EUROPOL 2025 CYBERCRIME CONFERENCE

DISSECTING DATA CHALLENGES ON THE DIGITAL FRONTLINES

THEME

Dissecting Data Challenges on the Digital Frontlines

DATE & LOCATION

2-3 October 2025
Europol HQ, The Hague, The Netherlands

CONFERENCE IN NUMBERS:

More than 500 participants from 100 countries attended the conference. The event consisted of a plenary session and 8 side events and welcomed in total, 70 speakers.

STAKEHOLDERS

Law enforcement from the EU Member States, private industry, international organisations, EU institutions and agencies, academia and NGOs

ORGANISER

Europol's European Cybercrime Centre (EC3)

Dear participants of the Europol Cybercrime Conference 2025,

Thank you for attending the conference and largely contributing to its success.

This bulletin aims to highlights the main points mentioned during the conference.

I hope you will enjoy it and that I will see you next year again!

Mr. Edvardas Šileris, *Head of EC3, Europol*

WELCOMING SPEECHES

- Europol Cybercrime Conference 2025 brought together participants from all over the world to discuss the cybercrime challenges and importance of cooperation.
- The stakes are high, with the risk of leaving children vulnerable to crime and the need to ensure that the European cities are safe and the rule of law is enforced online as well as offline.
- Lawful access is a critical topic and the use of analogue warrants in the physical world should be equally applied to the digital world.
- Data protection is essential but not absolute. Therefore, a balanced approach should be adopted to ensure that law enforcement can access data while protecting individual rights.
- Adolescents are being drawn to crime facilitated by the end-to-end encryption (E2EE), which poses a significant challenge for law enforcement.
- The Roadmap on Encryption is a key initiative to address the risks of E2EE. The mandate of the G7 Lawful Access Working Group has been extended to incorporate work with regard to this area.
- Lawful access requires a balanced approach, integrating access by design and an oversight mechanism.

SPEAKERS:

Ms. Catherine De Bolle,
Executive Director, Europol
Mr. Edvardas Šileris, *Head of the European Cybercrime Centre (EC3), Europol*

BLOCK I: "BYTE THE BULLET:DATA ACCESS VS. PRIVACY"

OPENING KEYNOTE

SPEAKER:
Cssr. Dr. Magnus Brunner *Internal Affairs and Migration, European Commission*

- Law Enforcement Agencies (LEAs) need access to data to combat threats but this must be balanced with privacy rights. In this relation, the Roadmap for Effective and Lawful Access to Data for Law Enforcement provides a harmonised and transparent solution.
- The European Union needs to invest in defence. A defence whitepaper published in March 2025 allocated €800 billion to this domain.
- The digital world is a key area of focus, with drone defence and cybersecurity being the core aspects of security.
- With regard to LEAs, simplification, efficiency and use of AI in the European environment is of a high importance.
- The goal is to uphold European values and provide a harmonised and transparent solution that respects citizens' privacy, while acknowledging that criminals profit from fragmentation and that threats are now more acute than ever.
- There is a need for cooperation and collective action to face the challenges of the digital world.

BLOCK I: “BYTE THE BULLET:DATA ACCESS VS. PRIVACY”

STRATEGIC PANEL DISCUSSION

The Lawful Access Paradox: Fighting Crime Without Breaking Trust

- It is important to adopt a nuanced approach regarding the aim to achieve effective law enforcement and cybersecurity, while taking into account individual rights and freedoms.
- LEAs need to access relevant data in a more targeted and efficient manner in order to investigate the crimes and at the same time, protect the rights.
- There are challenges associated with introducing data into the criminal prosecution process and they call for judicial expertise.
- Cooperation and dialogue between all stakeholders are essential for finding solutions to the lawful access paradox. Potential strategies include access by design, decryption capabilities and behavioral data analysis.

SPEAKERS:

***Mr. Edvardas Šileris,** Head of the European Cybercrime Centre (EC3), Europol*
***Mr. Juan Corriat,** 1st Chief Superintendent, Head of Unit, Director or NTSU*
Belgian Federal Police – Department of the Special Units
***Mr. Jan Kerkhofs,** Federal Magistrate, Head of the Cyber Unit, Belgian Federal Prosecutor's Office*
***Mr. Jo De Muynck,** Head of Unit “Operational Cooperation”, ENISA*
***Ms. Anna Buchta,** Head of Unit “Policy & Legislative Consultation”, EDPS*

BLOCK II "Ctrl + Caught: Data in Operations”

Operation Cumberland

Operation Ratatouille

SPEAKERS:

Operation Ratatouille *(AP Cyborg, FR, UA)*
Operation Tomsk *(AP Terminal, UK)*
Operation Cumberland *(AP Twins and Paypal)*
Operation Eastwood*: Disrupting Pro-Russian Hacktivism (AP Cyborg, ES, DE)*

- The operations discussed in this block underlined the significance of data availability for investigations and its exploitation by criminals.
- The presented operations also showcased the necessity of international cooperation and collaboration between law enforcement agencies and their industry partners as well as the importance of following the money trail and data sharing.
- The presentations emphasised the significance of understanding the trust dynamics within the cybercriminal communities. Cybercriminals use forums to connect, communicate and build trust.
- The importance of careful planning and execution in operations to avoid causing unnecessary harm to innocent parties was highlighted.

Operation Eastwood

Operation Tomsk

BLOCK III "Surrounded by Data, Starved for Insights"

- The three success stories of joint operations and initiatives presented in this block stressed that the public-private partnerships (PPPs) are critical in combating cybercrime and there is a need for an increased cooperation between law enforcement, the industry and other stakeholders.
- Building trust and sharing success stories involving PPPs can encourage more partners to join such initiatives and to provide more information to law enforcement.
- Use of advanced threat intelligence and disruption strategies can be effective in relation to preventing cybercrime and protecting victims.

