25 YEARS OF CYBER JUSTICE

CYBER SECURITY COALITION

IGO IFJ

hosted in Brussels by

BNP PARIBAS FORTIS

Your hosts:

Catherine Van de Heyning
Public Prosecutor; Professor
European Fundamental Right
University of Antwerp

Baptiste Flumian
Cybercrime Reference Magistrate
Brussels Public Prosecutor's Office

CYBER SECURITY COALITION

IGO IFJ

hosted in Brussels by
BNP PARIBAS FORTIS

Rob Beenders

Minister of Consumer Protection, Social Fraud Prevention, Persons with Disabilities, and Equal Opportunities

Panel: Balancing privacy & law enforcement in the digital age

Moderator: Charlotte Conings
Stibbe

Irene Kamara
Tilburg Institute for Law, Technology, and Society

Olivier Leroux
Brussels Court of Appeal

The shift from legislation focusing on targeted privacy intrusive measures to legislation targeting everyone's data

By moving from laws allowing targeted investigative measures to laws introducing regimes of mass data retention and data scanning, we are treating every citizen as a potential suspect, but this is the price we must pay for maintaining security in the digital age.

End-to-end encryption

By making encrypted communication untouchable, we are creating digital safe havens for criminals — it's time to accept that privacy should not outweigh collective security.

AI and the future

The rise of AI-driven policing and predictive algorithms risks turning citizens into data points rather than individuals — and as technology evolves, we may soon face challenges that make today's debates over encryption and data retention seem minor.

Any questions ?

Panel: AI – a new frontier in cybercrime

Moderator:
Elise
Delhaise
UNamur

Robin Khalfa
Ghent University

Julie Petersen
Artes Law

Christophe Van Bortel
Computer Crime Unit
FGP Antwerpen

Any questions ?

Panel: Hack the right path: Turning risk into responsibility

Moderator: Peter Peereboom
Public Prosecutor's Office Antwerp

Veerle Peeters
CybHERStrong

Niels Hofmans
Cresco

Any questions ?

Coffee break

See you back
at 4:10 PM !

Panel: Building trust across borders and sectors in cyber investigations

Moderator:
Mona Giacometti
ULB

Lorelien Hoet
Microsoft

Vanessa Franssen
University Liège

The biggest obstacle to cross-border digital evidence collection in the EU is not the technology but a deep trust deficit among law enforcement authorities and the private sector.

Microsoft

Trust in cyber investigations

- Trust
- Threat landscape
- Proactive approach
- Public-private co-operation
- Balancing security and fundamental rights
- How we work with LEA

Our breadth and depth of signals

100 trillion
security signals processed daily

4.5 million
net new malware file blocks every day

38 million
identity risk detections analyzed in an average day

15,000+
Partners in our security ecosystem, making it one of the largest in the world

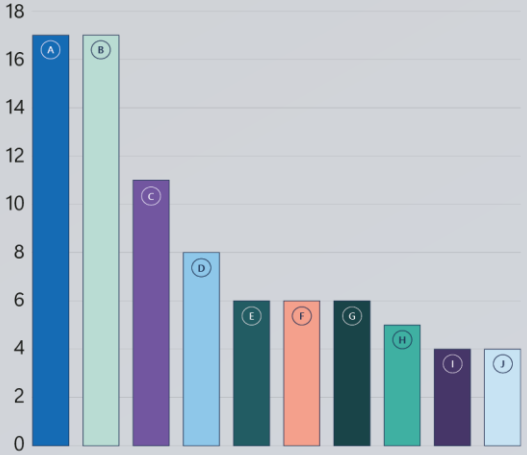
34,000
full-time equivalent security engineers employed worldwide

5 billion
emails screened daily on average to protect users from malware and phishing

Key trends

- Adversaries are targeting **data**
- Most attacks are for **money** (only 4% were exclusively espionage)
- **Research and Academia** are more targeted than ever
- Adversaries are using **AI** to scale and tailor operations

