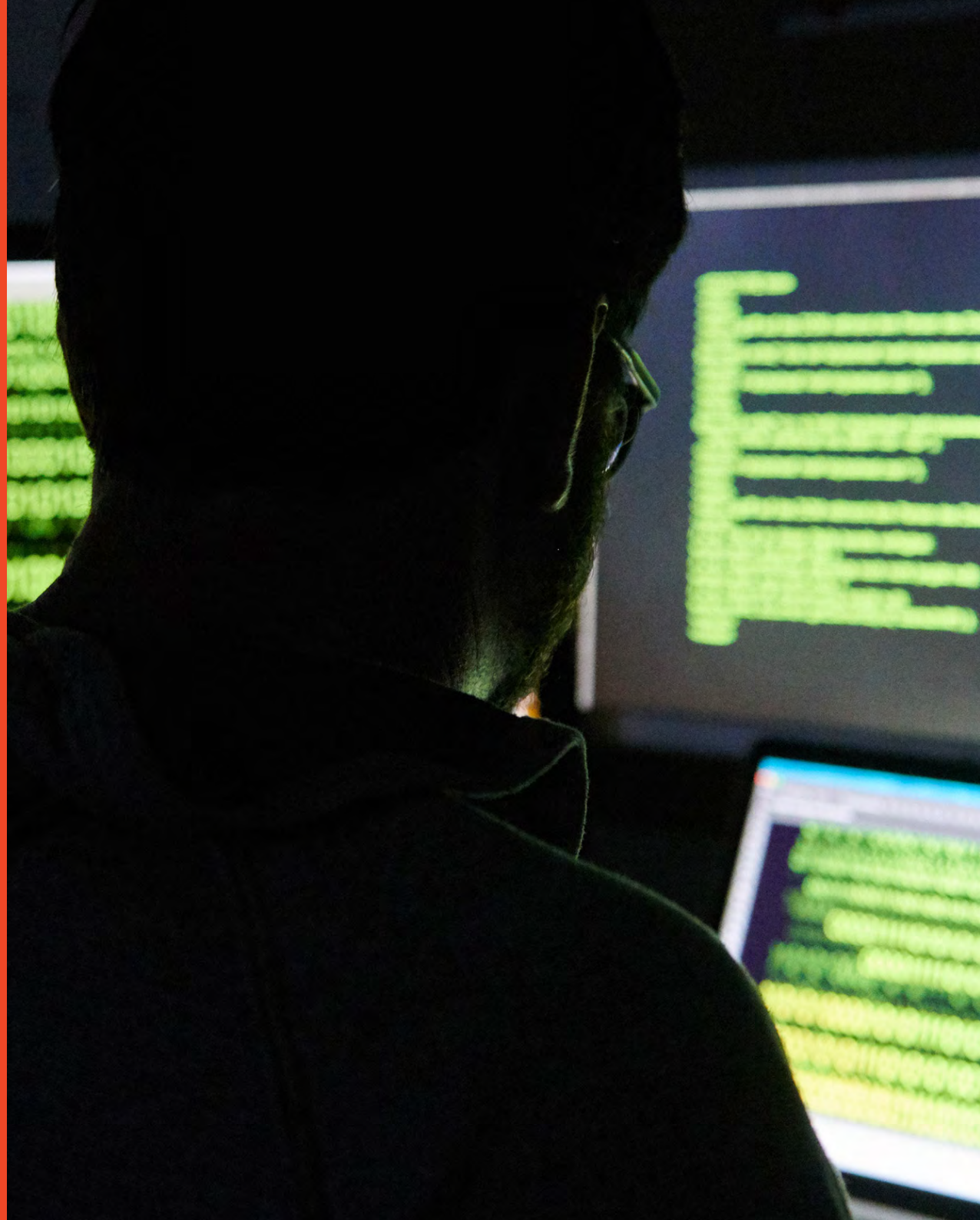
BUILD CYBER CAPABILITY AND COOPERATION FOR AN EVOLVING THREAT LANDSCAPE

DR JENNIFER S. HUNT



Context and background

To deepen cooperation on cyber issues, Australia should restore critical bilateral and multilateral cyber efforts while also recognising that cyber-enabled disinformation is part of the expanding cyber threat landscape.

