111 COVID-19 Cyber Threat Coalition, https://www.cyberthreatcoalition.org.
112 CTI League (undated), 'Open Letter to the Health Care Community', https://cti-league.com/open-letter.
113 Shivers, C. (2020), 'COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic', FBI News, 9 June 2020, https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic.
114 Europol (2020), 'Europol Launches the European Financial and Economic Crime Centre', Press Release, 5 June 2020, https://www.europol.europa.eu/newsroom/news/europol-launches-european-financial-and-economic-crime-centre.
115 INTERPOL (2020), 'INTERPOL report shows alarming rate of cyberattacks during COVID-19', 4 August 2020, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19; United Nations Office on Drugs and Crime (2020), *Cybercrime and COVID19: Risks and Responses*.

impacted by the virus), the capacity to attribute, disrupt and bring to justice the activities of cybercriminals and to impose consequences (both punitive and deterrent) on other malicious cyber actors may be weakened at a time when cybercrime remains tremendously high under any measure and the perpetrators continue to evolve in their TTP.[116] The private sector can – and does – play a big role in working with criminal justice actors to identify cybercriminals and disrupt their infrastructures, but only governments have the legal authority to prosecute and bring them to justice.[117] Cooperation between the public and private sectors on cybercrime is therefore vital, but this has historically been subject to significant challenges, including issues around trust and communication.[118] Similarly, cooperation between criminal justice actors within and across borders has been impeded by a number of factors, including issues around capacity building and harmonization of laws.[119] Progress in cyber enforcement will require better cooperation within and between these sectors, and the new mechanisms and networks that have been established in response to COVID-19 cybercrime may prove to be enormously helpful in addressing the challenges that have always existed in facilitating greater cooperation. But it is unclear whether – beyond the context of the pandemic as the unifying factor binding the critical relationships and networks together – these positive steps can be sustained in the long term in a way that is both inclusive and underpinned by the necessary resources and political will.

The new mechanisms and networks that have been established in response to COVID-19 cybercrime may prove to be enormously helpful in addressing the challenges that have always existed in facilitating greater cooperation.

Second, and somewhat related, is the question of what – if any – impact the cybercrime developments arising from the COVID-19 crisis might have on trends in government actions that were evident before the pandemic, and that could hinder longer-term progress on public–private cybercrime cooperation. For example, prior to the pandemic a number of governments were taking steps to pass anti-encryption laws and mandate exceptional access to encrypted technologies, in the face of strong opposition from many technology companies. In 2018, the Five Eyes intelligence alliance[120] committed to a Statement of Principles that encouraged information and communications technology (ICT) service providers to establish 'lawful access solutions' to their products and services, and highlighted that they would take steps to achieve solutions to the issue of encryption if they continued

116 For more information on the potential impact of COVID-19 on law enforcement, see United Nations Office on Drugs and Crime (2020), *Cybercrime and COVID19: Risks and Responses*.
117 Daniel, M. et al. (2020), 'How do we beat COVID-19 cybercrime? By working together', World Economic Forum, 6 July 2020, https://www.weforum.org/agenda/2020/07/alliance-tackling-covid-19-cybercrime.
118 Germano, J. (2014), *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, New York: Center on Law and Security, October 2014, https://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf.
119 Peters and Jordan (2020), 'Countering the Cyber Enforcement Gap'.
120 The Five Eyes alliance comprises Australia, Canada, New Zealand, the UK and the US.

to be impeded.[121] This declaration was further strengthened in a statement issued in October 2020, with the addition of India and Japan as signatories.[122] Also in 2018 Australia moved the process forward by adopting legislation on access to encrypted communications;[123] and other governments are attempting to follow suit.[124] Some observers in civil society have argued that not only do these moves to weaken encryption raise alarm bells for their potential impact on privacy and human rights, but they could undermine national security.[125] These efforts have been met with strong opposition from technology companies, whose cooperation with the broader public sector is critical to making progress in reducing the global cyber enforcement gap.[126] However, law enforcement authorities in many countries have argued that, in the absence of a solution to the issue they call 'going dark' (the encryption of data that can impede investigations), their ability to investigate cybercrime and other threats will continue to be hindered.[127] While this area of contention is not new, that the pandemic has cast further light on the continued rise and evolution of cybercrime makes it possible that governments could double down on their argument for further action against encryption. Given the divide between the two sides on this and other issues, this could mean a tremendous challenge to the public–private relationships that are ultimately critical to reducing the global cyber enforcement gap.

Third, what impact will these developments have on broader efforts towards building consensus and promoting cooperation between governments on behavioural norms for nation states in cyberspace? Before the pandemic, a number of multilateral processes were under way to develop and enhance the so-called 'rules of the road' guiding responsible state behaviour in cyberspace.[128] These efforts have attempted to set parameters for what is and is not acceptable cyber behaviour for states, and to promote voluntary, non-binding norms on cooperation in cybercrime investigations – as enshrined through the Council of Europe's Convention on Cybercrime.[129] In response to cyber operations conducted, directed or sponsored by nation states during the pandemic, a number of governments have called for established cyber norms to be updated. The Netherlands, in particular, has called for norms restricting the intentional damage of critical infrastructure to be enhanced

---

121 Five Country Ministerial (2018), 'Statement of Principles on Access to Evidence and Encryption', https://www.ag.gov.au/sites/default/files/2020-03/joint-statement-principles-access-evidence.pdf.
122 United States Department of Justice (2020), 'International Statement: End-To-End Encryption and Public Safety', Office of Public Affairs, 11 October 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.
123 Stilgherrian (2019), 'The Encryption Debate in Australia', Carnegie Endowment for International Peace, International Encryption Brief, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217.
124 Examples include bills being introduced in the US Congress: Eoyang, M. and Garcia, M. (2020), 'Weakened Encryption: The Threat to America's National Security', Third Way, 9 September 2020, https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security; a regulation moving forward in India: Newton, C. (2020), 'India's proposed internet regulations could threaten privacy everywhere', The Verge, 14 February 2020, https://www.theverge.com/interface/2020/2/14/21136273/india-internet-rules-encryption-privacy-messaging; and proposals put forward in the UK: Lomas, N. (2019), 'Apple, Google, Microsoft, WhatsApp sign open letter condemning GCHQ proposal to listen in on encrypted chats', TechCrunch, 30 May 2019, https://techcrunch.com/2019/05/30/apple-google-microsoft-whatsapp-sign-open-letter-condemning-gchq-proposal-to-listen-in-on-encrypted-chats.
125 Eoyang and Garcia (2020), 'Weakened Encryption: The Threat to America's National Security'.
126 Lomas (2019), 'Apple, Google, Microsoft, WhatsApp sign open letter condemning GCHQ proposal to listen in on encrypted chats'.
127 Eoyang and Garcia (2020), 'Weakened Encryption: The Threat to America's National Security'.
128 Geneva Internet Platform Digital Watch (undated), 'UN GGE and OEWG', https://dig.watch/processes/un-gge.
129 Also known as the Budapest Convention. See Council of Europe Portal (undated), 'Budapest Convention and related standards', https://www.coe.int/en/web/cybercrime/the-budapest-convention.

specifically to reflect attacks on the healthcare sector.[130] There has historically been wide disagreement, when it comes to cyber norms, between governments that support an open, free and secure internet, and those with a more authoritarian view of internet control. This fragmentation has been evident in a number of areas of concern, including in debate on the applicability of international law in cyberspace, which led to the eventual breakdown of the 2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[131] Similar divides were seen during the 2019 vote in the UN General Assembly on whether a new global convention on cybercrime should be negotiated.[132] However, as certain countries are now being accused of violating agreed norms, and with the increasing blurring of the boundary between state and non-state cyber activity, the gulf between the two sides will likely only continue to widen. This could ultimately hinder progress in building some consensus across the international community on future cyber norms. Furthermore, it could impede practical cooperation across borders on cybercrime and other cyber-related issues.

