FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Quali saranno le minacce cyber nel medio periodo? le previsioni di ENISA per il 2030

FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Interviene:

Rossella Mattioli

Cybersecurity Expert, European Union Agency for Cybersecurity (ENISA)

Quali saranno le minacce cyber nel medio periodo? le previsioni di ENISA per il 2030

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

QUALI SARANNO LE MINACCE CYBER NEL MEDIO PERIODO? LE PREVISIONI DI ENISA PER IL 2030

Rossella Mattioli

03 06 2024

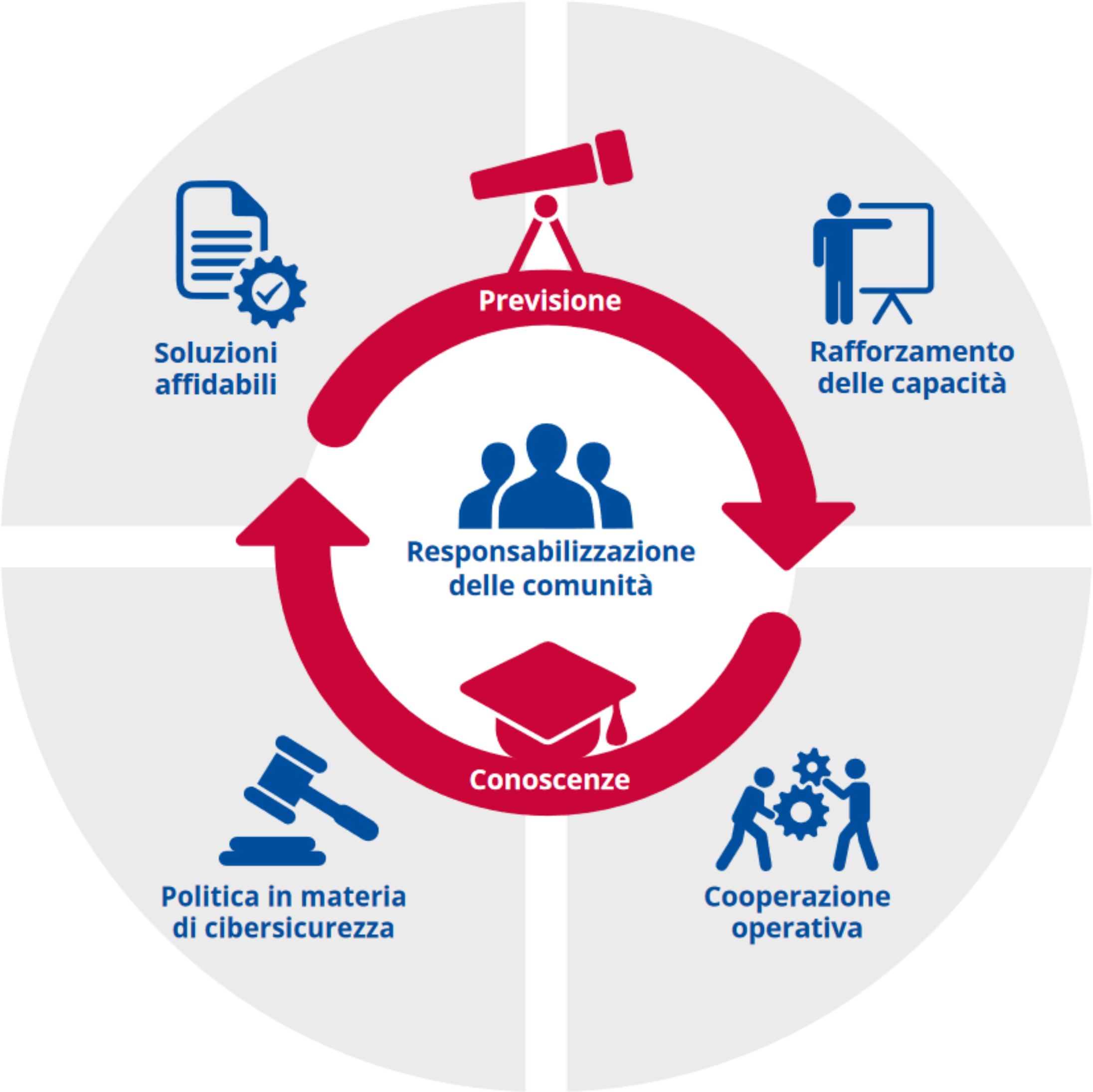
WHO WE ARE

Dal 2004, ENISA, l'Agenzia dell'Unione Europea per la Cybersicurezza svolge un ruolo determinante per realizzare l'ambizione dell'UE di rafforzare la fiducia e la sicurezza digitali in tutta Europa

