ARI 94/2020
14 July 2020

COVID-19: reaffirming cyber as a 21st century geopolitical battleground

Danny Steed | Author, Public Speaker and Consultant | @TheSteed86

Theme

The COVID-19 global pandemic carries huge numbers of ramifications globally, with consequences that will extend far past the end of the current crisis. This paper examines the geopolitical impact on cyber security that coronavirus is having.

Summary

No industry, profession, or nation has been left unaffected by the COVID-19 global pandemic. With the world in lockdown, many things have simply stopped, but not cyber security. As all organisations and businesses reverted to a work from home model, cyber security immediately elevated itself as an even higher priority than before.

This author argues that although some cyber-criminal activities have shifted emphasis to exploit the pandemic, the bulk of the evidence suggests that the same geopolitical objectives are being pursued at the international level. COVID-19, for all the change that it both is and will continue to bring, has served to reaffirm the centrality of cyberspace as a twenty first century geopolitical battleground.

Analysis

Introduction

The impact of COVID-19 has extended far beyond the medical consequences of a global pandemic, with a whole raft of clichés that has also emerged in an exceptionally short cycle as influencers and thought leaders have sought to jump on the coronavirus bandwagon. “The office is dead” and the “new normal” among others have proliferated as the world went into lockdown (surely the top contender for OUP’s annual word of the year) and adopted remote working as a new standard. The scramble to fully equip workforces with laptops, remote access and (hopefully) VPNs changed the calculus of risk for any organisation adopting these measures –they all became purely online businesses immediately.

This realisation seems to have been overlooked by many on the impact of COVID-19 on cyber security, who have in the main focused purely on matters such as how the tactical direction of cybercrime shifted rather than looking for the larger lessons. It is this author’s contention that the activities proliferating during lockdown across cyberspace illustrate a truth that has been emerging for many years; that cyber itself is a fully-fledged geopolitical battleground of the 21st century. Coronavirus has simply served to make this reality more explicit than when it was somewhat masked in the background of remaining strategic priorities during the “old normal.”

There are two arenas that serve to highlight cyber security's place as a key battleground of this century: the COVID-19 "infodemic", and allegations of IP theft against coronavirus research. While IP theft and fake news are certainly not new –with accusations long levelled at various nation states on both fronts during this century– broader public awareness of both issues has been established in lockdown, with the issue moving past just the informed elites most invested in the issue.

The Infodemic

Astonishingly, during a pandemic when political leaders have been declaring their deference to scientific guidance, fake news, conspiracy theories, and bogus coronavirus cures proliferated to exploit the fears of many and sow dissent. This led to the Director General of the World Health Organisation (WHO) Adhanom Ghebreyesus to state that 'We're not just fighting an epidemic; we're fighting an infodemic.'[1] In response, and much in common with the emergence of fact checkers during election cycles, the WHO established "mythbusters" to work with social media giants and search engine providers. Their objective is to weed out erroneous facts and rumours in circulation, for example that the virus cannot survive in hot weather, taking chloroquine medicine will help, or that 5G cellular towers somehow help transmit the virus.

The EU's External Action Service also released a report on the infodemic, accusing Russia and China in particular of targeting European citizens with such stories, especially throughout April as the world went into lockdown.[2] Reports quickly followed that the EU's public report was watered down in its assessment on Russia and China, with an internal version[3] that was far more direct in outlining the believed objectives of those nations among others. That report states its belief that Russia's top objective is twofold in 'undermining the EU and its crisis response, and to sow confusion about the origins health implications of COVID-19.'[4] For China, it argues a 'Continued and coordinated push by official Chinese sources to deflect any blame for the outbreak of the pandemic.'[5]

The rise of the infodemic, however, simply confirms existing geopolitical concerns when employing fake news and disinformation tactics; that the global pandemic has in some quarters only served as another opportunity to pursue geopolitical objectives against democratic nations. With this in mind, it is necessary to briefly examine the centrality of

[1] United Nations, Department of Global Communications, "UN Tackles 'Infodemic' of misinformation and cyber crime in COVID-19 crisis", 31/III/2020, https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19