Conclusion

The threat of cybercrime is not a phenomenon unique to the context of COVID-19. Indeed, the dramatic spikes seen at the onset of the pandemic may already be moderating. Yet both cybercrime and the enforcement gap were running at unacceptably high levels before the pandemic, and have continued to do so throughout the crisis. While the actors perpetrating malicious cyber activity have largely remained the same, they have continued to evolve in their approaches to take advantage of the pandemic context and exploit a pool of potential victims that has ballooned exponentially. The possible consequences of cybercrime are, arguably, higher now for some sectors than ever before, as the world grapples with the dual task of stemming the spread of the virus and mitigating the grave economic consequences of the pandemic. Imposing effective punitive measures on the different types of perpetrators engaged in cybercrime will require intense cooperation within and across borders and between different sectors. The COVID-19 crisis is likely to impact this cooperation in many different ways, not all of which may be for the better. However, the attention currently being paid by policymakers to the extent of the threat of cybercrime, as a result of the spikes seen at the beginning of the pandemic, can – and should – be harnessed to move forward policy changes aimed at fostering greater collaboration across and within borders. Ultimately, it will be a missed opportunity if any progress, galvanized in the context of COVID-19, in global cooperation to tackle cybercrime is not maintained for the long term.

---

130 Kingdom of the Netherlands (2020), *The Kingdom of the Netherlands' response to the pre-draft report of the OEWG*, April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf.
131 Ruhl, C. et al. (2020), 'Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads', Carnegie Endowment for International Peace, 26 February 2020, https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.
132 Hakmeh, J. and Peters, A. (2020), 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet', Council on Foreign Relations, Net Politics blog, 13 January 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

04
The infodemic and COVID-19 disinformation

Efforts to combat online disinformation must be channelled towards an inclusive, whole-of-society approach, based on strategic thinking in policymaking.

Sophia Ignatidou

The evolving, uncertain circumstances of the COVID-19 pandemic created the conditions for what the World Health Organization (WHO) has termed an 'infodemic': 'an over-abundance of information – some accurate and some not – that makes it hard for people to find trustworthy sources and reliable guidance when they need it'.[133] The imposition of lockdowns in many countries, together with physical distancing measures, pushed a growing number of citizens online, with more than 40 per cent of respondents to a Global Web Index survey conducted in May 2020 stating that they were spending more time on social media because of the pandemic.[134] But the world found itself scrambling for answers in an information environment where professional gatekeepers were replaced by algorithmically driven and opaque infrastructures, where the trust deficit between citizens and political leaders had widened, and where the increasingly polarized public discourse was less conducive to nuanced, complex debates on matters such as what effective pandemic management looks like.

133 World Health Organization (2020), 'Novel Coronavirus (2019-nCoV): Situation Report – 13', 2 February 2020, https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6.
134 Gilsenan, K. (2020), 'Closely connected: social media's role during COVID-19', GlobalWebIndex, 1 July 2020, https://blog.globalwebindex.com/trends/social-media-covid-19.

Digitally scaled misinformation and disinformation[135] were already a challenge of global proportions when the pandemic hit, and contested knowledge – such as that relating to an unknown virus – was more susceptible to abuse by malicious actors who could easily exploit the pervading ambiguity. The pandemic exacerbated certain pre-existing trends, but also brought into sharp focus changing geopolitical dynamics.

COVID-19 disinformation is not just a public health issue; it is also a security issue. The increasing weaponization of disinformation and control of the information space by influential political figures have demonstrated how democracies' media environments have grown more susceptible to cyber influence operations (CIOs)[136] than have the closed ecosystems of non- or weak democracies.[137] Tech companies have also developed to become geopolitical actors in their own right, advancing their interests by lobbying governments[138] or using their market power to shape public opinion.[139] On the other hand, the diminishing power of a press affected – like so many sectors – by the pandemic is alarming, precisely because it is one of the few actors holding not just governments but also big tech to account.

COVID-19 trends and security concerns

Cracking down on press freedom

In the aftermath of CIOs across the world, various governments moved to introduce anti-disinformation legislation, raising concerns over its potential use for clamping down on press freedom and opposition voices, both key components of functional democracies. Unfortunately, the COVID-19 pandemic and the state of exception it introduced lent credence to these concerns, with emergency laws and new regulations being used to suppress freedom of expression and criticism of governments' handling of the crisis.

The UN High Commissioner for Human Rights, Michelle Bachelet, has criticized Bangladesh, Cambodia, China, India, Indonesia, Malaysia, Myanmar, Nepal, the Philippines, Sri Lanka, Thailand and Vietnam for the use of emergency and anti-disinformation legislation to clamp down on freedom of expression or stifle

---

135 According to a widely used Council of Europe report, disinformation pertains to false information knowingly shared to cause harm, while misinformation refers to the unintentional sharing of false information without awareness of the fact it is inaccurate. See Wardle, C. and Derakhshan, H. (2017), *Information Disorder: Toward an interdisciplinary framework for research and policymaking*, Council of Europe, September 2017.
136 The Center for Security Studies (CSS) defines CIOs as 'illegitimate (sometimes illegal) activities that are run in cyberspace, leverage the distributed vulnerabilities of cyberspace, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations, and interfere with its decision-making processes'. Crucially, CIOs do not have to rely on false information but strategic and selective representation of events. See Cordey, S. (2019), *Cyber Influence Operations: An Overview and Comparative Analysis*, Center for Security Studies, ETH Zürich, October 2019, p. 11, https://css.ethz.ch/en/services/digital-library/publications/publication.html/c4ec0cea-62d0-4d1d-aed2-5f6103d89f93.
137 Kreps, S. (2020), *Social Media and International Relations*, p. 3, Cambridge University Press, doi:10.1017/9781108920377.
138 Wells, G., Horwitz, J. and Viswanatha, A. (2020), 'Facebook CEO Mark Zuckerberg Stoked Washington's Fears About TikTok', *Wall Street Journal*, 23 August 2020, https://www.wsj.com/articles/facebook-ceo-mark-zuckerberg-stoked-washingtons-fears-about-tiktok-11598223133.
139 Zhou, N. (2020), 'Google's open letter to Australians about news code contains 'misinformation', ACCC says', *Guardian*, 17 August 2020, https://www.theguardian.com/technology/2020/aug/17/google-open-letter-australia-news-media-bargaining-code-free-services-risk-contains-misinformation-accc-says.

criticism of the states' COVID-19 response.[140] The Council of Europe has also criticized this worrying trend in Asia.[141] Iran,[142] Turkey[143] and Hungary[144] have been showcasing similar trends, while in Russia police arrested protesting journalists, effectively using public health restrictions to impinge on freedom of assembly.[145]

States should refrain from clamping down on opposition forces, but it is worth bearing in mind that it was tech companies' inability to contain disinformation[146] that led to the increasing securitization of the digital media space,[147] used in turn as a pretext for the political suppression we are witnessing.