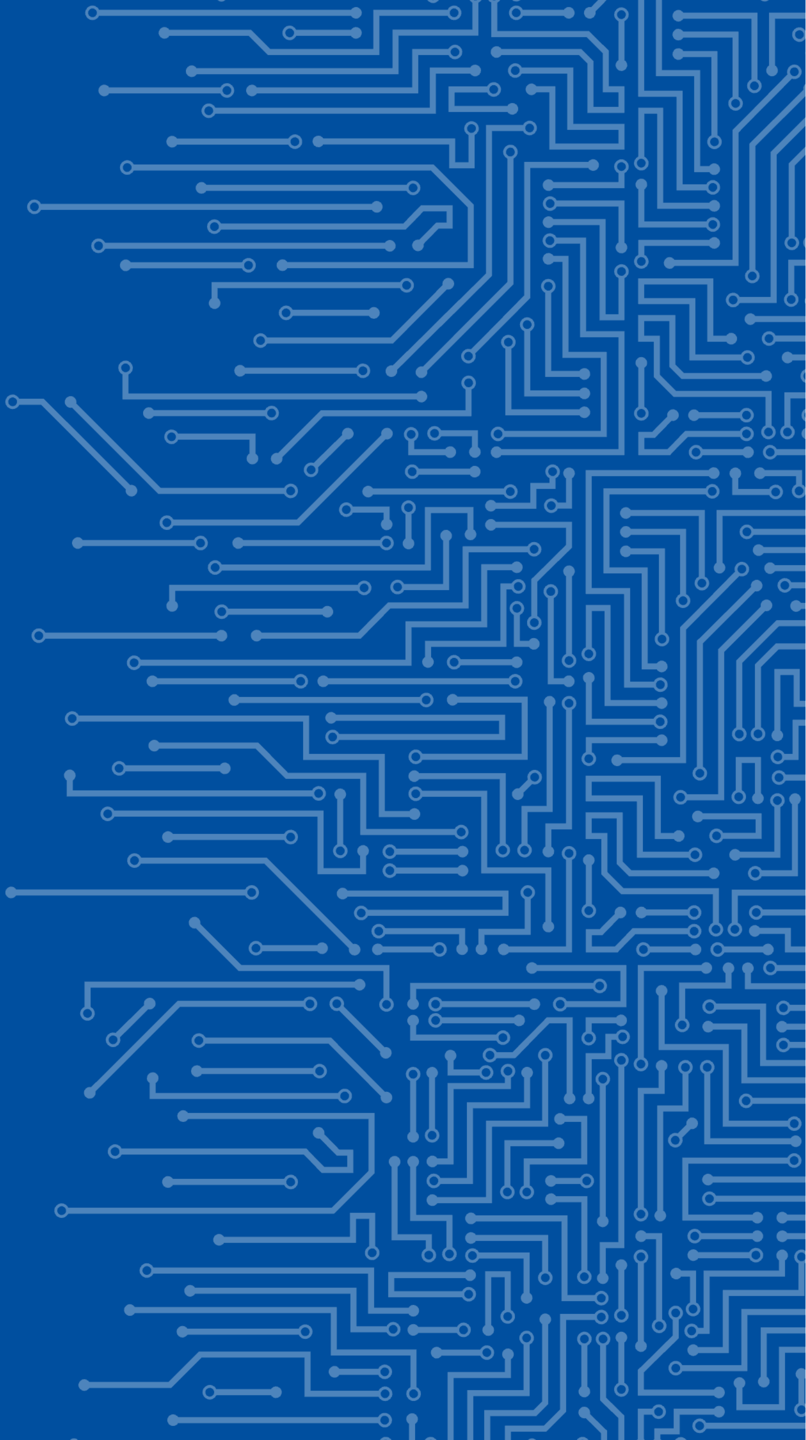
- La missione di ENISA consiste nel conseguire un elevato livello comune di Cybersicurezza in tutta l'Unione, collaborando con tutte le comunità.
- Il nostro obiettivo è rafforzare la fiducia nell'economia connessa, aumentare la resilienza e l'affidabilità delle infrastrutture e dei servizi dell'UE e garantire la sicurezza digitale della nostra società e dei nostri cittadini.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
BUILDING A TRUSTED AND CYBER SECURE EUROPE
#ENISA

