Flinders UNIVERSITY

Jeff Bleich Centre
for the US Alliance
in Digital Technology,
Security & Governance

JBC
Flinders University
Bedford Park SA 5042
https://www.flinders.edu.au/jeff-bleich-centre

Department of Home Affairs
PO Box 6100, Parliament House
Canberra ACT 2600

Australia's 2020 Cyber Security Strategy: Social Cyber Security

The research of the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance leads us to caution that cyber security should be understood as a social issue and not simply a matter of technology. The social impact of technology is profound. This submission will focus on the need to re-centre cyber security within its human and social context and to further appreciate the challenges of *social* cyber security.

(Q1) What is your view of the cyber threat environment? What threats should Government be focusing on?

Cyber threats exist in an irreducibly social space. The relationship between society and technology poses its own opportunities and challenges in a rapidly changing strategic environment. These opportunities and challenges should form a key component of the 2020 Cyber Security Strategy. Australia's strategic environment can be understood in terms of a discourse on society-centric warfare.[1]

Trends in 21st century warfare have blurred the lines between peace and war and between the civilian and military domains. Persistent conflict and competition are taking place below the traditional threshold of conventional armed conflict which mean that the whole of society is involved, and targeted.[2] Where traditional cyber-attacks use information networks to target physical infrastructure critical to the nation's political economy, and traditional information misuse has sought to alter people's beliefs through narratives akin to propaganda, the current environment opens up a third kind of threat: 'efforts to manipulate or disrupt the information *foundations* of the effective functioning of economic and social systems'.[3]

[1] Maryanne Kelton, Michael Sullivan, Emily Bienvenue, and Zac Rogers, "Australia, the Utility of Force and the Society-Centric Battlespace," *International Affairs* 95, no. 4, 2019, pp. 859-876.
[2] Ariel E. Levite and Jonathan (Yoni) Shimshoni, "The Strategic Challenge of Society-Centric Warfare," *Survival* 60, no. 6, 2018, pp. 91–118.
[3] Michael J. Mazarr et al., "The Emerging Risk of Virtual Societal Warfare", *RAND Corporation,* 2019, p. xii, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2714/RAND_RR2714.pdf.

JBC
Flinders University
Bedford Park SA 5042
https://www.flinders.edu.au/jeff-bleich-centre

Put otherwise, the tactics of society-centric warfare target *trust.*[4] Information is manipulated to the extent that confidence in information itself is diminished and the already weakened legitimacy of centralised institutions such as government and banks is placed under further strain. This is a fundamental attack. The trust that binds societies together, the trust that the public holds in institutions, and the trust in relationships between like-minded states, is all under attack. Such an environment poses a considerable challenge for national government, as action must be taken to mitigate these threats while also working towards rebuilding public trust in government in order that their actions will be accepted as legitimate.[5]

(Q2) Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

The concept of 'cyber risk' needs significant revision before the question of assigning responsibility can be addressed. Currently, most government departments receive a briefing on cyber matters from the Australian Cyber Security Centre (ACSC). ACSC diligently prosecutes its remit to inform and alert government and businesses to the threat of malware, known vulnerabilities, and exploitable weaknesses in computer networks. It also supplies the most up-to-date information on the activities of Advanced Persistent Threat (APT) actors.

These are essential services, but they pertain exclusively to the physical and technological nature of the cyber threat. ACSC is currently not involved in exploring the socio-cognitive implications of the digital age more broadly on Australia's national security and democratic resilience. We suggest that either the ACSC is encouraged to expand its remit beyond attacks on physical infrastructure and network penetration into the social cybersecurity domain, or a new government body focusing on social cybersecurity would need to be created. Ideally, given the well-known issues with cross-department synergy, a single department with an expanded remit would be preferable. The essential feature of a well-conceived assessment of cyber risk incorporates a whole-of-government and a whole-of-society response. The risk is society-wide and so must be the response.

---

[4] Neal A. Pollard, Adam Segal, and Matthew G. Devost, "Trust War: Dangerous Trends in Cyber Conflict," War on the Rocks, January 16, 2018, https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict/; Zac Rogers, "Targeting Our Blind Spot of Trust: Five Impossibilities of Liberal Democracy in a Dangerous Digital Age," The Strategy Bridge, January 28, 2019, https://thestrategybridge.org/the-bridge/2019/1/28/targeting-our-blind-spot-of-trust-five-impossibilities-of-liberal-democracy-in-a-dangerous-digital-age.

[5] Emily Bienvenue, Zac Rogers, and Sian Troath, "Cognitive Warfare: The Fight We've Got," The Cove, September 19, 2018, https://www.cove.org.au/adaptation/article-cognitive-warfare-the-fight-weve-got/.

JBC
Flinders University
Bedford Park SA 5042
https://www.flinders.edu.au/jeff-bleich-centre

(Q3) What role should Government play in addressing the most serious threats to institutions and business located in Australia?

Market forces cannot be relied on to develop and deploy the necessary response to social cybersecurity. The incumbent Internet business model favours the exploitation of information insecurity and the lag when it comes to regulatory and legislative intervention, in order to continue making profit under the current system. Government's most central responsibility is the protection of individuals, families, communities, and ultimately the nation from deceptive and exploitative practices. A holistic approach is needed. Government should lead this approach by coordinating its legislative and regulatory agenda with input and buy-in from industry, civil society, communities, families and individuals. A markets-only approach will leave the nation vulnerable to new and unpredictable forms of exploitation that leverage rapid technological change at the human-computer interface. A recent ACCC report has confirmed this assessment: it emphasizes the need to protect both Australian businesses *and* individuals (eg society) from the negative consequences of digital platforms.[6]

(Q4) How can Government maintain trust from the Australian community when using its cyber security capabilities?