Wielding geopolitical power via CIOs

As a truly global common denominator, the COVID-19 pandemic led to the globalization of CIOs of which the apparent aim has been predominantly to undermine adversaries by misrepresenting their handling of the crisis, promoting authoritarian solutionism and deflecting responsibility. Both China and Russia have deployed COVID-19-related CIOs that seem to attempt to undermine trust in the effectiveness of EU institutions, improving their own image and sowing confusion about the virus's origin.[148]

CIOs do not even have to be based on false claims. An investigation by the Australian Strategic Policy Institute (ASPI) uncovered coordinated inauthentic activity by Chinese-speaking but unidentified actors that sought to skew the public debate by the automated amplification of authentic content that criticized the US response to the pandemic.[149]

---

140 Office of the United Nations High Commissioner for Human Rights (2020), 'Asia: Bachelet alarmed by clampdown on freedom of expression during COVID-19', 3 June 2020, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25920. See also Sochua, M. (2020), 'Coronavirus 'Fake News' Arrests Are Quieting Critics', *Foreign Policy*, 22 May 2020, https://foreignpolicy.com/2020/05/22/coronavirus-fake-news-arrests-quiet-critics-southeast-asia.
141 Council of Europe: Commissioner for Human Rights (2020), 'Press freedom must not be undermined by measures to counter disinformation about COVID-19', 3 April 2020, https://www.coe.int/en/web/commissioner/-/press-freedom-must-not-be-undermined-by-measures-to-counter-disinformation-about-covid-19.
142 Article 19 (2020), 'Iran: Coronavirus crisis highlights need for the free flow of information', 27 February 2020, https://www.article19.org/resources/iran-coronavirus-crisis-highlights-need-for-the-free-flow-of-information.
143 Amnesty International (2020), 'Turkey: Stifling free expression during the COVID-19 pandemic', 16 June 2020, https://www.amnesty.org/en/latest/campaigns/2020/06/turkey-stifling-free-expression-during-the-covid19-pandemic.
144 Gábor, P. (2020), 'Hungary's two pandemics: COVID-19 and attacks on media freedom', European Centre for Press & Media Freedom, 17 June 2020, https://www.ecpmf.eu/hungarys-two-pandemics-covid-19-and-attacks-on-media-freedom.
145 Human Rights Watch (2020), 'Russia: Dozens of Journalists Detained for Peaceful Protests', 10 July 2020, https://www.hrw.org/news/2020/07/10/russia-dozens-journalists-detained-peaceful-protests.
146 Helberger et al. have put forward the concept of 'cooperative responsibility', whereby both platforms and users agree on a set of rules to manage responsibility in the online public sphere, but until that settlement the private actors devising and operating information systems should bear the brunt of responsibility for their vulnerabilities and subsequent abuse by malign actors. For more on cooperative responsibility, see Helberger, N., Pierson, J. and Poell, T. (2018), 'Governing online platforms: from contested to cooperative responsibility', *The Information Society*, 34(1): pp. 1–14, doi:10.1080/01972243.2017.1391913.
147 A recent world poll found so-called 'fake news' – a usual disinformation misnomer – to be the number one concern of internet users worldwide. The Lloyd's Register Foundation World Risk Poll, 6 October 2020, https://wrp.lrfoundation.org.uk/explore-the-poll/fake-news-is-the-number-one-worry-for-internet-users-worldwide.
148 EUvsDisinfo (2020), 'EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19/Coronavirus Pandemic (Updated 2–22 April)', 24 April 2020, https://euvsdisinfo.eu/eeas-special-report-update-2-22-april. See also European Commission: High Representative of the Union for Foreign Affairs and Security Policy (2020), *Tackling COVID-19 disinformation – Getting the facts right*, 10 June 2020, p. 3, https://ec.europa.eu/info/sites/info/files/communication-tackling-covid-19-disinformation-getting-facts-right_en.pdf.
149 Thomas, E., Zhang, A. and Wallis, J. (2020), *Automating Influence on COVID-19*, Australian Strategic Policy Institute, August 2020.

Equally worrying are authoritarian-driven CIOs exploiting the COVID-19 crisis with the apparent aim of undermining support for democracies and geopolitical competitors. According to the Oxford Internet Institute (OII), social media distribution networks operated by state-backed outlets in China, Russia, Iran and Turkey, and generating millions of engagements, sought to portray democracies as incompetent in their response to the pandemic and, as a counterpoint, to show authoritarian regimes as successful.[150] Some states focused on regional geopolitical rivals, with Saudi Arabia, for instance, leveraging social media posts by its state media to criticize Qatar, Iran and Turkey.[151]

There was partial alignment in terms of narratives between Iran, Russia and China. The Russian state television network RT's English-language social media accounts portrayed a positive image of both Russia's and China's reactions to the pandemic,[152] and the Iranian influence group International Union of Virtual Media (IUVM) took a pro-China line, attacking Western media for their coverage of the crisis.[153] The head of Iran's Islamic Revolutionary Guard Corps also engaged in conspiracy theorizing, claiming in March 2020 that COVID-19 might be a result of a US biological attack[154] – a narrative widely circulated in China.

In the absence of meaningful deterrence, and with an information space that is not just polluted but also open to abuse, state and non-state[155] actors are likely to feel compelled to deploy their own CIOs to counteract adversaries. CIOs enable countries to counterbalance hard power and economic asymmetries, while the plausible deniability of the opaque information space diminishes the risks of escalation and sanctions.

The value of obscuring attribution was also evident in Russia's deployment of COVID-19 propaganda,[156] often spreading its messages through websites and 'inauthentic personas' – i.e. multi- or single-use fake accounts impersonating journalists and contributing op-eds and articles.[157] In the current context, when

---

150 Bright, J. et al. (2020), *Coronavirus Coverage by State-Backed English-Language News Sources: Understanding Chinese, Iranian, Russian and Turkish Government Media*, Data Memo 2020.2, Oxford Internet Institute, 8 April 2020, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2020/04/Coronavirus-Coverage-by-State-Backed-English-Language-News-Sources.pdf.
151 Grossman, S. (2020), 'Virality Project: Saudi Arabia State Media and COVID-19', Stanford Internet Observatory, 24 June 2020, https://cyber.fsi.stanford.edu/io/news/saudi-arabia-state-media-and-covid-19.
152 Bush, D. (2020), 'Virality Project (Russia): Penguins and Protests', Stanford Internet Observatory, 9 June 2020, https://cyber.fsi.stanford.edu/io/news/penguins-and-protests-rt-and-coronavirus-pandemic.
153 Nimmo, B. et al. (2020), *Iran's IUVM Turns to Coronavirus*, Graphika, https://public-assets.graphika.com/reports/Graphika_Report_IUVM_Turns_to_Coronavirus.pdf.
154 U.S. Department of State (2020), 'Iran: COVID-19 Disinformation Fact Sheet', 23 March 2020, https://www.state.gov/iran-covid-19-disinformation-fact-sheet.
155 Facebook-driven disinformation is claimed to be expanding in the Middle East as well. See Crisp, W. and al-Salhy, S. (2020), 'Iraqi groups paying Facebook millions to churn out fake news', *Telegraph*, 14 June 2020, https://www.telegraph.co.uk/business/2020/06/14/iraqi-groups-paying-facebook-millions-churn-fake-news; Alimardani, M. and Elswah, M. (2020), 'Online Temptations: COVID-19 and Religious Misinformation in the MENA Region', *Social Media + Society*, 6(3), doi:10.1177/2056305120948251.
156 Even though the terms 'disinformation' and 'propaganda' are sometimes used interchangeably, the latter does not need to rely on false information, is buttressed by a more long-term ideological framework and attempts to prime targeted populations in a specific way, while disinformation operations tend to be more opportunistic, with aims that vary from confusion to disenfranchisement or crowding out rational debate. See U.S. Department of State (2020), *Pillars of Russia's Disinformation and Propaganda Ecosystem*, Global Engagement Center, GEC Special Report, August 2020, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf; Barnes, J. and Sanger, D. (2020), 'Russian Intelligence Agencies Push Disinformation on Pandemic', *New York Times*, 28 July 2020, https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html.
157 Mandiant (2020), *'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests*, FireEye, 29 July 2020, https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf.

