Pukhraj Singh
Centre for Epistemic Security Pty Ltd
www.epistemicsecurity.org
Brisbane, QLD
ACN: 656571854

Jared Cunningham
Ravinn Pty Ltd
www.ravinn.com
Brisbane, QLD
ACN: 630181832

Dated: 08th March 2023

2023-2030 Australian Cyber Security Strategy Discussion Paper

---

Submission On Counter-disinformation, Cyber Threat Information Sharing and Automated Threat-Blocking at Scale

By

Centre for Epistemic Security Pty Ltd and Ravinn Pty Ltd

Dear Minister O'Neil and the Expert Advisory Board:

1. The founders of Centre for Epistemic Security Pty Ltd and Ravinn Pty Ltd carry forty years of combined experience in offensive and defensive cyber operations, multinational strategies for allied information deterrence, military cyber doctrine formulation and cyber threat intelligence.

2. They are leveraging their deeply technical operational experience to provide recommendations on the three most underexplored areas of cyber strategy:

    a. Response to question # 1: Merging cybersecurity with cognitive security;
    b. Response to question # 7: Progressing from information to intelligence sharing; and,
    c. Response to question # 10: Moving away from antiquated threat blocking at scale to Courses of Action

Pukhraj Singh
Centre for Epistemic Security Pty Ltd
www.epistemicsecurity.org
Brisbane, QLD
ACN: 656571854

Jared Cunningham
Ravinn Pty Ltd
www.ravinn.com
Brisbane, QLD
ACN: 630181832

Part I: Merging cybersecurity with cognitive security

Response to question # 1 - What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

3. Liberal democracies are highly susceptible to cyber-enabled information operations (IO), disinformation, influence operations and computational propaganda. They are the most invasive and existential of threats exploiting the cognitive vulnerabilities arising from a free and open cyber-informational environment.

4. Latest research and experience gleamed from the cyber-informational environments of Ukraine, Taiwan and the US suggest that most adversarial cyber operations are dominantly cognitive in nature. More than the disruption of the power grid or other critical infrastructure, they are aimed to undermine the will of the populace, exacerbate internal strife, radicalise the citizenry and weaken the democratic institutions.[1] The tragedy at Wieambilla and domestic misinformation around vaccination and Covid-19 are a stark reminder of that.

5. Research also indicates that cyber-enabled IO exploit the same Confidentiality-Integrity-Availability triad as cyber operations. Experts associated with us have created threat ontologies like DISARM Framework which extend the methodology behind MITRE ATT&CK to cover cyber-enabled IO.[2]

6. The liberal Western order has had a tense and uneasy relationship with IO due to the ethical issues that arise with political warfare. IO as a domain has been relegated to the military, with the military doctrine treating IO as largely a tactical instrument. It constrains thinking that IO is a wartime activity, while our adversaries are consistently targeting us even in peacetime.

7. The hyperconverged and hyperconnected information environment of cyberspace have brought the actors and audiences in very close proximity. It makes the deliberative processes of democracy extremely susceptible to foreign interference, something which the Hon Minister O'Neil and Mr. Mike Burgess of the Australian Security Intelligence Organisation have alluded to.[3] Political leaders and military commanders find it challenging to control the narrative, and thus, the initiative.

8. The era of treating IO as the poor cousin of cyber operations is over. The whole-of-government approaches to cognitive security which the Western liberal order experimented with during the Cold War need to be reactivated.

9. There are mechanisms of constructive socio-political engineering and strategic communication that can be institutionalised under the rigorous scrutiny of a democratic

[1] Pukhraj Singh, 'Critical Infrastructure Legislation Should Also Set the Parameters of Cognitive Security', *Australian Strategic Policy Institute's The Strategist*, 1 October 2021, https://www.aspistrategist.org.au/critical-infrastructure-legislation-should-also-set-the-parameters-of-cognitive-security/.
[2] 'DISARM Foundation', https://www.disarm.foundation/, n.d.
[3] 'ASIO Director-General's Annual Threat Assessment', 2022, https://www.asio.gov.au/resources/speeches-and-statements/director-generals-annual-threat-assessment-2021.

system, respecting the strong ethical sensitivities on the subject.[4] The Finnish model of cognitive security is a great example of that.[5]

10. The authors of this submission have written on how cognitive security is an inviolable tenet of national cybersecurity and even critical infrastructure protection.[6]

11. It is a whole new subdiscipline, taxonomy and ontology that the Commonwealth of Australia needs to enable by merging cybersecurity with cognitive security – and the first step will be its inclusion in the 2023-2030 Australian Cyber Security Strategy as a policy domain.

Part II: Progressing from information to intelligence sharing

Response to question # 7: What can government do to improve information sharing with industry on cyber threats?

12. Back in 2015, governments were increasingly optimistic about information sharing becoming the catalyst for national cyber resilience.

13. Various laws and governmental initiatives (mainly in the US) legitimised machine-to-machine information sharing standards like Structured Threat Information eXchange (STIX). Collaborative cyber defence started acquiring a sectoral shape with the rise of sector-specific Information Sharing and Analyses Centres (ISAC) and Information Sharing and Analysis Organisations (ISAO).

