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.

Artificial Intelligence, Cybercrime, and the Reassessment of Security | Karryl Kim Sagun Trajano, Benjamin Ang, and Ysa Marie Cayabyab

This issue builds on practical insights surfaced through the RSIS event, "AI-Enabled Cybercrime: Exploring Risks, Building Awareness, and Guiding Policy Responses." Organised by our Future Issues and Technology (FIT) research cluster in collaboration with our Digital Impact Research (DIR) team, the exercise saw policymakers, practitioners, and industry stakeholders stress-testing responses to AI-enabled cyber incidents in Singapore and the broader region. Led by Dr Gil Baram (Center for Long-Term Cybersecurity, University of California-Berkeley) and Mr Derek Manky (Fortinet), the discussions underscored a recurring theme reflected across this issue: AI does not merely introduce new threats; it changes how decisions must be made, often before intent, scope, or responsibility are fully clear.

AI is rapidly reshaping the cybercrime landscape, not by inventing entirely new forms of criminality, but by transforming the speed, scale, and organisation of illegal activities. In domains such as fraud, impersonation, malware deployment, and online exploitation, AI functions as a force multiplier. It compresses decision timelines, lowers barriers to entry, and complicates attribution and response. These shifts force a necessary reassessment of 'security' from the lenses of science and technology, where technical innovation intersects with governance capacity, institutional judgement, and policy design.

In this issue of Science, Technology, and Security, we curate perspectives that illuminate the evolution of AI-enabled cybercrime, the responses of states and institutions, and how existing security frameworks are being stretched. Rather than treating AI as an abstract or futuristic risk, the contributors examine how automation, generative systems, and algorithmic decision-making are already embedded in real-world criminal operations and policy responses. Collectively, the articles demonstrate that the true security challenge is less about technological novelty, and more about whether governance, legal, and organisational systems can function effectively under conditions of uncertainty.

At the regional level, Himal Ojha (United Nations Office on Drugs and Crime) situates AI-enabled cybercrime within Southeast Asia's rapid digitisation. He illustrates how automation and AI are being woven into every stage of criminal operations, from high-volume scam campaigns and adaptive malware to synthetic identities and cryptocurrency-enabled laundering. Crucially, Ojha highlights that these developments are not peripheral, but as part of increasingly industrialised criminal ecosystems that integrate cyber tools with financial crime, underground banking, and, in some cases, forced criminality. By prioritising operational realities over speculative risks, the article reframes AI-enabled cybercrime as a structural security challenge for Southeast Asia. It argues that the impact extends beyond individual victims, threatening broader financial stability and institutional trust.

Where Ojha maps the threat landscape, Helena Yixin Huang (RSIS) turns attention to the governance and decision-making pressures created by AI-enabled cyber incidents. Drawing on the October 2025 tabletop exercise, Huang argues that AI's primary impact lies in the compression of response timelines and the narrowing of margins for certainty, rather than in fundamentally changing criminal motivations or cybersecurity principles. Her analysis shows how early-stage responses are often shaped by organisational clarity, or the lack of it, and how attribution and escalation function as strategic policy choices rather than technical endpoints. By examining the interplay between uncertainty, speed, and institutional roles, the article contributes a governance-centred lens often absent from technically focused discussions of AI and cybercrime.

Complementing these perspectives, Dr Fitriani's (Australian Strategic Policy Institute) examination of Australia's approach to AI-enabled crime provides a concrete case study on operationalising principles into practice. Rather than pursuing AI-specific criminal statutes, Australia maintains a technology-neutral legal posture, instead leveraging on existing cybercrime, telecommunications, and online safety laws to address AI-enabled harms. The article illustrates how civil-regulatory mechanisms, such as the powers of the eSafety Commissioner, reinforce this framework, enabling rapid harm reduction even when criminal attribution is difficult or offenders are offshore. By highlighting amendments addressing non-consensual deepfake material and the embedding of AI risk into critical infrastructure resilience, Fitriani demonstrates how AI-enabled cybercrime governance can be distributed across criminal law, regulation, and institutional design.

Read together, the contributions underscore a shared insight: AI-enabled cybercrime exposes the limits of reactive, siloed, or purely technical responses. Automation and generative systems allow criminal activities to scale faster than traditional investigative, legal, and diplomatic processes were designed to handle. As a result, security outcomes increasingly depend on pre-established governance arrangements, cross-sector coordination, and established escalation pathways. The emphasis across the articles is not on abandoning existing frameworks, but on sharpening them so they can operate under conditions of speed, ambiguity, and cross-border complexity.

Ultimately, AI-enabled cybercrime serves as a vital case study for how societies must manage emerging technologies. The challenge is not simply to counter malicious uses,

but to ensure that security institutions, legal systems, and policy processes remain resilient in an AI-ubiquitous environment. By combining regional threat analysis, governance insights from applied exercises, and national policy responses, this collection aims to advance a more integrated understanding of AI, cybercrime, and security: one that recognises technology as inseparable from the institutional contexts in which it is governed.

About the Authors

Karryl Kim Sagun Trajano is a Research Fellow with the FIT research cluster at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Her research examines the intersection of policy, strategy, and emerging technologies, including artificial intelligence (AI), space, quantum, energy, and biotechnology, within Southeast Asia and the broader Asia-Pacific region.

Benjamin Ang is Head of the Centre of Excellence for National Security (CENS), FIT, and DIR at RSIS, NTU, Singapore. He leads the policy research think tank that focuses on national security aspects of cyber, hybrid threats, disinformation, foreign interference, extremism, emerging technologies, AI, quantum, space, biotech, energy, and smart cities.

Ysa Marie Cayabyab is an Associate Research Fellow at FIT. Her research focuses on the intersection of technology and society, examining the governance, public communication, and societal implications of emerging technologies.

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