Neapolis University Pafos, Cyprus
AI-Z-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by the European Union

Policy Brief

Cyber-Attacks and the

Model of Crime-as-a-Service

NUP Jean Monnet / UNESCO Policy Briefs

46/2026

Co-funded by the European Union

Neapolis University Pafos

UNESCO Chair in Human Development, Security & the Fight against Transnational Crime and Illicit Trafficking in Cultural Property

unesco Chair

The NUP Jean Monnet / UNESCO working papers and policy briefs can be found at:

https://www.nup.ac.cy

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP UNESCO/JEAN MONNET WORKING PAPER or POLICY BRIEF NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

Cyber-Attacks and the Model of Crime-as-a-Service

Executive Summary

Europol's Spotlight Report 'Cyber-Attacks: The Apex of Crime-as-a-Service' (2023) presents a detailed assessment of the growing sophistication, scale, and organisation of cyber-attacks across the European Union. The report illustrates how ransomware, distributed denial-of-service (DDoS) operations, and data theft have evolved within a highly professionalised underground economy where cybercriminals increasingly operate as service providers.

The Crime-as-a-Service (CaaS) model allows even unskilled actors to purchase access to malware, stolen data, or compromised systems, fuelling an ecosystem that combines financial, ideological, and opportunistic motives. The report positions ransomware as the most dominant and disruptive cybercrime threat, supported by affiliate networks, Initial Access Brokers (IABs), and infrastructure rental services.

Europol's analysis underscores that cyber-attacks now represent the apex of this model—where services, expertise, and tools converge into industrial-scale operations. The report calls for a unified European approach to enhance resilience, strengthen public-private cooperation, and build investigative capacity against cyber-enabled organised crime.

Keywords

Europol, Cybercrime, Ransomware, DDoS, Malware-as-a-Service, Initial Access Brokers, Crime-as-a-Service, Cybersecurity, EC3, Digital Forensics.

Background

The Europol Spotlight Report series provides targeted analyses of emerging criminal phenomena, complementing the agency's annual Internet Organised Crime Threat Assessment (IOCTA). The 2023 edition focuses on cyber-attacks as the apex of the Crime-as-a-Service ecosystem, drawing on Europol's operational data, national law enforcement contributions, and industry intelligence.

This assessment demonstrates how cybercrime has evolved from isolated incidents into a systemic threat to economic stability, critical infrastructure, and public trust. The convergence of cyber and organised crime, combined with growing technical specialisation, enables threat actors to execute complex operations at scale. Through its European Cybercrime Centre (EC3), Europol coordinates operational responses, facilitates intelligence-sharing, and develops digital forensics capabilities to counter this threat.

Key Findings and Trends

The report highlights several interrelated developments defining the current cyber threat landscape:

• Ransomware as the Primary Threat: Ransomware remains the most pervasive and profitable cybercrime. Modern groups operate under an affiliate model, where developers provide malware to partners who execute attacks and share profits.

• Initial Access Brokers (IABs): IABs sell compromised credentials and network access, serving as crucial enablers of ransomware and data theft operations. This specialisation streamlines cybercrime and reduces entry barriers.

• DDoS and Extortion: Distributed denial-of-service attacks are increasingly used for extortion or distraction, often linked to politically motivated groups or financially driven actors offering DDoS-as-a-Service.

• Data Theft and Exfiltration: The focus of many attacks has shifted from encryption to data exfiltration. Stolen data is sold, leaked, or used to extort victims, amplifying reputational and legal damage.

• Malware-as-a-Service Ecosystem: Ready-made malicious software, infrastructure hosting, and laundering services create a complete supply chain for digital crime.

These developments confirm that cybercrime has reached an industrial scale, where roles are divided, risks outsourced, and profits maximised through global collaboration among criminal networks.

Operational and Policy Implications

The industrialisation of cybercrime presents significant operational and policy challenges for law enforcement and policymakers across the EU.

• Professionalisation of Criminal Ecosystems: Cybercriminals increasingly mirror legitimate business structures, with hierarchies, service contracts, and reputation systems on underground forums.

• Cross-Border Complexity: Attacks frequently span multiple jurisdictions, complicating evidence collection, attribution, and prosecution.

• Infrastructure Resilience: The reliance of essential services on interconnected digital systems amplifies the potential impact of cyber-attacks.

• Public-Private Partnerships: Cooperation with cybersecurity firms and financial institutions is crucial to identify threats early and disrupt infrastructure.

• Capacity Building: Continuous training, digital forensic tools, and AI-assisted analysis are essential for effective detection and response.

The report stresses that the response must combine preventive measures, intelligence coordination, and judicial cooperation to dismantle the ecosystem enabling cyber-attacks.

Europol's Response and Strategic Outlook

Europol's European Cybercrime Centre (EC3) leads the EU's operational response to cyber-attacks, coordinating investigations and capacity building. The report details several initiatives, including joint operations and the strengthening of the Joint Cybercrime Action Taskforce (J-CAT). Key actions include:

- Supporting major takedowns of cybercrime infrastructure and marketplaces;
- Providing real-time intelligence exchange among national cyber units;
- Expanding forensic expertise and threat intelligence capabilities;
- Facilitating cooperation with third countries and international organisations.

Europol's strategic outlook focuses on pre-emptive disruption, integrating cyber threat intelligence into broader law enforcement operations, and enhancing preparedness through EU-funded innovation programmes.

Strategic Recommendations

To strengthen resilience and counter the growing sophistication of cyber-attacks, Europol proposes several strategic priorities:

• Enhance Threat Intelligence Sharing: Improve real-time data exchange between national cyber units, Europol, and private partners.

• Promote Public-Private Cooperation: Institutionalise cooperation with technology companies and CERTs to ensure rapid response and mitigation.

• Develop Cyber Hygiene Standards: Support education and awareness campaigns to reduce exposure to phishing and credential theft.

• Expand Forensic and Analytical Capacity: Invest in AI-driven digital forensics, malware analysis, and evidence correlation.

• Advance Legal and Policy Frameworks: Strengthen cross-border data-sharing protocols and harmonise criminal law related to cyber offences.

• Enhance Attribution and Sanctions: Support coordinated EU and international efforts to identify, sanction, and deter major cyber actors.

These recommendations underline that combating cyber-attacks requires sustained cooperation, technical innovation, and policy coherence at the EU level.

Concluding Remarks

Europol's 'Cyber-Attacks: The Apex of Crime-as-a-Service' report depicts a mature, interconnected criminal economy that thrives on the commoditisation of cybercrime tools and services. Addressing this threat demands a combination of deterrence, resilience, and proactive intelligence-led enforcement.

The report concludes that cyber-attacks now represent not only a technological but also a systemic challenge to EU security. Law enforcement agencies must adapt through collaboration, innovation, and long-term investment in skills and technology. Only through coordinated European and international action can the cycle of digital crime-as-a-service be effectively disrupted.

Further Reading

- Europol (2023), 'Spotlight Report: Cyber-Attacks – The Apex of Crime-as-a-Service' (link)