the economic implications of COVID-19 are threatening the survival of established press outlets,[158] the rise of websites purporting to be news outlets but that in reality act as vectors for disinformation is quite alarming. Technological developments such as OpenAI's GPT-3 are also likely to raise the threat level.[159]

Conspiracy theories go mainstream

A trend of particular concern that has implications for public health and the containment of COVID-19 is the proliferation of conspiracy theories and their move from the fringes to the mainstream of popular discourse. The digital platforms' combination of relativization[160] – the flattening of communicative hierarchies, with all sources appearing equivalent – and the algorithmic boosting of sensational and emotive content that raises online engagement metrics, the dwindling trust in institutional authority – precipitated by a series of mismanaged crises – and the dismembering of the news media landscape have all created fertile ground for conspiracy theories to take hold, with those being more likely to trust what they see through their own 'research'[161] and unverified sources via their social media than to trust professional journalists.[162]

A trend of particular concern that has implications for public health and the containment of COVID-19 is the proliferation of conspiracy theories and their move from the fringes to the mainstream of popular discourse.

A variety of conspiracy theories and clusters have come to the fore to provide simplistic – albeit totally unfounded – narratives that, in the context of an often incoherent or complex pandemic response, have proven compelling to growing numbers of people. Online communities active before the pandemic, such as 'anti-vaxxers' and QAnon – a group identified as a terrorist threat by the FBI but latterly embraced by Donald Trump in the latter part of his presidency[163] – have coalesced to disseminate content that threatens public safety. QAnon, the conspiracy theory network propagating the notion of a 'deep state' plotting to

---

158 Since the beginning of the pandemic a number of news providers, including the *Guardian*, *The Economist*, BuzzFeed and Quartz, have announced redundancies or the closure of regional offices.
159 GPT-3 is a language-generating AI model that uses a stunning 175 billion parameters to create synthetic text. If used for malign purposes, it has the potential to supercharge the speed in which disinformation is created. For more see DiResta, R. (2020), 'The Supply of Disinformation Will Soon Be Infinite', *The Atlantic*, 20 September 2020, https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400.
160 Julie Cohen explains how relativization and the overabundance of information lead to new types of power asymmetries. See Cohen, J. (2019), *Between Truth and Power: The Legal Constructions of Informational Capitalism*, New York: Oxford University Press, p. 88.
161 LaFrance, A. (2020), 'The Prophecies of Q', *The Atlantic*, June 2020, https://www.theatlantic.com/magazine/archive/2020/06/qanon-nothing-can-stop-what-is-coming/610567.
162 Satariano, A. (2020), 'Coronavirus Doctors Battle Another Scourge: Misinformation', *New York Times*, 17 August 2020, https://www.nytimes.com/2020/08/17/technology/coronavirus-disinformation-doctors.html.
163 Ghaffary, S. (2020), 'Trump just embraced followers of the QAnon conspiracy movement', Vox, 19 August 2020, https://www.vox.com/2020/8/19/21376639/trump-qanon-conspiracy-theory-appreciate-support-comments-fbi-domestic-terrorism.

torpedo Trump's political career, has been expanding both geographically[164] and politically,[165] and has been cited as contributing to the violent storming of the US Capitol in January 2021.[166]

Conspiracy theories linking 5G technology to the coronavirus have spread all the way from Europe[167] to Latin America,[168] and have led to various acts of violence. Another strand of theories attacks George Soros and Bill Gates as symbols of the most co-opted term in populist rhetoric, the 'elite', claiming they seek population control via the spread of COVID-19 or are hiding a cure.[169] Such conspiracy theories portraying 'elites' as the sole culprits of the crisis or, even worse, theories targeting 'othered' scapegoated populations[170] and minorities have appeared in the past, but in the era of social media the speed of their dissemination so far exceeds the capacity to counteract or contain them. Right-wing groups have extensively used COVID-19 conspiracy theories and disinformation to influence public opinion on policy issues or to target minorities.[171]

Conspiracy theories can be heavily politicized, providing ammunition for rising and empowered populist leaders and for radical movements that thrive on division. Conspiratorial narratives have been disseminated by the Italian[172] and the French right wings to foment racism and anti-immigration sentiment,[173] and in India COVID-19 disinformation has been weaponized to target Muslim groups.[174]

By injecting into popular debate the fantasy that obscure forces are working against the public interest, conspiracy theorists have been able to make the wearing of face masks and lockdown measures[175] a 'wedge issue' – a position cutting across party lines and framed in zero-sum terms whereby one side is wholly right and the

---

164 Labbe, C. et al. (2020), 'Special Report: QAnon in Europe', NewsGuard, https://www.newsguardtech.com/special-report-qanon.
165 Stracqualursi, V. (2020), 'The congressional candidates who have embraced the baseless QAnon conspiracy theory', CNN, 12 August 2020, https://edition.cnn.com/2020/08/12/politics/qanon-congressional-candidates/index.html.
166 Argentino, M. (2021), 'QAnon and the storm of the US Capitol: The offline effect of online conspiracy theories', Quartz, 7 January 2021, https://qz.com/1954265/the-attack-on-the-us-capitol-shows-the-real-danger-of-qanon.
167 Fildes, N., Di Stefano, M. and Murphy, H. (2020), 'How a 5G coronavirus conspiracy spread across Europe', *Financial Times*, 16 April 2020, https://www.ft.com/content/1eeedb71-d9dc-4b13-9b45-fcb7898ae9e1.
168 Phillips, T. et al. (2020), 'Tsunami of fake news hurts Latin America's effort to fight coronavirus', *Observer*, 26 July 2020, https://www.theguardian.com/world/2020/jul/26/latin-america-coronavirus-tsunami-fake-news.
169 Institute for Strategic Dialogue (2020), *COVID-19 Disinformation Briefing No. 2: Far-right mobilisation*, 9 April 2020, London: Institute for Strategic Dialogue, https://www.isdglobal.org/isd-publications/covid-19-disinformation-briefing-no-2.
170 The COVID-19 pandemic has notably given rise to an increase in the incidence of anti-Asian and anti-Semitic incidents. See for example Grierson, J. (2020), 'Anti-Asian hate crimes up 21 per cent in UK during coronavirus crisis', *Guardian*, 13 May 2020, https://www.theguardian.com/world/2020/may/13/anti-asian-hate-crimes-up-21-in-uk-during-coronavirus-crisis. Past viruses also had their own scapegoats. The 2009 H1N1 outbreak, for example, was initially blamed on Mexico, rendering Mexican migrants subjects of attacks or discrimination. For an analysis on the 'geographies of blame', see Sparke, M. and Anguelov, D. (2011), 'H1N1, globalization and the epidemiology of inequality', *Health & Place*, 18(2012): pp. 726–736. And what became known as the 'Spanish' flu at the end of the First World War is now understood not to have originated in Spain, but was reported on by Spanish press at a time when other European countries were censoring news reports. See McNeil Jr, D. G. (2009), 'Finding a Scapegoat When Epidemics Strike', *New York Times*, 31 August 2009, https://www.nytimes.com/2009/09/01/health/01plague.html.
171 Andriukaitis, L. and Pellegatta, A. (2020), 'Pro-right Italian media target African immigrants over coronavirus', Atlantic Council's Digital Forensic Research Lab via Medium, 19 March 2020, https://medium.com/dfrlab/pro-right-italian-media-target-african-immigrants-over-coronavirus-5d0e741cdb8c.
172 Ibid.
173 Smith, M., McAweeney, E. and Ronzaud, L. (2020), 'The COVID-19 'Infodemic'', Graphika, Special Report, 21 April 2020, https://graphika.com/reports/the-covid-19-infodemic.
174 Sutaria, S. (2020), 'Coronavirus Misinformation in India Is Not Limited to Health Misinformation', BOOM FactCheck, Meedan, https://meedan.com/reports/coronavirus-misinformation-in-india-is-not-limited-to-health-misinformation.
175 Anti-lockdown protests have sparked in countries including the US, UK, Australia and Germany.

