

Picture courtesy of Gas Connect Austria

# Joint ENTSOG, EASEE-Gas, GIE Workshop

## DAY TWO: Cybersecurity

18<sup>th</sup> October 2023

ENTSOG offices, Brussels

# 1. Welcome



Andrea Chittaro

Chair of the ENTSOG/GIE Joint Task  
Force on Cybersecurity

## 2. Agenda



Douglas Walker Hill  
Interoperability & Data Exchange  
ENTSOE

ENTSOE

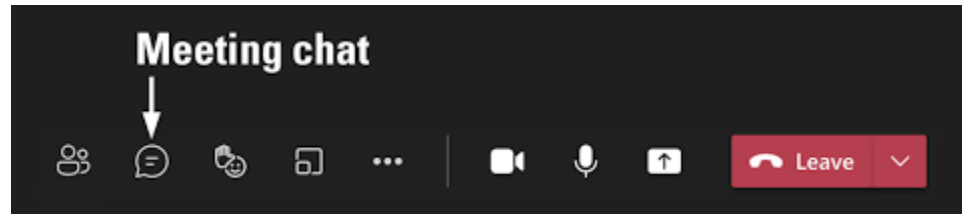
# Cybersecurity session 09:00-14:00 New lunch time =12:20



Speaking slot	DAY 2. 18th October - CYBERSECURITY - Presentation topics	Presenter and affiliation	From	To	04:00:00	
1	Introduction and welcome	Douglas Hill - ENTSOG	09:00:00	09:05:00	00:05:00	Physical
2	Agenda	Douglas Hill - ENTSOG	09:05:00	09:10:00	00:05:00	Physical
3	<b>Threats:</b> ENISA Cybersecurity landscape threat assessment	Konstantinos Moulinos - ENISA	09:10:00	09:25:00	00:15:00	Dial in
4	<b>Threats:</b> Evolution of Cybersecurity attacks - A TSO perspective	Lucrezia Tunesi - Snam	09:25:00	09:40:00	00:15:00	Dial in
5	<b>Threats:</b> Threat mitigation - A CS hardware provider perspective	Orlin Rachev & Yavor Enev Balkentel Ltd	09:40:00	09:55:00	00:15:00	Physical
6	<b>Legislation:</b> NIS 2.0 updates	Alessandro Lazari - F24	09:55:00	10:10:00	00:15:00	Dial in
	BREAK	20 Mins	10:10:00	10:30:00	00:20:00	
7	<b>International CS:</b> A research perspective on future cybersecurity issues using AI and quantum computing	Dr. Alexandru Georgescu - ICI	10:30:00	10:45:00	00:15:00	Dial in
8	<b>International CS:</b> ENTSOG ReCo Security of Supply	Anton Kolisnyk - ENTSOG	10:45:00	11:00:00	00:15:00	Dial in
9	<b>International CS:</b> Downstream perspectives of an electricity EU DSO and ENCS	Olivier Clement - DSO entity Maarten Hoeve - ENCS	11:00:00	11:15:00	00:15:00	Dial in
10	<b>International CS:</b> ENTSO-E. "ENTSO-E reflections on the challenges facing in the electricity sector."	Ivan Stefek - ENTSO-E	11:15:00	11:30:00	00:15:00	Dial in
11	<b>International CS:</b> European Defence Agency. The value of CS Table top exercises in the energy sector	Ioannis Chatzialexandris Brigadier General (retired), EDA	11:30:00	11:45:00	00:15:00	Dial in
12	<b>Awareness:</b> Introduction to the ENISA awareness package	Dr. Alexandros Zacharis - ENISA Dr. Georgia Bafoutsou - ENISA	11:45:00	12:15:00	00:30:00	Now dial in
13	Thank you, Q&A questions and goodbye	Douglas Hill - ENTSOG	12:15:00	12:20:00	00:05:00	Physical
	LUNCH	1 hour	12:20:00	13:20:00	01:00:00	

# Questions

---



- *Online please ask your questions via the Teams chat*
- *Physical attendance please ask questions at the end of the presentation*



# 3. ENISA Cybersecurity landscape threat assessment

Konstantinos Moulinos

Information security expert, EU  
Agency for Cybersecurity - ENISA

Agency for Cybersecurity - ENISA  
Information security expert



This document is marked as **TLP AMBER**



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

# ENTSOG WORKSHOP ON DATA EXCHANGE AND CYBERSECURITY IN THE ENERGY SECTOR

## ENERGY SECTOR CYBERSECURITY LANDSCAPE (OCTOBER 2023)

Konstantinos Moulinos  
Policy Development and Implementation Unit

**PLEASE CONTACT ENSIA FOR  
ACCESS TO THESE SLIDES, SEE  
BELOW THANK YOU**

**European Union Agency for Cybersecurity**

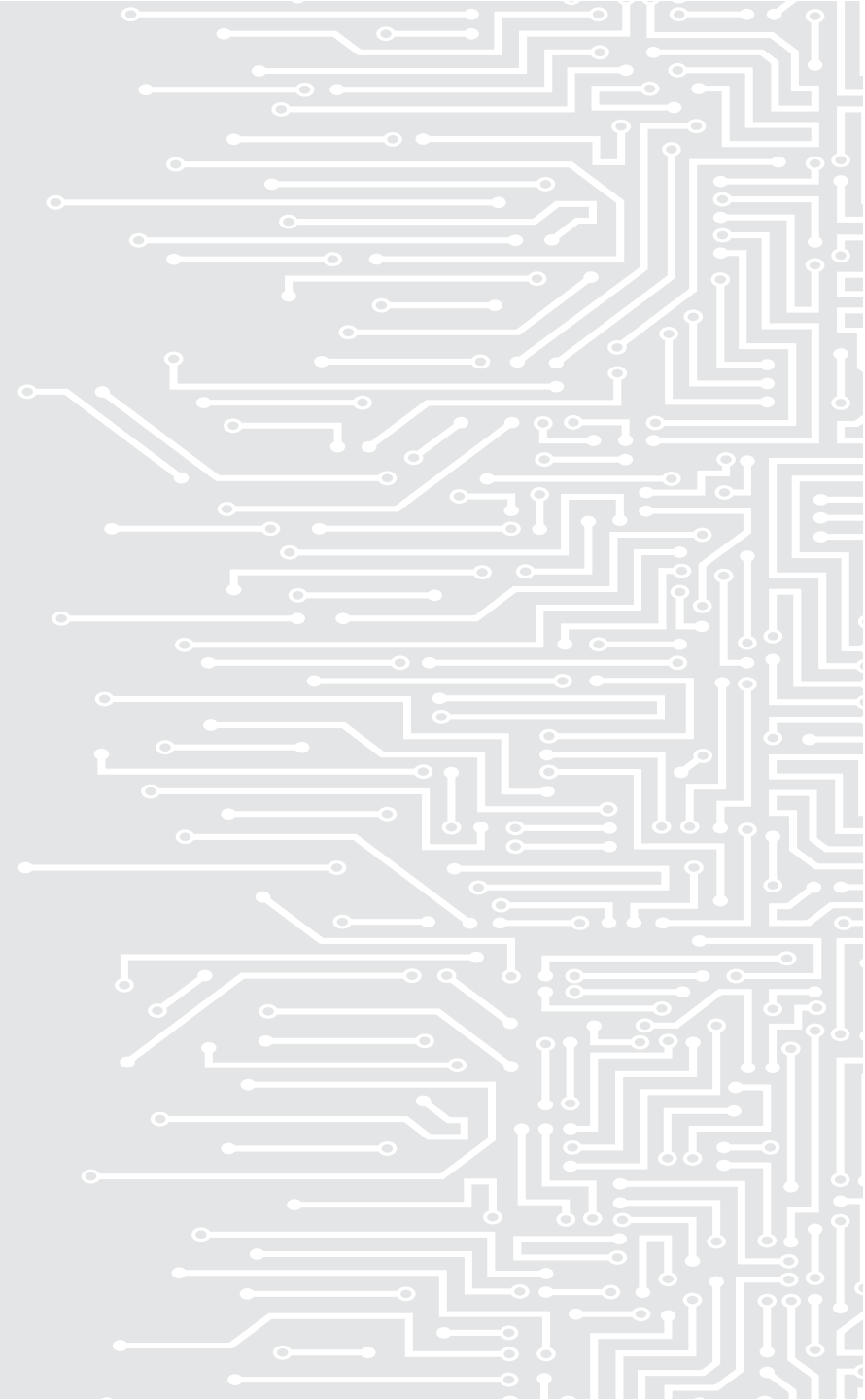
Agamemnonos 14 Str., 15231 Chalandri Attiki,

Greece

 +30 28 14 40 9711

 [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

 <http://www.enisa.europa.eu>





## 4. Evolution of Cybersecurity attacks - A TSO perspective



Lucrezia Tunesi  
Cyber security expert  
Snam

T H E E N E R G Y S E C T O R :  
C Y B E R T H R E A T L A N D S C A P E

Snam - Lucrezia Tunesi  
CTI Expert



# CYBER THREAT LANDSCAPE



**FINANCIALLY  
MOTIVATED**



**NATION-STATE  
ACTOR**



**HACKTIVIST**

# CYBER THREAT LANDSCAPE



PROFIT-ORIENTED CYBER CRIMINALS. CONSTANTLY SEARCH FOR NEW WAYS TO INCREASE REVENUE. FOCUSED ON HIGH-PROFILE VICTIMS

## TOP 10 RANSOMWARE GROUPS



"Researchers observed the double extortion model as the most common tactic exhibited by the adversaries"

*CrowdStrike2023GlobalThreatReport*

**LOCKBIT** IS THE MOST ACTIVE. FOCUSED ON **CRITICAL INFRASTRUCTURES** SINCE JANUARY 2020

**LOCKBIT 3.0**



# CYBER THREAT LANDSCAPE

HIGHLY SOPHISTICATED THREAT ACTORS COMMONLY ASSOCIATED WITH STATE-SPONSORED GROUPS. ABLE TO INFILTRATE THEIR VICTIM'S NETWORK AND STAY UNDETECTED FOR A PROLONGED PERIOD OF TIME.



## CHANGES IN THE GLOBAL ENERGY SUPPLY CHAIN AND NEW SCENARIOS



**NATION-STATE  
ACTOR**

**FBI warns energy sector of likely increase in targeting by Chinese, Russian hackers**

RUSSIA-UKRAINE CONFLICT

**German spy chief warns of cyberattacks targeting liquefied natural gas terminals**

ISRAEL-HAMAS CONFLICT

**Gaza-Based Cyber Threat Actor 'Storm-1133' Strikes Israeli Energy and Defense Sectors, Microsoft Reveals**

Oct 9, 2023 News

# CYBER THREAT LANDSCAPE



HISTORICALLY ASSOCIATED WITH UNSOPHISTICATED ATTACKS, THEY HAVE INCREASED THEIR CAPABILITIES. FOCUSED ON **HIGH-PROFILE VICTIMS** TO GAIN HIGHER MEDIA ATTENTION

## HACKTIVIST GROUPS:

*Killnet*

*NoName057(16)*

*Anonymous Russia*

*Xaknet*

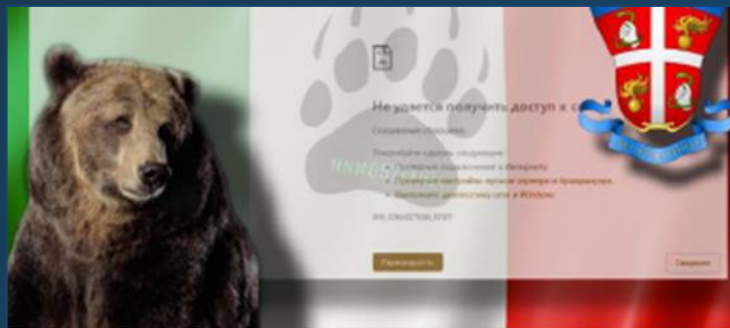
*Anonymous Sudan*

*AnonGhost*

*Cyber Av3ngers*

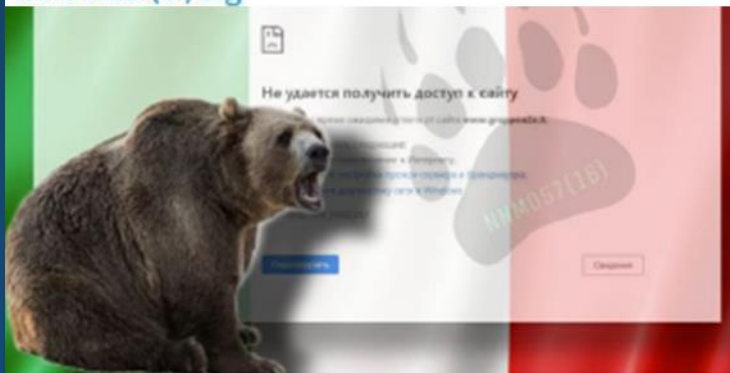
## TTPs:

- DENIAL OF SERVICE
- DATA EXFILTRATION

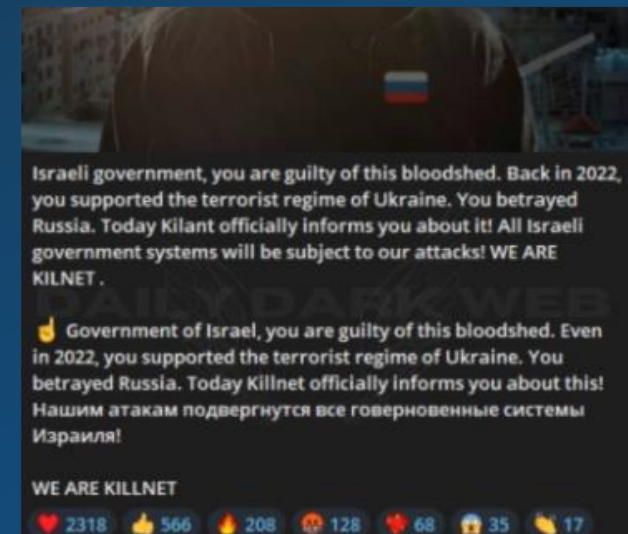


▼ Italy will supply Ukraine with the sixth military assistance package, which will include three types of air defense systems. As Italian Prime Minister Giorgia Meloni said during a press conference in Kyiv, it is talked about the SAMP-T, Skyguard, and Spike anti-tank systems.

NoName057(16) Eng



We shut down the website of the Italian energy company A2A SpA:



## 5. Threat mitigation - A hardware provider perspective.



Orlin Rachev Yavor Enev  
Business Development Manager  
Balkentel Ltd

Yavor Enev  
Project consultant  
Balkentel Ltd

# Overview, presented by Orlin Rachev, BDM





# BALKANTEL at a Glance

Leading company in the Transport, Telecom, Defense and Utility sectors with an integrated offer of high-tech solutions

Balkantel offers end-to-end solutions, from design and manufacturing to integration and long-term maintenance. Established in Sofia, Bulgaria in **1990**, we bring over three decades of experience in **Railways, Aviation, Defence, Telecom, and Utility** sectors. Our **180+** technical experts are the driving force behind our success. We provide field-proven products in communication, information, and control. With offices in **Bulgaria, Serbia, and the USA**, we serve clients globally.



