

The New Face of Cybercrime: Scam Factories and Polycriminality

Federico Varese

To cite this article: Federico Varese (2026) The New Face of Cybercrime: Scam Factories and Polycriminality, The RUSI Journal, 171:4, 102-105, DOI: [10.1080/03071847.2026.2683253](https://doi.org/10.1080/03071847.2026.2683253)

To link to this article: <https://doi.org/10.1080/03071847.2026.2683253>



Published online: 16 Jun 2026.



Submit your article to this journal [↗](#)



Article views: 260



View related articles [↗](#)



View Crossmark data [↗](#)



The global geography of cybercrime.
Courtesy of Oleksii/Adobe Stock.

The New Face of Cybercrime

Scam Factories and Polycriminality

Federico Varese

In recent years, the face of cybercrime has changed radically. It is no longer just a matter of isolated hackers breaking into computer systems, but rather a global industry of fraud and extortion. It is organised and territorially rooted, and involves hundreds of thousands of people. The case of the ‘scam factories’ in Southeast Asia, particularly in Cambodia, Myanmar and China, is the clearest example of this transformation. Moreover, cybercrime is increasingly intertwined with the geopolitical objectives of countries such as the People’s Republic of China and Russia. Analysts must adapt their data collection tools accordingly.

Most information on cybercrime concerns victims, the costs for companies and citizens, and the countries targeted by operations. By contrast, the geography of production remains surprisingly opaque: where do digital frauds originate and thrive?

Lately, several territorial hubs have emerged clearly. Among these is Southeast Asia. Here, online fraud is not an activity carried out by individuals or small groups, but a form of production organised in large-scale enterprises. Clashes along the border between Thailand and Cambodia in 2025 and 2026 forced some ‘entrepreneurs’, often of Chinese nationality, to abandon their operational facilities, which were subsequently taken over by the Thai army. Reporters from *Reuters* and *New York Times* visited the sites from which the scams were launched.

According to them, such places resembled bank branches with motivational slogans on the walls: ‘Nothing is impossible’; ‘Making money matters the most’.¹

Authorities have found detailed dossiers on targets. For example, a Japanese pensioner with phone number and bank statements, and an American woman who had shared sensitive personal data. When a financial scam failed, operators moved on to sexual extortion, even exploiting intimate images generated through AI to blackmail users. Interpol estimates that AI-enhanced frauds are up to 4.5 times more profitable than traditional ones.²

The ‘employees’ of these scammer enterprises are subjected to a punitive labour regime and are themselves often victims of trafficking. They are recruited under false promises, deprived of their documents and forced to work under threat. Those who fail to meet daily scam quotas are punished. Scam factories have developed into fully-fledged firms, with several functions internalised in a single structure. Interpol has coined the term ‘polycriminality’, in which scams intersect with human trafficking, money laundering, terrorism and illegal digital markets. In some cases, the premises of these prison-like compounds have been used to launch drones during the conflict between Thailand and Cambodia.³ In recent months, more than 100,000 people have fled from these compounds due to the conflict. Many have poured into Phnom Penh in search of help, in

1. Poppy McPherson and Tim Kelly, ‘Scammers’ Abandoned Cambodia Compound Exposes Brutality and Banality of Fraud’, *Reuters*, 6 February 2026; Hannah Beech, ‘At This Office Park, Scamming the World was the Business’, *New York Times*, 13 January 2026.

2. Online fraud caused approximately \$442 billion in losses in 2025 worldwide and is now among the main global criminal threats. See Interpol, ‘Global Financial Fraud Threat Assessment’, Second Edition, March 2026.

3. *Ibid.*

what Amnesty International has described as a 'humanitarian crisis'.⁴

This combination of coercion, organisation and technology is not an anomaly. According to an Interpol report published in March, scam centres are no longer confined to Southeast Asia but now also exist in the Middle East, North and West Africa and Central America, and involve trafficked individuals from nearly 80 countries.⁵ Repression in one place often displaces the phenomenon to another. This was the case with anti-mafia efforts in Italy in the 1960s and 1970s, which contributed to the spread of organised crime from the south to the north of the country, and with anti-gang policies in the US, which fostered the emergence of maras in Central America.⁶

But not all countries are likely to host scam factories. Therefore, a key question is: what accounts for the emergence of these production units in one locale and not in another?

In parallel, other forms of cybercrime also display a similar evolution towards industrial models. As Anja Shortland observes in her new book, *We Know You Can Pay a Million: Inside the Dark Economy of Hacking and Ransomware*, ransomware is no longer developed by individual hackers but produced by specialised groups who develop code, distribute it and negotiate ransoms according to standardised procedures.⁷ For example, the Russian government tolerates their operations as long as they do not target Russian nationals and their targets include foreign political and military objectives.⁸

Therefore, a key question is: what accounts for the emergence of these production units in one locale and not in another?

A research group based at the University of Oxford and Sciences Po in Paris, funded by the European Research Council, is mapping the global geography of cybercrime starting from its sites of production.⁹ Their analyses, which have produced a World Cybercrime Index, confirm that cybercrime is organised into distinct geographical clusters associated with specific types of offences. For example, criminals based in Romania specialise in data and identity theft; those in Iran and North Korea in attacks and extortion; and US- and UK-based scammers are cashing in the proceeds. Russia, Ukraine and China are significant nodes in almost all types of crime, and India is an emerging power in this ecosystem.¹⁰

There is therefore no single 'cybercrime', but rather a plurality of digital criminal economies, each with its own territorial bases, organisational models and divisions of labour. Such work will help to identify the factors that make each country more or less vulnerable to cybercrime by incorporating the World Cybercrime Index as a dependent variable in multilevel statistical models.