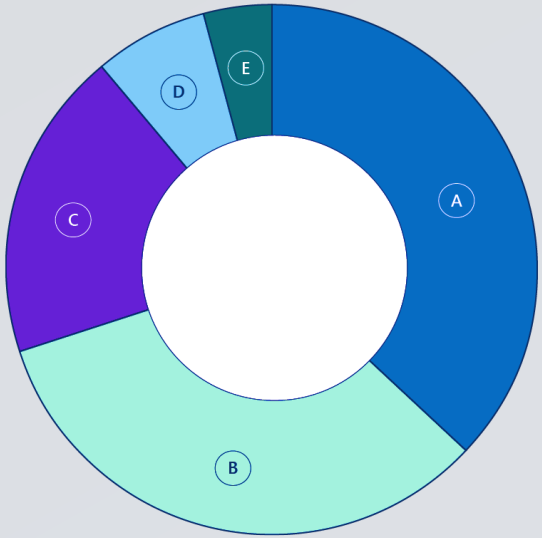
Ten global sectors most impacted by threat actors (January-June 2025)



	%
A. Government agencies & services	17
B. Information technology	17
C. Research and academia	11
D. Non-governmental organizations	8
E. Critical manufacturing	6
F. Transportation systems	6
G. Consumer retail	6
H. Communications infrastructure	5
I. Financial services	4
J. Healthcare and public health	4

Source: Microsoft Threat Intelligence

Identified motivations in incident response engagements



	%
A. Data theft	37
B. Extortion	33
C. Destruction/human-operated ransomware	19
D. Infrastructure building	7
E. Espionage	4

Source: Microsoft Incident Response, Detection and Response Team

Regional sample of nation-state activity levels observed

Observed event activity count per country

- Over 200 events
- 100—200
- 50—100
- 0—50

Americas

Top activity levels

United States	623
Canada	51
Brazil	24
Peru	16
Argentina	11
Colombia	10
Mexico	9
Dominican Republic	5
Chile	4
Costa Rica	3

Asia & Pacific

Top activity levels

Taiwan	143
Korea	126
India	100
Hong Kong SAR	95
China	49
Australia	47
Thailand	39
Japan	38
Singapore	33
Indonesia	32

Europe

Top activity levels

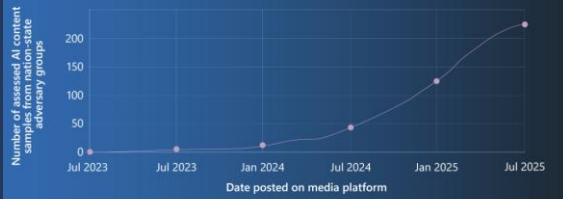
Ukraine	277
United Kingdom	144
Poland	97
Germany	74
France	72
Spain	61
Russia	60
Italy	51
Azerbaijan	35
Belgium	30

Middle East & Africa

Top activity levels

Israel	603
United Arab Emirates	166
Saudi Arabia	70
Türkiye	70
Iraq	67
Jordan	44
Lebanon	39
Egypt	32
Iran	27
Morocco	26
South Africa	31
Ethiopia	20
Angola	9
Kenya	9
Nigeria	8
Tanzania	5
Mali	4
Namibia	4
Botswana	2

Rapid growth in assessed AI content samples attributed to nation-state adversaries