[2] Peter Beaumont, Julian Borger and Daniel Boffey, "Malicious forces creating 'perfect storm' of coronavirus disinformation", *The Guardian,* 24/IV/2020, https://www.theguardian.com/world/2020/apr/24/coronavirus-sparks-perfect-storm-of-state-led-disinformation

[3] European External Action Service, "Disinformation on COVID-19 – Information Environment Assessment", 20/IV/2020, https://www.documentcloud.org/documents/6877118-INTERNAL-Coronavirus-3rd-Information-Environment.html

Sourced via Sean Lyngaas, "Internal EU report on coronavirus disinformation was harsher on China than public release", *Cyberscoop,* 24/IV/2020, https://www.cyberscoop.com/coronavirus-china-european-union-disinformation/

[4] Ibid report, p. 4 (sic.).

[5] Ibid, p. 7.

information war in the Russian conception of geopolitical contest. Fridman's recent article outlines the inherent conflation of information war with strategic communications in the Russian strategic mindset, he also details that concepts behind such campaigns date back to the early 1990s.[6]

To best illustrate, Fridman also cites a key source of this Russian conceptualisation in the words of Yuri Grigor'yev, part of whose definition of information war includes:

"The purpose of information war is not the destruction of people, but an alteration of certain fragmented variables that dominate the informational domain of a considerable part of the citizens to a degree when these variables fall out of the unified informational domain of the native country, thus forcing these citizens to start organising themselves in different opposing structure.'[7]

Grigor'yev essentially calls for, in very academic terms, the deliberate targeting of shared uncertainties in societies, precisely in order to sow division and dissent which, to autocratic regimes that prey on shaping false narratives as a key measure of control, enables the creation of alternative realities that suit geopolitical purposes. The use of such tactics has since become the stuff of impeachment in America, as election controversies fuelled the Mueller Inquiry, and have clearly continued unabated during the global pandemic. Russia, in the words of *The Economist*, has long been playing a game of "My Truth Against Yours."[8]

Similar to Russia, China's practice also predates the COVID-19 pandemic, stemming back as a fundamental foundation to its "three warfares' strategy" of public opinion, legal, and media warfare, outlined in its 2003 Political Work Guidelines.[9] During the pandemic however, efforts have been primarily geared towards obfuscating the origins of the virus, undermining and avoiding the types of questions that democratic nations face in their respective handlings of the pandemic, while simultaneously criticising some countries' domestic approaches, as in the case of France. Mathew Ha at the Federation for the Defense of Democracies states that the CCP has exploited bots and proxy accounts in order to spread false stories about the origins of COVID-19 worldwide, further to this are actions to share untrue assertions, such as Chinese diplomat Zhao Lijian sharing a conspiracy theory that a member of the US Army brought the virus into China.[10] In a post-truth world, the global lockdown of COVID-19 has provided a perfect battleground for "your truth versus mine" to take place.

[6] Ofer Fridman, "'Information War' as the Russian Conceptualisation of Strategic Communications", *RUSI Journal* (January 2020), Vol. 165, No. 1.

[7] Yuri Grigor'yev quoted in ibid, p. 46.

[8] Article within Special report "The Future of War", *The Economist* (27 January – 2 February 2018), p. 7.

[9] Peter Mattis, "China's Three Warfares' in Perspective", *War on the Rocks,* 30/I/2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/

[10] Mathew Ha, "China's Coronavirus Disinformation Campaigns are Integral to its Global Information Warfare Strategy", Federation for the Defense of Democracies, 30/IV/2020, https://www.fdd.org/analysis/2020/04/30/chinas-coronavirus-disinformation-campaigns-are-integral-to-its-global-information-warfare-strategy/

Numerous other incidents could be cited from the EU's report on the information environment, or from further afield. The key point to establish in this exploration of Russian and Chinese actions has been to illustrate that COVID-19 has been seized on as an additional opportunity to pursue the geopolitical objective of undermining western democratic nations and alliances. Ingram tables the term "Influence Activities" to describe such measures, with the underlying strategic logic of such activities aimed at undermining the core tenets of trust in open societies. Specifically, Ingram argues these activities target trust in a three-pronged approach; social trust, trust in authorities/experts, and trust in the democratic process.[11]