Russian Speaking Cybercrime Underground Ecosystem

Cyber Intelligence Extension Programme Showcase

LUMMA Joint Actions

SPEAKERS:

Russian Speaking Underground Cybercrime Ecosystem *(EC3 Cyber Intelligence, Cisco Talos Intelligence, Intel471, Mandiant Intelligence, Trend Micro)*
Cyber Intelligence Extension Programme Showcase *(EC3 Cyber Intelligence, Bitdefender, Microsoft Digital Crimes Unit, Shadowserver, Qintel)*
Lumma Joint Actions *(EC3 Cyber Intelligence, Microsoft Digital Crimes Unit, OFAC FR, FBI)*

OPENING KEYNOTE

- In relation to cybersecurity, our mindset should change to lean towards active rather than passive defence. Every country has the responsibility to engage in active defence and to help the victims of cybercrime.
- Influencing standards and making incidents public can be effective ways to improve cybersecurity and raise awareness.
- Having legal requirements in place to access information needed for investigations is crucial.

SPEAKER:

MEP Bart Groothuis, *Renew Europe Group*

THOUGHTS ON DATA ACCESS BY DESIGN

SPEAKER:

Mr. Álvaro Azofra Martinez,
Head of EC3 Expertise and Stakeholder Management Unit, Europol

- In every criminal investigation there is an affection to the privacy of the suspect investigated. The rule of law in democracies foresee these assessments and establishes robust legal processes to assess on a case by case basis every lawful request.
- Lawful access to data is always supervised by judicial authorities, targeted, limited in time and content and involves cooperation with the service providers.
- Standardised protocols of requesting data from service providers is the safest and most transparent and economic way of providing criminal evidence to competent authorities in a lawful manner.

BLOCK IV "Standardising the Cyber-Social Contract"

THE FUTURE OF ENCRYPTION

Challenges for Law Enforcement and Insights from Cutting-Edge Research

- Quantum computing poses a significant risk to the current cryptographic systems and new technologies are needed to protect against such threats.
- Researchers are working on developing new cryptographic techniques, such as PQC and encrypted computing, to stay ahead of the emerging threats.
- Use of end-to-end encryption is becoming more widespread and it is essential to ensure that these systems are secure and reliable.

SPEAKER:
Prof. Dr. Jürgen Freudenberger*, Director Key Technologies, Cyberagentur*

BLOCK IV "Standardising the Cyber-Social Contract"

NAVIGATING THE MAZE

Law Enforcement's Role in Tackling Standardisation Challenges Today and Tomorrow

SPEAKER:

Ms. Michaela Klopstra, *Security Delivery Manager, Accenture*

- Standards are critical in helping law enforcement navigate the complex landscape of technology and cybersecurity.
- Standardisation development organisations play a key role in supporting law enforcement by standardising interfaces, architecture and testing frameworks as well as by developing secure communication protocols.
- Law enforcement wants to use the front doors, not the backdoors to access data and standards can help facilitate this approach.
- Standards matter in several areas, including security, interoperability and innovation enablement.

BLOCK V Data-Driven Legislation: A 'Right' to be Seen!”

EUROPEAN COMMISSION’S ROADMAP ON ACCESS TO DATA

- The European Commission’s Roadmap outlines how the European Union will improve lawful access to the digital data for law enforcement.
- The roadmap focuses on modernising tools and legal frameworks while protecting the fundamental rights.
- The roadmap targets six key areas: data retention, lawful interception, digital forensics, decryption, standardisation and AI solutions.

EUROPEAN COMMISSION'S
ROADMAP ON ACCESS TO DATA
Dr. Monika Kopcheva
Head of Unit "Security in the digital age",
DG Home, European Commission
EUROPOL

SPEAKER:
Dr. Monika Kopcheva, *Head of Unit “Security in the Digital Age”, European Commission*

BLOCK V Data-Driven Legislation: A 'Right' to be Seen!”

The Australian Telecommunications and Other Legislation Amendment Act 2018 TOLA

SPEAKER:
Mr. Mitchell Pearson-Goff, *Detective Sergeant, Cyber Liaison Officer J-CAT, Australian Federal Police*

- TOLA is a legal framework for industry assistance and enhanced cooperation to address technological challenges affecting investigations.
- This framework does not serve as an independent channel to obtain private communication or metadata or conduct surveillance. Interception of communications, access to metadata or search powers still require the existing thresholds to be met.

THE ICC’S POLICY ON CYBER-ENABLED WAR CRIMES

- In March 2025, ICC released a draft policy for public consultation concerning cyber enabled war crimes. The policy underlines that all crimes under the ICC jurisdiction may be carried out or facilitated by cyber means.
- Proving conduct in cyberspace can help prove purely physical conduct as it can lead to for instance, revealing criminal intent or patterns.

SPEAKER:

Mr. Matthew Cross, *Appeals Counsel, Office of the Prosecutor, International Criminal Court*

CLOSING REMARKS

SPEAKER:

Mr. Jean-Philippe Lecouffe, *Deputy Executive Director Operations (DEDO), Europol*

- Improving privacy and security is facilitated by building trust and strengthening partnerships.
- Europol's actions have a global reach and PPPs and common standards bring an added value in this respect.
- Lawful access by design must become a standard feature of future technologies.
- Collaboration with industry is not optional. It is essential.
- Cross-border cooperation will have to be strengthened due to the transnational nature of crime.
- We have the responsibility to bring lawful access from just a promise, to practice.

THANK YOU &

SEE YOU NEXT TIME!