other wholly wrong, with no space for the concessions. This approach is obviously dangerous for a complex social, economic and health issue such as a pandemic. In attempting to shore up their position against rational evidence, COVID-19 conspiracy theorists seek to undermine the credibility of authorities and officials. In the US, the extreme-right 'Boogaloo'[176] network has used anti-establishment false narratives to animate and recruit disenfranchised Americans,[177] leading in some instances to real harm.[178]

Last but not least, conspiracy theories and the environment of pervasive ambiguity they create also provide an enabling environment for CIOs by state actors. In March 2020, for instance, China's foreign ministry spokesman Zhao Lijian lent credence to a conspiracy theory suggesting that COVID-19 was brought to Wuhan by the US army.[179]

Domestic information control

The exertion of influence by means of communication strategies has as much to do with the information hierarchies that are presented as with the facts that are deliberately omitted. State actors have attempted to report information selectively, in what could be an effort to avoid public anger. China and Saudi Arabia, for example, deployed social media to boost reporting of COVID-19 recovery rates rather than transmissions.[180]

UNESCO has highlighted that public access to information is a fundamental right that becomes even more important during a health emergency.[181] Even though neither China nor Saudi Arabia are signatories to the Aarhus Convention,[182] it is worth considering whether selective representation of facts would contravene a ratifying party's obligation to provide the public with the necessary information to prevent or mitigate harm during a health crisis.

In Brazil – also a non-signatory – official government channels have been used to disseminate messages that contravene WHO recommendations, with President Jair Bolsonaro promoting false information about COVID-19 cures and effects[183] while staunchly opposing lockdowns that could aggravate the economic recession

---

176 In May 2020 Facebook and its subsidiary Instagram banned the use of 'boogaloo'-related terms accompanied by armed violence content.
177 *The Economist* (2020), 'America's far right is energised by covid-19 lockdowns', 17 May 2020, https://www.economist.com/united-states/2020/05/17/americas-far-right-is-energised-by-covid-19-lockdowns.
178 Indeed, 'Boogaloo' boys appear to have participated in the attack on the US Capitol in January 2021. See for example Hesson, T., Parker. N., Cooke, C. and Harte, J. (2021), 'U.S. Capitol siege emboldens motley crew of extremists', Reuters, 8 January 2021, https://www.reuters.com/article/usa-election-extremists/us-capitol-siege-emboldens-motley-crew-of-extremists-idUSL1N2JJ0A0.
179 Lijian, Z. (@zlj517) (2020), '2/2 CDC was caught on the spot. When did patient zero begin in US? How many people are infected? What are the names of the hospitals? It might be US army who brought the epidemic to Wuhan. Be transparent! Make public your data! US owe us an explanation!', tweet, 12 March 2020, https://twitter.com/zlj517/status/1238111898828066823?lang=en (accessed 26 Nov. 2020).
180 Grossman (2020), 'Virality Project: Saudi Arabia State Media and COVID-19'.
181 Mendel, T. and Notess, L. (2020), *The Right to Information in Times of Crisis: Access to Information – Saving Lives, Building Trust, Bringing Hope!*, UNESCO, https://en.unesco.org/world-media-trends.
182 United Nations Economic Commission for Europe (UNECE) (1998), *Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters* (Aarhus Convention), Aarhus: UNECE, 25 June 1998, https://www.unece.org/fileadmin/DAM/env/pp/documents/cep43e.pdf.
183 Ricard and Medeiros report Bolsonaro as having stated that '90% of people infected [by COVID-19] will not feel any symptoms' and that because of his 'athletic background' he would experience COVID at most as a 'gentle flu'. See Ricard, J. and Medeiros, J. (2020), 'Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil', *The Harvard Kennedy School Misinformation Review*, 1(2): p. 3, https://misinforeview.hks.harvard.edu/wp-content/uploads/2020/04/final_brazil.pdf.

that hit the country.[184] Bolsonaro was not the only political leader who attempted to avoid difficult measures that could dent economic recovery and, consequently, voter support. In the US, Donald Trump also repeatedly downplayed the effects of the virus, even when he fell victim to it and was himself hospitalized.

The pandemic struck in an already datafied world, so statistics in terms of recoveries, deaths and new cases became tools for states to broadcast their public health management credentials and, conspicuously, their legitimacy. In some instances, when those numbers were not favourable or for reasons of political expediency, political figures identified a variety of scapegoats, from immigrants[185] to China. In the case of the US, for example, the Trump administration's constant blaming of China[186] for the COVID-19 pandemic seems to have had some effect on public sentiment. Pew research published in mid-2020 showed that 78 per cent of Americans blamed China's initial handling of the novel virus for the global outbreak.[187]

Steps taken

Tech companies respond

As the infodemic spread online, tech companies adjusted their policies and launched new features, taking a markedly more decisive approach than was evident in their previous stance towards political disinformation. For example, following widespread outcry at QAnon's activities, in July 2020 Twitter banned the conspiracy theory group, with Facebook following suit.[188] In the aftermath of the US Capitol riots, online platforms have doubled down on efforts to block QAnon groups.

There now exists a patchwork of policies[189] in terms of downranking, flagging or removing health disinformation content across platforms, developed as government, public and civil society's exasperation grew. Tech companies have predominantly prioritized elevating authoritative guidance by official public health authorities and WHO, creating information hubs or providing free advertising credits to governments and health bodies. However, an Avaaz investigation[190] of the efficacy of this approach by Facebook has been damning: it found that content from the