# Key sectors and customers

Delivering turnkey solutions with a focus on safety and reliability in mission-critical sectors

In brief, our clients can be best described as 'Mission Critical.'

## TRANSPORT

### Air Traffic Control

- > Air Navigation Service Providers
- > Airport Operators
- > Investment & Construction companies

### Railways

- > National railway companies
- > Railways Operators
- > Construction companies

## DEFENCE

### Ministry of Defence

- > Air Forces
- > Land Forces
- > Navy
- > Communications Division

## PUBLIC SERVICES

**Electronic Governance Infrastructure**  
**Interior Ministry**  
**Telecoms**

## UTILITIES

### Electricity

- > Electricity plants
- > TSOs

### Oil & Gas

- > TSOs
- > Gas distribution operators

### Water Suppliers

# Problems solved by Balkantel for gas stakeholders

Our focus in the gas industry

- > Network Security;
- > Data Protection;
- > Remote Monitoring and Control;
- > Resilience to Cyberattacks;
- > Emergency Response;
- > Predictive Maintenance;



# Hardware mitigation of cyber threats

Proven and designed for critical infrastructure including the gas sector

- > Inherent Resilience;
- > Isolation from Software Vulnerabilities;
- > Speed and Real-time Protection:  
Tamper Resistance.
- > Consistency Across Environments;
- > Reduced Attack Surface;
- > Longer Lifecycle;
- > Compliance to the Cyber Resilience Act;
- > ATEX certification when necessary to be applied.



# Hardware mitigation Essentials

Overview of the most Important features

- > Remote Monitoring;
- > Encrypted Communications;
- > Reliable Honeypot and detection devices ;
- > Network segmentation and isolation -;
- > 99,99% availability and redundancy –Any OT device should remains in service in any event;
- > Security of Endpoint Devices – the end point device in the critical infrastructure such as RTUs and PLC need an additional protection.



## Suite for Cyber Security solutions

Recommended hardware solution

- > Network Decoy;
- > Early warning systems with detection and alerting of cyber breaches and network intrusion;
- > Network Isolation, creating operational isolation zones;
- > Failover systems for redundancy;
- > Detecting data leaks with forensic analysis in near real time;
- > Cyber Secure Rack with no-single point-of-failure;
- > Endpoint device security solution.



## Network Isolation (Kill) Switch

Isolate digital assets in a cyber attack

- > Network Isolation in a cyber-attack;
- > Create LAN / WAN isolation;
- > Create operational isolation zones;
- > Isolate SAN/NAS, Data Storage, Back-up servers;
- > Provides manual and automatic isolation of LAN from WAN, in an event of a network security breach / cyber-attack ransomware attack;
- > Create Operational Zones or secure parameter zones with the external network isolate the network in the event of the detection of a network in the cyber-security perimeter of the network's demilitarized zone;
- > Port for isolation of Network Port and Management Port;
- > External triggers using dry-contact alarm relay;
- > Script assisted switching through serial interface;
- > Fail-safe. The unit itself should never becomes a point of failure, even in power down condition.



# Automatic Ethernet Failover Switch

Failover systems Switch for network and equipment redundancy - 99.99% availability and redundancy

- > Delivers 1+1 Automatic Ethernet Failover Protection, seamlessly transitioning between 'active' and 'standby' equipment;
- > Enhances equipment and network availability, meeting 99.99% uptime requirements;
- > Designed for reliability: remaining fail-safe even during power-down situations for uninterrupted operation.
- > Offers comprehensive End-to-End network link monitoring with user-configurable parameters for testing and switching.





## Network Traffic Sniffer

Detecting data leaks with forensic analysis in real time

- > Continuously scans inbound and outbound traffic, generating alerts for unauthorized data transmissions from servers or IEDs (e.g., RTUs, PMUs, Bay Control Units);
- > Real-time detection of firewall breaches, network intrusions, and cyber-attacks.
- > Identifies and alerts on data leaks within the organization
- > Provides user data for forensic analysis and attack route tracing, aiding in identifying network vulnerabilities.;
- > A valuable tool for bolstering cybersecurity in Power Utility Networks, Power Sub-Stations, SCADA Networks, and Oil and Gas Pipelines



## Endpoint device security solution

Ultra-resilient and failsafe protection of RTU, PLC etc. IED

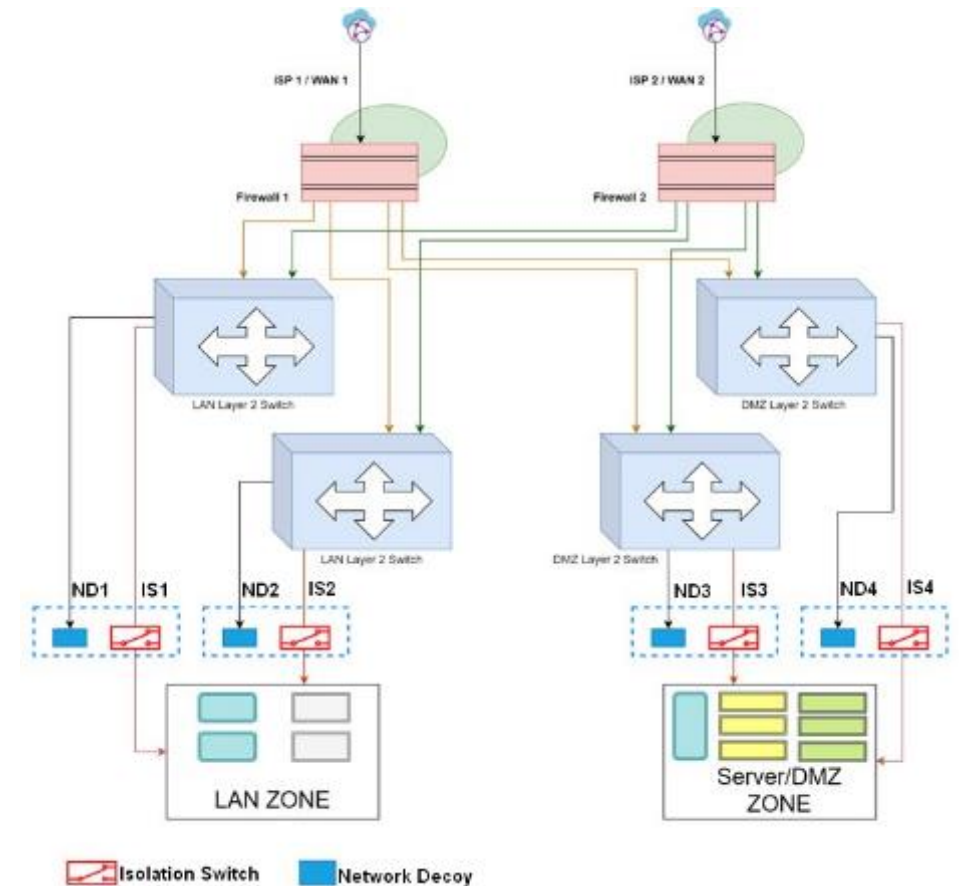
- > Detailed packet inspection and per frame authentication;
- > Finger-prints and logs all unauthorized traffic and access attempts;
- > Detailed logging of MODBUS and IEC-104 traffic including ASDU types;
- > Whitelist and blacklist firewall modes;
- > Customizable IP/MAC/port filter to drop all non-conforming communication / packets;
- > Does not add any measurable latency. The latency added under full load conditions is less than 1ms;
- > Timestamping with millisecond accuracy using NTP.



# Main requirements to the equipment suite

## Important check list

- > Automatically executes a counter-defense strategy if a network intrusion / cyber-attack is detected by isolating the critical infrastructure assets;
- > Provides audio-visual alerts in the event of detection of a cyber-attack;
- > Monitoring and visualization of all cyber-security equipment, alarms, and events in real-time;
- > Assists in providing forensic analysis in near real-time;
- > Customizable IP/MAC/port filter to drop all non-conforming communication / packets;
- > Provides the option of 1+1 redundancy with automatic failover of equipment and networks;
- > No single point of failure in the network for enhanced resilience.



---

**Thank you!**

**Orlin Rachev**

Business Development and Marketing Manager

M: +359 888 206 308

E: [orlin.rachev@balkantel.net](mailto:orlin.rachev@balkantel.net)

**Yavor Enev**

Project consultant

M: +359 87 837 5089

E: [yavor.enev@balkantel.net](mailto:yavor.enev@balkantel.net)



## 6. Legislation: NIS 2.0 updates



Alessandro Lazari  
Senior key account manager  
F24 (critical infrastructure consultancy)

**ENTSOG's Joint Annual Workshop on Data  
Exchange & Cybersecurity  
in the energy sector  
18<sup>th</sup> October 2023**



**Legislation: NIS 2.0 updates**

# The Cyber Resilience ACT



Brussels, 15.9.2022  
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020**

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

Hardware and software products suffer from **two major problems** adding costs for users and the society:

1. a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
2. an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

**Two main objectives** were identified aiming to ensure the proper functioning of the internal market:

1. create conditions for the **development of secure products** with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and
2. create conditions allowing users to **take cybersecurity into account when selecting and using products** with digital elements.

**Four specific objectives** were set out:

1. ensure that **manufacturers improve the security of products** with digital elements since the design and development phase and throughout the whole life cycle;
2. ensure a **coherent cybersecurity framework**, facilitating compliance for hardware and software producers;
3. enhance the **transparency of security properties** of products with digital elements, and
4. enable businesses and consumers to **use products with digital elements securely**.

# The Cyber Resilience ACT (2)



Brussels, 15.9.2022  
COM(2022) 454 final  
2022/0272 (COD)

Proposal for a  
**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
**on horizontal cybersecurity requirements for products with digital elements and**  
**amending Regulation (EU) 2019/1020**



(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

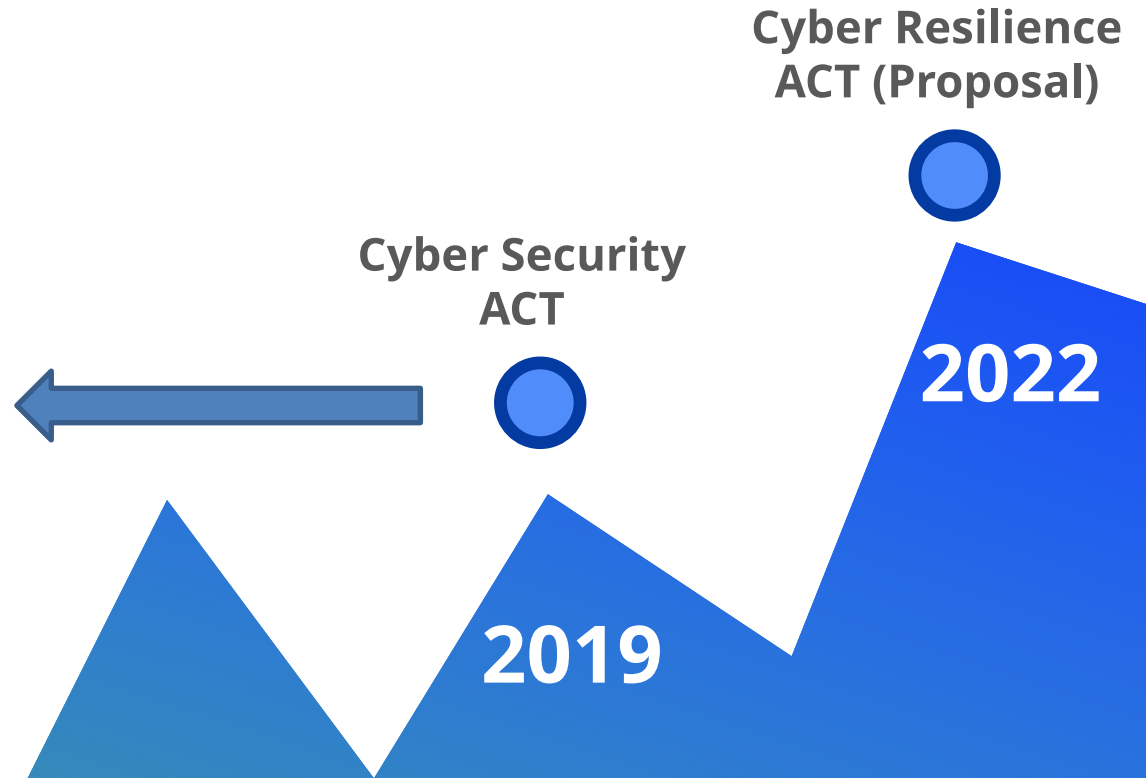




# Measures aimed at improving the security of products

High level objectives:

1. Harmonization of certifications in the EU
2. Involvement of National Accreditation and Certification bodies
3. Fostering a single market of certified products, services and processes
4. Creation of horizontal and vertical schemes



# Security requirements for ICT product certification



## Cybersecurity – security requirements for ICT product certification

Have your say > Published initiatives > Cybersecurity – security requirements for ICT product certification

- In preparation
- Draft act**  
Feedback period  
03 October 2023 - 31 October 2023  
**FEEDBACK: OPEN**
- UPCOMING
- Commission adoption  
Planned for  
Fourth quarter 2023

### About this initiative

**Summary** This initiative will establish the European cybersecurity certification scheme (EUCC) based on common criteria.

The voluntary scheme will introduce a set of security requirements for ICT security products (e.g. firewalls, encryption devices, electronic signature devices) and ICT products with an inbuilt security functionality (i.e. routers, smartphones, bank cards).

Users of products certified under this scheme will have greater security.

