Australian Journal of Defence and Strategic Studies

Volume 3, Number 1 (2021)

ISSN 2652-3728 (PRINT) 2652-3736 (ONLINE)
https://www.defence.gov.au/ADC/Publications/AJDSS
https://doi.org/10.51174/AJDSS.0301

Commentary
Countering cyber-enabled disinformation: implications for national security

Jennifer S Hunt

Published online: 1 July 2021

The Australian Journal of Defence and Strategic Studies is published twice a year by the Australian Department of Defence. It is the flagship academic journal of the Australian Defence Force. ADC Publications are managed by the Centre for Defence Research on behalf of the Australian Defence College.

PO Box 7917 CANBERRA BC ACT 2610 Tel + 61 02 6266 0352
Email cdr.publications@defence.gov.au Web www.defence.gov.au/adc/publications/ajdss

Countering cyber-enabled disinformation: implications for national security

Jennifer S Hunt

As state conflicts expand to cyberspace, foreign adversaries have been linked to increased campaigns that target democratic function. Is Australia ready?

Cybersecurity encompasses a vast threat landscape, involving both state and non-state-based actors with differing motivations and tactics. While cybersecurity was once exclusively a technical domain, the increasing sophistication and severity of cyber attacks has elevated it on the national security and popular agenda.[1] In the wake of high-profile attacks against state agencies, industries and critical infrastructure such as hospitals and utilities, cyber attacks now consistently rank in the top five threats in global surveys.[2] Recent cyberattacks in the US, such as SolarWinds and Facebook data breaches, represent near constant attacks. In Australia, significant cyber attacks have been detected against ASIO, the Bureau of Meteorology and research sectors.[3] In these examples, the goal is to exploit vulnerabilities to gain systems access and information, or deny them to others. Typically, cyber attacks are measured in dollars, though they may eventually be measured in lives. In February 2021, a water treatment plant in Florida was hacked through remote access and the sodium hydroxide mix remotely changed

1 Myriam Dunn Cavelty and Andreas Wenger, 'Cyber security meets security politics: Complex technology, fragmented politics, and networked science', *Contemporary Security Policy*, 2020, 41(1):5–32, https://doi.org/10.1080/13523260.2019.1678855.

2 Jacob Poushter and Christine Huang, 'Climate Change Still Seen as the Top Global Threat, but Cyberattacks a Rising Concern', *Pew Research Center*, 10 February 2019, https://www.pewresearch.org/global/2019/02/10/climate-change-still-seen-as-the-top-global-threat-but-cyberattacks-a-rising-concern/.

3 Australian Broadcasting Corporation, 'ANU Data Breach stretching back 19 years detected', *ABC News*, 4 June 2019, https://www.abc.net.au/news/2019-06-04/anu-data-hack-bank-records-personal-information/11176788.

to dangerous levels.[4] System alerts allowed the change to be detected and reversed in real time by the plant operator.

The latest evolution of cyber attacks target democracy itself. Democratic infrastructure constitutes the soft underbelly of the modern liberal democratic state. It comprises not just electoral systems but the information commons of democratic discourse. In four public volumes, US Senate intelligence committee reports confirm the cyber tools used by Russia to interfere with the 2016 US Presidential election. These included cyber-intrusion into voter rolls and electoral systems, email hacking of candidates, and algorithmically targeted propaganda and disinformation campaigns launched over social media designed to rupture civil society.[5] Similar efforts have been reported in the UK, France and Germany. A former Soviet disinformation officer described disinformation as 'a carefully constructed false message leaked to an opponent's communication system in order to deceive the decision-making elite or the public'.[6] The purpose is to create doubt and confusion about the facts and sources of those facts. These revamped 'Active Measures' campaigns pushed conspiracy theories around salient issues such as election integrity and COVID-19, which were then laundered through traditional media and in some cases, officials and public office-seekers.[7] An April 2021 report from US Treasury detailed how the Kremlin sought, and received, polling data from the Trump campaign to microtarget voters.[8] In one particularly effective campaign, US Senate investigations have detailed how the

4 Pinellas Sheriff Dept, 'Treatment Plant Intrusion Press Conference', 'On Monday, February 8, 2021, Sheriff Bob Gualtieri gave a press conference surrounding the unlawful intrusion to the City of Oldsmar's water treatment system. He was joined by Mayor Eric Seidel and City Manager Al Braithwaite', Oldsmar FL USA, 8 February 2021, video, duration 15:28, accessed via Youtube, https://www.youtube.com/watch?v=MkXDSOgLQ6M&ab_channel=PinellasSheriff; Carlie, Porterfield, Carlie Porterfield, 'Hacker Tried to Raise Chemicals in Drinking Water to Dangerous Levels at Florida Treatment Plant', Breaking News, *Forbes*, 8 February 2021 05:38pm EST, https://www.forbes.com/sites/carlieporterfield/2021/02/08/hacker-tried-to-raise-chemicals-in-drinking-water-to-dangerous-levels-at-florida-treatment-plant/?sh=6db2df021f21.