---

184 Harris, B. (2020), 'Coronavirus tips Brazil into recession', *Financial Times*, 1 September 2020, https://www.ft.com/content/dc045f17-c90b-4098-bda1-4f7471699070.
185 Trilling, D. (2020), 'Migrants aren't spreading coronavirus – but nationalists are blaming them anyway', *Guardian*, 28 February 2020, https://www.theguardian.com/commentisfree/2020/feb/28/coronavirus-outbreak-migrants-blamed-italy-matteo-salvini-marine-le-pen.
186 Vasquez, M. and Klein, B. (2020), 'Trump again defends use of the term 'China virus'', CNN, 19 March 2020, https://edition.cnn.com/2020/03/17/politics/trump-china-coronavirus/index.html.
187 Silver, L., Devlin, K. and Huang, C. (2020), 'Americans Fault China for Its Role in the Spread of COVID-19', Pew Research Center, 30 July 2020, https://www.pewresearch.org/global/2020/07/30/americans-fault-china-for-its-role-in-the-spread-of-covid-19.
188 Wong, J. C. (2020), 'Twitter announces broad crackdown on QAnon accounts and content', *Guardian*, 22 July 2020, https://www.theguardian.com/technology/2020/jul/21/twitter-broad-crackdown-qanon-accounts-content; Facebook (2020), 'An Update to How We Address Movements and Organizations Tied to Violence', 19 August 2020, https://about.fb.com/news/2020/08/addressing-movements-and-organizations-tied-to-violence.
189 See Twitter Inc. (2020), 'Coronavirus: Staying safe and informed on Twitter', blog post, 3 April 2020, https://blog.twitter.com/en_us/topics/company/2020/covid-19.html; Google (2020), 'Coronavirus disease (COVID-19) Google Ads policy updates', Google Ad Help, 15 June 2020, https://support.google.com/google-ads/answer/9811449; Facebook (2020), 'Coronavirus (COVID-19) Response', https://about.fb.com/news/tag/covid-19; TikTok (2020), 'Supporting Our Community Through COVID-19', TikTok Safety Center, https://www.tiktok.com/safety/resources/covid-19.
190 Avaaz (2020), 'Facebook's Algorithm: A Major Threat to Public Health', 19 August 2020, https://secure.avaaz.org/campaign/en/facebook_threat_health.

top 10 websites spreading health misinformation had almost four times as many estimated views as content from organizations such as WHO and, in the US, the Centers for Disease Control and Prevention (CDC). Earlier research by the Institute for Strategic Dialogue (ISD) think-tank also showed engagement with disinformation websites far surpassed interactions with health bodies.[191] Facebook's moderation policies may be no match for the damage done by its own algorithm.

Researchers at OII also discovered that junk news websites[192] publishing harmful content in relation to COVID-19 deployed targeted search engine optimization (SEO) strategies to achieve high ranking in search results.[193]

Equally uncertain is the actual implementation of existing policies. In the Facebook sample investigated by Avaaz in its study, only 16 per cent of misinformation had a warning label. Earlier research showed that a substantial proportion of misinformation on Twitter, YouTube and Facebook lacked any flags even after it was debunked by fact-checkers.[194]

Even where flags identifying content as false do exist, their effectiveness remains open to question. In the context of information on COVID-19, a Cornell University study[195] found that the use of enhanced corrections – providing contextual information, for example – is more effective in countering misperceptions. Contextual information also decreased the propensity of interviewees to share false information, but a substantial portion (40 per cent) continued to believe false stories despite the existence of contextual information.[196]

Despite social media companies' efforts to date, it is clear that problems such as disinformation going viral persist, and are unlikely to go away unless the platforms radically change their business model – a move that will hurt their bottom line and therefore one that they will have every incentive to avoid. CIOs tend to take advantage of platforms' business models as well as the opacity for which they allow in terms of actors, propagation patterns and differentiated messages. Others have suggested that social media's reinforcement of individual mental models via user profiling and algorithmic personalized recommendations may impact the public's situational awareness[197] at a time where a common-ground truth would assist the group decision-making necessary to overcome the crisis.

---

191 Institute for Strategic Dialogue (2020), *COVID-19 Disinformation Briefing No. 3: Far-right Exploitation of COVID-19*, 12 May 2020, London: Institute for Strategic Dialogue, p. 6, https://www.isdglobal.org/isd-publications/covid-19-disinformation-briefing-no-3.
192 The Oxford Internet Institute (OII) uses this terminology for publishers that 'deliberately publish misleading, deceptive or incorrect information purporting to be real news about politics, economics or culture'. See Liotsiou, D., Kollanyi, B. and Howard, P. N. (2019), 'The Junk News Aggregator: Examining junk news posted on Facebook, starting with the 2018 US Midterm Elections', The Computational Propaganda Project, 18 April 2019, https://arxiv.org/pdf/1901.07920.pdf.
193 Taylor, E. et al. (2020), *Follow the Money: How the Online Advertising Ecosystem Funds COVID-19 Junk News and Disinformation*, ComProp Working Paper 2020.1, Oxford: Project on Computational Propaganda, https://comprop.oii.ox.ac.uk/research/posts/follow-the-money-how-the-online-advertising-ecosystem-funds-covid-19-junk-news-and-disinformation.
194 Brennen, J. S. et al. (2020), 'Types, sources, and claims of COVID-19 misinformation', Reuters Institute for the Study of Journalism, 7 April 2020, https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation.
195 Kreps, S. and Kriner, D. (2020), 'The COVID-19 Infodemic and the Efficacy of Corrections', Department of Government, Cornell University via SSRN, p. 21, https://ssrn.com/abstract=3624517.
196 Ibid.
197 Bunker, D. (2020), 'Who do you trust? The digital destruction of shared situational awareness and the COVID-19 infodemic', *International Journal of Information Management*, 55: 102201, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7402236.

The World Health Organization mobilizes stakeholders

At the international level, WHO has launched the Information Network for Epidemics (EPI-WIN)[198] initiative to provide the public with timely, accurate information on COVID-19, to convene interdisciplinary meetings with key stakeholders,[199] and to put forward a framework for managing infodemics. WHO's approach to tackling disinformation and the infodemic is to understand the dynamics and propagation patterns, who is targeted, and what the impact is, rather than just focusing on individual pieces of false information. It is deploying social listening,[200] and investing resources into developing high-quality and easily accessible health information, an intervention toolkit, countering disinformation, monitoring impact and promoting greater digital literacy with the aim of reducing public susceptibility to misinformation. It is also working with UN Global Pulse to deploy speech-to-text technology in order to analyse the feedback of offline communities, and with UNESCO to help community radio stations promote reliable health information across the world. WHO has also launched the Africa Infodemic Response Alliance (AIRA) to help coordinate actions against COVID-19 disinformation in Africa.

WHO's approach to tackling disinformation and the infodemic is to understand the dynamics and propagation patterns, who is targeted, and what the impact is, rather than just focusing on individual pieces of false information.

In addition, WHO is also working with UNICEF and the International Federation of Red Cross and Red Crescent Societies (IFRC) on ground-level community engagement in regions with weak digital media penetration. Vulnerable groups such as refugees and internally displaced persons can be exposed to digital disinformation and may be already in extremely compromised positions because of increased prices in food or personal hygiene items, or because of difficulty in physical distancing.[201]

International cooperation and coordination are central to WHO's approach, and it is uniquely placed to bring different stakeholders together, learn from best practices and take an iterative approach to policymaking. The stakes could not be higher as the effectiveness of multilateralism in supporting cooperation, coordination and synergies is put to the test by the convergence of coronavirus, its devastating economic implications and the rise of authoritarianism and protectionism.

---

198 World Health Organization (2020), 'EPI-WIN updates', https://www.who.int/teams/risk-communication/epi-win-updates.
199 Tangcharoensathien, V. et al. (2020), 'Framework for Managing the COVID-19 Infodemic: Methods and Results of an Online, Crowdsourced WHO Technical Consultation', *Journal of Medical Internet Research*, 22(6): e19659, https://www.jmir.org/2020/6/e19659.
200 World Health Organization (2020), 'Immunizing the public against misinformation', 25 August 2020, https://www.who.int/news-room/feature-stories/detail/immunizing-the-public-against-misinformation.
201 Ramizova, C. (2020), *COVID-19: perceptions of people in need in Iraq*, Ground Truth Solutions, June 2020, https://groundtruthsolutions.org/wp-content/uploads/2020/06/COVID_19-_-Iraq-_-R1.pdf.