**Topic** Digital economy and society

**Type of act** Implementing regulation

**Committee** [C106400](#)

### Draft act

**FEEDBACK: OPEN**

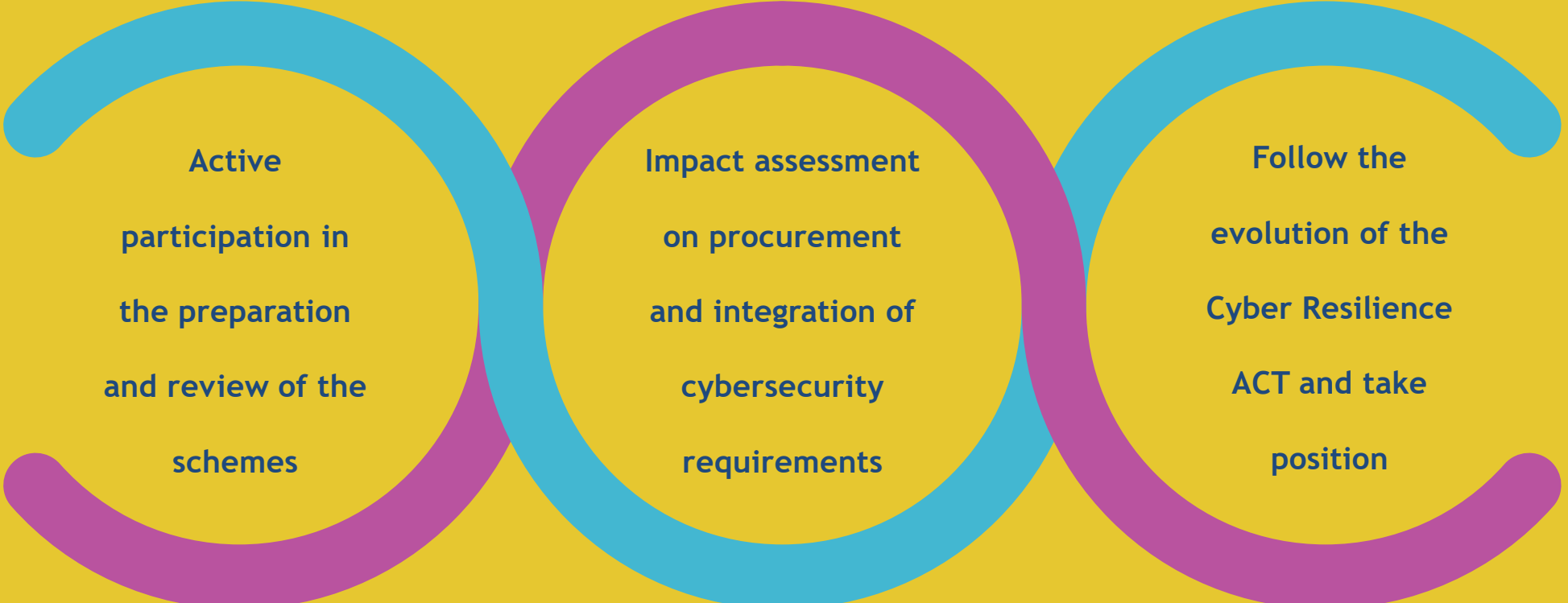
**Feedback period**  
03 October 2023 - 31 October 2023 (midnight Brussels time)

**The Commission would like to hear your views.**

\* <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product->



# Areas of interest for the GAS SECTOR

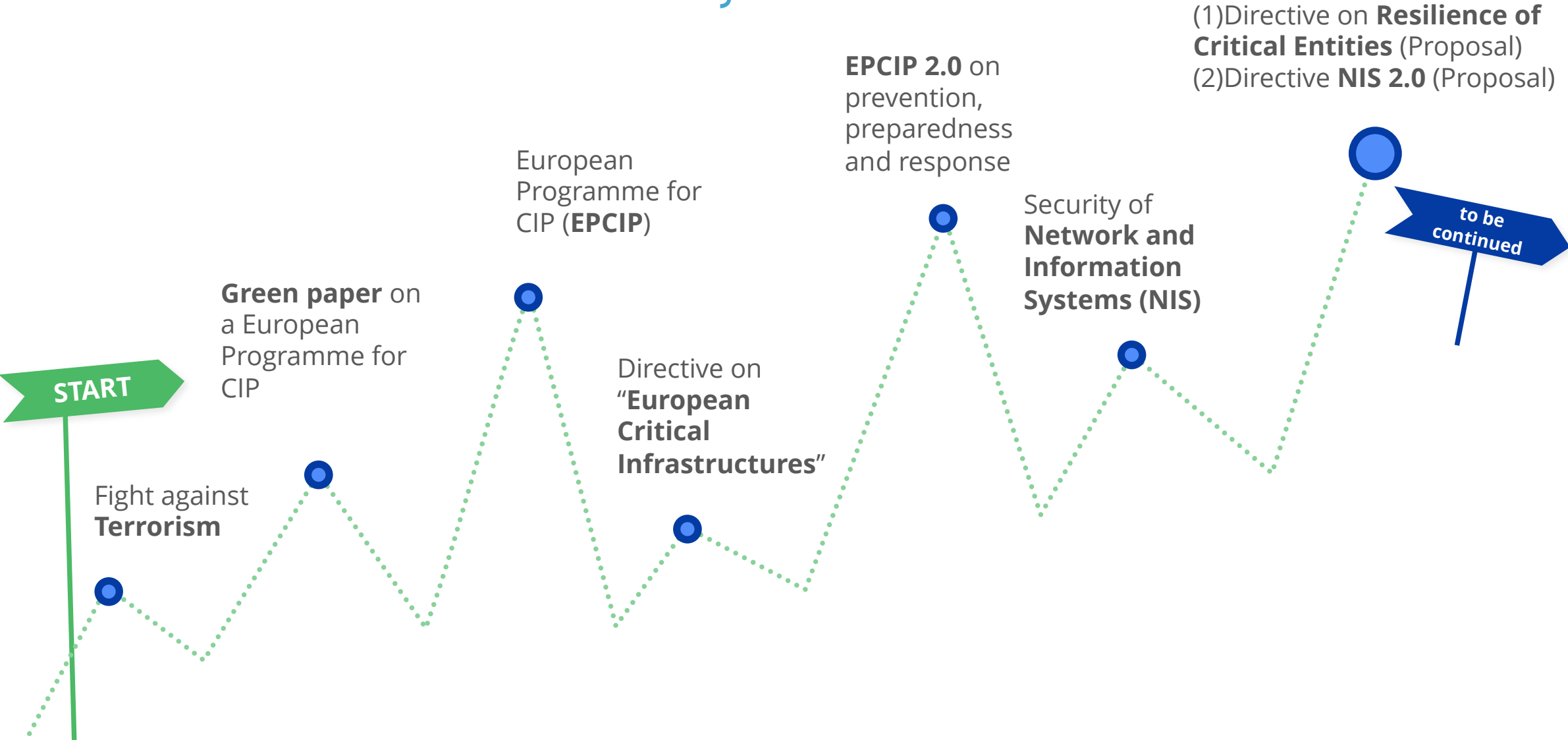


Active participation in the preparation and review of the schemes

Impact assessment on procurement and integration of cybersecurity requirements

Follow the evolution of the Cyber Resilience ACT and take position

# Normative Landscape in Security and Resilience



# Normative Landscape in Security and Resilience (2)

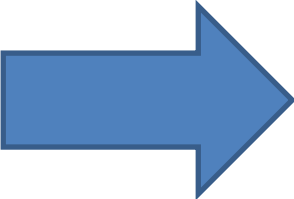
(1) Directive on Resilience of Critical Entities (Proposal)

(2) Directive NIS 2.0 (Proposal)

NIS 2.0  
CER  
DORA regulation  
(promulgated)

2022

2020



27.12.2022 EN Official Journal of the European Union L 333/80

**DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
of 14 December 2022  
on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

27.12.2022 EN Official Journal of the European Union L 333/164

**DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
of 14 December 2022  
on the resilience of critical entities and repealing Council Directive 2008/114/EC

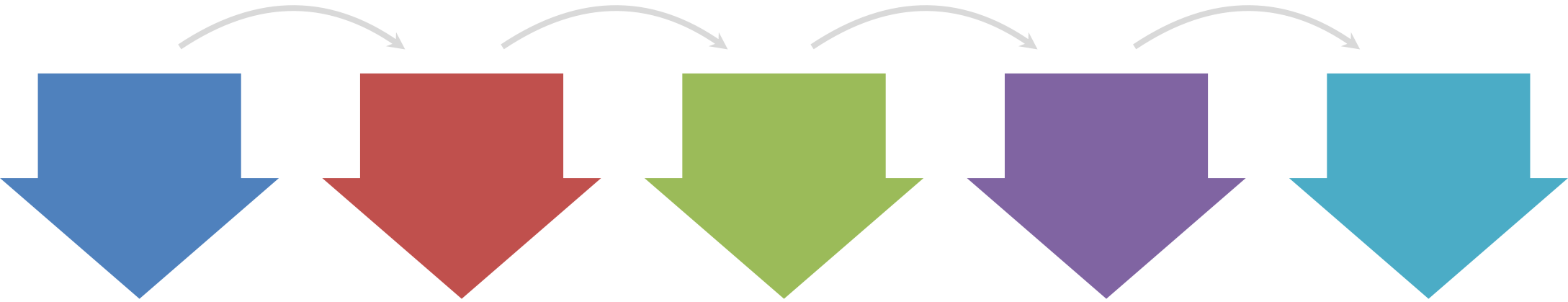
27.12.2022 EN Official Journal of the European Union L 333/1

**REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
of 14 December 2022  
on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

# The NIS 2 Directive (some highlights)

27.12.2022 EN Official Journal of the European Union L 333/80

**DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
**of 14 December 2022**  
**on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)**



creating the necessary  
cyber crisis management  
structure (CyCLONe)

increasing the level of  
harmonization regarding  
security requirements and  
reporting obligations

encouraging Members  
States to introduce new  
areas of interest in their  
national cybersecurity  
strategies

covering a larger share of  
the economy and society  
by including more sectors

bringing novel  
harmonization efforts  
such as the peer reviews  
for enhancing  
collaboration and  
knowledge sharing  
amongst the Member  
States



# Areas of interest for the GAS SECTOR

Art. 21

more detailed  
cybersecurity risk  
management  
measures

Art. 23

Improved reporting  
obligations and  
definitions of  
significant incident

Art. 24

Use of cybersecurity  
certification schemes to  
demonstrate compliance  
with requirements of  
Art. 21

## Something more about article 21



The measures shall be based on an **all-hazards approach** that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

1. policies on risk analysis and information system security;
2. incident handling;
3. business continuity, such as backup management and disaster recovery, and crisis management;
4. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
5. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
6. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
7. basic cyber hygiene practices and cybersecurity training;
8. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
9. human resources security, access control policies and asset management;
10. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.



## Something more about article 23



An incident shall be considered to be significant if:

- it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
- it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Member States shall ensure that the entities concerned submit to the CSIRT :

- a. without undue delay and in any event **within 24 hours of becoming aware of the significant incident**, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
- b. without undue delay and in any event **within 72 hours of becoming aware of the significant incident**, an incident notification, which, where applicable, shall update the information referred to in point (a) and **indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise**;
- c. upon the request of a CSIRT or, where applicable, the competent authority, **an intermediate report on relevant status updates**;
- d. **a final report not later than one month** after the submission of the incident notification

# The CER Directive (some highlights)

27.12.2022

EN

Official Journal of the European Union

L 333/164

**DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**of 14 December 2022**

**on the resilience of critical entities and repealing Council Directive 2008/114/EC**



new rules strengthen the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage

security requirements and reporting obligations complementary to the NIS 2

Members States to adopt a strategy on the resilience of critical entities and perform National Risk Assessments

covering a larger share of the economy and society by including 11 sectors

creation of the Critical Entities Resilience Group



# Areas of interest for the GAS SECTOR

Art. 12

Risk assessment  
by critical entities

Art. 13

Resilience  
measures of  
critical entities

Art. 14

Background checks

Art. 15

Incident notification

## Something more about article 12



1. Member States shall ensure that critical entities carry out a **risk assessment within nine months** of receiving the notification referred to in Article 6(3), whenever necessary subsequently, **and at least every four years**, on the basis of Member State risk assessments and other relevant sources of information, in order to **assess all relevant risks that could disrupt the provision of their essential services** ('critical entity risk assessment').
2. Critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541. A critical entity risk assessment shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities in such other sectors, including, where relevant, in neighbouring Member States and third countries.

## Something more about article 13



Member States shall ensure that critical entities **take appropriate and proportionate technical, security and organisational measures to ensure their resilience**, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- a. prevent incidents from occurring, duly considering **disaster risk reduction and climate adaptation measures**;
- b. ensure adequate **physical protection of their premises and critical infrastructure**, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;
- c. **respond to, resist and mitigate the consequences of incidents**, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
- d. **recover from incidents, duly considering business continuity measures and the identification of alternative supply chains**, in order to resume the provision of the essential service;
- e. **ensure adequate employee security management**, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
- f. raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly **considering training courses, information materials and exercises**.

## Something more about article 14



Member States shall specify the conditions under which a critical entity is permitted, in duly reasoned cases and taking into account the Member State risk assessment, to **submit requests for background checks on persons who:**

- a. **hold sensitive roles in or for the benefit of the critical entity**, in particular in relation to the resilience of the critical entity;
- b. **are authorised to directly or remotely access its premises, information or control systems**, including in connection with the security of the critical entity;
- c. **are under consideration for recruitment to positions that fall under the criteria set out in point (a) or (b).**

## Something more about article 15



Member States shall ensure that critical entities notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Member States shall ensure that, unless operationally unable to do so, **critical entities submit an initial notification no later than 24 hours after becoming aware of an incident**, followed, where relevant, by a **detailed report no later than one month thereafter**. In order to determine the significance of a disruption, the following parameters shall, in particular, be taken into account:

- a. the number and proportion of users affected by the disruption;
- b. the duration of the disruption;
- c. the geographical area affected by the disruption, taking into account whether the area is geographically isolated.

# Some literature for your attention

## NEWS ITEM

### Cyber Insurance: Fitting the Needs of Operators of Essential Services?

The new report by the European Union Agency for Cybersecurity (ENISA) explores the challenges faced by Operators of Essential Services in the EU, when seeking to acquire cyber insurance.

Published on February 23, 2023



Focused on the potential challenges faced by Operators of Essential Services (OESs), the analysis performed also explores aspects of cyber insurance from a policy development perspective, and suggests recommendations to policymakers and to the community of OESs.

### What does the report reveal?

With the current trend of increasing cyber incidents also affecting OESs to a large extent, a majority of them perceive cyber insurance as a service they cannot afford given the outstanding premiums and disadvantageous coverage. According to data gathered through a survey targeting 262 OESs across the EU, **three in four do not currently have cyber insurance coverage**. The survey also reveals that other risk mitigation strategies are often considered more favourable by OESs.

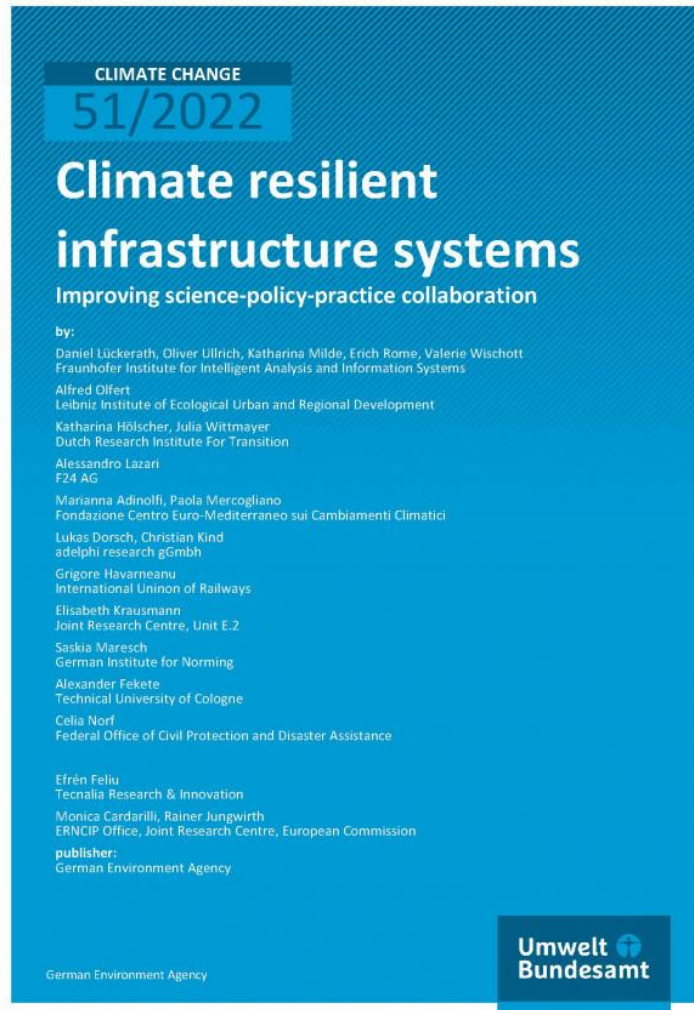
For 77% of respondents, a formalised process has been set to identify cyber risks. **The remaining 23% do not have any such process in place**. On the other hand, **64% of organisations declare not quantifying cyber risks**. However, all interviewed contributors declare having risk-management practices in place and a process to determine controls.

