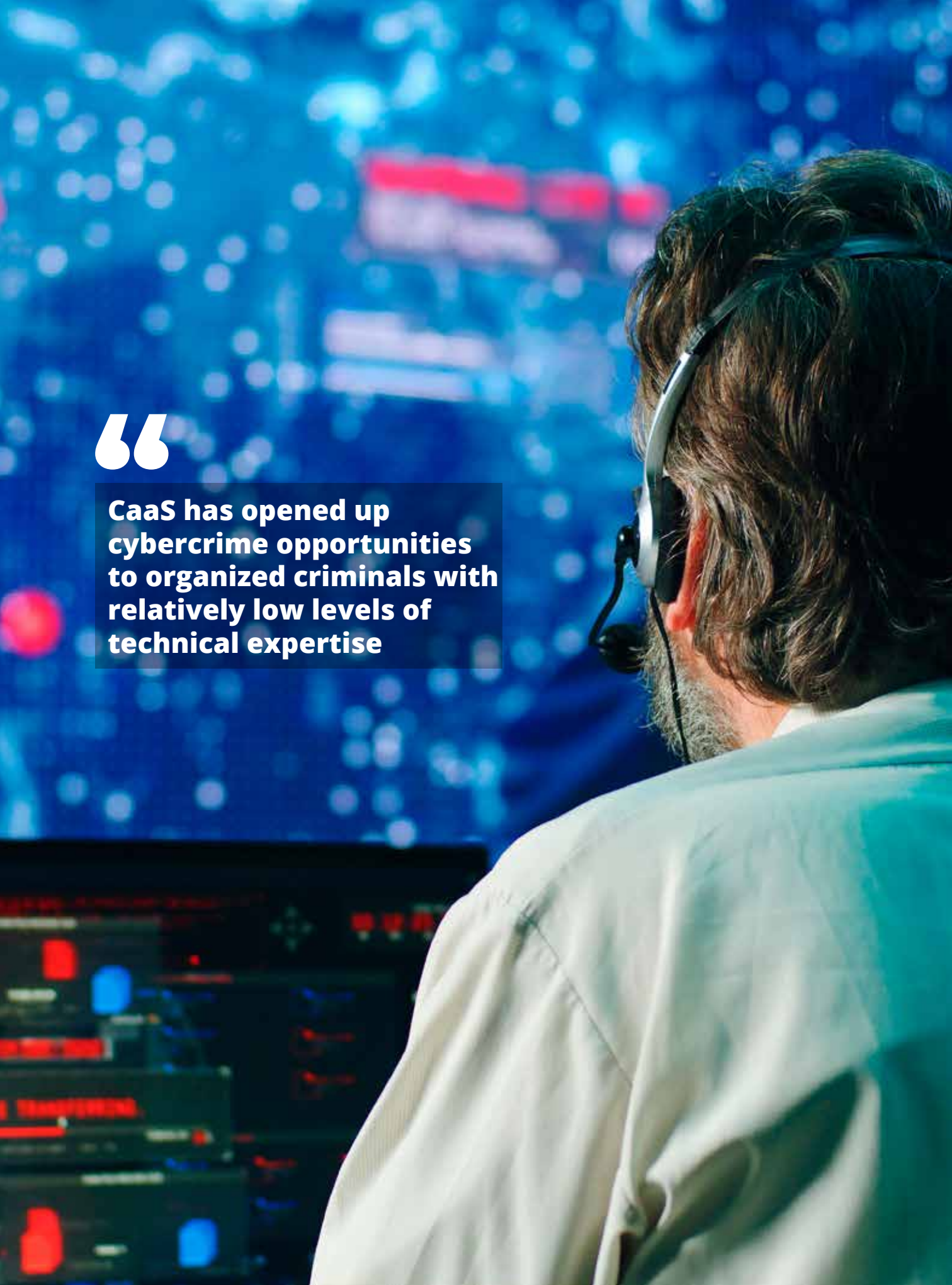

> **CaaS has opened up cybercrime opportunities to organized criminals with relatively low levels of technical expertise**

Tracking the unseen: measuring the financial impact of cybercrime

by **Seán Doyle** and **Giulia Moschetta**

As the global economy digitizes, cybercriminals have ignored any and all attempts at deglobalization.[1] Their technical and personal networks continue to expand across regions, making it increasingly difficult to disrupt online criminal activities.

In the United States of America alone, the Federal Bureau of Investigation (FBI) reports that victim complaints exceeded USD 16 billion in 2024.[2] Research from the Global Anti-Scam Alliance suggests that scammers stole more than USD 442 billion worldwide in 2024-25.[3]

Changing structure and culture of cybercriminal groups

Cybercriminal activities are shifting – metaphorically and literally – into the sphere of traditional transnational organized crime groups.[4] They build on a trend spanning more than a decade in which technically sophisticated cybercriminals have withdrawn from roles as the direct executors of primary offences, such as a ransomware attack, to become developers and providers of criminal services. Their activities range from malware creation to ransom negotiation, and are known collectively as "Cybercrime-as-a-Service" (CaaS).