WHAT WE DO: OBIETTIVI STRATEGICI


Previsione
Soluzioni affidabili
Rafforzamento delle capacità
Responsabilizzazione delle comunità
Conoscenze
Politica in materia di cibersicurezza
Cooperazione operativa

PREVEDERE LE SFIDE EMERGENTI E FUTURE



DALL'OGGI AL DOMANI – ANTICIPARE PER PREVENIRE

ENISA THREAT LANDSCAPE 2021

April 2020 to mid-July 2021

OCTOBER 2021

ENISA THREAT LANDSCAPE: TRANSPORT SECTOR

(January 2021 to October 20

ERSECURITY ENGES

ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

JULY 2021

ENISA THREAT LANDSCAPE 2022

(July 2021 to July 2022)

OCTOBER 2022

NISA THREAT ANDSCAPE FOR ANSOMWARE TTACKS

Y 2022

FORESIGHT CHALLENGES

A study to enable foresight on emerging and future cybersecurity challenges

NOVEMBER 2021

IDENTIFYING EME CYBER SECURITY THREATS AND CHALLENGES FOR

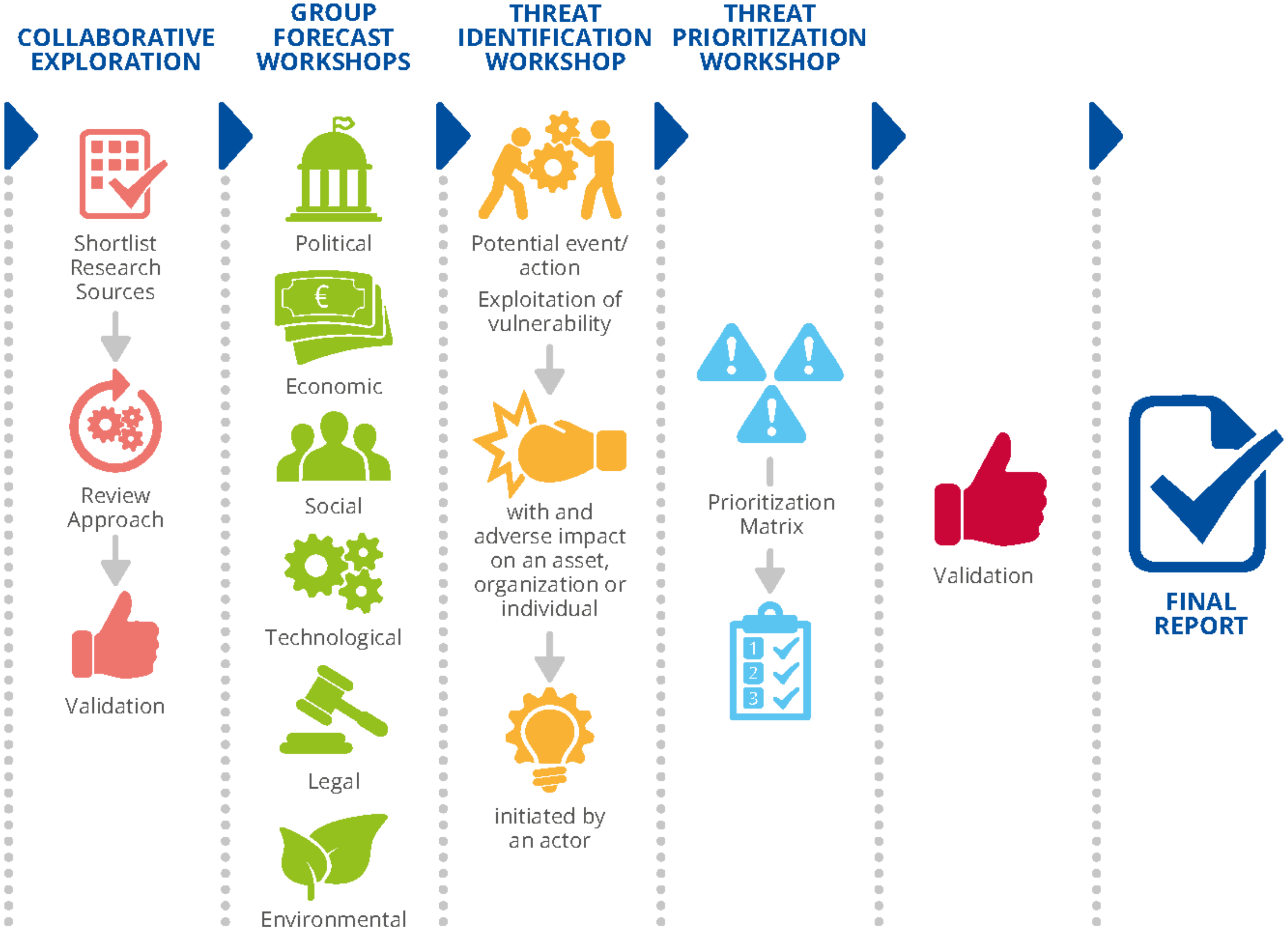
MARCH 2023

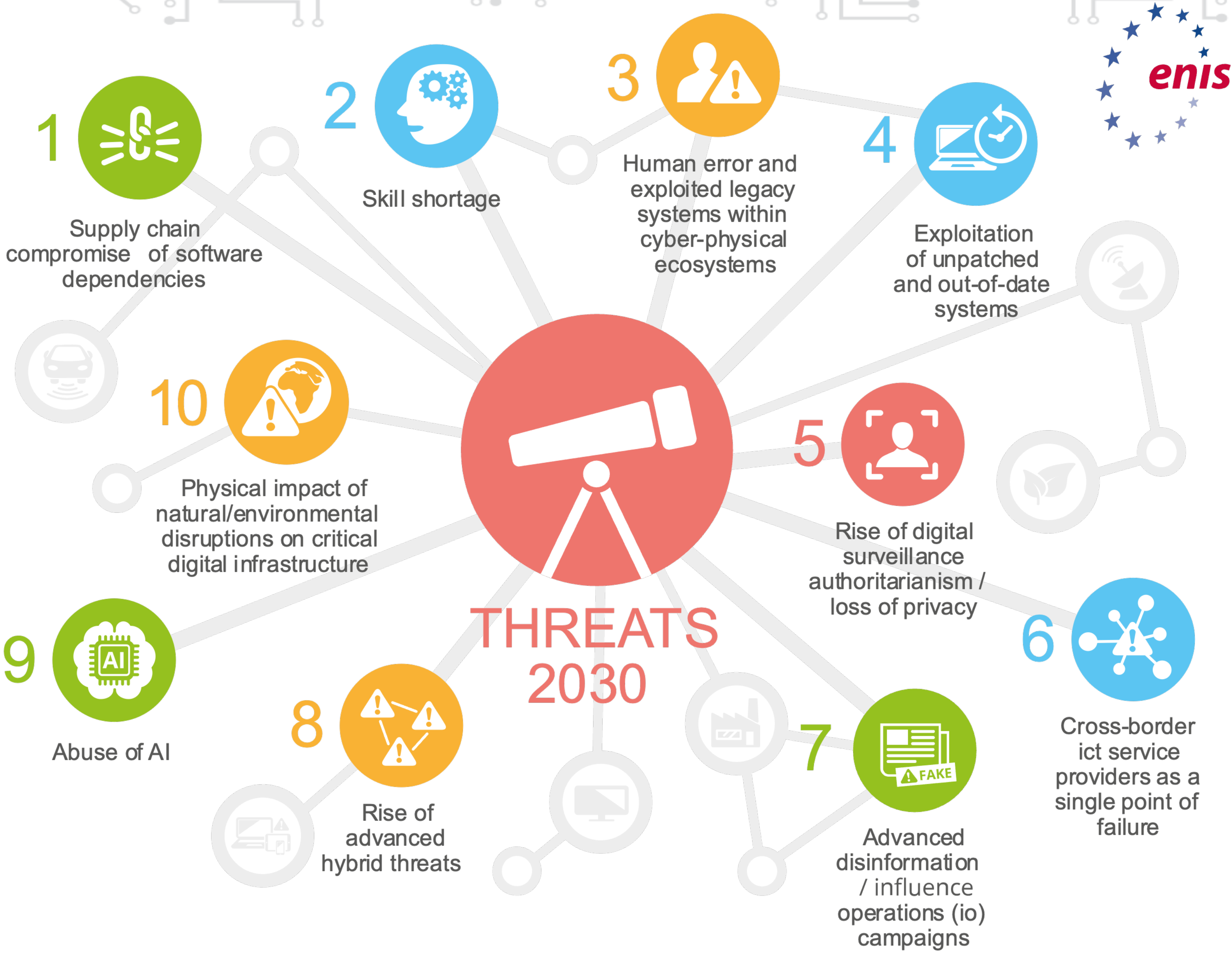
FORESIGHT 2030 THREATS

Today

Tomorrow

CYBERSECURITY FORESIGHT FOR 2030


COLLABORATIVE EXPLORATION
Shortlist Research Sources
Review Approach
Validation
GROUP FORECAST WORKSHOPS
Political