The motivators behind the decision to contract insurance coverage include coverage in case of a loss as a result of a cyber incident for 46%, requirement by law for 19%, pre-incident or post-incident expert knowledge from insurance companies.

**56% of respondents declared they considered other risk mitigation tools more effective than cyber insurance.**



## Some literature for your attention (2)



In 2021 [UBA](#) commissioned workshops to discuss **how research outputs on climate resilient infrastructure systems could be more consistently transferred into practice of infrastructure operation**. This paper presents barriers for successful transfer and provides recommendations to overcome them. The target audiences for these recommendations are funding bodies, policy makers, and standardization bodies that can influence the framework conditions under which infrastructure resilience research takes place, research project coordinators and other academic/researcher institutions who design research projects, and **practitioners who design and manage (critical) infrastructure systems**.

## Some literature for your attention (3).



In 2014 NATO's Centre of Excellence-Defence Against Terrorism (COE-DAT) launched the inaugural course on "Critical Infrastructure Protection Against Terrorist Attacks." As this course garnered increased attendance and interest, the core lecturer team felt the need to update the course in critical infrastructure (CI) taking into account the shift from an emphasis on "protection" of CI assets to "security and resiliency." What was lacking in the fields of academe, emergency management, and the industry practitioner community was a handbook that leveraged the collective subject matter expertise of the core lecturer team, a handbook that could serve to educate government leaders, state and private-sector owners and operators of critical infrastructure, academicians, and policymakers in NATO and partner countries. *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency* is the culmination of such an effort, the first major collaborative research project under a Memorandum of Understanding between the US Army War College Strategic Studies Institute (SSI), and NATO COE-DAT.

**ENTSOG's Joint Annual Workshop on Data  
Exchange & Cybersecurity  
in the energy sector  
18<sup>th</sup> October 2023**



**Thanks for your attention!**

20 min Coffee break 10:10 - 10:30



## 7. International CS: A research perspective on future cybersecurity issues using AI and quantum computing



Dr. Alexandru Georgescu – ICI Bucharest  
Scientific Researcher  
National institute for research and development in  
informatics



**NATIONAL INSTITUTE FOR RESEARCH AND DEVELOPMENT  
IN INFORMATICS - ICI BUCHAREST**

# **Perspectives on future cybersecurity issues using AI and quantum computing**

---

**Dr. Alexandru Georgescu  
ICI Bucharest**

# How did we end up here

- The digitalization of life, society, the economy and politics
- Hybrid warfare and asymmetric warfare, including tactics such as state sponsored actors and proxies
- Targeting civilian infrastructure – banks, power generation and transmission, retailers, hospitals
- Transborder (dis)organized crime
- Global challenges related to networks, technologies, infrastructure, standards, regulations, conduct etc.
- Emerging technologies rapidly being implemented for profit and efficiency



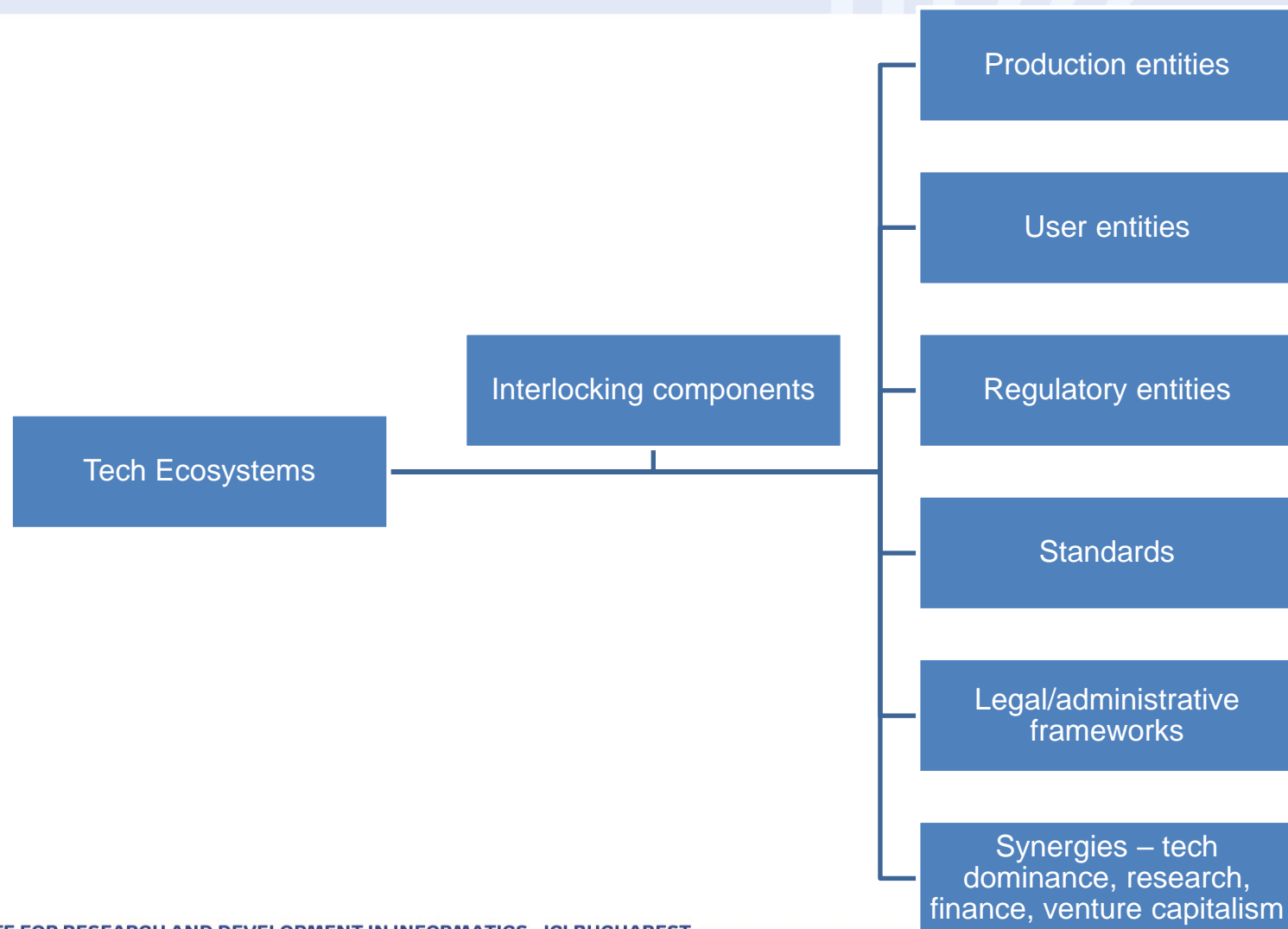
# What is cybersecurity innovation about?

- The allocation of resources for cybersecurity purchases
- The pipeline for new products and services
- The pipeline and maturation rate for new technologies
- The possibility of the exchange of information, including in an automated way
- The development of cybersecurity culture as part of security culture in general
- Resilience by design in new critical infrastructures/critical entities
- A strategic culture that prioritizes cybersecurity
- Education that prioritizes lifelong training, competence certification and retention
- The deliberate reinforcement of strategic targets such as the Three Seas Initiative project
- Regional and global cybersecurity governance

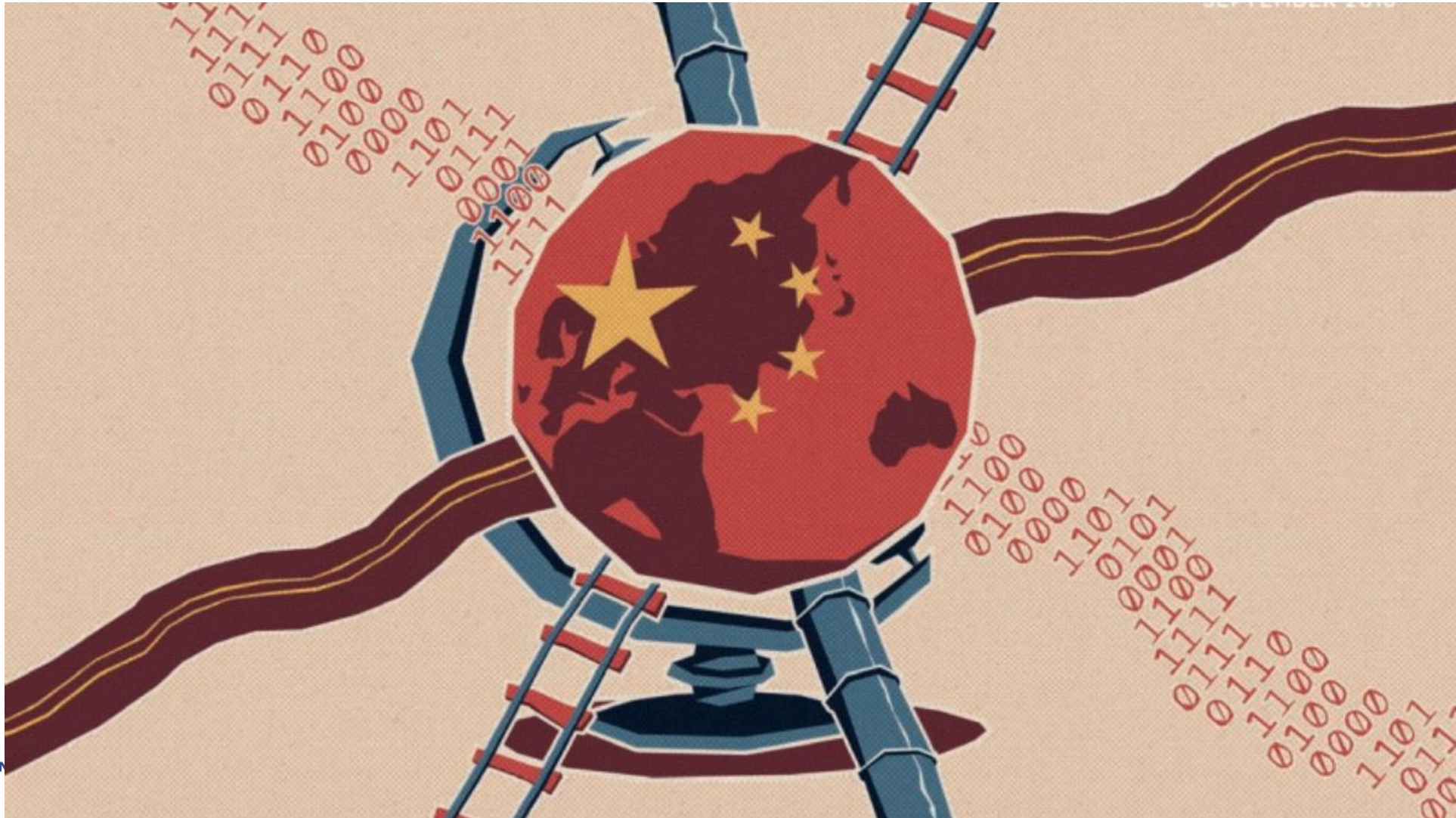




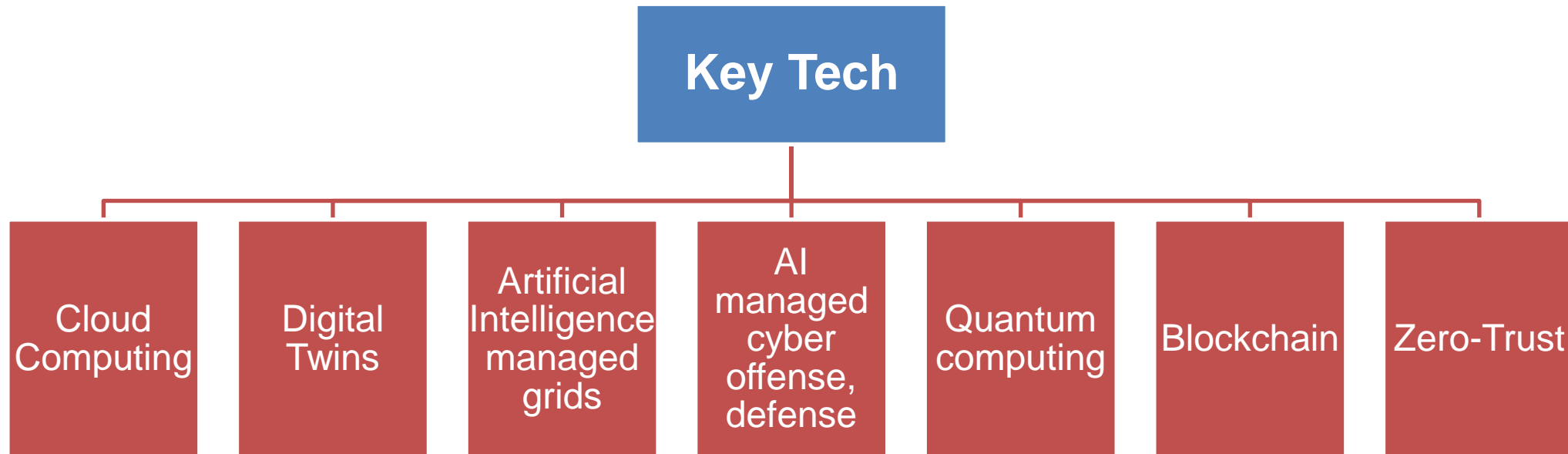
# What is the ecosystem composed of?