Australians and Americans consistently rank cyber attacks in the top five of global threats.[16.1] It is easy to see why. Recent cyberattacks in the United States have targeted critical infrastructure including government agencies, hospitals and utilities. In February 2021, a water treatment plant in Florida was hacked through remote access and the sodium hydroxide mix remotely changed to dangerous levels before being caught and reversed in real-time by the plant operator.[16.2] In 2020, at least two foreign governments breached the US Department of Homeland Security and Treasury and exposed Fortune 500 companies in what was described by some as the "Cyber Pearl Harbor" by inserting malicious code into a popular software product.[16.3]

Cyber is the connective tissue through critical state, economic, social and strategic systems. Increasingly the soft underbelly, however, is democratic infrastructure. As state conflicts expand to cyberspace, cyberattacks now target not just information systems, but electoral systems and even voters themselves through cyber-enabled disinformation campaigns.[16.4] Cyber scholar Herb Lin notes the difficulties of defence – while traditional cybersecurity threats exploit the vulnerabilities of the system, these evolving attacks exploit its virtues, as cyber-enabled disinformation harnesses the openness and virality of social media to spread disinformation and conspiracy theories to poison democratic function.[16.5] Whether for great power competition, private profit or pure entertainment, these tactics represent an evolving strategic challenge to democracies and Australia is not immune.[16.6] The COVID-19 pandemic in particular has only heightened these challenges. In March 2020, the Australian Cyber Security Centre issued an alert warning of malicious websites masquerading as trustworthy authorities on coronavirus information, disinformation that could have undermined state responses to the pandemic.[16.7]

Australia invested significantly in cyber capacity and coordination under the Turnbull government including the introduction of a Special Advisor on Cyber Affairs (within the Department of Prime Minister and Cabinet), a Cyber Ambassador (within the Department of Foreign Affairs and Trade) and the Australian Cyber Security Centre (within the Australian Signals Directorate). Under the Morrison government, cyber policymaking has shifted to Home Affairs, the cyber diplomatic portfolio has expanded to include critical technologies and Australian Cyber Security operations in the Australian Signals Directorate have been given a significant boost in funding. Alongside the government's 2020 Cyber Security Strategy, Canberra announced A$1.35 billion over 10 years, in part for training and recruiting more than 500 cyber specialists.[16.8] These domestic efforts have been paired with significant engagement on the international front, but some bilateral efforts were abandoned under the Trump administration.

The Biden administration

Individual US states have focused on bolstering their cyber defences but the federal government and the United States more broadly have lost valuable time in countering the newest evolution of attacks due to the Trump administration's neglect of cyber issues. This neglect included: the dismissal of the Cybersecurity Coordinator position at the White House, the shrinking of the State Department's cyber diplomacy wing, and repeatedly ignored calls for bolstering electoral security. President Trump publicly sided with Vladimir Putin over US intelligence agencies' assessment of hostile foreign interference in cyber and electoral matters.[16.9] In one of his last acts in office, President Trump dismissed the director of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security after the official confirmed Joe Biden's win in the 2020 election.[16.10]

The Biden cyber team

The Biden administration used its first month to signal the prioritisation of cyber issues on the national agenda through the appointment of officials with cyber experience across multiple departments.

- Biden's National Security Council includes five experienced cybersecurity officials including:
  - Anne Neuberger as Deputy National Security Advisor for Cyber and Emerging Technology, a new position designed to elevate the subject internally
  - Senior Director for Cyber, Michael Sulmeyer
  - Homeland Security Advisor Elizabeth Sherwood-Randall, her deputy, Russ Travers as Deputy Homeland Security Advisor and Caitlin Durkovich as Senior Director for Resilience and Response at the National Security Council.
- In the White House's Office of Management and Administration, David Recordon will become Director of Technology.
- The Deputy Attorney General nominee, Lisa Monoca, also comes with cybersecurity portfolio experience.