CaaS has opened up cybercrime opportunities to organized criminals with relatively low levels of technical expertise. Apart from increasing the pool of cybercriminals and the volume of attacks, this marked a turning point in the culture of cybercriminals: from a group that generally tried to bypass law enforcement attention by avoiding crimes that directly resulted in death or physical harm, to a culture where active disruption of key services, including disruption leading to death[5], such as by shutting down a hospital, has become common.

1 World Economic Forum, Global Cybersecurity Outlook 2026, January 2026.

2 Federal Bureau of Investigation Internet Crime Report 2024.

3 Global Anti-Scam Alliance, Global State of Scams 2025 Report.

4 As one example, see the movement of the Black Axe criminal network and cult into cyber-enabled fraud, "United States Attorney's Office, District of New Jersey, Prominent Leader of Black Axe Extradited to United States for Conspiring to Engage in Internet Scams and Money Laundering, 16 December 2024.

5 BBC, Ransomware attack contributed to patient's death", 25 June 2025.

New technologies, new markets, new victims

Technologies such as generative artificial intelligence (GenAI) and AI-supported deepfakes are making it easier for cybercriminals to enter new markets at low cost, by supporting translation of social engineering tricks into impersonations that are culturally credible in multiple countries and support initial access into the victim's systems (if an organization) or trust (if an individual).[6]

These technologies allow criminal groups who might previously have focused on populations with widely spoken languages like English, Mandarin, French, Russian, Arabic and Spanish, to target new populations of victims, in countries where traditional cybercriminal social engineering tactics had previously not been successful.

What is the impact of cybercrime on societal security?

Cybercrime's growth requires urgent attention. The funding it provides to organized crime creates an ongoing risk of state capture in some jurisdictions,[7] and challenges in countering it can exacerbate tensions between states where victims are concentrated and states from which cybercriminals operate.[8]

The culture of cybercrime is also changing – for the worse. This is occurring globally, with some of

the starkest examples in Anglophone regions where there has been an increase in "cyber thuggery",[9] as a reference to the rising risk appetite of cybercriminal groups with a lower age profile, from mid-20s to late teens.

An example of this is "the Com" a shifting community of more than a thousand – mostly young - hackers whose activities, according to the US FBI, are spread across cyber-enabled and violent crime, like "swatting/hoax threats, extortion/sextortion of minors, production and distribution of child sexual abuse material, violent crime, and various types of cyber crimes."[10]

---

6 Europol, Steal, Deal and Repeat - How Cybercriminals Trade and Exploit Your Data – *Internet Organised Crime Threat Assessment, Publications Office of the European Union, Luxembourg, 2025.*

7 Assessment based on multiple sources including, Amnesty International, "I was someone else's property": Slavery, Human Trafficking and Torture in Cambodia's Scam Compounds, 26 June 2025.

8 International Crisis Group, Border Dispute with Cambodia Sparks Political Disarray in Thailand, 1 July 2025. See also tensions between Thailand and Myanmar, CNN Power Cut to Site of Global, Billion-Dollar Scam Industry. But Will It Halt the Swindling?, 5 February 2025.

9 Martin, Ciaran, Thugs, Thieves and Other Threats: How What We Need to Worry About in Cyberspace is Changing, 16 September 2025.

10 FBI Public Service Announcement I-072325-3-PSA, The Com: Theft, Extortion and Violence are a Rising Threat to Youth Online, 23 July 2025.

> **"The FBI describes the motivations behind the crimes as varied, but extending beyond pure financial gain to include "retaliation, ideology, sexual gratification, and notoriety."[11]"**

Similar to the script kiddies[12] more prevalent in the early 2000s and largely motivated by entertainment or notoriety, today's emerging cybercriminal groups often rely on relatively unsophisticated social engineering techniques to gain access to systems.[13] Yet, the level of harm they can inflict is now significantly greater, due to the deep interconnectivity and interdependence of digital supply chains. Groups like Scattered Spider appear to be connected with online violent subcultures and have been cited as the source of cyber-attacks on manufacturing giants such as Jaguar Land Rover and retail chain M&S in the United Kingdom.[14] The shift we are witnessing is not so much in the choice of targets as in the nature of the attacks themselves; contemporary attacks increasingly aim to disrupt or halt the operations of critical services such as manufacturing, healthcare, and food supply.

Is there an impact on state security?

Governments may already be adopting similar approaches, with the focus of cyber-attacks moving from espionage to coercion. For example, in August 2025, Norway blamed an adversarial state, or attackers in sympathy with it, for a cyber-attack that targeted the operations of a dam. The cyber-attack released large volumes of water over several hours and was interpreted by the Norwegians as an attempt to demonstrate destructive capability without acting on it.[15] Otherwise put, the aim of the attack was seen as supporting the attacker's political goals by intimidation.