Maintaining the trust of the Australian people is fundamental in a fragmented information environment, which will only undergo further disruption as the technological landscape changes with the expansion of AI and 5G networks.[7] For Government to maintain trust as it responds to these challenges will require greater openness and transparency than has been the norm in national security. It will also require rebuilding the trust that has been in decline with increasing rapidity over the past decade in particular.[8] Without addressing existing trust deficits, Government cannot hope to maintain trust from the Australian community when cyber becomes, as it will, an even more significant threat to societal cohesion and harmony. Government cannot avoid this responsibility; the errors of the past that left so many newly vulnerable under the impact of digital transformation cannot be repeated in the face of far more alarming and advancing threats.

---

[6] ACCC, 'Digital Platforms Inquiry: Final Report', June 2019, p. 2.
[7] Emily Bienvenue, Zac Rogers, and Sian Troath, 'Trust as a Strategic Resource for the Defence of Australia', *The Cove,* October 29 2018, https://www.cove.org.au/war-room/article-trust-as-a-strategic-resource-for-the-defence-of-australia/.
[8] See 2019 Edelman Trust Barometer, https://www.edelman.com/sites/g/files/aatuss191/files/2019-01/2019_Edelman_Trust_Barometer_Global_Report.pdf?utm_source=website&utm_medium=global_report&utm_campaign=downloads; Gerry Stoker, Mark Evans, and Max Halupka, 'Trust and Democracy in Australia: Democratic Decline and Renewal', *Democracy 2025 Report No. 1,* 2018.

Existing trust deficits are evident in social surveys showing the decline in satisfaction with democracy, and the decrease in trust in politicians, political parties, and other key institutions such as banks and the media.[9] While the Australian public appears to be relatively satisfied with democratic infrastructure, they are not satisfied with the way democracy currently works, with one survey indicating a severe decline in public satisfaction from 2013 (72 per cent satisfied) to 2018 (41 per cent satisfied).[10] The same survey found that in 2018 the federal government was trusted by only 31 per cent of the population.[11]

Ensuring the government maintains the trust of the Australian community when using its cyber security capabilities will require a two-fold effort: a whole-of-government approach to addressing the existing trust deficit, and a strategy to improve trust when it comes to national security issues in particular. The former will require a long-term and broad-based effort to rebuild trust and to find ways to address the sources of the decline of trust and the concerns of the Australian people before AI and 5G once again transform the bonds of trust within Australian society. The latter will require increased openness and transparency surrounding national security and national security agencies. It is important to balance secrecy and openness to redress the existing trust deficit and buttress societal trust for the challenges ahead:

> At a time of declining public trust in all kinds of institutions – government, corporate and private – getting the balance between openness and secrecy right is essential, if government agencies are to retain the 'licence to operate' from the public and the parliament.[12]

One way to improve openness and transparency is to ensure national security agencies present a more public-facing persona, ensuring the Australian people understand their purpose and remit. ASD's Director-General Mike Burgess has been making strides in this direction with pubic addresses conveying greater openness about policy decisions..[13]

---

[9] Gerry Stoker, Mark Evans, and Max Halupka, 'Trust and Democracy in Australia: Democratic Decline and Renewal', *Democracy 2025 Report No. 1,* 2018, p. 9.
[10] Gerry Stoker, Mark Evans, and Max Halupka, 'Trust and Democracy in Australia: Democratic Decline and Renewal', *Democracy 2025 Report No. 1,* 2018, p. 9.
[11] Gerry Stoker, Mark Evans, and Max Halupka, 'Trust and Democracy in Australia: Democratic Decline and Renewal', *Democracy 2025 Report No. 1,* 2018, p. 10.
[12] Michael Shoebridge, 'Balancing secrecy and openness: getting it right and getting it wrong', *ASPI*, 26 August 2019, https://www.aspi.org.au/opinion/balancing-secrecy-and-openness-getting-it-right-and-getting-it-wrong.
[13] Michael Shoebridge, 'ASD Moves into the Light with Landmark Speech', *ASPI,* 30 October 2018, https://www.aspistrategist.org.au/asd-moves-into-the-light-with-landmark-speech/.

JBC
Flinders University
Bedford Park SA 5042
https://www.flinders.edu.au/jeff-bleich-centre

Senior intelligence officials assuming a more public and open presence will 'help build confidence and it will help foster public trust'.[14]

(Q11) What specific market incentives or regulatory changes should Government consider?

The most important shift from the current approach is the incorporation of the social dimension in all aspects of 'cyber security'. Government must lead an agenda-driven discursive change whereby industry, businesses, individuals, and government departments are encouraged to broaden their existing understanding of 'cyber'.

A consistent and targeted government approach will encourage market incentives to shift as well, so that they are in line with the prevailing change in attitudes to the set of challenges Australian society faces when it comes to digital information systems and platforms. Government must lead a regulatory and legislative agenda which prohibits the exploitative and deceptive practices which have unfortunately characterised the digital age so far. Industry and business will take their cues from this leadership, and only then will market forces produce outcomes for Australian families and communities which strengthen and harden the nation against exploitation. The market alone does not contain the incentives required to deliver this outcome: it will require government leadership based on an understanding of the social impacts of digital transformation so far, and an appreciation of the further societal costs to come from the next wave of very rapid technological change.

[14] Danielle Cave, 'National security: the public debate and the end of 'just trust us'', *ASPI*, 10 July 2018, https://www.aspistrategist.org.au/national-security-the-public-debate-and-the-end-of-just-trust-us/.