€
Economic
Social
Technological
Legal
Environmental
THREAT IDENTIFICATION WORKSHOP
Potential event/ action
Exploitation of vulnerability
with and adverse impact on an asset, organization or individual
initiated by an actor
THREAT PRIORITIZATION WORKSHOP
Prioritization Matrix
1
2
3
Validation
FINAL REPORT



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

https://www.enisa.europa.eu/topics/foresight

1. ATTACCO ALLA CATENA DI FORNITURA DELLE DIPENDENZE SOFTWARE

Supply chain compromise of software dependencies:
More integrated components and services from third party suppliers and partners could lead to novel and unforeseen vulnerabilities with compromises on the supplier and customer side.

[2022 ENISA Threat Landscape for Supply Chain Attacks]

[2023 ENISA Good Practices for Supply Chain Cybersecurity]

2. CARENZA DI COMPETENZE

Skill shortage
Lack of capacities and competencies could see cybercriminal groups target organisations with the largest skills gap and the least maturity.

2022 European Cybersecurity Skills Framework (ECSF)

#CYBERALL – breaking the bias code in cybersecurity

Upcoming 3rd ENISA Cybersecurity Skills Conference

3. ERRORE UMANO E SFRUTTAMENTO DI SISTEMI LEGACY ALL'INTERNO DI ECOSISTEMI CYBER-PHYSICAL

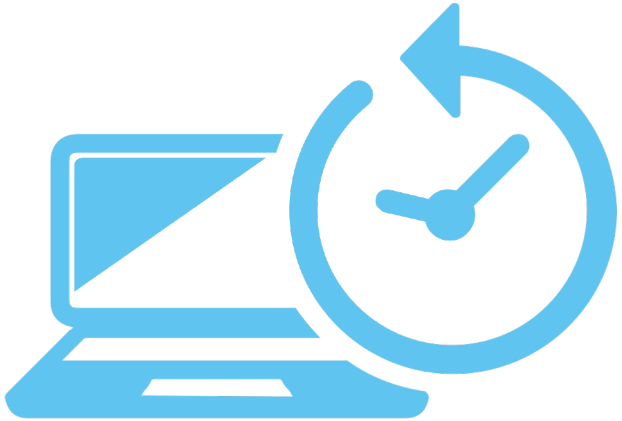
Human error and exploited legacy systems within cyber-physical ecosystems:
The fast adoption of IoT, the need to retrofit legacy systems and the ongoing skill shortage could lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem, which can lead to security maintenance issues.

ENISA Good practices for Critical infrastructures cybersecurity

ENISA Good practices for IoT Cybersecurity

New entry

4. SFRUTTAMENTO DI SISTEMI NON AGGIORNATI E OBSOLETI ALL’INTERNO DEL ECOSISTEMA TECNOLOGICO INTERSETTORIALE



↑

Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem:
Everything-as-a-service leads to a multitude of tools and services that require frequent and synchronized updates as well as orchestrated maintenance. This fact combined with the skill shortage presents a difficult to manage extended and unmanageable surface of vulnerabilities that can be exploited by threat actors.

