RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Science, Technology and Security

January 2026

Published by the Future Issues and Technology (FIT) Research Cluster, RSIS. This Bulletin comes as a series of articles on science and technology from the angle of national security.

Australia's Approach to Addressing AI-Enabled Crime | *Fitriani*

Australia sees artificial intelligence (AI) as an economic and public-sector enabler. However, it also reserves concerns that generative AI may enable criminals to scale their activities through fake videos, synthetic voices, and phishing emails. Following high-profile cases of local mayors and councils falling victim to AI impersonators, 84,700 cybercrime reports in concerns that generative AI may enable criminals to scale their activities through fake videos, synthetic voices, and phishing emails. Following high-profile cases of local mayors and councils falling victim to AI impersonators, 84,700 cybercrime reports in 2024-25, and nearly A$260 million in scam losses the first nine month of 2025, Australia is forced to pursue a more practical operationalisation of its 2019 AI Ethics Principles.

The National AI Plan published in December 2025 by the Department of Industry, Science and Resources articulates a vision where "technology works for people, not the other way around." The plan centres government action around three goals: capturing opportunity, spreading benefits, and "keeping Australians safe as technology evolves." Minister for Industry and Innovation and Minister for Science Tim Ayres emphasised the need to "seize new opportunities and act decisively to keep Australians safe", though critics note these remain relatively broad aspirations.

Where Australia becomes particularly instructive is in how its principles and plan translate into a legal posture to address AI-enabled crime. By maintaining "tech-neutrality" in legislative design, Australia avoids referencing specific technologies, focusing instead on underlying issues that need addressing. This ensures laws remain relevant while practices evolve. Rather than creating a broad "AI crimes" statute, Australia leverages on existing regulations to address AI-enabled harms, including unauthorised access, data interference, identity crime, deception, and misuse of telecommunications services. It anchors on the Commonwealth Criminal Code Act 1995, which covers computer and cybercrime offences, including modification, impairment and deception provisions. Remarkably, a law that was passed three decades ago is still deemed current to regulate modern-day generative models.

Australia's second approach involves pairing criminal law with civil-regulatory remedies, particularly where AI amplifies the speed and scale of harms. The Commonwealth Online Safety Act 2021 and the eSafety Commissioner's schemes create enforceable pathways to remove harmful online material and penalise non-compliance. This approach is often more practical than relying solely on criminal prosecution especially when perpetrators are anonymous, based offshore, or moving faster than courts can respond. This matters for cybercrime because many AI-enabled harms, such as impersonation, extortion content, and “nudify” deepfakes, sit at the intersection of content moderation and criminality. It relies on responsive regulators to mitigate victims’ harm quickly while police investigations are ongoing.

An example is eSafety bringing Anthony Rotondo to court in 2023 for non-consensual deepfake pornography and non-compliance with takedown orders under the Online Safety Act. Rotondo had created deepfake images of both prominent and underage Australians, uploading it to online platform MrDeepfakes. Through this institutional design, Australia has empowered its online-safety regulator with tools that can be activated quickly and subsequently escalated. This was evidenced when the regulator secured court orders for Rotondo’s arrest after he continued to disseminate deepfakes using him not residing in the country as the reason.

Following the Rotondo case, Australia amended its Criminal Code to include the criminalisation of deepfake sexual material in late 2024. The law is also seen as gender-responsive as AI-enabled crime disproportionately targets women and girls. By criminalising the transmission of technologically altered sexually explicit content, Australia has created a clear pathway for targeting this conduct in court. This sets Australia apart from many nations that see deepfakes as minor offences compared to fraud or hacking, overlooking the psychological, reputational, and safety-related harms that impact society as a whole.

Australia’s third approach embeds “AI risk” into national resilience strategies to increase private sector participation. The Security of Critical Infrastructure Act 2018 (SOCI Act) and its subsequent amendments mandates critical infrastructure (CI) operators to manage cyber risk and to report incidents, shifting emphasis from reactive enforcement to building preparedness. This approach fosters multistakeholder cooperation and ensures the government can monitor national security risks across the CI sectors. The law enables Australia’s Department of Home Affairs to build awareness of AI-enabled automatic attacks and help uplift capacity through the Trusted Information Sharing Network (TISN) where data from cyber incident monitoring is shared.

The fourth approach involves the timely update of public information on AI governance. The 2024 voluntary AI Safety Standard was succeeded by the Guidance for AI Adoption, accompanied a year later by “10 guardrails” to provide practical support for organisations that wish to adopt AI into their operations. The Guidance offers foundational information as well as implementation practices to build public confidence while managing risks. Specifically for cybercrime, the goal is to support secure AI development, supplier risk, access control, monitoring, and incident response. In addition to public-facing guidance, Australia has also published AI requirements for government policy use and issued additional protective direction where required. An example is the February 2025 directive to remove China-origin AI DeepSeek products from all government systems and mobile devices.

Australia's latest approach to combating AI-enabled crime is the collaboration between Australia's Police Forces with scientists from Monash University to produce digital tools that hamper the creation of deepfakes images. The AI-disrupter, 'Silverer', currently in the prototype stage, adds a protective layer on original images so they cannot be used by AI generators. The product will be made available for Australians who want to protect their uploaded images on social media and for law-enforcement to improve its capability.

For other countries, Australia's AI approach offers a compelling case study. Canberra's eSafety-style institutional model with its mix of civil powers with court escalation to remove harmful AI output from public domain provides a reference point for building victim-centred remedies. This framework prioritises rapid harm reduction without compromising options for criminal enforcement. But more than that, Australia's approaches to AI-enabled crime through legislation, CI sector risk management, and multi-stakeholders' innovation could be worthy of emulation.

Arguably, Australia may also benefit from the experiences of countries, especially those that have compatible governance and risk-mitigation perspectives in addressing AI-enabled crime. For example, the Department of Industry, Science and Resources has noted that Australia and Singapore share "human-centric" and trust-oriented AI frameworks. As such, Canberra may benefit to look into Singapore's approach of whole-of-community scam prevention and coordinated public advisories to raise awareness. Just as technology is developing, governance should too. For now, Australia's National AI Plan is the latest government policy to ensure that AI serves the people and keeps the nation safe, however the country should not be complacent to sit back and wait until the 2030 review to assess whether it is heading in the right direction.

About the Author

Dr Fitriani is a Senior Analyst with Australian Strategic Policy Institute's Cyber, Technology and Security Program. Her research focuses on hybrid threats in the Indo-Pacific, as well as foreign policy and non-traditional security issues.

The authors' views are their own and do not represent an official position of the S. Rajaratnam School of International Studies. Articles published in Science, Technology and Security may be reproduced only with prior permission. Please email the editor at kk.trajano@ntu.edu.sg

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg