DOI: 10.38146/BSZ-AJIA.2024.v72.i9.pp1707-1714

Europol's role in the fight against cybercrime

Europol European Cybercrime Centre
Europol
O3@europol.europa.eu

Csaba Szabó ✉
PhD, deputy editor-in-chief, associate professor, police lieutenant colonel
Ministry of Interior,
Editorship of Belügyi Szemle/
Academic Journal of Internal Affairs,
University of Győr,
Deák Ferenc Faculty of Law and Political Sciences
csaba.szabo3@bm.gov.hu

Abstract

Aim: The aim of the study is to present the role and activities of Europol's European Cybercrime Centre (EC3) in combating cybercrime, with a particular focus on the latest technological solutions and cooperation mechanisms.
Methodology: The research involved analysing the strategies and tools employed by the EC3. Data collection and analysis utilised Europol's internal reports, publicly available sources, and case studies to provide a comprehensive overview of EC3's activities and effectiveness.
Findings: The EC3 plays a crucial role in the fight against cybercrime, particularly in dealing with transnational criminal organisations and advanced cyber threats. The EC3 is divided into three main divisions: the operational unit, the digital support unit, and the expertise unit. The operational unit maintains four permanent analytical projects, each focusing on different areas of cybercrime.
Value: The study provides valuable insights into the functioning of the EC3 and its contributions to the global fight against cybercrime. It highlights Europol's effective cooperation model, which aids in international collaboration against cyber threats. EC3's activities significantly enhance information sharing and operational cooperation among member states, thereby increasing the effectiveness of defences against cybercrime.

Keywords: cybercrime, Europol, cybersecurity, transnational criminal organisations

The manuscript was submitted in English. Reciecved: 22 May 2024. Revised: 15 July 2024. Accepted: 23 July 2024.

✉ Corresponding author with the permission of Europol.

Cybercrime in the past decades

To understand Europol’s role in the fight against cybercrime we first have to understand how the phenomenon has evolved over the past decades and what are the dangers it poses.

At the turn of the millennium the world had already gone online, which meant that everyone connected to the world wide web had become susceptible to the early forms of cybercrime. The early 2000s was the golden era for computer worms,[1] that were shared through email attachments and infected websites, while leveraging vulnerabilities in applications to spread themselves to other users. While the intent behind some of the most infamous campaigns (e.g. LOVEBUG [URL1]) was unclear, the damages caused to the infected systems were immense. The same could be said about hackers launching distributed denial of service (DDoS) attacks that were able to take down many international commercial websites like Yahoo, Amazon, CNN and others (URL2).

It didn’t take long before criminals started looking for ways to monetise these novel forms of crime, which gave rise to online scams and the spread of banking Trojans (e.g. Zeus [URL3]) aiming to steal people’s money and personal information. Coincidentally, the Zeus banking Trojan also became one of the most well-known pioneers of cybercrime being offered as a service, as the actors behind the operation started licensing their code to other cybercriminals to carry out their attacks. Infecting a computer with the Trojan gave the operators full control over the system, which in addition to stealing the victim’s credit-card details, also allowed to them to deliver malware to the system and/or add the device to their botnet.[2]

The first versions of ransomware also started appearing around the same time as Zeus but it was not until 2013, when Crypto Locker appeared in the wild, that the world started to understand the devastating effects of modern ransomware campaigns. Crypto locker ransomware used 2048-bit RSA encryption and leveraged botnets (Gameover Zeus botnet) in addition to the more conventional distribution methods, to increase its reach (URL4). By this time, the first cryptocurrencies, which criminals could abuse to hide their illicit proceeds, had already hit the market. These evolutions had set the stage for what can be described as the modern era of organised, service-based cybercrime.

[1] Self-propagating malicious computer program (i.e. malware).
[2] Network of infected devices that can be used to distribute malware and/or launch DDoS attacks.

Law enforcement response

In response to these emerging threats, Europol's European Cybercrime Centre (EC3) was established in 2013. Today, EC3 consists of three branches – Operations, the Digital Support and the Expertise and Stakeholder Management units. The operational unit houses 4 permanent Analysis Projects (APs) each dedicated to a specific cybercrime area:

- AP Cyborg – cyber-dependant crime;
- AP Terminal – online fraud schemes;
- AP Twins – online child sexual exploitation;
- AP Dark Web – cross-crime cyber facilitators (e.g. bulletproof hosting, counter-antivirus services, criminal use of the Dark Web).

In addition, EC3 also hosts the Joint Cybercrime Action Taskforce (J-CAT), which consists of a standing operational team of cyber liaison officers from 13 EU Member States (MS) and 7 non-EU cooperation partners. The J-CAT operates in tandem with EC3 operational teams to drive intelligence-led, coordinated action against key cybercrime threats and targets.

Modern cybercrime threat landscape

In the course of the last ten years, the cybercrime threat landscape has evolved into a highly-specialised underground economy for transnational criminal networks and (infra) structures (URL5).

Criminal networks in all cybercrime areas are often composed of geographically dispersed actors and their operations are ran on complex infrastructure that is hosted across the globe, making it resistant to LE take-downs. Due to the borderless nature of cybercrime, the victims of the offences are almost always international, spanning across multiple jurisdictions, regions and even continents.

The service-based criminal economy has also lowered the entry-barrier both in terms of the required technical skills as well as the time and resource investment necessary to set up the operations. For example, ransomware-as-a-service (RaaS) providers lend out their malicious code to other cybercriminals in exchange of a percentage of their criminal proceeds.

Offenders from all areas of cybercrime take advantage of hosting and anonymity services in their online activity to avoid law enforcement (LE) detection and identification. Most common examples are bullet-proof hosting (BPH) services and virtual private network (VPN) providers catering to criminals, which enable them to set up their infrastructure as well as to connect to their victims and each other through proxies.

Cryptocurrencies also play a huge role in the laundering of cybercrime proceeds. In addition to not being tied to centralised financial institutions or to the identities of the wallet owners, the transactions on the blockchain can be made more difficult to trace through the use of cryptocurrency mixers[3] and swapping services[4].

Dark Web forums and marketplaces supply criminals with all the necessary tools, services and stolen data to carry out attacks, while also serving as platforms for knowledge sharing and recruitment.

These transformations, combined with the increasing anonymity offered by modern communication technologies contribute to the continued increase of new and old forms of cybercrime.

Fight against modern forms of cybercrime

Due to the transnational nature of cybercrime, only an internationally coordinate LE response can be effective to identify the offenders and disrupt their operations. To this end, EC3 plays a unique role in identifying high-value targets (HVT), coordinating international LE operations and providing technical support to EU MS and to countries with operational cooperation agreements with Europol.

EC3 operational teams and the J-CAT facilitate the joint identification, prioritisation, initiation and execution of cross-border investigations against key cybercrime threats and targets. These actions are intelligence-led as Europol is in a position to identify cross-matches and overlaps in national criminal investigations and coordinate the international operations involving law enforcement agencies (LEAs) from numerous countries. This approach is the key to fighting international criminal networks because, as discussed earlier, the actors, their victims and infrastructure are scattered across multiple jurisdictions.

This approach has led to the takedowns of EMOTET (URL6), which is one of most significant botnets of the past decade, RaidForums (URL7) that was considered one of the world's biggest hacking communities, Genesis Market (URL8) that was one of the most dangerous marketplaces selling stolen account credentials to hackers worldwide as well as the disruption of prolific ransomware services like LockBit (URL9) and Hive (URL10).

[3] Mixing potentially identifiable cryptocurrency funds with other funds to obfuscate their original source.

[4] Exchanging one cryptocurrency for another.

Other examples of outstanding international operational actions, that also involved Hungarian LEAs, are the takedown of the infrastructure of the FluBot spyware, which was one of the fastest-spreading mobile malware to date (URL11) as well as the action taken against VPNLab (URL12), which was a service offering shielded communications and internet access to cybercriminals engaged in serious criminal acts such as ransomware deployment.

Additional examples of recurring intelligence-led actions coordinated by EC3 and also involving Hungary, among other the participating countries, are:

- Carding Action (URL13) – operation targeting fraudsters selling and purchasing compromised card details on websites selling stolen credit card data, with the aim of mitigating and preventing losses for financial institutions and cardholders. In 2020, over 90,000 pieces of card data were analysed, which prevented approximately €40 million in losses.
- European Money Mule Action (URL14) – operation to combat mules and their recruiters. In 2023, several operational phases identified 10,759 money mules and 474 recruiters, leading to the arrest of 1,013 individuals worldwide.
- Victim Identification Taskforce (URL15) – initiative to identify victims and offenders depicted in child sexual abuse material. In 2021, experts analysed around 580 sets of images and video files depicting unknown victims of child sexual abuse and were able to identify 18 children and apprehend two offenders. In addition, the likely country of production was located in 211 instances and intelligence packages were sent to the relevant countries for investigation.
- Cyber Patrol Week (URL16) – initiative to gather intelligence on high value targets (vendors and buyers) operating on Dark Web marketplaces.

As mentioned previously, cybercriminals are good at exploiting modern privacy enhancing technologies, which can pose challenges for LE to track their activity and to acquire digital evidence from locked and encrypted devices. Tools and techniques to counteract criminals' operational security measures do exists, but they are costly and require a high level of expertise to deploy. In addition, because of the rapid evolution of new technologies, constant research and development is needed to keep up with the market. It is difficult for all EU Member States to maintain these capabilities, which is why EC3 has established the Digital Support Unit (DSU) to bolster the collective LE response against dangerous criminal networks and HVTs. Some of the most noteworthy capabilities of the DSU are:

- Providing on-site forensic support during international operations to seize and capture evidentiary data from the suspects devices;

- Running the Europol decryption platform (URL17), that helps decrypt information lawfully obtained in criminal investigations;
- Offering crypto-tracing support to track the illicit proceeds of cybercriminals;
- House the Europol Malware Analysis Solution (EMAS), which is a LE restricted dynamic analysis platform for the examination of malware (e.g. ransomware) behaviour to enrich cross-border investigations against the operators.

Looking ahead

The threat of digitalised crime only continues to increase as criminals in all crime areas are adopting technological countermeasures to conceal their activities. This includes encrypted communication, using Dark Web markets to sell illegal goods and services and adopting cryptocurrencies as forms of payment to make it more difficult to trace their criminal proceeds. Criminal networks currently engaged in more conventional forms of crime are looking to expand their portfolios through lucrative offences like online fraud schemes. Organisations and individuals continue adopting new technological solutions, which increases the potential attack-surface for cyber-attacks, malware campaigns and intrusions.

Considering all of these trends, it is more vital than ever to build meaningful operational cooperation between countries, private companies and academic institutions to counteract the threat that cybercriminals pose to our collective security.

Online links in the article

URL1: *ILOVEYOU virus.* https://www.techtarget.com/searchsecurity/definition/ILOVEYOU-virus

URL2: *DDos attacks – one year later.* https://www.hpcwire.com/2001/02/09/ddos-attacks-one-year-later/

URL3: *The Zeus Trojan malware – definition and prevention.* https://www.crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware/

URL4: *The history and evolution of ransomware attacks.* https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/

URL5: *Internet Organised Crime Threat Assessment (IOCTA) 2023.* https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

URL6: *World's most dangerous malware EMOTET disrupted through global action.* https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

URL7: *One of the world's biggest hacker forums taken down.* https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

URL8: *Takedown of notorious hacker marketplace selling your identity to criminals.* https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals

URL9: *Law enforcement disrupt world's biggest ransomware operation.* https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

URL10: *Cybercriminals stung as HIVE infrastructure shut down.* https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down

URL11: *Takedown of SMS-based FluBot spyware infecting Android phones.* https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

URL12: *Unhappy New Year for cybercriminals as VPNLab.net goes offline.* https://www.europol.europa.eu/media-press/newsroom/news/unhappy-new-year-for-cybercriminals-vpnlab-net-goes-offline

URL13: *Officers foil fraudsters from stealing €40 million in payment card scam.* https://www.europol.europa.eu/media-press/newsroom/news/officers-foil-fraudsters-stealing-%E2%82%AC40-million-in-payment-card-scam

URL14: *Paper trail ends in jail time for 1 013 money mules.* https://www.europol.europa.eu/media-press/newsroom/news/paper-trail-ends-in-jail-time-for-1-013-money-mules

URL15: *Global Europol taskforce identifies 18 child victims of sexual abuse.* https://www.europol.europa.eu/media-press/newsroom/news/global-europol-taskforce-identifies-18-child-victims-of-sexual-abuse

URL16: *Cyber-patrolling Week.* https://www.europol.europa.eu/operations-services-and-innovation/operations/cyber-patrolling-week

URL17: *Europol and the European Commission inaugurate new decryption platform to tackle the challenge of encrypted material for law enforcement investigations.* https://www.europol.europa.eu/media-press/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement

Reference of the article according to APA regulation

Szabó, Cs. & Europol's European Cybercrime Centre (2024). Europol's role in the fight against cybercrime. *Belügyi Szemle*, *72*(9), 1707–1714. https://doi.org/10.38146/BSZ-AJIA.2024.v72.i9.pp1707-1714

Statements

Conflict of interest

The authors have declared no conflict of interest.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Ethics

No dataset is associated with this article.

Open access

Corresponding author

The corresponding author of this article is Valér Dános, who can be contacted at
csaba.szabo3@bm.gov.hu