The EU integrates COVID-19 into its long-term fight against disinformation

The EU is taking a multi-pronged approach to the issue of the infodemic, and the European Regulators Group for Audiovisual Media Services (ERGA) is tasked with assessing the effectiveness of platforms' response to COVID-19 disinformation. The signing of the EU's Code of Practice by a group of tech companies in October 2018 was a useful first step in providing private actors with the opportunity to contain disinformation, but it has subsequently been criticized by EU member states,[202] ERGA[203] and the Commission itself,[204] for its voluntary nature and the lack of sanctions, redress mechanisms and independent compliance verification.[205] Still, an enhanced group of signatories has begun submitting monthly reports on their COVID-19-specific policy changes.[206]

The office of the High Representative of the Union for Foreign Affairs and Security Policy also conceded in June 2020 that EU public policy could benefit from a faster and more coordinated response, calling for the security dimension of disinformation in general to be reflected in the forthcoming Security Union Strategy[207] (for the period 2020–25). COVID-19 disinformation has also affected the Commission's thinking in terms of the European Democracy Action Plan[208] and the proposed Digital Services Act (DSA).[209]

National level responses

At national level, some countries have addressed COVID-19 disinformation through dedicated crisis units[210] and enhanced digital health communication;[211] others, such as Portugal, have taken steps to boost the communication capacities

---

202 Stolton, S. (2020), 'EU code of practice on disinformation 'insufficient and unsuitable,' member states say', EURACTIV, 5 June 2020, https://www.euractiv.com/section/digital/news/eu-code-of-practice-on-disinformation-insufficient-and-unsuitable-member-states-say.
203 European Regulators Group for Audiovisual Media Services (2020), *ERGA Report on disinformation: Assessment of the implementation of the Code of Practice*, May 2020, https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf.
204 European Commission (2020), 'Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement', Staff Working Document (SWD(2020)180), 10 September 2020, https://ec.europa.eu/digital-single-market/en/news/assessment-code-practice-disinformation-achievements-and-areas-further-improvement.
205 European Regulators Group for Audiovisual Media Services (2020), *ERGA Report on disinformation: Assessment of the implementation of the Code of Practice*.
206 European Commission (2020), 'First baseline reports – Fighting COVID-19 disinformation Monitoring Programme', 10 September 2020, https://ec.europa.eu/digital-single-market/en/news/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme.
207 European Commission, High Representative of the Union for Foreign Affairs and Security Policy (2020), *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling COVID-19 disinformation – Getting the facts right*, Brussels: European Commission, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0008&from=EN.
208 The European Democracy Action Plan has highlighted the impact of COVID-19 on press freedom and media plurality among others. See European Commission (2020), 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423.
209 Among the purposes of the European Commission's forthcoming Digital Services Act package, a long-debated overhaul of the e-Commerce Directive, will be to regulate social media. It incorporates regulatory avenues that will impact COVID disinformation, from limiting microtargeting to providing more user control over AI-driven services, or enhanced platform liability for selling unsafe products.
210 The UK, for example, is operating a Rapid Response Unit from within the Cabinet Office and No. 10 Downing St, to address harmful COVID narratives.
211 Taiwan and South Korea have been praised as success stories in this regard. Tworek, H. (2020), 'Lessons learned from Taiwan and South Korea's tech-enabled COVID-19 communications', Brookings, 6 October 2020, https://www.brookings.edu/techstream/lessons-learned-from-taiwan-and-south-koreas-tech-enabled-covid-19-communications.

of health ministries. Other measures national governments have put in place include public information and digital literacy campaigns, as well as dedicated instant messaging channels.[212]

Next steps

The infection patterns of coronavirus are in some ways illustrative of why the study of propagation patterns and dynamics – rather than of individual cases of false information – is more important in tackling disinformation.[213] Fact-checking is certainly a crucial part of the puzzle, but it lacks the necessary system-level view that can have network effects.

Strategic thinking in policymaking is key to tackling disinformation, so obstacles and constraints to policy implementation should be considered in advance, and methods to circumvent or counteract them should be planned accordingly. Establishing benchmarks for successful policy monitoring, implementation and impact assessment is also paramount. Multidisciplinary cooperation is necessary so that important trade-offs – such as that between freedom of expression and public health – can be negotiated meaningfully. The issue of an appropriate division of labour in content creation, moderation and dissemination that sustains a democratic public sphere also needs to be addressed.

Conflict of interest considerations should limit the role of tech companies in dictating the solutions to the problems they themselves helped create, in the same way that the tobacco industry should not be asked to draft health regulations, or oil companies to devise environmental standards. Even though ensuring the buy-in of tech companies is necessary, strategic thinking in terms of the scope and form of their engagement is necessary for other actors such as civil society to not be sidelined in terms of framing, analysing and addressing the issue at hand. Political leadership, by parliamentarians, international organizations and governments, is absolutely key for tackling COVID-19 disinformation and the infodemic.

A whole-of-society approach should remain central to the efforts, as COVID-19 disinformation flows not only in a top-down direction (for example, from politicians or celebrities), but also from the bottom up. Politicians and leading figures must take responsibility for the messages they disseminate. The question of whether the amplification of COVID-19 disinformation by state officials and political leaders effectively 'violates the right to health'[214] merits urgent attention.

---

212 Organisation for Economic Co-operation and Development (2020), 'Transparency, communication and trust: The role of public communication in responding to the wave of disinformation about the new Coronavirus', 3 July 2020, https://www.oecd.org/coronavirus/policy-responses/transparency-communication-and-trust-bef7ad6e. The OECD also has a useful COVID-19 responses tracker: https://stip.oecd.org/covid.
213 Andrews, E. L. (2019), 'How fake news spreads like a real virus', Stanford Engineering, 9 October 2019, https://engineering.stanford.edu/magazine/article/how-fake-news-spreads-real-virus.
214 Abrusci, E., Dubberley, S. and McGregor, L. (2020), 'An 'Infodemic' in the Pandemic: Human Rights and COVID-19 Misinformation', in Ferstman, C. and Fagan, A. (eds) (2020), *COVID-19, Law and Human Rights: Essex Dialogues. A Project of the School of Law and Human Rights Centre*, University of Essex, p. 290, https://www.hrbdt.ac.uk/download/an-infodemic-in-the-pandemic-human-rights-and-covid-19-misinformation.

UN agencies and regional organizations such as the EU, committed to a rules-based order and democratic values, should enhance their collaboration to set a clear path forward. There are already efforts under way aimed at fostering closer collaboration between UN agencies including WHO, UNICEF and the International Telecommunication Union (ITU), and their work on how health disinformation spreads and how individuals interact with it should inform the work of the EU in terms of the European Democracy Action Plan and the forthcoming DSA. In December 2020, anticipating the incoming US administration under the presidency of Joe Biden, the high representative for EU external action, Josep Borrell, notably highlighted the need for a transantlantic rapprochement and cooperation on issues of COVID-19 and technology, among other areas of joint concern.[215] National authorities should also lead domestic counter-disinformation efforts by drawing on the expertise and the ongoing cooperation of WHO.