# Emerging digital technologies as a source of geopolitical power

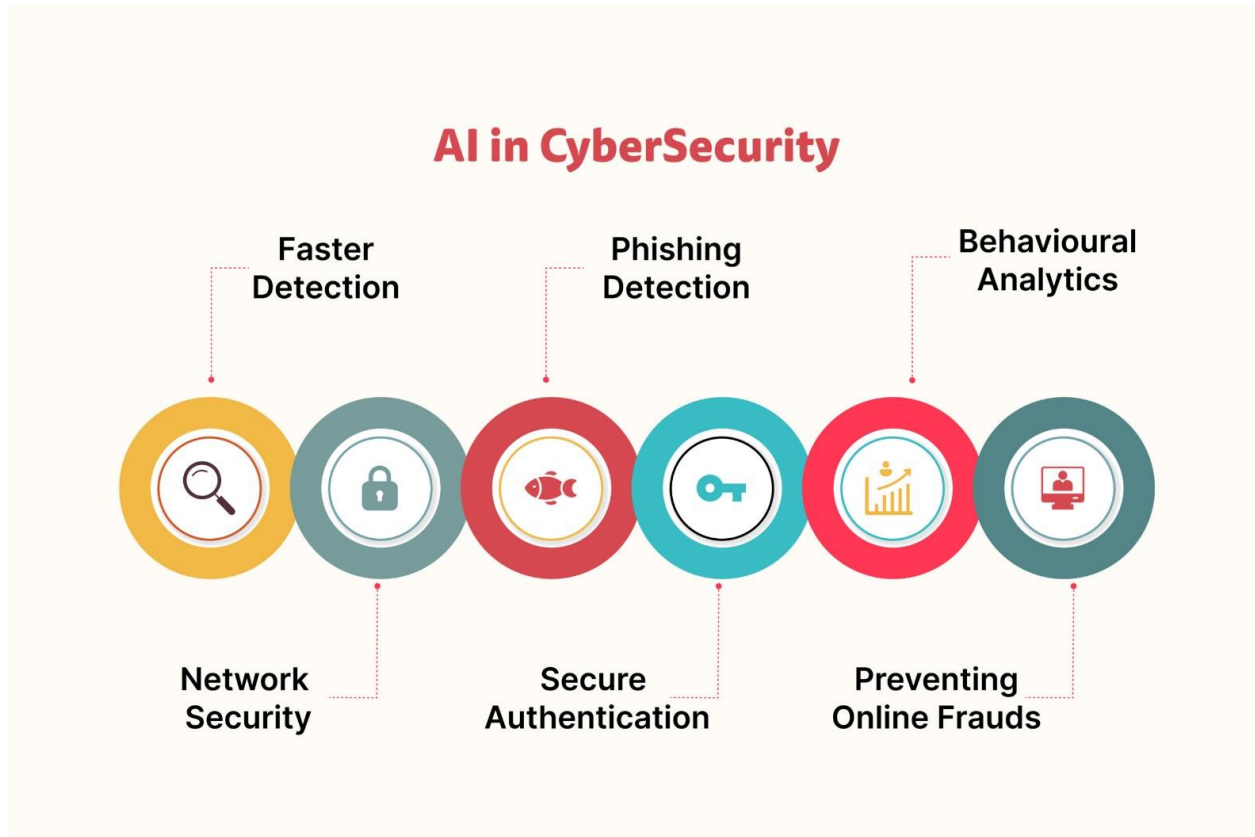


# Digital (Emerging) Technologies Affecting Cybersecurity in Energy

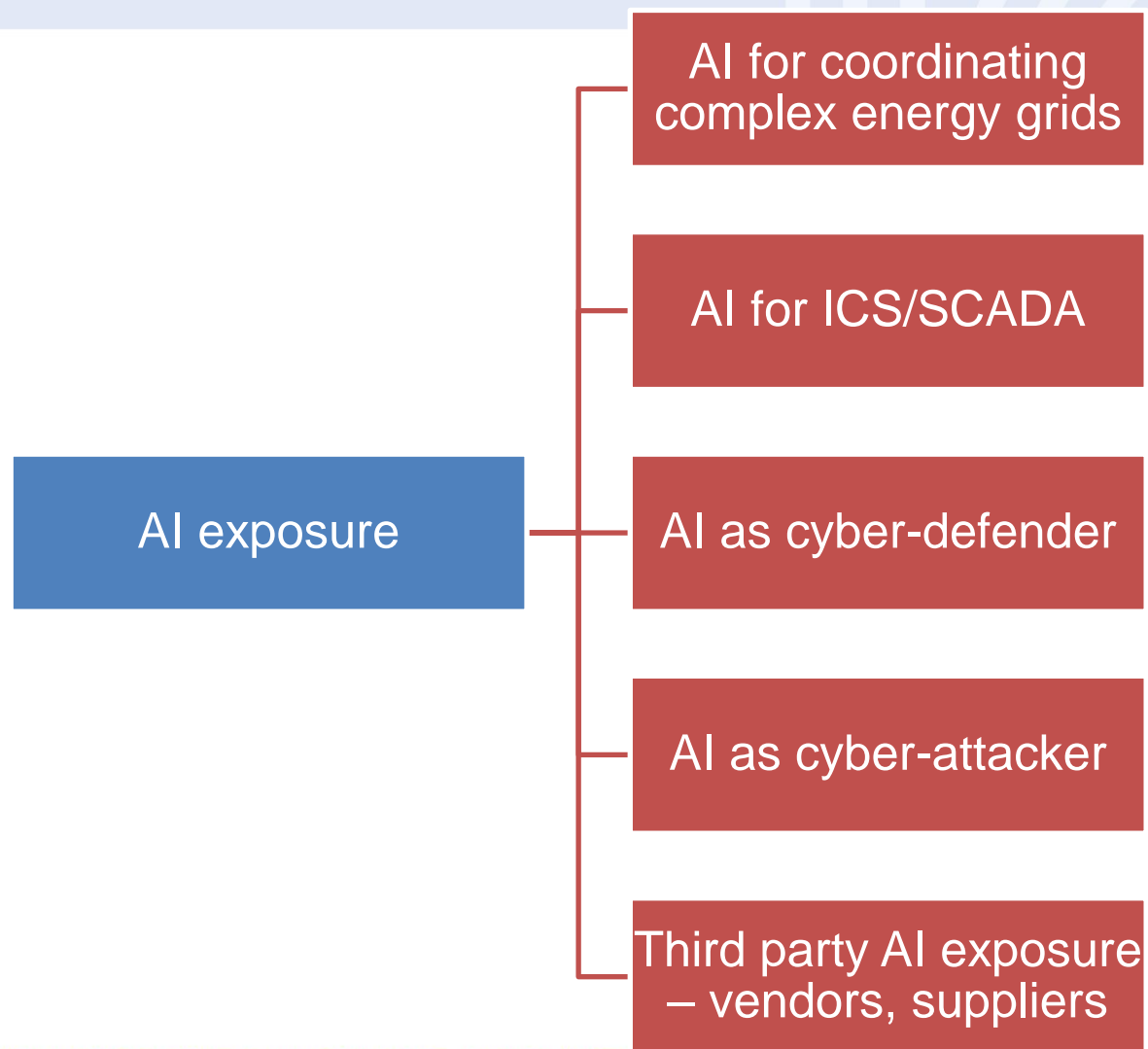


## Artificial Intelligence (and Machine Learning)

- AI can become a gamechanger in cybersecurity, both as defender and attacker
- These systems can analyze enormous amounts of data quickly, without the need for human oversight, making them ideal for identifying suspicious activity and defending against advanced threats.
- Cybersecurity professionals are already leveraging AI and ML to detect real-time cyberattacks, making their role even more important in maintaining a secure online environment.







## Exposure to AI in the energy sector



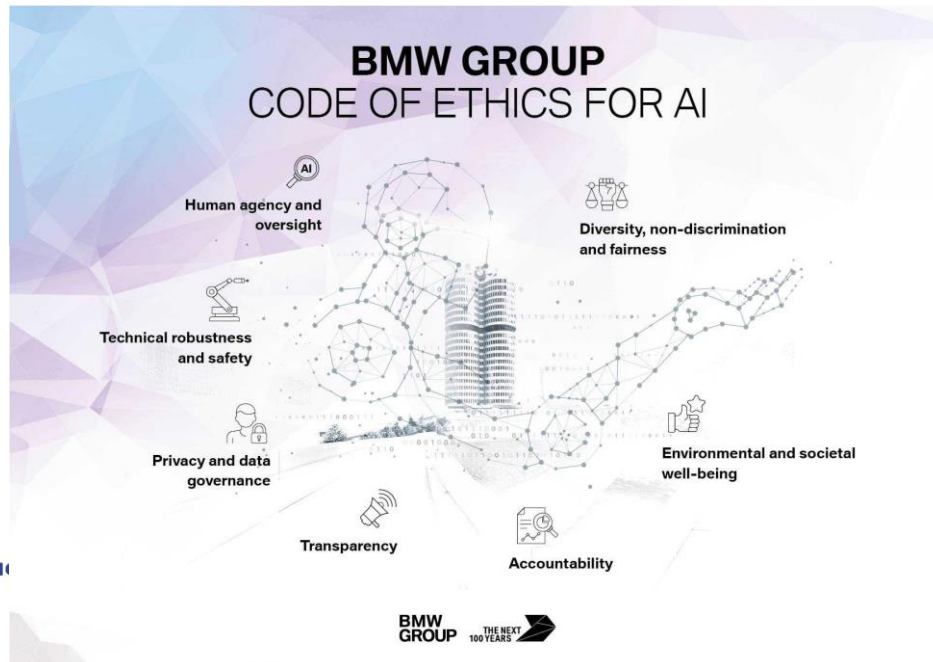
# AI regulation – who, what, where?

## Values-based principles

-  Inclusive growth, sustainable development and well-being >
-  Human-centred values and fairness >
-  Transparency and explainability >
-  Robustness, security and safety >
-  Accountability >

## Recommendations for policy makers

-  Investing in AI R&D >
-  Fostering a digital ecosystem for AI >
-  Providing an enabling policy environment for AI >
-  Building human capacity and preparing for labour market transition >
-  International co-operation for trustworthy AI >



## DoD Principles on AI (DoD, 2019)

- Responsible. Exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.
- Equitable. The Department will take deliberate steps to minimize unintended bias in AI capabilities.
- Traceable. The AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation.
- Reliable. The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life-cycles.
- Governable. The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.

## NATO Principles on AI (NATO, 2021)

- Lawfulness. AI applications will be developed and used in accordance with national and international law, including international humanitarian law and human rights law, as applicable.
- Responsibility and Accountability. AI applications will be developed and used with appropriate levels of judgment and care; clear human responsibility shall apply in order to ensure accountability.
- Explainability and Traceability. AI applications will be appropriately understandable and transparent, including through the use of review methodologies, sources, and procedures. This includes verification, assessment and validation mechanisms at either a NATO and/or national level.
- Reliability. AI applications will have explicit, well-defined use cases. The safety, security, and robustness of such capabilities will be subject to testing and assurance within those use cases across their entire life cycle, including through established NATO and/or national certification procedures.
- Governability. AI applications will be developed and used according to their intended functions and will allow for: appropriate human-machine interaction; the ability to detect and avoid unintended consequences; and the ability to take steps, such as disengagement or deactivation of systems, when such systems demonstrate unintended behaviour.
- Bias Mitigation. Proactive steps will be taken to minimise any unintended bias in the development and use of AI applications and in data sets.

## What about AI regulation? High Level EU Commission on AI

### Unacceptable risk

- A very limited set of applications that violate fundamental rights;
- Totally forbidden;
- Child exploitation, social scoring, subliminal influence, live biometric identification in public (with very clear exceptions).

### High risk

- Impact on security and on rights;
- Can only be developed under certain conditions - the quality of datasets used; technical documentation and evidence; transparency and information for users; human oversight; robustness, accuracy and cybersecurity;
- An obligation to provide access to data and systems to the authorities

### Limited risk

- The most important principle is that of transparency;
- Users must be aware that they are interacting with a robot;
- Chatbots etc.;
- Manipulation risk.

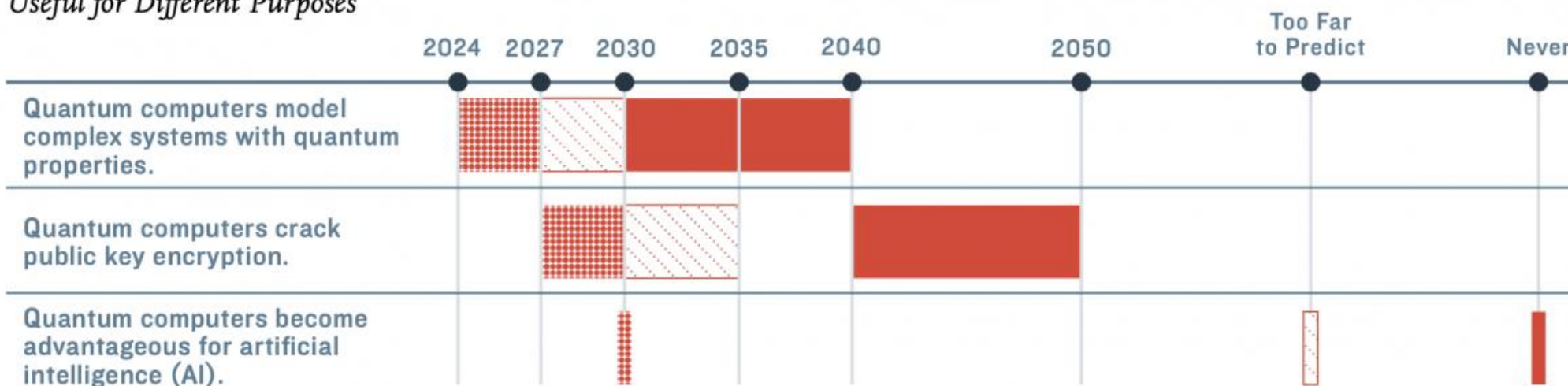
### Minimal risk

- The vast majority of AI systems in the European Union;
- Owners can apply voluntary codes and Trustworthy AI principles.

# Quantum Computing

- Quantum computers will be able to solve problems that are far too complex for classical computers to figure out. This includes solving the algorithms behind encryption keys that protect our data and the Internet's infrastructure.
- Not yet fulfilling its promise to render current encryption obsolete
- RSA encryption, a widely used form of encryption, particularly for sending sensitive data over the internet, is based on 2048-bit numbers.
- Cyber criminals - "Harvest Now, Decrypt Later"
- "quantum-safe" encryption necessary - U.S. National Institute of Standards and Technology (NIST) is already evaluating 69 potential new methods for what it calls "post-quantum cryptography (PQC)."