5 US Senate Select Committee on Intelligence, *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns And Interference In The 2016 U.S. Election Vol I–V*, Senate Report 116–290, US Government Publishing Office, Washington, 10 November 2020, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures.

6 Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider's View*, Pergamon-Brasseys, Washington, 1985.

7 Clint Watts, Testimony to US Senate Intelligence Committee, Washington DC, 30 March 2017, transcript available as PDF via https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf and video available via c-span.org https://www.c-span.org/video/standalone/?c4664397#; Ilya Yablokov, 'Conspiracy theories as a Russian public diplomacy tool: The case of Russia Today (RT)', *Politics*, 2015, 35(3):301–315, p 302, https://doi.org/10.1111/1467-9256.12097.

8 US Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 5: Counterintelligence Threats and Vulnerabilities*, S. Rpt. 116-290, US Senate, p 28, https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf, for context see also Justin Hendrix, 'US Treasure Provides Missing Link: Manafort's Partner Gave Campaign Polling Data to Kremlin in 2016', *Just Security*, 15 April 2021, https://www.justsecurity.org/75766/us-treasury-provides-missing-link-manaforts-partner-gave-campaign-polling-data-to-kremlin-in-2016/.

Kremlin leveraged social and traditional media to amplify myths around voter fraud in order to erode trust in electoral infrastructure and democratic processes. In January 2021, this narrative was used to help motivate and coordinate the insurrection at the US Capitol building which left 140 Capitol police injured, several participants dead and hundreds arrested.[9]

Stanford Professor of Cybersecurity, Herb Lin has noted the difficulties democratic states face defending against these cyber-enabled disinformation campaigns. Traditional cybersecurity threats exploit the vulnerabilities of the system; however, these evolving attacks exploit the virtues of the system, harnessing the openness and virality of social media.[10] These avenues are then used to peddle cyber-enabled disinformation. In *Like War*, Peter Singer details how the weaponisation of social media has exacerbated challenges in nearly every policy area, from aiding terrorist recruitment to being a state tool of great power competition and damaging the vitality of democracy.[11] While policymakers work to secure technological systems, they should also recognise the target is not the machine but the mind of the user.

Cyber-enabled disinformation as a tool of state-based conflict is not limited to elections. The COVID-19 pandemic illustrates how disinformation can be used to undermine national security efforts. A report by the European Commission last year found foreign actors and countries, led by Moscow and Beijing, had carried out targeted disinformation campaigns aimed at stoking confusion about the COVID-19 pandemic.[12] Similarly, an August 2020 report from the US State Department confirmed Kremlin-linked sites were boosting conspiracy theories that alleged COVID-19 was created in a lab as a bioweapon, that billionaire Bill Gates was plotting to use the pandemic as an excuse to microchip people, and that plans for the vaccine were a well-orchestrated money grab by pharmaceutical companies.[13] As far away as Australia, protestors held up 'Arrest Bill Gates' signs; while in the UK, angry citizens attacked 5G towers and the

9 Jennifer Hunt, 'Trump Evades Conviction again as Republicans opt for Self-Preservation', *The Conversation*, 14 February 2021, https://theconversation.com/trump-evades-conviction-again-as-republicans-opt-for-self-preservation-155283

10 Herb Lin, 'Cyber Operations v. Information Operations', *11th International Conference on Cyber Conflict (Cycon)*, Tallinn, Estonia. May 2019, video, 1:02:55, available via YouTube at https://www.youtube.com/watch?v=KyCDvEzq25s.

11 Peter W Singer and Emerson T Brooking, *Like War: The weaponization of social media,* Mariner Books, Boston, 2018.

12 European Commission (EC), 'Coronavirus: EU Strengthens action to tackle disinformation', press release, EC Press Corner, Brusels,10 June 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006.