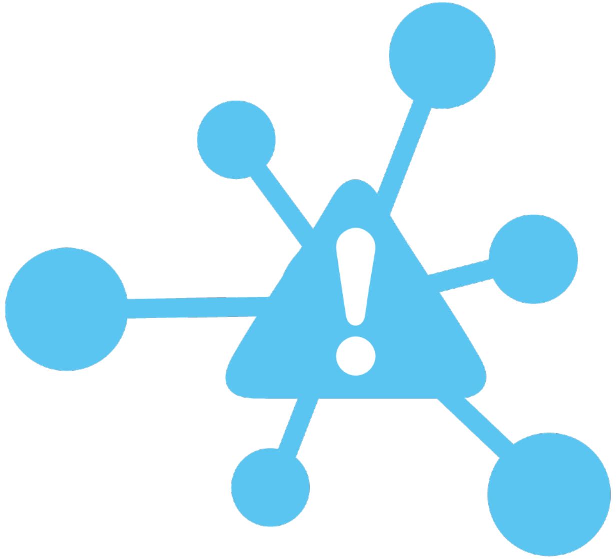
[2023 ENISA Health Threat Landscape]

[ENISA Good practices for Critical infrastructures cybersecurity]

5. AUMENTO DELLA SORVEGLIANZA DIGITALE NEI REGIMI AUTORITARI / PERDITA DI PRIVACY

Rise of digital surveillance authoritarianism/ loss of privacy:
Facial recognition, digital surveillance on internet platforms or digital identities data stores may become a target for criminal groups

[2024 ENISA Engineering Personal Data Protection in EU Data Spaces]



⬆

6. CROSS BORDER ICT SERVICE PROVIDERS COME SINGLE POINT OF FAILURE

Cross border ICT service providers as single point of failure:
ICT sector connecting critical services such as transport, electric grids and industry that provide services across borders are likely be to targeted by techniques such as backdoors, physical manipulation, and denials of service and weaponised during a future potential conflict.

2023 ENISA Transport Threat Landscape

2023 ENISA Cybersecurity and privacy in AI - Forecasting demand on electricity grids

7. CAMPAGNE AVANZATE DI DISINFORMAZIONE

Deepfake attacks can manipulate communities for (geo)political reasons and for monetary gain.

[2022 ENISA & EEAS Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape]

8. 8. AUMENTO DELLE MINACCE IBRIDE AVANZATE

Rise of advanced hybrid threats:
Physical or offline attacks are evolving and becoming often combined with cyberattacks due to the increase of smart devices, cloud usage, online identities and social platforms.

[2024 ENISA Remote ID Proofing - Good practices]

[2024 ENISA Best Practices for Cyber Crisis Management]

9. ABUSO DELL’IA

⬆

Artificial Intelligence Abuse:
Manipulation of AI algorithms and training data can be used to enhance nefarious activities such as the creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots and data poisoning.

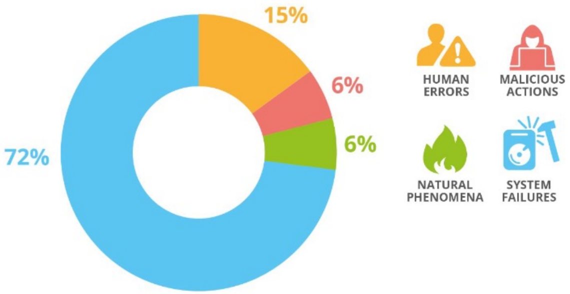
[2023 ENISA Multilayer Framework for Good Cybersecurity Practices for AI]

[2023 ENISA Cybersecurity and privacy in AI - Medical imaging diagnosis]

New entry

10. IMPATTO FISICO DELLE INTERRUZIONI NATURALI/AMBIENTALI SULLE INFRASTRUTTURE DIGITALI CRITICHE

Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure: The increased severity and frequency of environmental disasters following climate change may cause several unforeseen regional outages. Redundant back-up sites that maintain the availability of critical infrastructure are also affected by the massive and extreme weather phenomena.



ENISA Annual Telecom Security report – 2022 Incidents

JOIN US

BE A PART OF OUR ANNUAL FORESIGHT EXERCISE

Call for expression of interest

Join us by registering here: https://europa.eu/!3pRXw9

THANK YOU FOR YOUR ATTENTION

☎ ENISA Foresight team

✉ foresight@enisa.europa.eu

🌐 www.enisa.europa.eu

Break the bias code in Cybersecurity.

Diversity, equality and inclusion thrive in the cyber world.

They promote talent and innovative ideas.

Let's work together to promote a multidisciplinary cybersecurity culture and workforce.