*When Quantum Becomes Useful for Different Purposes*



OPTIMISTIC

CONSENSUS

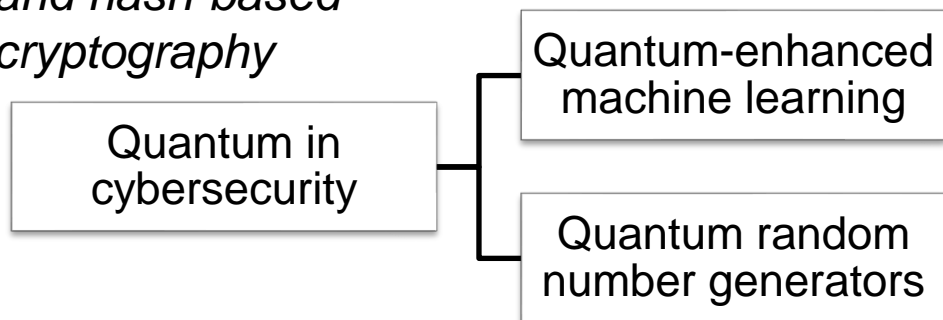
PESSIMISTIC



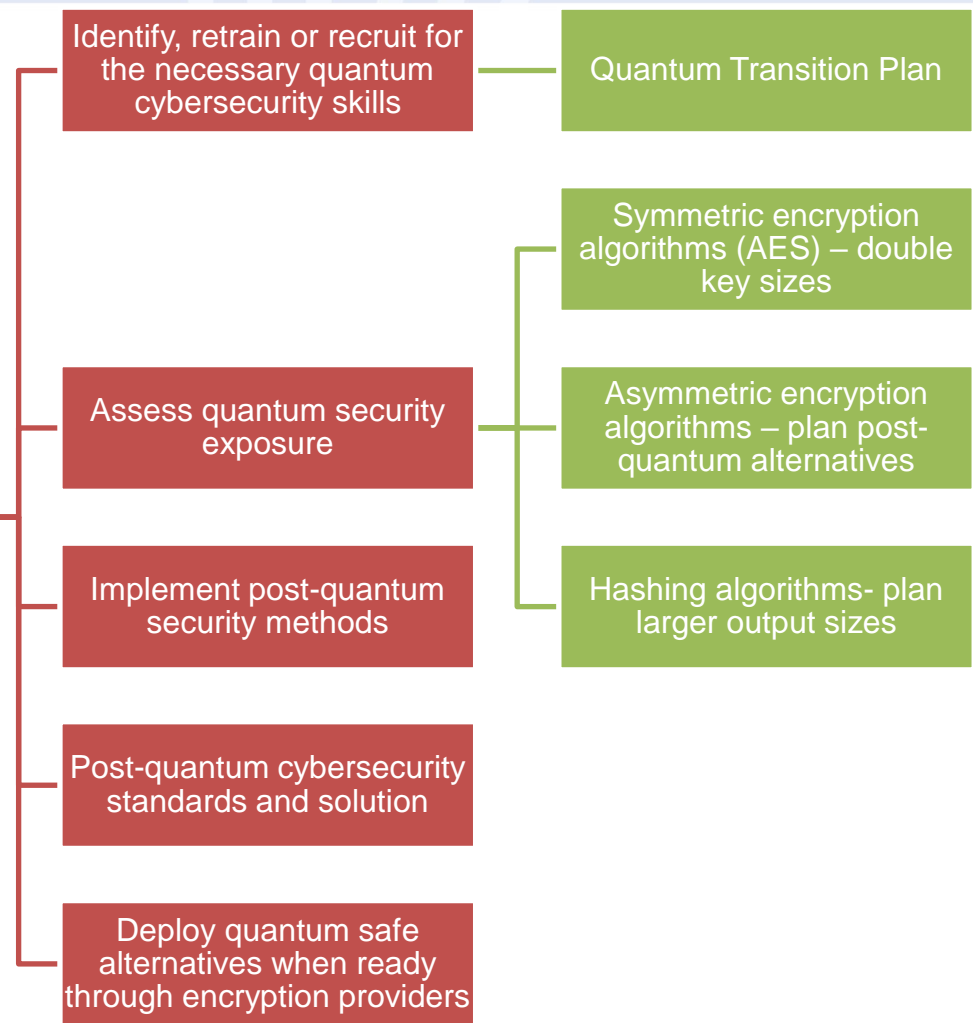
## What can we do? Quantum Safe vs Quantum Secure

- Large-scale quantum computers are not yet commercially available - future code-breaking quantum computers would need 100,000 times more processing power and an error rate of 100 times better.

*Proposed post-quantum solutions - lattice-based approaches, code-based cryptography, multivariate cryptography and hash-based cryptography*

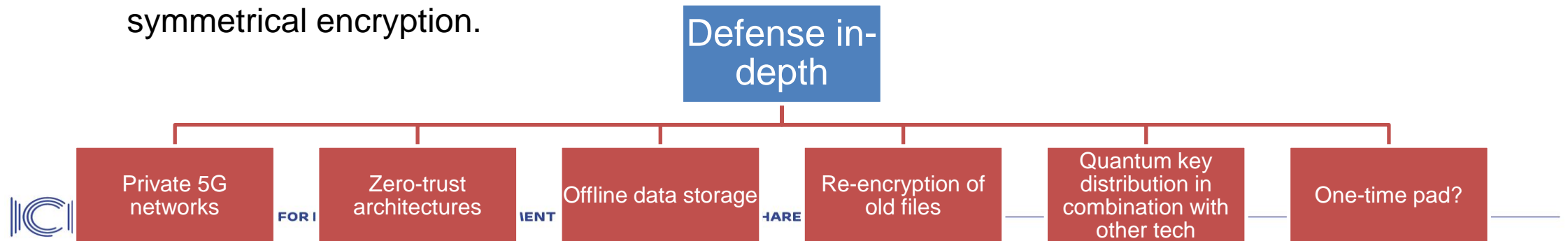


### What to do?



## What do we currently see in QC?

- November 9, 2022 - IBM 433 qubit Osprey processor. 2023 – Condor 1k qubit. Roadmap shows a progression toward a 4,000 plus qubit quantum computer, codenamed Kookaburra, due in 2025.
- U.S. HR passed the Quantum Computing Cybersecurity Preparedness Act requiring federal agencies to migrate information technology systems to post-quantum cryptography
- NIST released its first four quantum-proof algorithms in July 2022. Not long after, the CRYSTALS-Kyber public-key encryption and key encapsulation mechanism recommended by NIST had been broken using AI combined with side channel attacks.
- The securitization of quantum computing research in the transatlantic space
- “Harvest now, decrypt later” is real
- QKD does not prevent attacks, but makes attacks visible.
- Successful QKD paves the way for data to be transmitted using the latest and best symmetrical encryption.



# THANK YOU!

National Institute for Research and Development in Informatics - ICI Bucharest

Cybersecurity and Critical Infrastructure R&D Department  
8-10 Averescu Avenue, 011455, Bucharest, Romania  
[office@ici.ro](mailto:office@ici.ro)

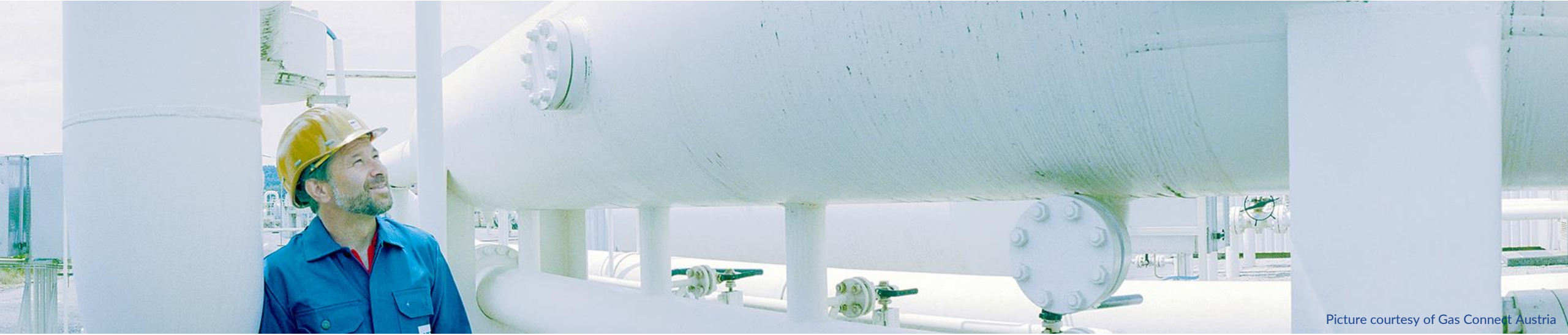
[WWW.ICI.RO](http://WWW.ICI.RO)

---

## 8. International CS: ENTSOG Managing cybersecurity risks



Anton Kolisnyk – ENTSOG  
ReCo KG Chair



Picture courtesy of Gas Connect Austria

# Regional Coordination (ReCo) System for Gas

Managing cyber security risks

*System Operation Team*

# ReCo System for Gas

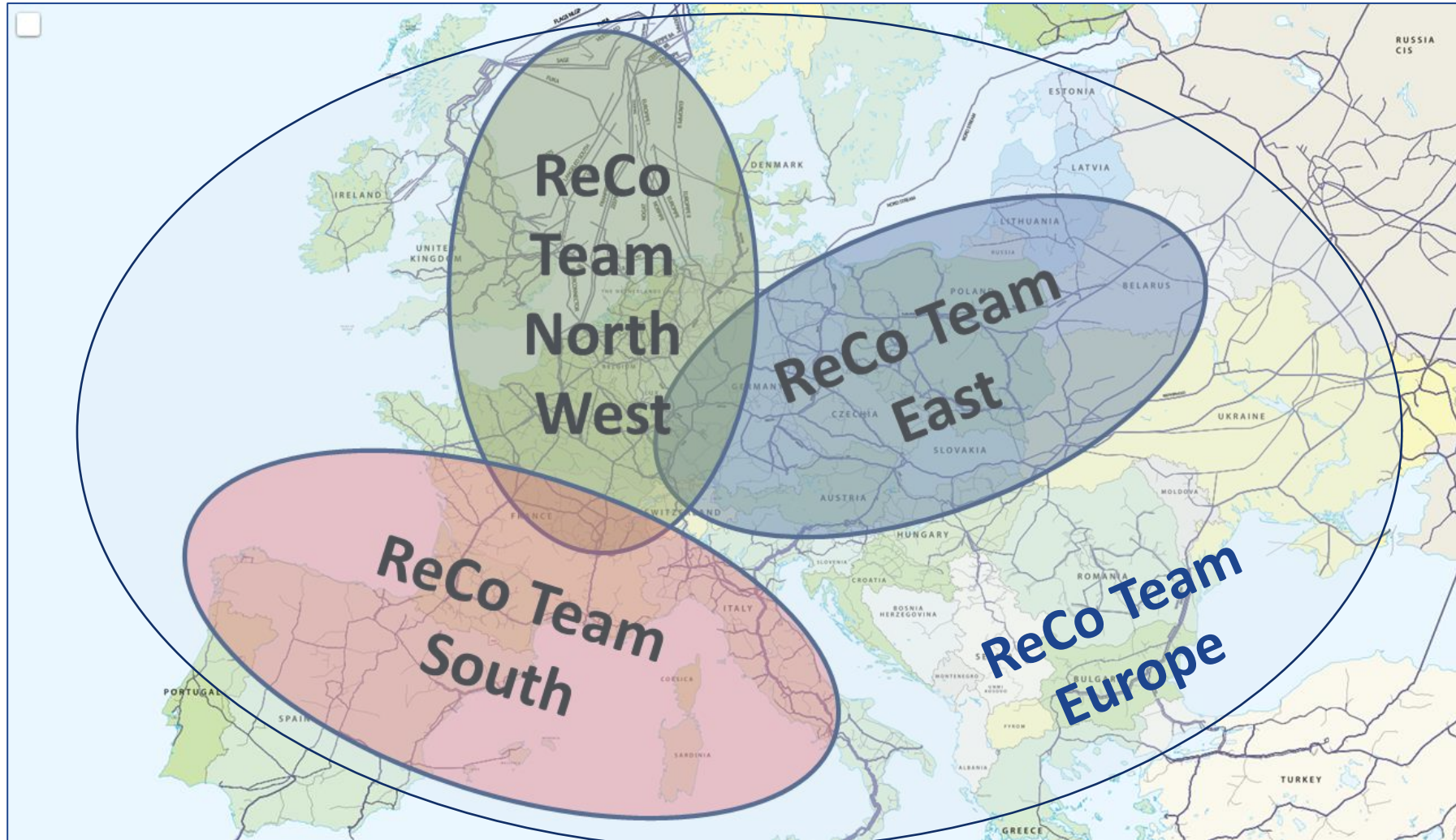
---



ReCo – a concept/solution for fast exchange of information and solutions between TSOs dispatching teams in case of:

- Potential risk for TSOs
  - ❑ Risks of gas flows disruptions
  - ❑ Unavailability of gas transport infrastructure
  - ❑ Extreme cold weather conditions
- Significant incidents impacting TSOs dispatching and operational procedures (incl. cyber-attacks)
- Declarations of crisis levels in MSs and extra need for cooperation
- Uncertainties and need of information exchange (relevant for SoS)

# ReCo Teams



- Four ReCo Teams (groups of TSOs)
- 24/7 reachability (e-mail and phone numbers of dispatchers)
- TSO responsible to set up a virtual meeting (Microsoft Teams)
- Documentation

# Cyber Security in the ReCo

---

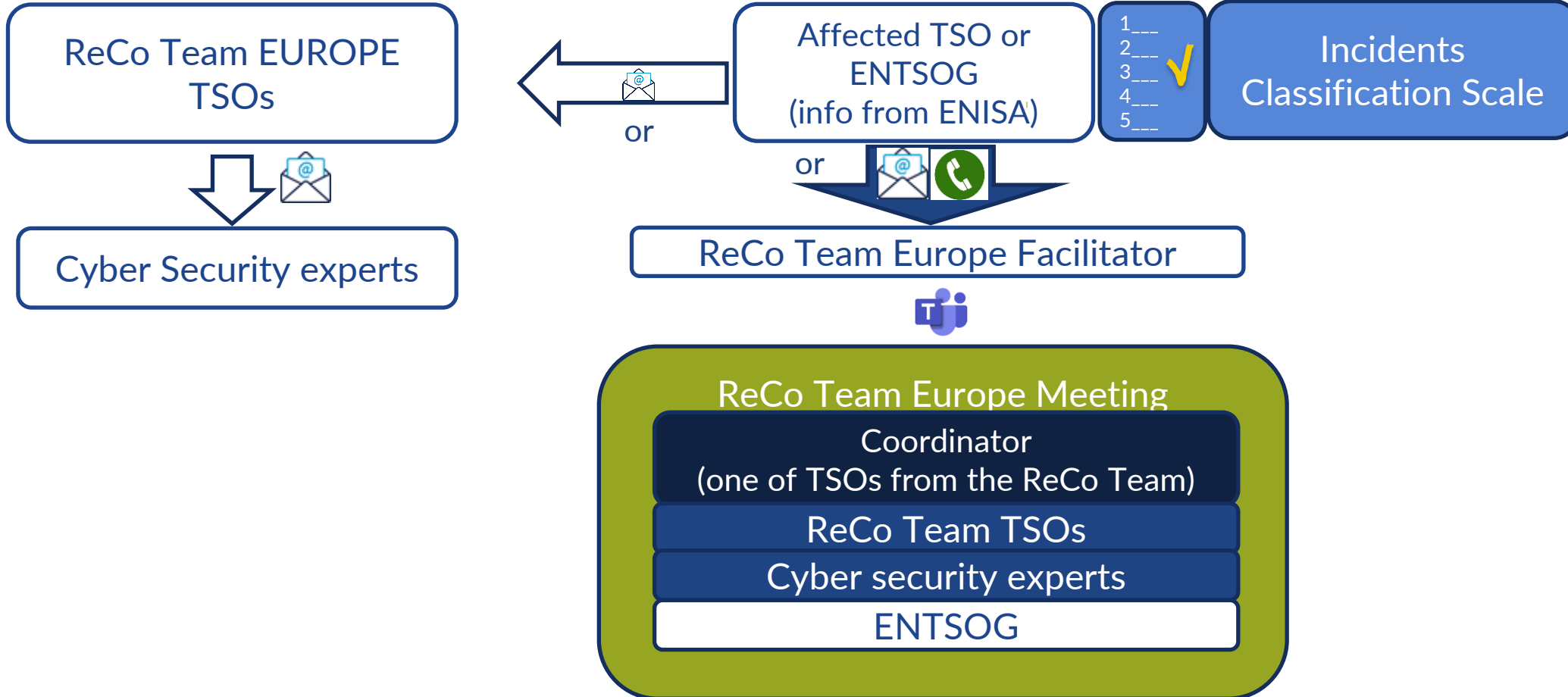


- Goal: To exchange information between TSOs about potential or current cyber-attacks causing risks for TSOs operational procedures and security of gas supply.
- Tools:
  - 24/7 reachability – TSOs dispatching centres
  - Incidents classification scale (ICS): *focus on any issues impacting TSOs operations*
  - Guidelines for TSOs about how to act
  - Responsible bodies (Facilitators, ENTSOG)