Four critical considerations

The four steps of emergency management[216] remain crucial in tackling COVID-19 disinformation:

1. **Mitigation:** Legislation, regulation, re-establishing competition in the digital media environment, the introduction of digital and media literacy programmes, lobbying reform, and enhancing technical and tech policy expertise within ministries.
2. **Preparedness:** Monitoring new media market entrants and changing dynamics, establishing protocols of cooperation between tech, media actors and governments, investing in strategic foresight, and alliance building.
3. **Response:** Ensuring organizational structures enable effective communication within government and between authorities and the public, monitoring and evaluating policy implementation, strategic communication, and infodemic management.
4. **Recovery:** Impact assessments of measures taken, consideration of sanctions for culpable agents, and notification systems for targets of disinformation.

---

215 European External Action Service, Delegation of the European Union to the United States (2020) 'EU-US: Press remarks by HR/VP Josep Borrell on the New Transatlantic Agenda for Global Change and on the College meeting', 2 December 2020, https://eeas.europa.eu/delegations/united-states-america/89762/eu-us-press-remarks-hrvp-josep-borrell-new-transatlantic-agenda-global-change-and-college_en.
216 Lindsay, B. R. (2012), *Federal Emergency Management: A Brief Introduction*, Congressional Research Service, 30 November 2012, p. 2, https://fas.org/sgp/crs/homesec/R42845.pdf.

05 Conclusion

The COVID-19 pandemic has underscored that tech governance must be based on human-centric values that protect the rights of individuals but also work towards a collective good.

Joyce Hakmeh

The role of information and communications technologies as the backbone of digital economies and as a critical element in enabling a sustainable future for all has become undisputable. Their role is increasingly acknowledged in fostering socio-economic development through enhanced productivity, trade facilitation and creation of new and different types of jobs; as well as in strengthening governance, tackling corruption and improving people's lives in vital ways. At the same time, there is greater awareness of the ways in which the same technologies can – and are – being used maliciously and in potentially harmful ways, and of policies governing their use that may have unintended consequences with long-lasting detrimental impacts.

The COVID-19 pandemic has put many of these aspects into sharp relief. The unprecedented digital adoption has shown how important and indispensable digital technologies are, and for the millions of people who have transitioned at speed into a more 'virtual' way of living, the benefits as well as the risks abound. Reaching a sound approach to tech policy has been made all the more complex by the pandemic. Decision-makers have found themselves having to respond swiftly and decisively to the colossal challenges brought to the fore by the crisis, and there is considerable uncertainty as to the long-term consequences of these responses.

This paper has examined some of the risks that have been aggravated by the pandemic, the ways in which they have been dealt with so far, and what could be some of the mitigating measures and key considerations for the future. The common denominator across the themes of the preceding chapters – the dynamics between big tech and governments, cybercrime, and disinformation and fake news – is the need to restore and build greater public trust in critical measures and policy approaches, and to increase cooperation nationally and internationally. The public needs to have confidence that technological solutions to public health emergencies, or any other kinds of emergencies, are temporary, necessary and proportionate. People need to be presented with a transparent narrative that

discourages false dichotomies, such as between health and privacy, and that does not normalize the deployment of mass surveillance as the only way to deal with a crisis such as the pandemic. And people need to be able to trust in the ability of governments and public-serving bodies to protect them, to respect their rights, and to empower them by ensuring that the information they receive is solid and reliable. This all necessitates a transparent and evidence-based approach, one that favours cooperation nationally and internationally rather than an inward-looking, 'isolated' response.

As the world looks to a future in which COVID-19 has been brought under control, and as technology penetrates even further every aspect of our lives, the pandemic has helped to shed light on the importance of developing and implementing effective policies based on human-centric values that protect the rights of individuals but also work towards a collective good.

About the authors

Joyce Hakmeh is a senior research fellow in the International Security Programme at Chatham House, and co-editor of the *Journal of Cyber Policy*. Joyce leads the institute's cyber policy work, and provides regular analysis on issues that sit at the nexus between technology and geopolitics. In addition, Joyce is implementing a number of cyber capacity-building programmes around the world, and is the chair of the Global Forum on Cyber Expertise (GFCE) Working Group on Cybercrime. Joyce received her MA in international law from SOAS, University of London.

Emily Taylor is an associate fellow with the International Security Programme at Chatham House, and the editor of the *Journal of Cyber Policy*. She is CEO of Oxford Information Labs. She is the author of several research papers, and is a frequent panellist and moderator at conferences and events around the world. Previous roles have included chair of ICANN WHOIS Review Team; member of the Internet Governance Forum Multistakeholder Advisory Group and the Global Commission on Internet Governance research network; and director of Legal and Policy for Nominet. She has written for the *Guardian*, *Wired*, Ars Technica, the *New Statesman* and Slate, among other outlets; and contributes regularly to BBC news and current affairs programmes. Emily is a graduate of the University of Cambridge, qualified as a solicitor in England and Wales, and has an MBA from the Open University.

Allison Peters is the former deputy director of the National Security Program at Third Way. She has deep expertise in international organizations and cooperation through her past work as a consultant adviser to the United Nations Office of Counter-Terrorism, and as a member of a technical expert group and consultant to the Organization for Security and Co-operation in Europe's Action against Terrorism Unit. She has presented her foundational assessments of the challenges in international capacity-building to combat cybercrime and other areas of expertise at high-level multilateral forums including the United Nations General Assembly and the Global Forum on Cyber Expertise. Allison holds a master's degree in international security studies from Georgetown University's School of Foreign Service, and a bachelor's degree in political science and psychology from Rutgers University. She has appeared in numerous media outlets, including *Foreign Policy*, Al Jazeera, *USA Today*, Lawfare and The Hill.

Sophia Ignatidou is an Academy associate with the International Security Programme at Chatham House. She researches artificial intelligence, disinformation, political campaigning, propaganda and surveillance. She previously worked as a freelance journalist and digital sub-editor for the *Guardian*, the *Sunday Times* and CNN, among others. Sophia holds an MA in journalism from Goldsmiths, University of London, and an MA/PGDip in international studies and diplomacy from SOAS, University of London.

Acknowledgments

We are grateful to DXC Technology for their generous funding for this paper. The contents of this publication are the sole responsibility of the authors, and can in no way be taken to reflect the views of DXC Technology.

For her chapter on the relationship between governments and big tech, Emily Taylor thanks William Buckland and Dr Nick Cavill for public health advice; Luke Redpath for advice on the app design; Ravi Naik on data protection; Paul Tipper on Ireland's app; and other medical and technical experts who agreed to speak on a non-attribution basis. Thanks are due to Amy MacKinnon and Alice Taylor for background research, to Lucien Taylor for technical expertise and incisive comments on early drafts; and to the team at Chatham House and the anonymous peer reviewers for helpful advice and comments. Errors are the responsibility of the author.

For chapter 3, on cybercrime, Allison Peters thanks Third Way colleagues Michael Garcia and Mieke Eoyang for their peer review and helpful feedback, and the many cybersecurity practitioners and researchers who have provided valuable data throughout the COVID-19 pandemic.

Collectively, the authors thank the peer reviewers and all those who provided comments on earlier drafts of the paper; Esther Naylor and Calum Inverarity in the International Security Programme at Chatham House; and Vera Chapman Browne and Jo Maher for editing the final paper, along with the wider Chatham House communications team.

Cover image: A person who has returned a positive test holds a mobile phone showing they have been told to self-isolate for a further eight days by the NHS COVID-19 app, on 9 January 2021 in Caerphilly, Wales.
Photo credit: Copyright © Huw Fairclough/Contributor/Getty Images

ISBN 978 1 78413 436 5

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

CHATHAM HOUSE

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223