BRUSSELS, 12/11/2024 PARLEU2024.PARLAMENT.HU

BACKGROUND NOTE #15

HU24EU PARLIAMENTARY DIMENSION

15TH MEETING OF THE JOINT PARLIAMENTARY SCRUTINY GROUP (JPSG) ON EUROPOL

III. THEMATIC AGENDA ITEM: THE FIGHT AGAINST CYBERCRIME, IN PARTICULAR CRIMES USING ARTIFICIAL INTELLIGENCE; POSSIBILITIES OF KNOWLEDGE SHARING INVOLVING CEPOL

The competitive advantage of increasing digitalisation, interconnected network and IT infrastructures, and the crises of recent years have reinforced the need for cybersecurity in Europe [JOIN(2020) 18 final, COM(2021) 170 final]. Artificial Intelligence (AI) has become part of everyday life as a tool to navigate through digital data sets. It requires continuous learning in order to monitor its relationship with cybercrime [COM(2023) 665 final] and to keep the responses to the risks up to date.

The European Multidisciplinary Platform Against Criminal Threats (EMPACT) is a tool for cooperation between Member States, the priorities in the fight against serious and organised crime are set by the Council of the European Union. One of these is the fight against cybercrime.

Europol and its European Cybercrime Centre (EC3) produce a wide range of operational and strategic reports. One of these reports maps how AI can be used by criminals (Europol Report 2020), such as AI powered password, CAPTCHA breaking (a test that can distinguish a human user from a machine), attacks using cryptography and psychological manipulation (so-called social engineering attacks), deepfake and the misuse of intelligent assistants.

Every year, the EC3 Centre publishes the Internet Organised Crime Threat Assessment (IOCTA). IOCTA 2023 presents summary findings on the different typologies of cybercrime. The report's supplement on cyber-attacks, for example, outlines the types of criminal organisations that are perpetrating cyber-attacks, highlights how they are exploiting geopolitical changes, and examines the nature of attacks caused by malicious software. The supplementary report on online fraud highlights the intense level of adaptability of criminals, their modus operandi adapted to socio-economic trends and current crisis situations. IOCTA 2024 underlines the growing use of AI-based tools and services in cybercrime. The latest report on AI and policing (2024), which addresses issues of data bias, privacy, accountability and human rights protection [COM(2021) 206 final] in the context of the entry into force of the AI Act.

Launched in 2021, the AP4AI project aims to develop a validated framework for AI accountability in law enforcement, security and justice. Reflecting on the past regulatory discussions and the results of citizens' consultations in 30 countries, the report "Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain" (2022) was drawn up for law enforcement and internal security practitioners. The consultation with citizens suggests that AI could be used to protect vulnerable groups and society, and to prevent crime in the future. The report will be followed by continuous work with expert groups to translate the accountability principles into actionable steps, providing legal considerations and practical examples in the future.

In Europol's updated strategic priorities (2023), the focus is on law enforcement and research, in particular the development of data processing tools with AI. Europol's Consolidated Annual Activity Reports for 2022 and 2023 therefore mention the AIDA project which aims to create a descriptive and predictive analytics platform to enable law enforcement agencies to process real data in an operational environment. Europol Programming Document 2024 – 2026 refers to AI several times. It mentions, for example, the impact of the European data protection and AI regulatory framework on law enforcement activities, or tapping the potential of AI in further developing the EU platform to tackle illegal content online.

At the Joint Parliamentary Scrutiny Group's meeting in Gent in February 2024, Commissioner for Home Affairs Ylva Johansson underlined the need for Europol to fight against the malicious use of AI, which can facilitate disinformation campaigns, fraud and child sexual abuse. She stressed that this requires law enforcement authorities to develop effective AI tools. ◆

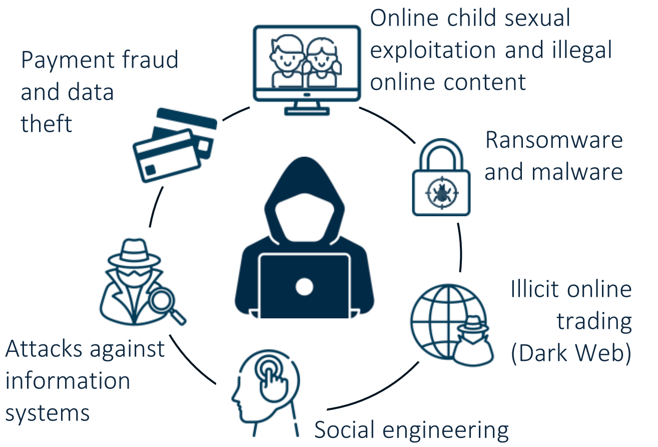
BACKGROUND NOTE #15

LAST UPDATE: 16/09/2024

ORSZÁGGYŰLÉS

1

THE MAIN TYPES OF CYBERCRIME



Online child sexual exploitation and illegal online content

Ransomware and malware

Illicit online trading (Dark Web)