14. While such information sharing did raise the collective resilience of member organisations, it has not proved to be coercive enough to the cyber threat actors. The reasons for this are many:
    a. It has been empirically proven that ingesting billions of indicators of compromise (IoC) only offers marginal gains to cyber detection and response.
    b. Standards like STIX are aimed at collecting attack data, not analysing it. Intelligence analysis remains siloed, manual, bespoke and non-interoperable. The cyber threat intelligence (CTI) industry as a whole has overcompensated the lack of interoperable intelligence analysis with excessive emphasis on collection.
    c. STIX is not rigid enough to weed out the subjectivity of the analyst. It is now overly invested in enabling detection than pursuing its true mission: sharing intelligence and rising through CTI's famed Pyramid of Pain.[7]
    d. The machine-to-machine paradigms are yet to touch the holy grail of CTI, its strategic parameters. CTI remains atomic and operational – it is actually not intelligence but information. It is why NATO delineates threat data from threat information and threat intelligence.

[4] Pukhraj Singh, 'Counterpropaganda Is Not a Dirty Word', *Australian Defence College's The Forge*, 29 June 2022, https://theforge.defence.gov.au/publications/counterpropaganda-not-dirty-word.
[5] Corneliu Bjola and Krysianna Papadakis, 'Digital Propaganda, Counterpublics, and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience', in *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, ed. Timothy Clack and Robert Johnson (Routeledge, 2021), 186–212.
[6] Singh, 'Critical Infrastructure Legislation Should Also Set the Parameters of Cognitive Security'.
[7] 'The Pyramid of Pain', SANS Institute, n.d., https://www.sans.org/tools/the-pyramid-of-pain/.

15. However, all is not lost, and the Commonwealth of Australia is perfectly poised to address these structural deficiencies of CTI. Cyber information sharing taxonomies like STIX and ontologies like MITRE ATT&CK have laid a decent foundation for interoperability. We recommend the following next step – devise ontological models to make sure that not just cyber threat information is machine-to-machine and interoperable, but also intelligence analysis. The authors of this submission are aiming to ideate such sovereign capabilities in Australia.

Part III: Moving away from antiquated threat blocking at scale to Courses of Action

Response to question # 10: What best practice models are available for automated threat-blocking at scale?

16. The authors of this submission have studied the "national cyber shields" of Israel, the UK, Germany, France, Japan and South Korea.[8] Israel had a "20-minute detection to response strategy" while the UK's National Cyber Security Centre has pioneered frameworks like Turing and Threat-O-Matic which declassify Five Eyes intelligence and push it downstream for blocking at the government Domain Name System (DNS).
17. Such strategies are over-centralised which may not be very conducive to the private sector wary of governmental intervention.
18. The concept of threat blocking at scale is also inspired from an antiquated paradigm of detection, where cyber intrusion sets are assumed to have a command-and-control (C2) architecture. As the 2016 DARPA Cyber Grand Challenge and recent advances in Chinese malware development prove, cyber intrusion sets are becoming autonomous and intelligent, thus moving away from the C2 architecture.
19. The objective of defensive frameworks should be to make cyber offence more attritive and costly for the adversary. The Australian cyberspace needs to be treated as an emergent system requiring reflexive, multidimensional and machine-to-machine cyber threat response, instead of unidimensional capabilities like blocking.
20. Extending the discussion of interoperability of intelligence from the previous section, even cyber threat response should adopt similar qualities.
    a. NATO's IST-152 (Intelligent Autonomous Agents for Cyber Defense and Resilience) needs its own research testbed in Australia.
    b. Collaborative Automated Course of Action Operations (CACAO), Open Command-and-Control (OpenC2), YARA and SIGMA introduce substantial interoperability in detection and response.
    c. Interoperable and machine-to-machine agent-based and agentless Courses of Action can be pushed and actualised in the same way as CTI.
    d. The authors of this submission are aiming to ideate such sovereign capabilities in Australia.

[8] Pukhraj Singh, 'What Does a "National Cyber Shield" Look Like?', *Pukhraj.Me* (blog), 27 January 2019, https://web.archive.org/web/20210228190656/https://pukhraj.me/2019/01/27/what-does-a-national-cyber-shield-look-like/.

Pukhraj Singh
Centre for Epistemic Security Pty Ltd
www.epistemicsecurity.org
Brisbane, QLD
ACN: 656571854

Jared Cunningham
Ravinn Pty Ltd
www.ravinn.com
Brisbane, QLD
ACN: 630181832

Summary

1. The summary of our submission is as follows:
    a. Response to question # 1: Treat cognitive security as an inviolable tenet of national cybersecurity and critical infrastructure protection. Introduce the subdiscipline, taxonomy and ontology of cognitive security in the national cyber policy discourse by considering it as a policy domain of cybersecurity in the 2023-2030 Australian Cyber Security Strategy.
    b. Response to question # 7: Promote the creation of ontological models ensuring that not only is cyber threat information sharing machine-to-machine and interoperable, but even cyber threat intelligence (CTI) analysis. The current CTI is subjective and tactical. The common ontological methodologies will allow us to reach the holy grail of CTI: its strategic parameters.
    c. Response to question # 10: Extend the discussion of interoperability from intelligence to cyber threat response. Replace the antiquated paradigms of automated threat blocking at scale with agentless or agent-based Courses of Action. They will allow Australia to look beyond the event horizon of current cyber threat analysis which has not considered the onset of autonomous and intelligent cyber offence. The objective of cyber defence should be to make offence more attritive and costly for the adversaries. The Australian cyberspace needs to be treated as an emergent system requiring reflexive, multidimensional and machine-to-machine cyber threat response instead of unidimensional capabilities like blocking.

Pukhraj Singh
Director, Centre for Epistemic Security Pty Ltd

Jared Cunningham
Director, Ravinn Pty Ltd