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.

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

Across Southeast Asia, the rapid expansion of digital connectivity has generated substantial opportunities for growth, while simultaneously creating vulnerabilities that criminal networks have been quick to exploit. The emergence of automation and artificial intelligence (AI) is now influencing the region's cybercrime landscape in ways that are both increasingly sophisticated and operationally efficient. These technologies, originally catalysts for innovation and economic advancement, are being misused to enhance the reach, precision, and resilience of illicit online activities.

One area where this shift is most visible is in cyber-enabled fraud and scam operations. Automated systems and AI-driven tools are enabling criminal groups to deploy deceptive content at an unprecedented scale. Messages, calls, and online interactions can now mimic human behaviour with convincing accuracy, making fraudulent communications appear more authentic and personalised. Tasks that previously required significant manual effort—phishing campaigns, scam calls, identity misuse—are becoming increasingly streamlined. This allows malicious actors to target large numbers of potential victims simultaneously.

Another emerging trend is the deployment of automated bots to create and maintain mule accounts or evade verification safeguards. These capabilities facilitate more seamless movement of illicit funds, including through cryptocurrency channels, where speed and limited transparency often work to the advantage of criminal networks. As a result, the implications transcend individual financial loss, undermining confidence in digital ecosystems and financial institutions across the region.

Emerging Modalities: How Criminal Groups Use AI and Automation

Automation and AI are being integrated into criminal operations across Southeast Asia in several ways:

- Adaptive AI-enhanced malware: Malware is increasingly incorporating AI-generated components that adjust to different operating environments. This adaptability reduces detectability by security systems and enables longer, more damaging intrusions.

- Autonomous botnets and high-volume intrusion attempts: AI-enabled botnets can independently scan for vulnerabilities, bypass verification tools, and maintain large-scale phishing or spam campaigns with minimal human input.
- Deepfakes, synthetic identities, and impersonation tools: AI-powered synthetic media—including cloned voices and fabricated identities—are being used to circumvent identity checks or deceive victims through highly tailored social manipulation.
- Integration with larger criminal infrastructures: Automation and AI rarely operate in isolation. They reinforce broader networks involved in underground banking, cryptocurrency-based laundering, online illicit markets, and operations where individuals may be exploited or coerced into criminal activity.
- Lowering barriers to entry in cybercrime: The growing availability of ready-made AI tools and automation kits allows individuals with limited technical expertise to conduct complex attacks. This accessibility significantly broadens the pool of potential threat actors.

Implications for Southeast Asia

The fusion of automation, AI, and organised crime carries profound implications for the region:

- Significant financial repercussions: Cyber-enabled fraud in East and Southeast Asia resulted in an estimated USD 18–37 billion in losses in 2023. A substantial proportion of these activities is now amplified by automated or AI-enabled methods.
- Broader global impact: While many operations are based in Southeast Asia, their digital nature allows them to target victims worldwide, reinforcing the need for international cooperation.
- Increased operational agility for criminal groups: AI-driven malware, synthetic identities, and automated bots allow criminal actors to adapt rapidly, avoid detection, and operate at high velocity. Traditional investigative methods often struggle to keep pace with these advancements.
- Convergence with other criminal economies: Cyber-enabled crime is increasingly intertwined with illicit financial flows, underground banking, and situations of forced criminality within scam operations. This interlinkage magnifies the complexity and societal impact of these threats.
- Expansion of threat actors: As cybercrime tools become easier to access and deploy, the number of individuals and networks capable of engaging in such activities is likely to grow, adding further pressure on law-enforcement and regulatory bodies.

These factors signal a fundamental shift from opportunistic crime toward a highly structured, industrialised ecosystem where AI and automation act as strategic enablers.

Priority Strategic Areas for Action

- Elevating AI-enabled cybercrime as a high-priority risk: Policy, legal, and operational frameworks must adapt to the distinct characteristics of AI-driven threats, including their speed, scale, and technical complexity.

- Strengthening financial oversight and virtual asset regulation: As illicit proceeds often flow through cryptocurrency platforms, virtual asset service providers, or informal transfer systems, stronger regulation and monitoring are essential to limiting the financial pathways available to criminal actors.
- Enhancing regional and international collaboration: Given the cross-border nature of many cyber-enabled crimes, coordinated efforts among national authorities, regional bodies, and international organisations are crucial for effective disruption.
- Building technical capabilities and investigative readiness: Investment in digital forensics, AI-detection tools, specialised training, and broader capacity-building is vital to counter increasingly adaptive threats. These capabilities are essential for identifying emerging patterns and strengthening operational responses.

Conclusion

The convergence of automation, AI, and organised criminal activity presents a particularly complex challenge for Southeast Asia. What distinguishes this emerging threat landscape is not simply the adoption of new technologies, but the integration of AI into every stage of criminal lifecycle—from initial contact with victims to the movement of illicit proceeds. This allows criminal networks to operate more efficiently, adapt more rapidly, and target victims across borders with greater ease.

If left unaddressed, AI-enabled cybercrime risks becoming deeply entrenched, evolving into more resilient and opaque forms over time. To counter this, a balanced, and comprehensive approach is essential. This must combine updated legislation, strengthened financial oversight, regional cooperation, and targeted investments in technical expertise to safeguard the region's digital environment and limit the ability of criminal groups to exploit technological advancements.

About the Author

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.

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