Ponder the Improbable since 1996

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.

In this Bulletin

For the fifth issue of Science, Technology and Security (STS) Bulletin, we bring together perspectives that collectively illuminate how AI-enabled cybercrime is evolving, how states and institutions are responding, and where 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. Taken together, the articles demonstrate that the security challenge posed by AI-enabled cybercrime is less about technological novelty alone, and more about whether governance, legal, and organisational systems can function effectively under conditions of uncertainty. An introduction to artificial intelligence, cybercrime, and the evolving reassessment of security is also featured. Images below were generated by AI (imagine.art).

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

Automation, Artificial Intelligence, and the Evolving Cybercrime Landscape in Southeast Asia
Himal Ojha

Responding to AI-Enabled Cybercrime: Governance, Attribution, and Escalation
Helena Yixin Huang

Australia's Approach to Addressing AI-Enabled Crime
Fitriani

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

STS is edited by the FIT research cluster and features thought pieces on key emerging technologies, such as artificial intelligence (AI), space, quantum technologies, energy, and biotechnology. In this issue, we build on practical insights surfaced through the RSIS event, "AI-Enabled Cybercrime: Exploring Risks, Building Awareness, and Guiding Policy Responses." This tabletop exercise was organised by FIT in collaboration with Digital Impact Research (DIR) in October 2025. The event brought together policymakers, practitioners, and industry stakeholders to stress-test responses to AI-enabled cyber incidents in Singapore and the broader region. The discussions underscored a recurring theme reflected across this issue: AI does not merely introduce new threats, but changes how decisions must be made, often before intent, scope, or responsibility are fully clear. Click to read more.

Karryl Kim Sagun Trajano is a Research Fellow at FIT. Benjamin Ang is a Senior Fellow and oversees the FIT cluster. He is also the Head of the Digital Impact Research (DIR) and the Centre of Excellence for National Security (CENS) at RSIS. Ysa Marie Cayabyab is an Associate Research Fellow at FIT.

Automation, Artificial Intelligence, and the Evolving Cybercrime Landscape in Southeast Asia | *Himal Ojha*

This article situates AI-enabled cybercrime within Southeast Asia's rapidly digitising environment. It shows how automation and AI are embedded across every stage of the increasingly industrialised criminal ecosystems. Overall, this article reframes AI-enabled cybercrime as a structural security challenge for Southeast Asia, with implications extending beyond individual victims to financial stability and institutional trust. Click to read more.

Himal Ojha is a Global Cybercrime Programme Officer (Digital Forensics Expert) with the United Nations Office on Drugs and Crime (UNODC), based in Bangkok, Thailand. He oversees projects across Southeast Asia and the Pacific, providing capacity- building assistance to criminal justice authorities on digital forensics and cybercrime investigations.

Responding to AI-Enabled Cybercrime: Governance, Attribution, and Escalation | *Helena Yixin Huang*

This article focuses on the governance and decision-making pressures created by AI-enabled cyber incidents. Drawing on observations from the October 2025 tabletop exercise, it posits that early-stage responses are often shaped by organisational clarity, or the lack of it, and that attribution and escalation function strategic policy choices rather than technical endpoints. Overall, this article provides a governance-centred lens that is often absent from technically focused discussions of AI and cybercrime. Click to read more.

Helena Yixin Huang is an Associate Research Fellow at RSIS. Her research examines cybercrime, cybersecurity policies, and the governance of emerging technologies, with a particular focus on how evolving forms of digital criminality shape international and regional responses.

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

This article examines Australia's approach to AI-enabled crime, providing a concrete case study on operationalising principles into practice. Australia maintains a largely technology-neutral legal posture, instead leveraging on existing cybercrime, telecommunications, and online safety laws to address AI-enabled harms. Overall, this article shows how AI-enabled

cybercrime governance can be distributed across criminal law, regulation, and institutional design. Click to read more.

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.

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