The Biden administration must rebuild an atrophied state and fortify industrial capacity to counter diverse attacks. President Biden has signalled the prioritisation of cyber issues with a proposed US$10 billion funding package and the appointment of cybersecurity officials in key leadership positions across multiple departments. Cybersecurity officials occupy five positions on the president's National Security Council, with others in senior posts across the Department of Justice, Treasury, State and Homeland Security. This allows for crossover and prioritisation of cyber in diverse portfolios. Overseeing coordination is the National Cyber Director, a position newly created by the 2021 Defense Authorization Act to improve US cyber defences through resilient networks, bolster offensive operations to impose costs on adversaries and coordinate with industry, the academy and close allies.[16.11]

To reflect the evolving national security challenges in cyberspace, President Biden's appointments also include disinformation and counterterrorism experts. Cyber increasingly sits at the nexus of growing domestic extremist activity, with online conspiracy theories about emails, servers and laptops leading to offline physical violence. In 2019, the FBI warned against "conspiracy-driven domestic terrorism" naming QAnon and conspiracies like Pizzagate.[16.12] When Facebook[16.13] finally shut down QAnon group pages in 2020, they found the

fastest online conspiracy group comprised one million members across 15 countries including Australia.[16.14] National security expert Peter Singer argues that the weaponisation of social media and the promulgation of extremist groups on Facebook has exacerbated challenges in nearly every policy area, from aiding terrorist recruitment to being a state tool of great-power competition to damaging the vitality of democracy.[16.15]

Australian interests

Australia's interests in the cyber realm similarly lie at the intersection of technical and disinformation challenges. ASIO has warned that far-right extremists are exploiting COVID-19 disinformation to recruit and radicalise Australians online.[16.16] While cyberattacks are generally measured in dollars, disinformation is measured in lives.[16.17] In 2020, separate reports by the European Commission[16.18] and the US State Department[16.19] found that foreign actors, led by Beijing, Moscow and Tehran had carried out targeted online disinformation campaigns aimed at stoking confusion about the COVID-19 pandemic. Australia's distance does not provide immunity to either a global pandemic or cyber-enabled disinformation as evidenced by Australian lockdown protestors shouting "Arrest Bill Gates" and attacking 5G infrastructure.[16.20]

Policy recommendations

Beyond recognising cyber-enabled disinformation as a part of the cyber threat landscape to build both defensive capacity and social cybersecurity resilience, Australia and the United States should also:

- **Resume the Cyber Security Track 1.5 Dialogue[16.21] in the 2021 Australia-US Ministerial Consultation[16.22] inclusive of Australia's inaugural Ambassador for Cyber Affairs and Critical Technologies.** These talks should be inclusive of Australia's Ambassador for Cyber and Critical Technologies, Dr Tobias Feakin. Australia's cyber ambassador has been in close contact with America's allies during Washington's relative hiatus from multilateral cooperation and can provide insight from extensive engagement on cyber issues with partner nations and the United Nations.[16.23]

- **Coordinate with NATO's efforts on collective defences to emerging cyber threats[16.24] including cyber disinformation operations and electoral interference.** The cyber realm is included in President Biden's emphasis on building resilience in democracies. While working to deepen cyber cooperation between Five Eyes partners, Australia should also continue to engage closely with multilateral efforts alongside the United States at the United Nations and NATO to strengthen cyber norms and build collective responses to diverse cyberattacks that threaten state institutions, industry and democratic function. This includes recognising cyber-enabled disinformation as a threat alongside breaches and hacks and building defensive social cybersecurity accordingly.[16.25] As countries like Finland[16.26] have demonstrated, resilience against cyber-enabled disinformation campaigns does not merely require a technical or engineering solution. Often, the best solutions can be found in the social sciences[16.27] and humanities.[16.28] Research and educational links such as international visiting fellowships,[16.29] scholarships and targeted grants can be used to efficiently explore the adaptation of allied efforts to counter disinformation to the Australian context.