# ReCo Team Meeting. High Level Setup

## Cyber security INCIDENT



# Cyber Security Threats in the ReCo

---

- Cyber-attack with significant risks to perform TSOs tasks and potential risks for other TSOs, including impact on TSOs dispatching activities  
*(ICS: Level 2 - potential events in the future and inability to execute data exchange)*
- Cyber-attack causing gas flow disruptions with significant impact on demand/supply situation in a balancing zone(s).  
*(ICS: Level 3 - a significant effect on gas transmission operation and reliability)*

# Coordination between TSOs in case of cybersecurity risks

---



ReCo setup will be used only for Cyber Security cases which impact TSOs operational and dispatching procedures

## Other relevant highlights:

- Cyber security for gas might be part of the new SoS regulation
- High importance and focus on cyber security from ACER, EC, MSs.
  - ENTSOG and ENISA developed an information session on cyber security issues where parties exchange their experiences, knowledge, and solutions for strengthening TSOs cyber security.
- TSOs & ENTSOG, ENTSOG & GIE, ENTSOG & ENISA working groups cover cyber security topics on a regular basis



Thank you for your attention

System Operation Team

[Anton.Kolisnyk@entsog.eu](mailto:Anton.Kolisnyk@entsog.eu)

ENTSOG - European Network of Transmission System Operators for Gas

Avenue de Cortenbergh 100, 1000 Bruxelles

[www.entsog.eu](http://www.entsog.eu) | [info@entsog.eu](mailto:info@entsog.eu)





Olivier Clement,  
Chair of the Cybersecurity  
Expert Group  
DSO entity

DSO entity  
Expert Group

## 9. International CS: Downstream perspectives of an electricity EU EDSO and ENCS



Maarten Hoeve,  
CS expert  
ENCS

ENCS



# **Network Code on Cybersecurity in the electric sector**



Olivier CLEMENT

Chair of the Cybersecurity Expert Group

An EU association legally mandated  
by EU Regulation 2019/943



“ Art. 52.1: Distribution system operators shall *cooperate at Union level through the EU DSO Entity*, in order to promote the *completion and functioning of the internal market for electricity*, and to promote optimal management and a coordinated operation of distribution and transmission systems. ”

A body of cooperation and expertise  
between all DSO in the EU

900+ DSOs  
connecting  
250 million  
customers in  
the EU

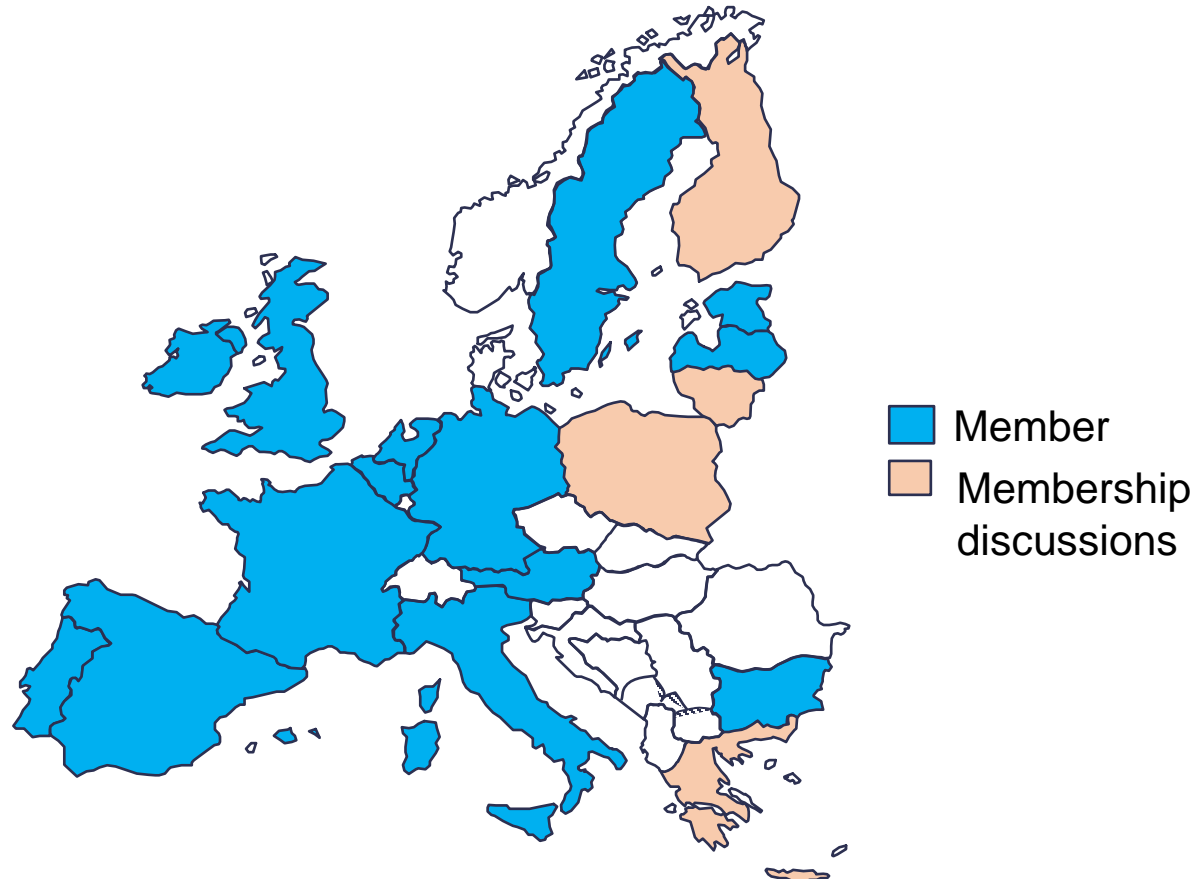


# European Network for Cyber Security

ENCS is an independent, non-profit organization owned by grid operators that helps its members cost-effectively reduce cyber-security risks



Maarten Hoeve  
Director Technology



- DSOs and TSOs
- Covering more than 100M European connections
- Partnerships with E.DSO and ENTSO-E

eeling



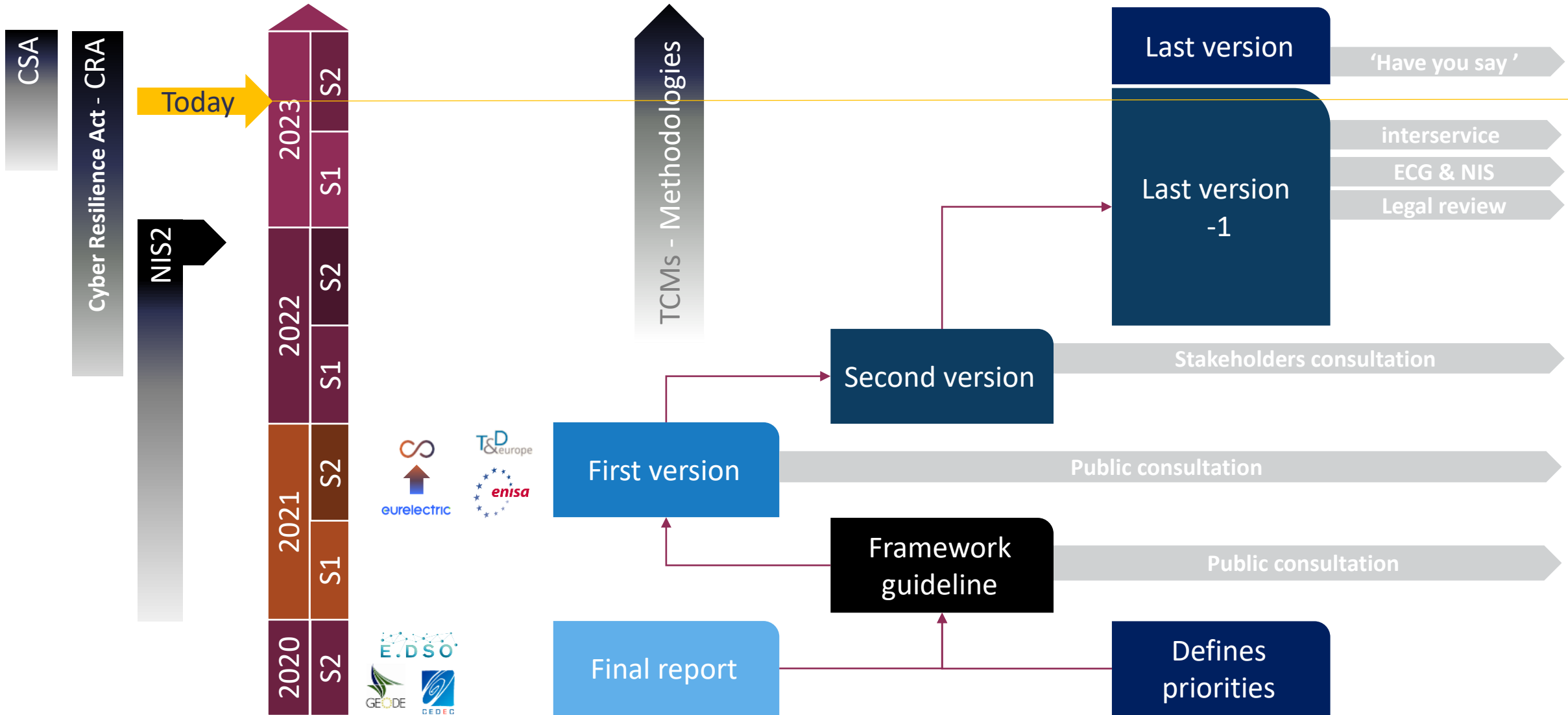
EUTC

gasunie

REN







# NCCS: requirements to entities

## NIS directive (1.0)

Take appropriate measures to manage risks

Notify authorities on incidents

## Network code

Risk management cycle

Cybersecurity controls

Management system

Verification

Cybersecurity operations center

Reporting of incident, vulnerabilities, threats

Incident response and crisis management

Exercises at entity, national, regional level

**Thank you**



# EU Regulation 2019/943 (Art. 55) gives DSO Entity a clear mandate



## Network Codes & Guidelines

Participates in drafting of Network Codes and Guidelines relevant for DSO grids

- Joint proposal with ENTSO-E on **Network Code Cybersecurity (14/1/22)**
- **Upcoming Network Code Demand-side Flexibility**
- **Review of existing network codes**



## DSO/TSO cooperation

Promotes optimal and coordinated planning and operation of DSO/TSO networks

- **MoU** with ENTSO-E (DSO-TSO work plan)
- Cooperation on **Network Codes**
- Joint initiative on **Vision 2050**

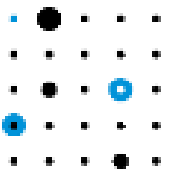


## Sharing best practice

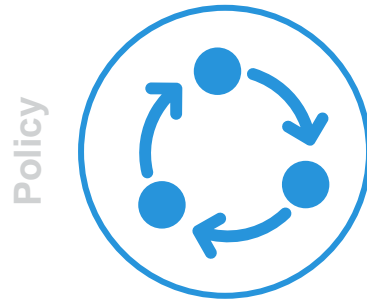
Expert Groups and forum provide expertise and enable exchange of views

- **Various forms of knowledge sharing** with DSO Entity's members
- Via **project teams** (e.g. events, expert tables)
- **DSO radar reports**

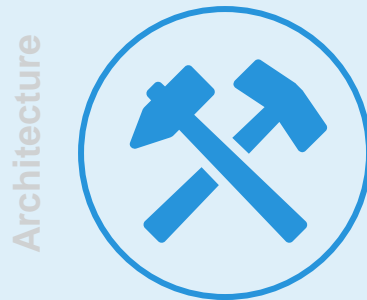
# Knowledge development in three security programs



ENCS



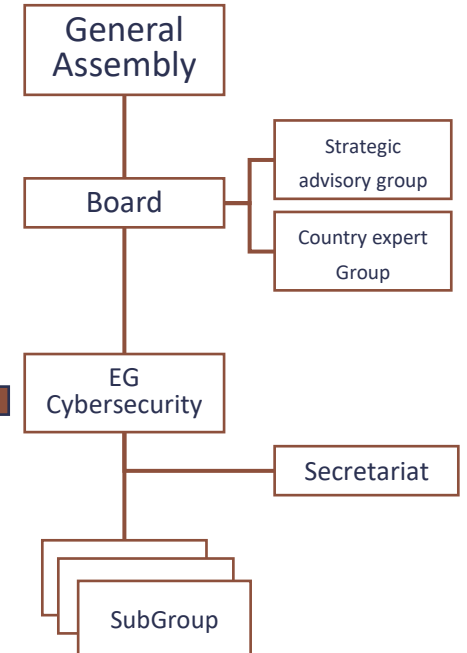
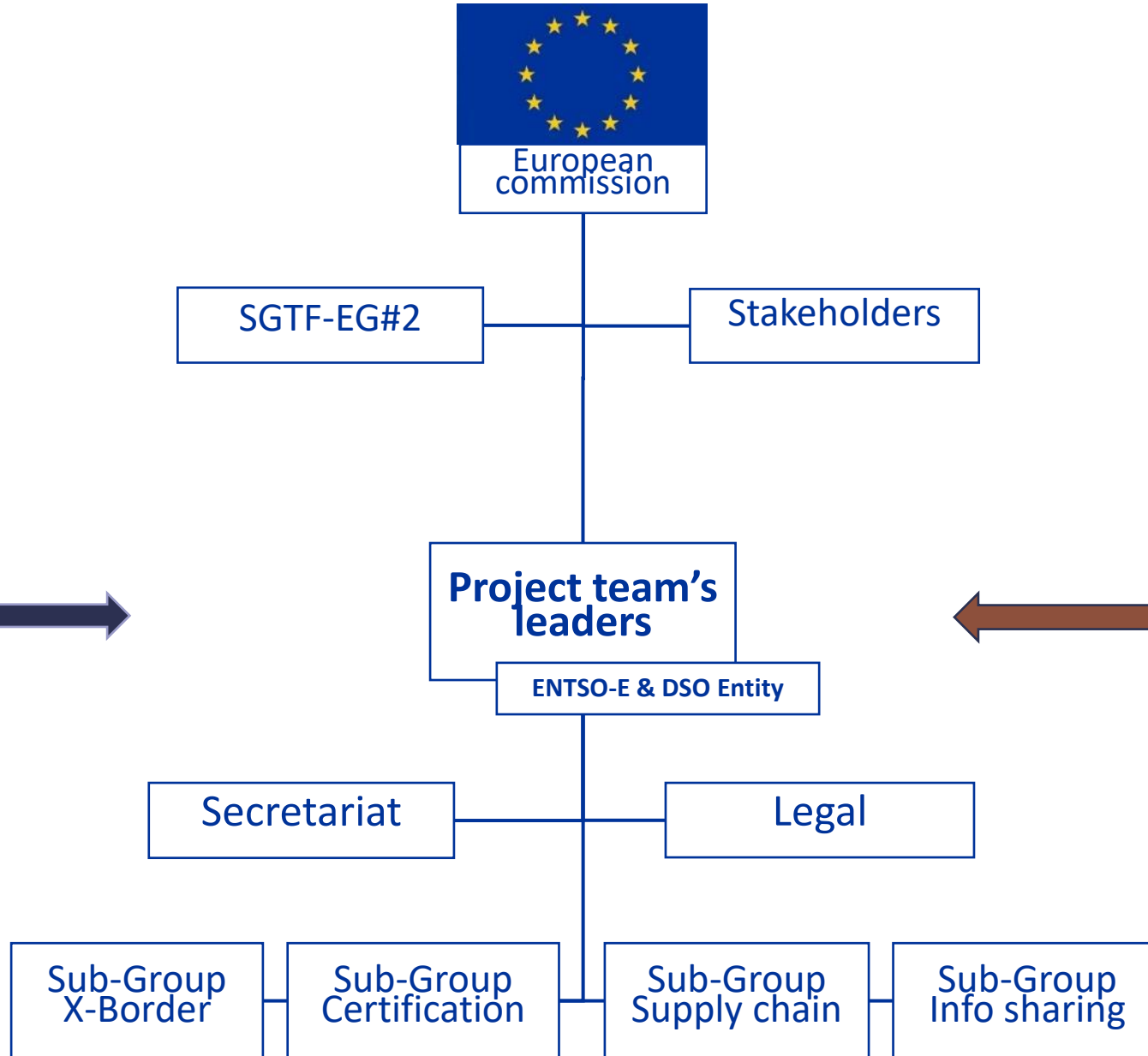
- Security officers
- ISMS implementation (ISO 27000)
- New legislation and regulation