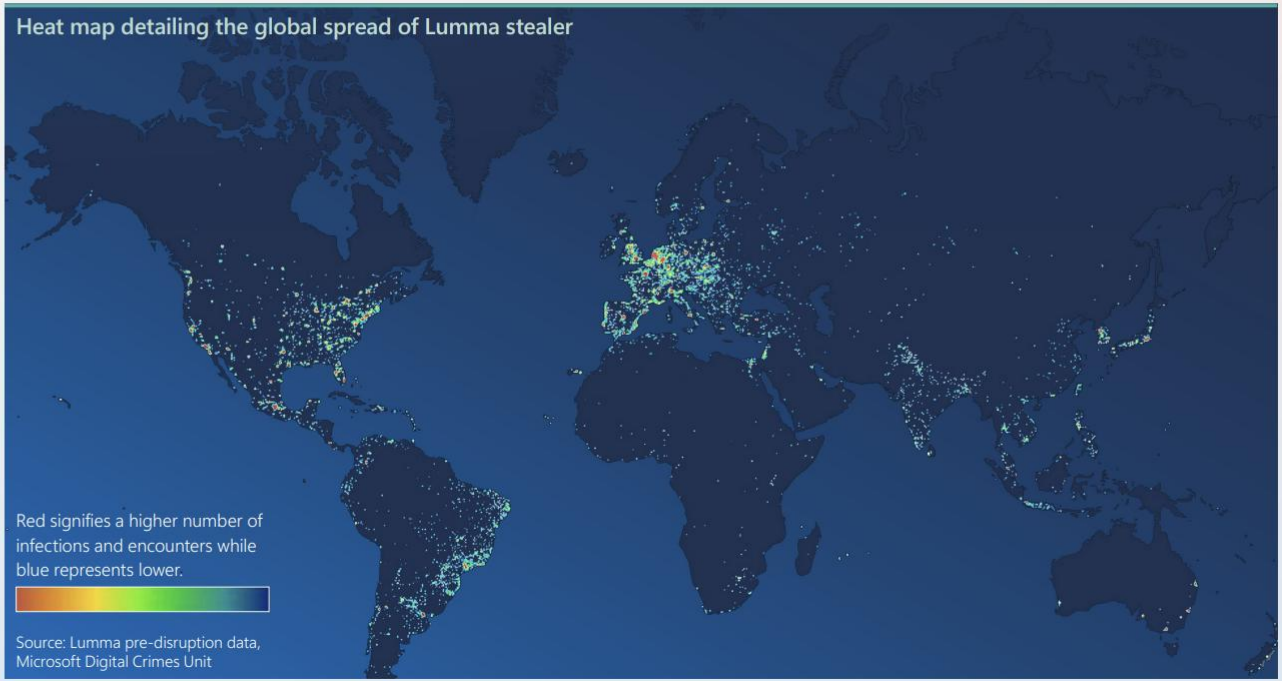
Source: Microsoft Threat Intelligence

Countering nation-state and emerging threats

Disrupting cybercrime ecosystems: Lessons from the Lumma Stealer takedown

Given Lumma Stealer's prominence in the infostealer ecosystem and its role in enabling broader cybercriminal operations, it became a high-priority target for disruption this year. In May 2025, the DCU, in collaboration with global law enforcement and cybersecurity partners, successfully disrupted the Lumma Stealer infrastructure in a joint operation exemplifying the power of public-private collaboration in proactive cyber defense.

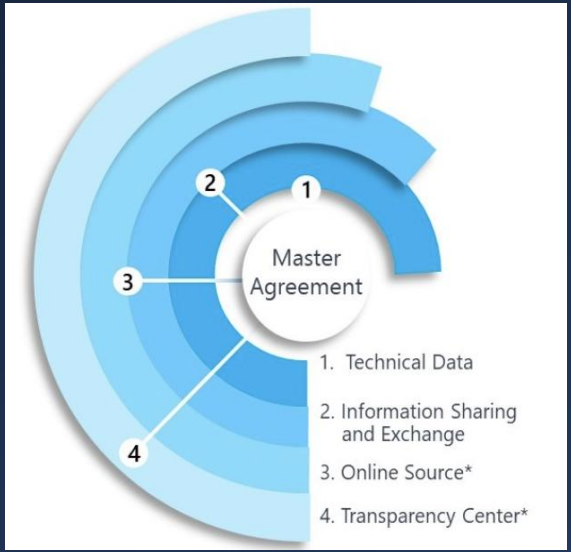
Through a US court order and coordinated actions with the US Department of Justice, Europol, Japan's Cybercrime Control Center (JC3), and private sector partners like ESET, Bitsight, Lumen, CleanDNS, and GMO Registry, over 2,300 malicious domains were seized or blocked. These domains formed Lumma Stealer's infrastructure backbone.



Public private co-operation

GSP

Share information – Microsoft shares CTI briefings and information, also through the Government Security Program (GSP). Intensifying the sharing of information between public and private entities should be continually fostered.



European Security Program (ESP)

- **Cybersecurity Report (3×/year):** Microsoft-led analysis of threat actor trends, notable TTPs, and recent actions against cybercrime — shared at TLP:AMBER/AMBER-STRICT.
- **Confidential Threat Briefings (3×/year):** Virtual sessions with Microsoft security teams following each report.
- **CTIP data access, prioritized for Europe:** Support for (re)onboarding to Microsoft's Cyber Threat Intelligence Program feed.
- **Ad-hoc security inquiries:** White-glove triage via GSP; Microsoft coordinates responses from threat intel and product teams. Responses will be limited by availability of country-specific data and adherence to timelines for requests.
- **Advance notice of select security communications (under embargo):** Where feasible, ESP members receive pre-publication heads-up.
- **Invitations to security events (space-permitting):** e.g., Digital Crimes Consortium (DCC), and an annual EBC day in Redmond.