We are getting better at disrupting cybercriminal networks

Law enforcement is steadily improving in its ability to coordinate cybercrime disruption across borders, enhancing the insights it gains into cybercriminal activities by working in partnership with experts in the private sector.

Cross-border operations, like the joint INTERPOL and Afripol Operation Serengeti 2.0 in 2025, supported by actionable insights into cybercrime from stakeholders outside law enforcement authorities, are now more frequent, more sophisticated and increasingly effective in dismantling international criminal networks.[16] Europol's European Cybercrime Centre (EC3) regularly relies on its network of operational partnerships with Internet security providers, financial services and telecommunication providers to increase the impact of its operations and investigative efforts across European and extra-European Member States. [17]

In Operation Serengeti 2.0, INTERPOL acted as a hub for sharing expertise and threat assessments between law enforcement, the private sector and non-governmental collaborations like the World Economic Forum-hosted Cybercrime Atlas, which

[11] *Ibid.*
[12] Okta, Script Kiddies and Skiddies: Identifying Unskilled Hackers, 2 September 2024.
[13] Sans, Defending Against Scattered Spider and the Com with Cybercrime Intelligence, 4 July 2024.
[14] BBC, Tidy, Joe "M&S Hacker Claims to be Behind Jaguar Land Rover Cyber Attack, 3 September 2025.
[15] Politico.eu, Russian Hackers Took Control of Norwegian Dam, Police Chief Says, 13 August 2025.
[16] Doyle, Seán and Umansky, Natalia, Cybercrime Is Borderless. This Global Bust Shows Law Enforcement Can Be Too, 27 August 2025.
[17] For example, Europol and Microsoft Disrupt World's Largest Infostealer, Lumma, 21 May 2025.

is a hub for the generation and distribution of private sector insights into cybercriminal networks.[18] The principles for developing sustained and effective operational partnerships to counter cybercrime[19] are now well-known, repeatable and integrated into international law enforcement trainings.

The accelerating scale and impact of cyber-enabled fraud call for systemic defence

Phishing and cyber-enabled fraud are a growing global threat to users, consumers, organizations, and countries. According to Global Cybersecurity Outlook 2026 survey data, 73% of respondents reported that they or someone in their network had been personally affected by cyber-enabled fraud in 2025.[20] Recognizing the need to rebalance responsibility for cybersecurity, the World Economic Forum's Partnership Against Cybercrime – together with the Institute for Security and Technology (IST) – have published the white paper "Fighting Cyber-Enabled Fraud: A Systemic Defence Approach."[21] Building on the Partnership's progress in fostering public–private operational collaboration, this white paper seeks to advance shared responsibility across the digital ecosystem by stimulating coordinated action and required policy reforms, led by key stakeholders.

This Systemic Defence framework calls on stakeholders to act across 3 pillars:

1. **Prevention** by embedding safeguards at the foundational layers of the Internet to reduce threat actors' ability to acquire, build, or operate digital infrastructure for malicious purposes.

Actions could include strengthening risk-based due diligence and oversight in domain registration and hosting, to detect and prevent misuse long before harm occurs.

2. **Protection** by ensuring safety by default, such as by embedding scalable solutions for consumer-facing services to shield users from phishing and cyber-enabled fraud. Governments can accelerate adoption and impact through national coordination hubs, enabling regulation, and targeted incentives.

[18] World Economic Forum, Cybercrime Atlas Annual Impact Report 2025, October 2025.
[19] World Economic Forum, Disrupting Cybercrime Networks: A Collaboration Framework, November 2024.
[20] World Economic Forum, Global Cybersecurity Outlook 2026, January 2026.
[21] World Economic Forum. (2025) Fighting Cyber-Enabled Fraud: A Systemic Defence Approach. November 2025.

3. **Mitigation** by improving ecosystem-wide capability to identify abuse, enable effective reporting, and share actionable signals, while also supporting rapid response, to both takedown malicious activities from upstream infrastructure and update downstream protection efforts.

With phishing and cyber-enabled fraud growing at an alarming rate – driven in part by cybercriminals' use of AI – stronger defences must be built with appropriate safeguards to ensure that legitimate users are protected from criminal abuse.

About the Authors

Seán Doyle leads the Cybercrime Atlas, an open-source investigations and applied research collaboration hosted at the World Economic Forum in Geneva, Switzerland. He has been at the World Economic Forum's Centre for Cybersecurity since its launch in 2018, leading the Forum's research into how organization's respond to cyberthreats while also building collaborations in cross-sector intelligence sharing. Before moving into cyber, Seán worked in cross-border financial crime intelligence and asset tracing. His career started as an Armed Forces Analyst focusing on Eastern Europe and the Former Soviet states.

Giulia Moschetta leads the Partnership against Cybercrime, an initiative fostering public–private collaboration to combat cybercrime, at the World Economic Forum's Centre for Cybersecurity. She also leads the Global Cybersecurity Outlook, the Forum's annual flagship report on key cybersecurity trends. She previously held roles at NATO and within the Italian government.