Part of the original conception for the World Wide Web was to realise the liberating promise of technology, particularly through the provision of access to information anywhere, allowing arbitrary lies to be challenged and disproven almost immediately. Indeed, the promise seemed so powerful that the possibility of a post-truth world emerging within a single generation would seem anathema to those emerging from the Cold War victory against communism. Despite this, weaknesses in the structures of cyberspace, its governance, and the democratic system have resulted in truth itself becoming a battleground, where fact checking and expertise are challenged, and trust gradually eroded. These challenges are performed by the spread of erroneous and unsupported statements, bypassing the editorial control measures in traditional media (as well the laws and regulations that govern print media in particular) and exploiting social media for mass dissemination. There is strong merit to Fridman's statement that a great deal of Kremlin success lies in shifting communications away from words and images towards *actions* as the core to any message. Such a method allows effectiveness to be measured not by real world impact, but instead 'by their influence on the virtual information dimension.'[12]

These activities certainly predate the global pandemic and were already aligned with a logical strategic conception of sowing division throughout democratic nations, as well as exploiting domestic divisions to enhance weakness wherever possible. The current global pandemic has served to shift the tactics to exploit COVID-19 specifically while still serving the primary objective of weakening western democratic nations, albeit with coronavirus serving as a catalyst. The current infodemic should not be seen as a standalone aberration, but instead as a harbinger of things to come at times of great division and uncertainty.

IP theft

While much has been made of the shift in cybercrime activity to huge surges in phishing campaigns and scams,[13] this article chooses instead to focus specifically on the shift in IP theft on pharmaceutical companies. According to various sources, cyber espionage efforts are very much in play for actors seeking any edge in the global race for treatments

[11] Hararo J. Ingram, "The Strategic Logic of State and Non-State Malign 'Influence Activities'", *RUSI Journal* (January 2020), Vol. 165, No. 1, p. 16.

[12] Fridman (2020), p. 48.

[13] Get the 600% surge etc.

against COVID-19; Oxford Analytica states that the pandemic has 'altered the strategic goals and intensity' of cyber espionage.[14] It is obvious that whichever country's pharmaceutical company goes to market first will command significant economic benefits over competitors in what would be become a perfect business school example of supply and demand.

China is the main alleged culprit –as it has been for many years in the realm of cyber espionage – with the American FBI having already issued a formal accusation that China has funded hacker cells to target American bodies working on COVID-19 treatments.[15] This is a view that has been echoed elsewhere, particularly the UK, where the National Cyber Security Centre (NCSC) released a joint advisory with the American CISA detailing the spike in targeting of medical and pharmaceutical bodies. The advisory specifically cites an attack tactic called "password spraying", 'in which the attacker tries a single and commonly used password against many accounts before moving on to a second account, and so on.'[16]

IP theft has long remained a point of serious contention, particularly between America and China, as there is a litany of allegations that stretch back through much of the 2000s thus far. From compromises of defence supply chains, to university research institutes and numerous government agencies themselves, it was hoped that the 2015 bilateral agreement between the US and China would halt cyber intrusions aiming for IP theft. For the Obama administration, clearly the hope was that a normative line had been drawn in the sand that China understood. As intrusions began to pick back up since 2016 however, it is clear the bilateral agreement is far from perfect, and now with the intensity of COVID-19 cyber espionage, real concern can be rightly levelled that an invisible line[17] has been crossed by targeting healthcare in this manner.