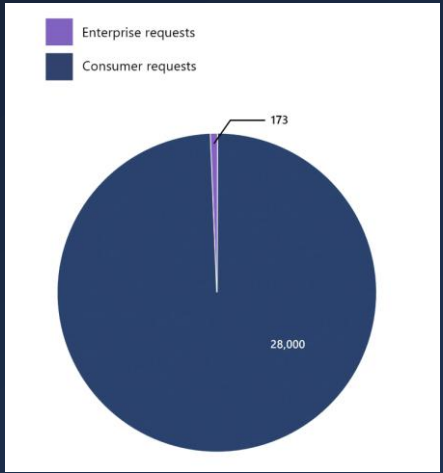
LEA : Balancing security and fundamental rights

- Microsoft does not provide any government with direct or unfettered access to customer data.
- Microsoft discloses customer data only when legally compelled to do so.
- Local compulsory process is required to request non-content data. A warrant is required for content data, typically issued through mutual legal assistance channels with Ireland or the United States when sought by foreign law enforcement.
- Microsoft reviews every legal demand to ensure it is valid and complies with appliable laws.
- Microsoft does not provide any government with our encryption keys or the ability to break our encryption.

Government Requests for Customer Data Report

Twice a year we publish the number of legal demands for customer data that we receive from governments around the world. Explore the reports and data we have compiled, divided into sections covering law enforcement, national security, and civil authorities.

Download the Law Enforcement Requests Report



Period H2 2024	
Requests WW	28.120
	of which 173 about enterprise customers
Requests US	5.560
	of which 0 requests about EU enterprise customers
Requests DE	5.296
Requests BE	331
Requests NL	165

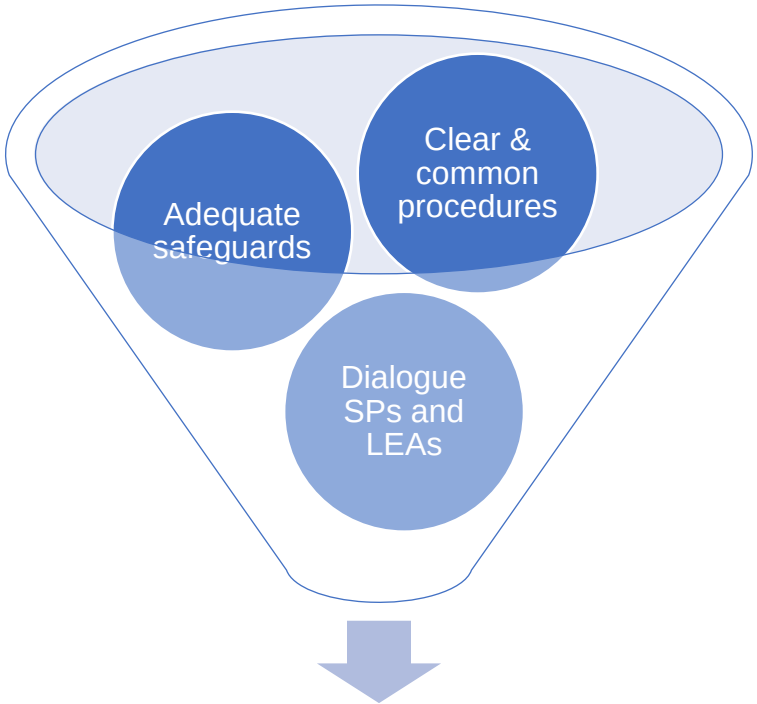
Building Trust Across Borders in Cyber Investigations – A Legal Perspective (Part I)

Prof. Vanessa Franssen

25 Years of Cyber Justice

Conference organised by Cyber Security Coalition & IGO-IFJ
Brussels, 27 November 2025

Trust-enhancing elements in legal framework on e-evidence gathering



Trust-enhancing elements in EU legal framework on e-evidence gathering (1)

- Cross-border gathering
- MLA -> EIO Directive -> e-Evidence Regulation
  - International cooperation (states)
  - Mutual recognition, judicial cooperation (judicial authorities)
  - Direct cooperation (judicial authority-service provider)

Big leap(s)!