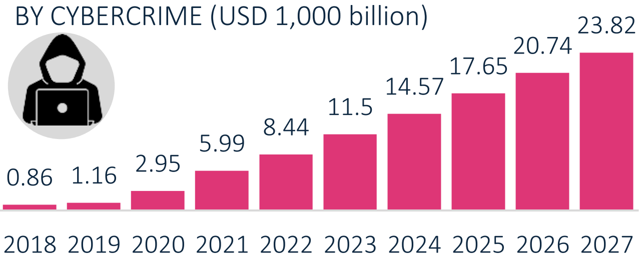
Social engineering

Attacks against information systems

Payment fraud and data theft

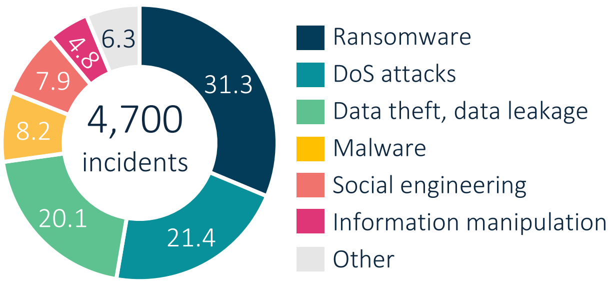
2

ESTIMATED VALUE OF GLOBAL DAMAGE CAUSED BY CYBERCRIME (USD 1,000 billion)



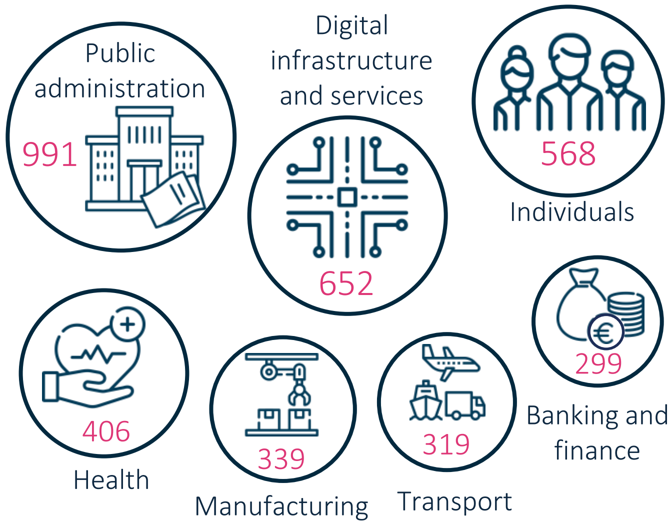
3

DISTRIBUTION OF INCIDENCE TYPES REPORTED TO THE EU AGENCY FOR CYBERSECURITY (ENISA), July 2022 – June 2023 (%)



4

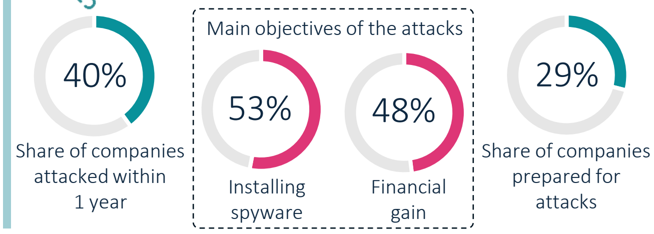
CYBER INCIDENTS INVESTIGATED BY ENISA BY MOST AFFECTED SECTORS, JULY 2022 – JUNE 2023 (pcs)



5

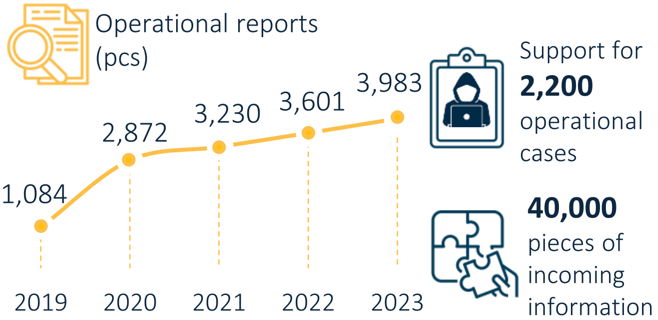
CYBERSECURITY OF EUROPEAN MARKETS, 2024

Data on 4,261 companies and organisations (BE, CZ, CH, DE, ES, DK, FR, IT, NL, NO, PL, SE, UK)



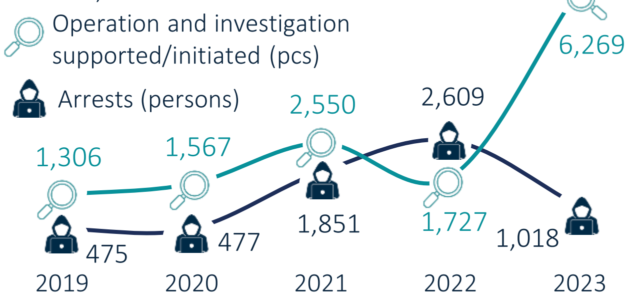
6

EUROPOL EC3 SUPPORTED OPERATIONS, 2019–2023



7

EMPACT RESULTS IN THE FIGHT AGAINST ONLINE FRAUD, 2019–2023



SOURCES

1 Council of Europe: Convention on Cybercrime, 2001; European Commission, 2024 | 2 Statista, 2024 | 3 | 4 ENISA, 2023 |
5 Cloudflare, 2024 | 6 Europol, CAAR 2019–2023 | 7 European Commission: EMPACT