The way that such a normative view can be tangibly observed is in the very recent conviction of Chinese national Hao Zhang on charges of economic espionage, stealing trade secrets and conspiracy to benefit his home government by an American court in San Francisco. Zhang was indicted for stealing smartphone technology from his previous two employers – Avago and Skyworks – before starting a rival venture in China to illegally share those stolen trade secrets with. That company then established links with Tianjin University to develop the stolen patented technology before planning to launch another business, Novana, out of the Cayman Islands. The words of US Attorney Dave Anderson are however the most illustrative of the broader American view of such behaviour:

[14] Oxford Analytica, "COVID-19 alters focus of cyber espionage", 11/VI/2020, https://dailybrief.oxan.com/Analysis/DB253199/COVID-19-alters-focus-of-cyberespionage

[15] Nick Statt, "US government accuses Chinese 'cyber actors' of trying to steal COVID-19 vaccine research", *The Verge,* 13/V/2020, https://www.theverge.com/2020/5/13/21257341/us-government-coronavirus-vaccine-china-theft-spy-accuses-fbi-cisa

[16] NCSC/CISA, "Advisory: APT groups target healthcare and essential services", 5/V/2020, p. 3, https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory

[17] Lily Hay Newman, "The US says Chinese hackers went too far during the COVID-19 crisis", *Wired,* 14/V/2020), https://www.wired.com/story/china-hackers-covid-19-spying-vaccine/

'Countries without freedom cannot match our innovation, and inevitably must resort to theft. Theft is not innovation.'[18]

When it comes to cyber espionage and IP theft, the COVID-19 pandemic has served to reaffirm that the stakes are too high in this century's multipolar geopolitical to not exploit cyberspace for its informational advantages. In a global normative framework that permits –or certainly does not explicitly rule out in international law–[19] espionage activities, recent events only serve to underlie further that not only is control of cyberspace a geopolitical battleground in itself,[20] but so is exploitation of that environment to gain any other advantage in the struggle become nations.

Conclusion – the diplomatic deep push

This author has previously argued that values, especially the liberal ones at the heart of cyberspace's creation, are the missing dimension in cyber security strategy today.[21] With cyber *in*security the most, perhaps only, reliable norm in operation, it is clear that the only concrete conclusion any observer can take from the impact of COVID-19 on cyber security is that it has intensified and, more importantly, reaffirmed the adoption of cyberspace as a key twenty first century geopolitical battleground in the multipolar system.

Not only is cyberspace contested for control of its governance, the 'battle for the soul of the internet' as Nigel Inkster states,[22] but it also serves as the key battleground both to wage the current infodemic and carry out espionage campaigns against treatment research for COVID-19. Cyber security strategies to date have been too narrow minded to recognise and call out the true nature of the threats that are faced in the long term if left unchecked. The requirements go far beyond establishing mere technical resilience and building pipelines of skilled professionals to resource the cyber security functions in society. The requirement must also include a deep diplomatic push throughout democratic nations to assert the value set by which cyberspace is to be both governed and used.

The norms by which cyberspace are used are under daily challenge and exploitation, with little to deter or change behaviour to acceptable standards. Domestically focused cyber security strategies have been proven by the evidence of the past decade to be

[18] CBS San Francisco, "'Theft is not innovation'; Chinese tech executive convicted of Silicon Valley industrial espionage, 27/VI/2020, https://sanfrancisco.cbslocal.com/2020/06/27/silicon-valley-tech-theft-chinese-tech-executive-convicted-industrial-espionage/

[19] The Tallinn Manual states that espionage activities are not '*per se* regulated' by international law. Michael N. Schmitt (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: CUP, 2017), pp. 168-173.

[20] As this author has argued. Danny Steed, *The Politics and Technology of Cyberspace,* Abingdon: Routledge, 2019.

[21] Danny Steed, "The UK's National Cyber Security Strategy Beyond 2021" The International Dimension", RUSI Commentary, 2/04/2019, https://rusi.org/commentary/The_UKs_National_Cyber_Security_Strategy_Beyond_2021_The_International_Dimension

[22] Nigel Inkster, *China's Cyber Power*, Abingdon: Routledge/IISS, 2016, p. 109.

necessary but insufficient in delivering a safe and secure cyberspace for all users. A diplomatic deep push with agreed values and principles must be established by democratic nations to ensure that trust is not irreparably broken by current and future infodemics, and that theft does not deny access to medical treatments so badly needed against the current pandemic. COVID-19 has reaffirmed the place of cyber security as a twenty first century geopolitical battleground, diplomacy must accept and declare that reality, and prepare for the battle to continue long after the world finally emerges from lockdown.