Neapolis University Pafos, Cyprus
AI-2-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by the European Union

Policy Brief

ENISA Foresight Report:

Key Takeaways on Emerging Cybersecurity Threats for 2030

NUP Jean Monnet / UNESCO Policy Briefs

25/2024

With the support of the Erasmus+ Programme of 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

Frontpage picture: Generated with AI (Bing Image Creator)

The support of the European Commission and of UNESCO for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors; the European Commission and UNESCO cannot be held responsible for any use which may be made of the information contained therein.

ENISA Foresight Report:

Key Takeaways on Emerging Cybersecurity Threats for 2030

Executive Summary:

The European Union Agency for Cybersecurity (ENISA) released a report outlining the top ten cybersecurity threats anticipated to emerge by 2030. This briefing explores the results and methodology of ENISA's foresight exercise, analyzes the identified threats, and highlights the importance of proactive measures to bolster cyber resilience.

Keywords

Cybersecurity,

Background

ENISA's foresight exercise serves as a valuable tool for policymakers, industry leaders, and individual citizens to gain insights into the evolving cybersecurity landscape and take necessary steps to mitigate future risks. By prioritizing proactive measures and fostering international cooperation, the EU can enhance its overall cybersecurity posture and build a more secure digital future.

The Threats

According to the latest ENISA report, this is the top ten list of the emerging cybersecurity threats to have an impact by 2030:

1. Supply Chain Compromise of Software Dependencies
2. Skill Shortage
3. Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems
4. Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [New in Top Ten]
5. Rise of Digital Surveillance Authoritarianism / Loss of Privacy
6. Cross-border ICT Service Providers as a Single Point of Failure
7. Advanced Disinformation / Influence Operations (IO) Campaigns
8. Rise of Advanced Hybrid Threats
9. Abuse of AI
10. Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [New in Top Ten]

ENISA's Methodology

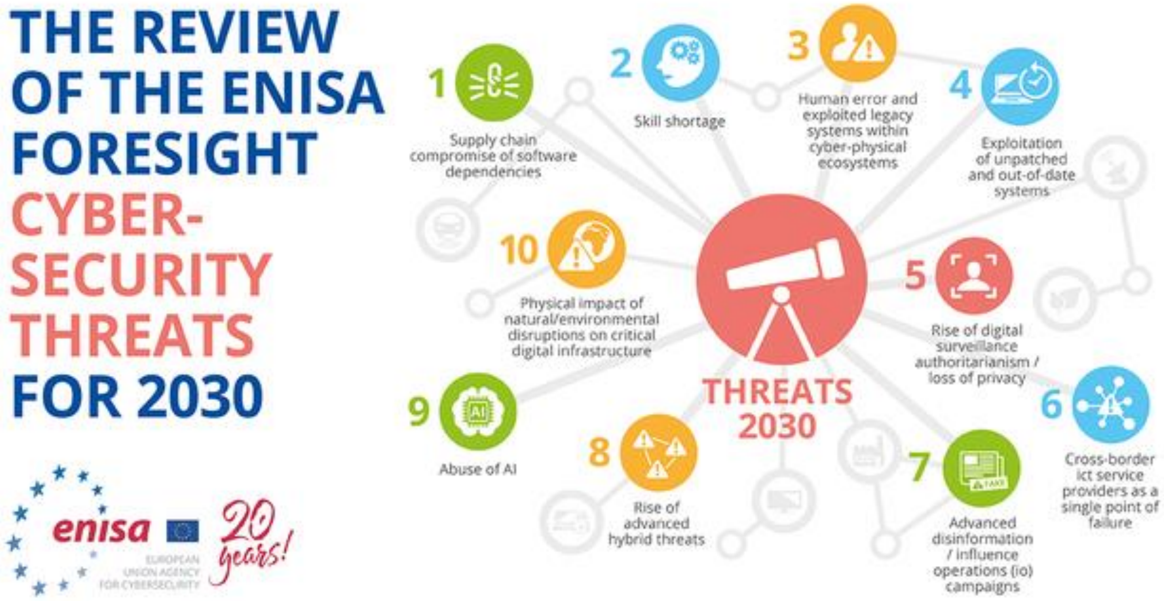
Regarding methodology, ENISA employs the following approaches to identify and rank these threats:

- **PESTLE Analysis:** This framework examined future trends in political, economic, social, and technological (PEST) factors, alongside legal and environmental (LE) considerations, to understand the broader context shaping the cybersecurity landscape.
- **Threat Identification Workshops:** Experts brainstormed potential threats through collaborative exploration and scenario planning exercises.
- **Science Fiction Prototyping (SFP):** Participants explored future scenarios through the lens of fictional characters, fostering out-of-the-box thinking and creative threat identification.
- **Threatcasting:** Drawing on traditional future studies and strategic thinking, this method involved inferring potential threats from research-based models of future environments.

Preparing for Action

By anticipating future threats, ENISA aims to encourage proactive measures to bolster cybersecurity resilience across the EU. The identified threats underscore the need for:

- **Continuous Investment in Threat Detection and Response:** Cybersecurity strategies must remain adaptable and responsive to ever-evolving threats.
- **Focus on Security in Infrastructure Development:** Robust security measures need to be integrated into the design and deployment of new technologies, including smart devices and space-based infrastructure.
- **Upskilling the Cybersecurity Workforce:** Addressing the cybersecurity skills gap is crucial to ensure a qualified workforce capable of managing future threats.
- **Promoting International Cooperation:** Combating cybercrime effectively requires collaboration between governments, law enforcement agencies, and private sector stakeholders across borders.
- **Balancing Security with Privacy:** Cybersecurity measures must be implemented with due consideration for fundamental privacy rights.


THE REVIEW OF THE ENISA FORESIGHT CYBER-SECURITY THREATS FOR 2030
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
20 years!
THREATS 2030
1 Supply chain compromise of software dependencies
2 Skill shortage
3 Human error and exploited legacy systems within cyber-physical ecosystems
4 Exploitation of unpatched and out-of-date systems
5 Rise of digital surveillance authoritarianism / loss of privacy
6 Cross-border ict service providers as a single point of failure
7 Advanced disinformation / influence operations (io) campaigns
8 Rise of advanced hybrid threats
9 Abuse of AI
10 Physical impact of natural/environmental disruptions on critical digital infrastructure

Infographic: Source ENISA 2024

Conclusions

The ENISA review serves as a valuable tool for understanding the evolving cybersecurity landscape and informing future actions. It emphasizes the need for continuous adaptation and collaboration to build strong and adaptable cybersecurity frameworks. More specifically:

- **Supply chain attacks remain a top threat:** The reliance on third-party software components creates vulnerabilities that attackers exploit.
- **Increased concern about single points of failure:** Interconnected critical infrastructure across countries could be crippled if a major ICT service provider is compromised.
- **Cybersecurity skills shortage is rising:** The lack of skilled professionals hinders efforts to patch systems and stay ahead of threats.
- **New threats emerge:** Unpatched systems and physical disruptions to critical infrastructure are growing concerns.
- **AI abuse becomes a top threat:** As reliance on AI grows, so does the potential for misuse.
- **Space threats and targeted attacks de-prioritized:** These dropped out of the top ten due to lower perceived risks compared to other threats.

Further Reading

- Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats (link)