Trust-enhancing elements in EU legal framework on e-evidence gathering (2)

- E-Evidence Regulation – mechanism

Role judicial authority
MS of suspect?

Trust-enhancing elements in EU legal framework on e-evidence gathering (3)

- E-Evidence Regulation and building trust?
  - Common EU-wide legal framework for preservation and production of data
  - Definition data categories
  - Data localisation no longer determining
  - Minimum rules on safeguards (e.g. judicial authorization, notification…)
  - Clear addressee (legal representative, data controller)
  - Common forms (certificates)
  - Decentralised IT system, ensuring
    - Authentication
    - Confidentiality
    - Secure connection and transmission of data
    - 24/7 access
  - Room for (some) dialogue between service providers and LEAs
  - Conflicts of law (proof of the pudding…?)
  - Gaps?

Comm. Implementing Reg. (EU) 2025/1550

Data sovereignty is impossible to conciliate with the effectiveness of criminal investigations.

Technology is a key factor in ensuring the authenticity and admissibility of evidence in court.

Building Trust Across Borders in Cyber Investigations – A Legal Perspective (Part II)

Prof. Vanessa Franssen

25 Years of Cyber Justice

Conference organised by Cyber Security Coalition & IGO-IFJ
Brussels, 27 November 2025

Ensuring authenticity and reliability of cross-border evidence

- EIO
  - Eg *EncroChat*
    - CJEU, 30 April 2024, C-670/22, *M.N.*
    - ECtHR, 17 October 2024, *A.L. et E.J. v. France*

- E-Evidence Regulation
  - Decentralised IT system = key
    - Authentication
    - Cyber security

  - Yet, once data produced to issuing authority, national law applies

Link with admissibility of evidence? (1)

- National law
  - Art. 32 PTCPP: admissibility of evidence – exclusionary rules
    - 2nd criterion: reliability of the evidence
    - 3rd criterion: right to a fair trial

- EU law
  - No common rules (yet)
    - Despite legal basis in TFEU! – Art. 82(2)a)
    - Despite academic research!
  - Case law CJEU
    - In relation to data retention
    - What to do with evidence if retained/obtained in violation of EU law?

Link with admissibility of evidence? (2)

- EU law
  - Case law CJEU (cont'd)
    - Rules on admissibility -> national law
      - Principle of procedural autonomy
      - Principle of equivalent protection
      - Principle of effectiveness
    - What 'sanctions' possible?
      - Assessment/weighing of evidence
      - Sentencing
      - Exclusion

But mind:

Objective?
'to prevent information and evidence obtained unlawfully from unduly prejudicing [the suspect]'

Link with admissibility of evidence? (3)

- EU law
  - Case law CJEU (cont'd)
    - Yet, national courts are to exclude the (retained) data obtained contrary to EU law in criminal proceedings where:
      - (1) the suspects are 'not in a position to comment effectively on [that] evidence',
      - (2) the evidence pertains 'to a field of which the judges have no knowledge', and
      - (3) it is 'likely to have a preponderant influence on the findings of fact'.

LQDN I and *Prokuratuur*

Right to fair trial (incl. adversarial principle)

- 'Blueprint' for future EU legal framework?
- *Quid* authenticity and reliability?

The lack of transparency seriously comprises trust in the results of a cyber investigations.

Any questions ?

Bernard Quintin

Minister of Security and Home Affairs, responsible for Beliris

Wrap-up:

Catherine Van de Heyning
Public Prosecutor; Professor
European Fundamental Right
University of Antwerp

Baptiste Flumian
Cybercrime Reference Magistrate
Brussels Public Prosecutor's Office

CYBER SECURITY COALITION

IGO IFJ

hosted in Brussels by BNP PARIBAS FORTIS

Networking cocktail

Ends at 6:30 PM !


25
YEARS
OF CYBER JUSTICE
CYBER SECURITY
COALITION
IGO
IFJ
hosted in Brussels by
BNP PARIBAS
FORTIS