13 US State Department, *GEC Special Report: Russia's Pillars of Disinformation and Propaganda*, Washington DC, August 2020, https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/.

engineers sent to repair them.[14] These tactics are not new but they are evolving. In 2018, public health researchers documented how online bots and trolls linked to the Kremlin have been sowing 'discord and confusion' over vaccination as far back as 2014.[15] These tactics, whether for great power competition or profit, represent a strategic challenge to democracies.

Cyber-enabled disinformation has been the nexus of conspiracy-driven extremism. From recruitment to radicalisation, technology is the conduit to access new audiences, and COVID-19 has provided ideal conditions for accelerating this trend. In a rare public briefing, the head of ASIO detailed how far-right extremists were exploiting COVID-19 disinformation.[16] In 2019, an internal FBI memo warned against 'conspiracy-driven domestic terrorism' naming groups from Pizzagate to QAnon that would later form part of the Capitol Building insurrection.[17] QAnon is a creature of the internet in that it has exploited the virtues of social media (engagement, virality, community) to connect users, validate their viewpoints, spread misinformation and recruit. Radicalisation can be rapid. A US man spent only three days absorbing the early QAnon/Pizzagate conspiracy theory online before packing guns and ammunition and heading to DC seeking to kill paedophiles he thought were operating out of a pizzeria; the gunman is currently serving four years in prison.[18] State and non-state actors have capitalised on the internal fractures. A recent report from the Soufan Centre suggests that actors from Russia, China, Iran, and Saudi Arabia have all entered the fray to amplify QAnon messaging as a means to sow further discord and division within the American population.[19] Australia is not immune. When

14 James Vincent, 'Something in the Air – Conspiracy theorists say 5G causes novel coronavirus, so now they're attacking UK telecoms engineers', *The Verge*, 3 June 2020, https://www.theverge.com/2020/6/3/21276912/5g-conspiracy-theories-coronavirus-uk-telecoms-engineers-attacks-abuse; Rachael Dexter, 'The crowd has broken into chats of "arrest Bill Gates" at the anti-lockdown protest at Parliament House in Melbourne @theage. The crowd has grown considerably since midday.', tweet and video (0:11) posted to twitter.com, @rachael_dexter, Parliament House, Melbourne Australia, 10 May 2020, accessed 13 May 2021, https://twitter.com/rachael_dexter/status/1259306149930651648?s=20.

15 David Broniatowski, Amelia M Jamison, SiHua Qi, Lulwah AlKulaib et al., 'Weaponised Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate', *American Journal of Public Health*, Oct 2018, 108(10):1378–1384, https://doi.org/10.2105/AJPH.2018.304567.

16 Mario Christodoulou, 'ASIO briefing warns that the far right is exploiting coronavirus to recruit new members' *ABC News*, 12 June 2020, https://www.abc.net.au/news/2020-06-12/asio-briefing-warns-far-right-is-exploiting-coronavirus/12344472.

17 Jana Winter, 'Exclusive: FBI document warns conspiracy theories are a new domestic terrorism threat', *Yahoo News*, 2 August 2019, https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html.

18 US Department of Justice, 'North Carolina Man Sentenced to Four-Year Prison Term for Armed Assault at Northwest Washington Pizza Restaurant', US Attorney's Office, District of Columbia, 22 June 2017, https://www.justice.gov/usao-dc/pr/north-carolina-man-sentenced-four-year-prison-term-armed-assault-northwest-washington.

19 Zachary Cohen, 'China and Russia "weaponized" QAnon conspiracy around time of US capitol attack, report says', *CNN*, 19 April 2021 updated 2133 GMT, https://edition.cnn.com/2021/04/19/politics/qanon-russia-china-amplification/index.html.

Facebook attempted to shut down QAnon groups in August 2020, membership surpassed 1 million members across 15 countries, including Australia.[20]

The implications for national security are considerable. From climate change to COVID-19, cyber-enabled disinformation hampers policy responses. Bot and troll accounts involved in a 'disinformation campaign' exaggerated the role of arson in Australia's bushfire disaster.[21] Vaccination efforts in allied countries have been undermined by disinformation campaigns targeting pharmaceutical companies, and the World Health Organization. By undermining trust in institutions and creating confusion over facts, it also stymes collective action and cooperation both domestically and with international partners. Noting the wider implications of disinformation, the former Deputy Secretary of the NATO, Rose Gottemoeller, called 'alternative facts a threat to the alliance' as they undermine a sense of shared reality and the will to fight together against common challenges.[22] In Australia, the vaccination effort may be hampered by similar false narratives, with the delayed roll-out providing time for hostile actors to coordinate and amplify campaigns.[23]