Despite the rhetoric of 'borderlessness', the production of cybercrime is concentrated in specific locations, where low labour costs, institutional collusion, criminal networks and access to technology seem to converge. Combating this phenomenon therefore requires a radical shift in perspective. It is not enough to protect victims or to counter individual operations. It is necessary to intervene in the places and infrastructures of production, and to initiate serious international cooperation. Unfortunately, the current state of the world renders this perspective utopian. We may therefore add another victim of today's global disorder: the fight against cybercrime. ■

Federico Varese is Professor of Sociology at Sciences Po, Paris, and Senior Research Fellow at Nuffield College, Oxford, where he is also the Director of the Extra-Legal Governance Institute.

4. Amnesty International, 'Cambodia: Growing Humanitarian Crisis as Escaped Scamming Compound Survivors Tell of Murder, Rape and Torture', 27 January 2026, <<https://www.amnesty.org/en/latest/news/2026/01/cambodia-growing-humanitarian-crisis-as-escaped-scamming-compound-survivors-tell-of-murder-rape-and-torture/>>, accessed 17 April 2026.

5. Interpol, 'Global Financial Fraud Threat Assessment'.

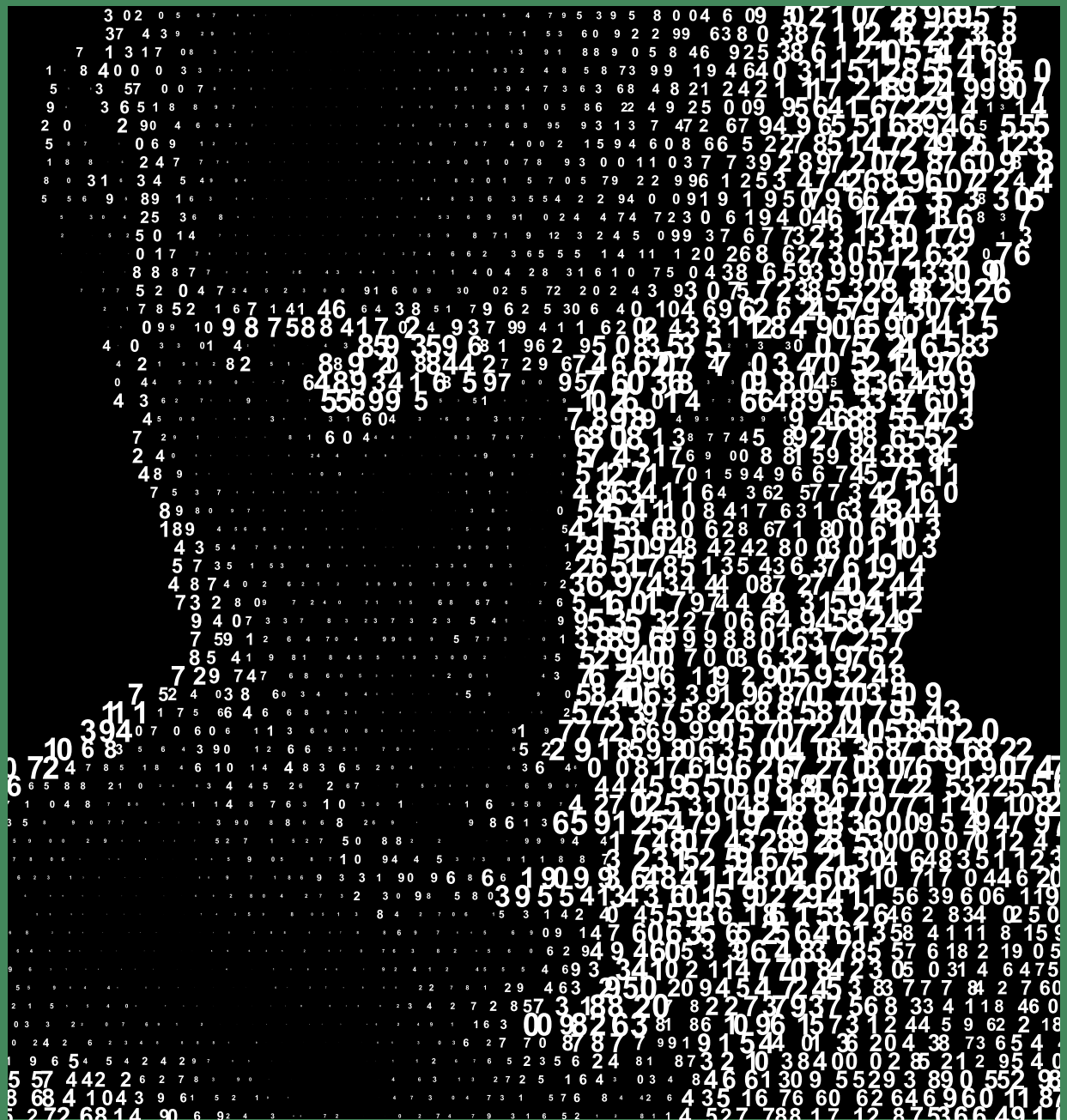
6. Federico Varese, *Mafias on the Move* (Princeton, NJ: Princeton University Press, 2011).

7. Anja Shortland, *We Know You Can Pay a Million: Inside the Dark Economy of Hacking and Ransomware* (London: Profile Books, 2026).

8. Federico Varese, *Russia in Four Criminals* (Cambridge: Polity Press, 2024).

9. European Research Council, 'CRIMGOV', <<https://cordis.europa.eu/project/id/101020598>>, accessed 22 May 2026, Grant Agreement Number 101020598, principal investigator: Federico Varese.

10. Miranda Bruce et al., 'Mapping the Global Geography of Cybercrime with the World Cybercrime Index', *PLOS One* (Vol. 19, No. 4, 2024).



Courtesy of Login/Adobe Stock.