To counter cyber-enabled disinformation, democracies have employed individual and collective responses. In April 2021, the US announced targeted sanctions against Russia for 'undermining the conduct of free and fair elections and democratic institutions in the United States and its allies and partners; and engaging in and facilitating malicious cyber activities against the United States and its allies and partners that threaten the free flow of information'.[24] Recognising both cyber capabilities for traditional and disinformation attacks, these sanctions are intended to impose costs and limit Russia's ability to finance malicious and disruptive cyber capabilities. They also follow the indictment of 12 Russian intelligence officials in 2018, as part of the Mueller investigation.[25]

20 Julia Carrie Wong, 'Revealed: QAnon Facebook Groups are growing at a rapid pace around the world', *The Guardian*, 11 August 2020 20:00AEST, https://www.theguardian.com/us-news/2020/aug/11/qanon-facebook-groups-growing-conspiracy-theory.

21 Stilgherrian, 'Twitter bots and trolls promote conspiracy theories about Australian bushfires', *ZDNET*, 7 January 2020 17:03AEST, https://www.zdnet.com/article/twitter-bots-and-trolls-promote-conspiracy-theories-about-australian-bushfires/.

22 Rose Gottemoeller, Deputy Secretary of General of NATO, Shangri-La Dialogue panel attended by the author, Singapore, 2 June 2018. See also NATO News Room, 'NATO Deputy Secretary General Rose Gottemoeller addresses the Shangri-La Dialogue in Singapore', NATO (website), 2 June 2018 17:22, https://www.nato.int/cps/en/natohq/news_155086.htm?selectedLocale=en.

23 Jennifer S Hunt, 'The COVID-19 Pandemic vs Post Truth', *Global Health Security Network*, 1 September 2020, https://www.ghsn.org/Policy-Reports.

24 US Department of Treasury, 'Treasury Sanctions Russia with Sweeping New Sanctions Authority', Washington DC, 15 April 2021, https://home.treasury.gov/news/press-releases/jy0127.

25 Mark Mazzetti and Katie Benner, '12 Russian Agents Indicted in Mueller Investigation', *New York Times*, 13 July 2018, https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html.

Collectively, allies are being called upon to help each other secure elections and combat cyber-enabled disinformation. At the NATO-accredited Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, substantial resources are being invested to help develop and institute cyber norms around conflict beneath the threshold of war, including cyber-enabled disinformation campaigns.[26]

Australia has recently prioritised cyber security and countering foreign interference, but has fewer resources directed at countering cyber-enabled disinformation. As part of the *2020 Cyber Security Strategy*, Canberra announced $A1.35 billion over 10 years, in part for training and recruiting more than 500 cyber specialists.[27] However, Australia should also invest in countering cyber-enabled disinformation as part of a larger strategy of cyber defence. As countries like Finland have demonstrated, defences are best found in the social sciences and humanities.[28] Social sciences research in psychology, political science and communication studies can also help support the design of counter-messaging strategies to fight disinformation in cyberspace.[29] Through technical and non-technical initiatives, Australia can strengthen its own cyber capability and resilience while contributing to emerging norms and practices in countering cybersecurity challenges in all their diverse forms.

26 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Cambridge University Press, February 2017, for further information see Cooperative Cyber Defence Centre of Excellence (CCDCOE), The Tallinn Manual, https://ccdcoe.org/research/tallinn-manual/.

27 Department of Home Affairs, *Australia's Cyber Security Strategy 2020*, Australian Government, 6 August 2020, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy.

28 Finland topped, by a significant margin, the annual Media Literacy index measuring resistance to fake news and disinformation amongst 35 countries. Media Literacy Index 2019 available at Open Society Institute Sofia, The Media Literacy Index 2019: Just think about, 29 November 2019, https://osis.bg/?p=3356&lang=en; Research links and targeted grants can be used to explore the adaptation of these tools to the Australian context. For example the Fulbright Cyber Security Scholar Award is available for US Scholars to conduct research at UK institution, but it is not yet available for Australian scholars or institutions or vice versa, https://awards.cies.org/content/fulbright-cyber-security-scholar-award; Jon Henley, 'How Finland starts its fight against fake news in primary schools', *The Guardian*, 29 January 2020, https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news.

29 National Academies of Sciences, Engineering, and Medicine, 'A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis', The National Academies Press, Washington DC, 2019, https://doi.org/10.17226/25335; Bionca Nogrady, 'Australia cuts research funding to universities', News, *Nature*, 19 December 2018, https://www.nature.com/articles/d41586-018-07840-w.