- Security architects
- Secure system design (zoning)
- Procurement of secure equipment

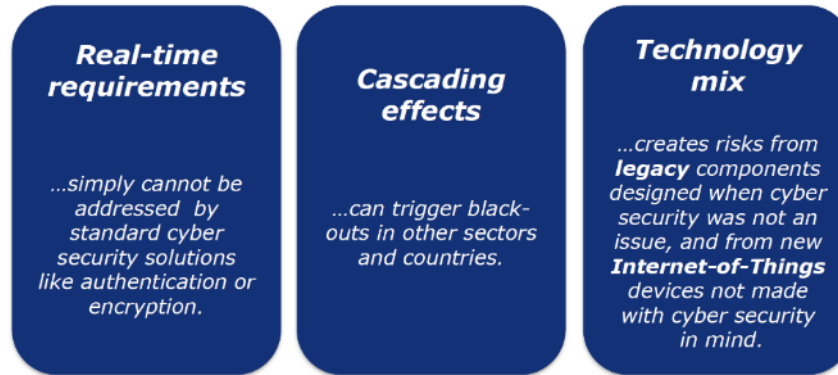


- Security operations analysts (SOC)
- Security monitoring and incident response
- Vulnerability management



# Why did we need a NCCS in the Electric Sector?

Is the energy sector special in cybersecurity implementation?



Urgency to define of a EU-wide cybersecurity regulation for the Energy Sector

1. Threat landscape/level keeps increasing
2. Different levels of maturity EU-wide
3. Guidance is needed for harmonized rules and approaches
4. Collaboration is needed – it is an European Power Grid



## 10. International CS: ENTSO-E. “ENTSO-E reflections on the challenges facing in the electricity sector.”

Ivan Štefek, Steering Group  
ICT Security Convenor,  
ENTSO-E

ENTSO-E



# ENTSO-E perspective on Cybersecurity in the electricity sector

Ivan Stefek, 18th October 2023





# Ensuring Cyber-resilience

Global

The UN

Interpol

No global regulatory oversight. Limited ability to cooperate and share info. 3<sup>rd</sup> country issue

EU-wide

Europol EC3, CSIRTs, CSIRT Network ...

Risk Preparedness Methodology, NCCS, Req. for real time data exchange between TSOs

NCCS still in the drafting process by the EC, risk assessment and mitigation needed for cross-border

Entity level

Informal communication & via ENTSO-E

Commitment to regulatory oversight (EU) & national.

Different maturity levels and resources

# Information & Communication Technologies Committee

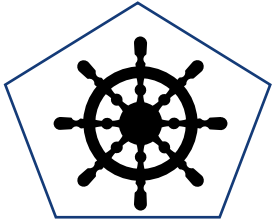
Established in 2023

Committee Chair: Radek Hartman, CEPS



# Network code on Cybersecurity: ENTSO-E in cooperation with the EU DSO Entity

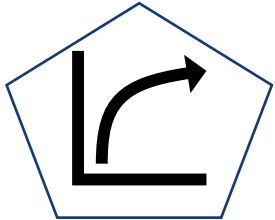
**For the whole community**



establishing a solid governance for cybersecurity in the electricity sector



determining common criteria for performing risk assessments based on defined risk scenarios for the operational reliability of the electricity system



fostering a common minimum electricity cybersecurity level across the Union



setting up a system for the collection and sharing of essential information



establishing effective processes to identify, classify and respond to cybersecurity incidents & setting up effective processes for crisis management to handle cybersecurity incidents

# ENTSO-E: tackling IT and OT systems

Generic Security Plan includes aspects of:

- \* Management
- \* Internal Organisation
- \* Human Resources
- \* Asset Management
- \* Access Control
- \* Cryptography
- \* Physical and Environmental Security
- \* Operations Security
- \* Communication Security
- \* Security Requirements
- \* Supplier Relationships
- \* Business Continuity
- \* Compliance

Security Plan A  
Security Plan B  
Security Plan C

Information Security Management System (ISMS) Process improvements

Define, implement and follow up controls

- Security Awareness
- Information Security Risk management (process, treatment + vendor aspects)
- Incident response planning
- Privileged Access management
- Teleworking
- Independent assessment follow up

Deploy Secure Software Development Life Cycle (SSDLC)

Apply custom security activities to ENTSO-E applications

- Define metrics / KPI's and measure
- Define generic security requirements
- Supplier Security
- Perform standardized threat modelling
- Protection of Code Secrets
- Validate the architecture security mechanisms
- Conduct Security Testing via the cybersecurity test lab



Continuous work on central Security information and event management (SIEM) technology

# One click away: ENTSO-E as a connection point for TSOs

**European Awareness System** - technology platform which allows transmission system operators to exchange information in real-time.

**Common Grid Model** - a pan-European mathematical model of the grid, for which, TSOs share their individual grid models with the other TSOs and the regional security coordinators (RSCs).

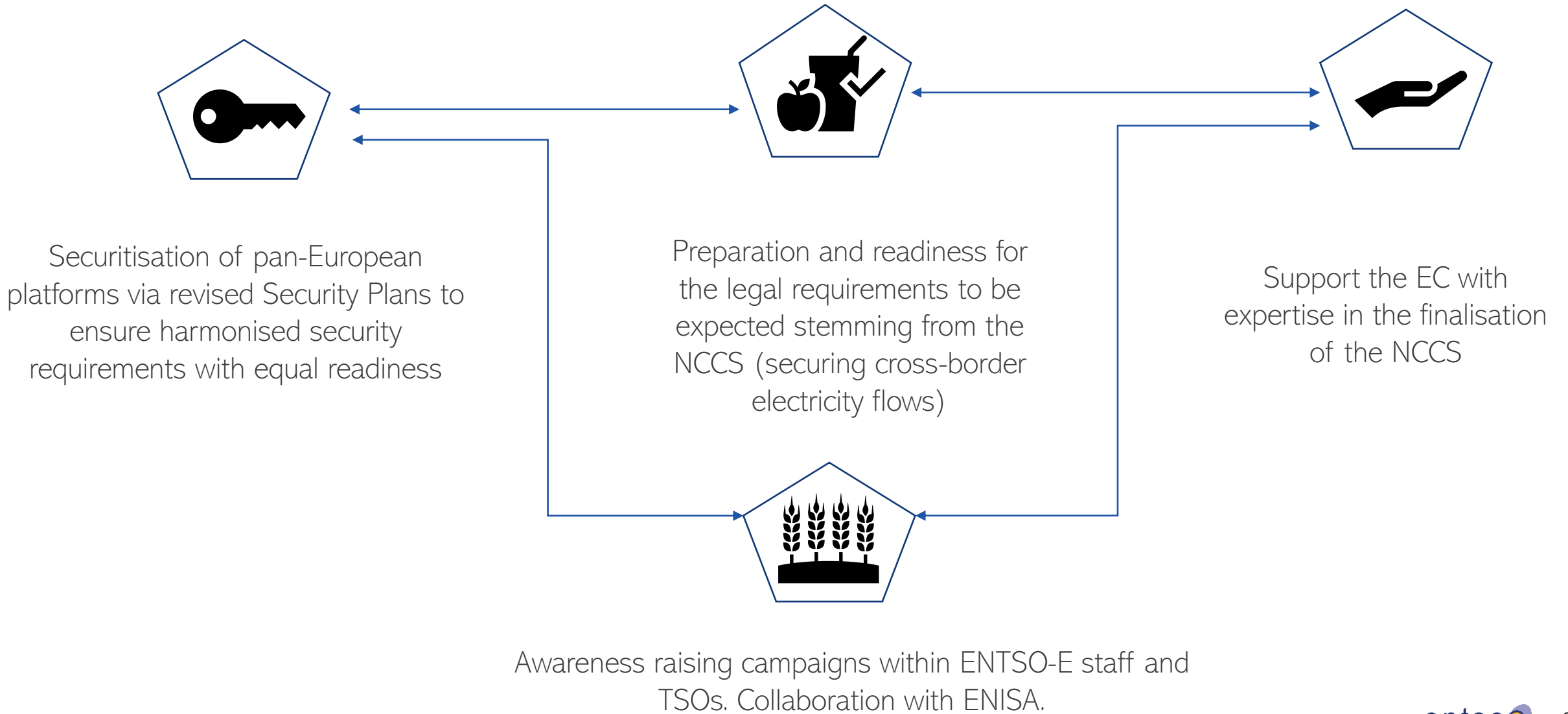
**Outage Planning Coordination (OPC) and Short-Term Adequacy (STA)** - balancing tool which is provided by RSCs.

**Energy Identification Codes** - devised a standard way of referencing the different pieces that enable exchange of information into the single energy market.

**Transparency Platform** - collects information, which is already publicly available and published by TSOs.



# ENTSO-E activities to ensure cyber-resilience





## 11. International CS: European Defence Agency. The value of CS Tabletop exercises in the energy sector



Brigadier General (retired)  
Ioannis Chatzalexandris  
European Defence Agency

European Defence Agency



## Workshop on Data Exchange & Cybersecurity in the energy sector 17-18 Oct 2023

Ioannis CHATZIALEXANDRIS

Project Officer Energy & Environment Systems  
[Ioannis.Chatzalexandris@eda.europa.eu](mailto:Ioannis.Chatzalexandris@eda.europa.eu)

# Boosting the defence energy transition



## EDA role in promoting sustainable energy in defence

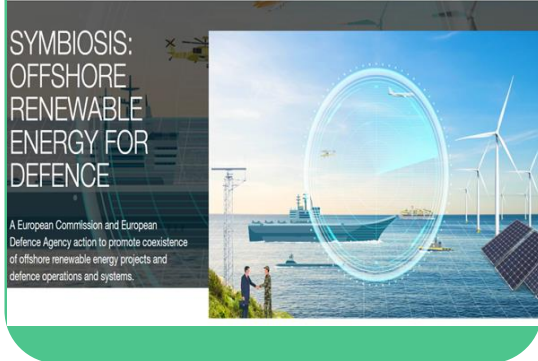
99

**EDA Energy and Environment Capability Technology Group**  
**EnE CapTech**

**Energy Defence Consultation Forum**  
**CF SEDSS**  
**H2020 funded**

**Offshore Renewable Energy in Defence**  
**SYMBIOSIS**  
**Horizon Europe funded**

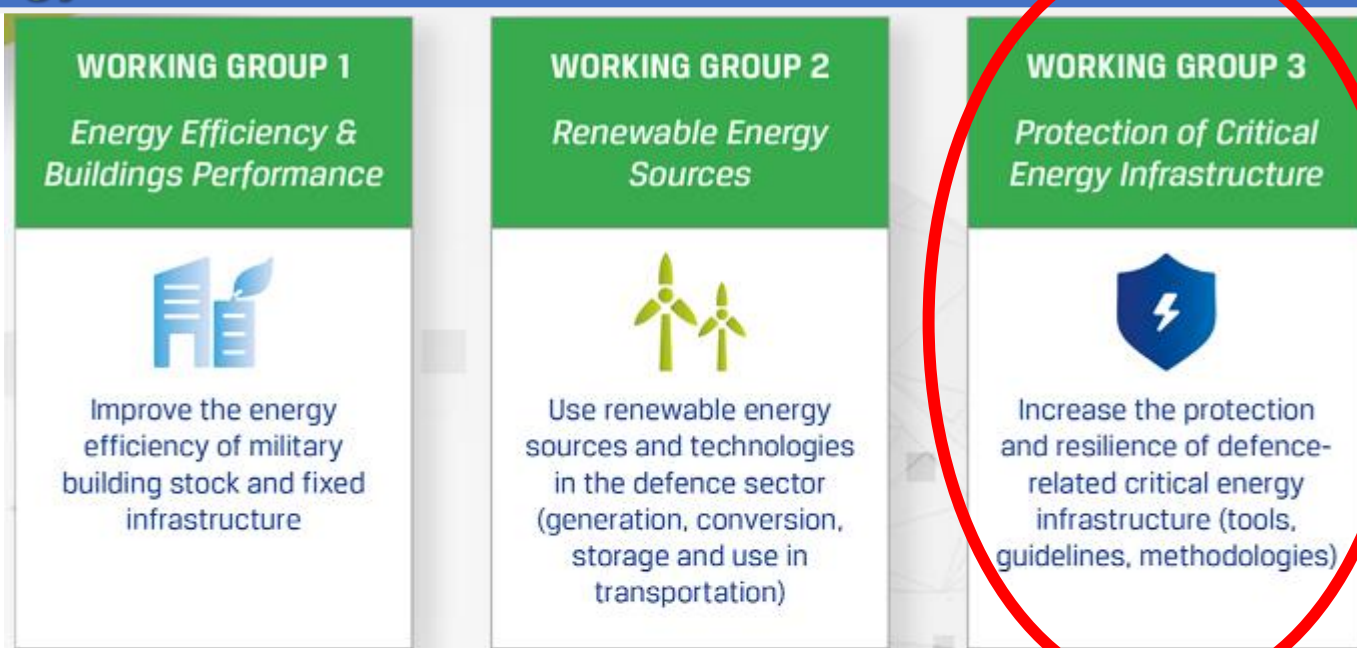
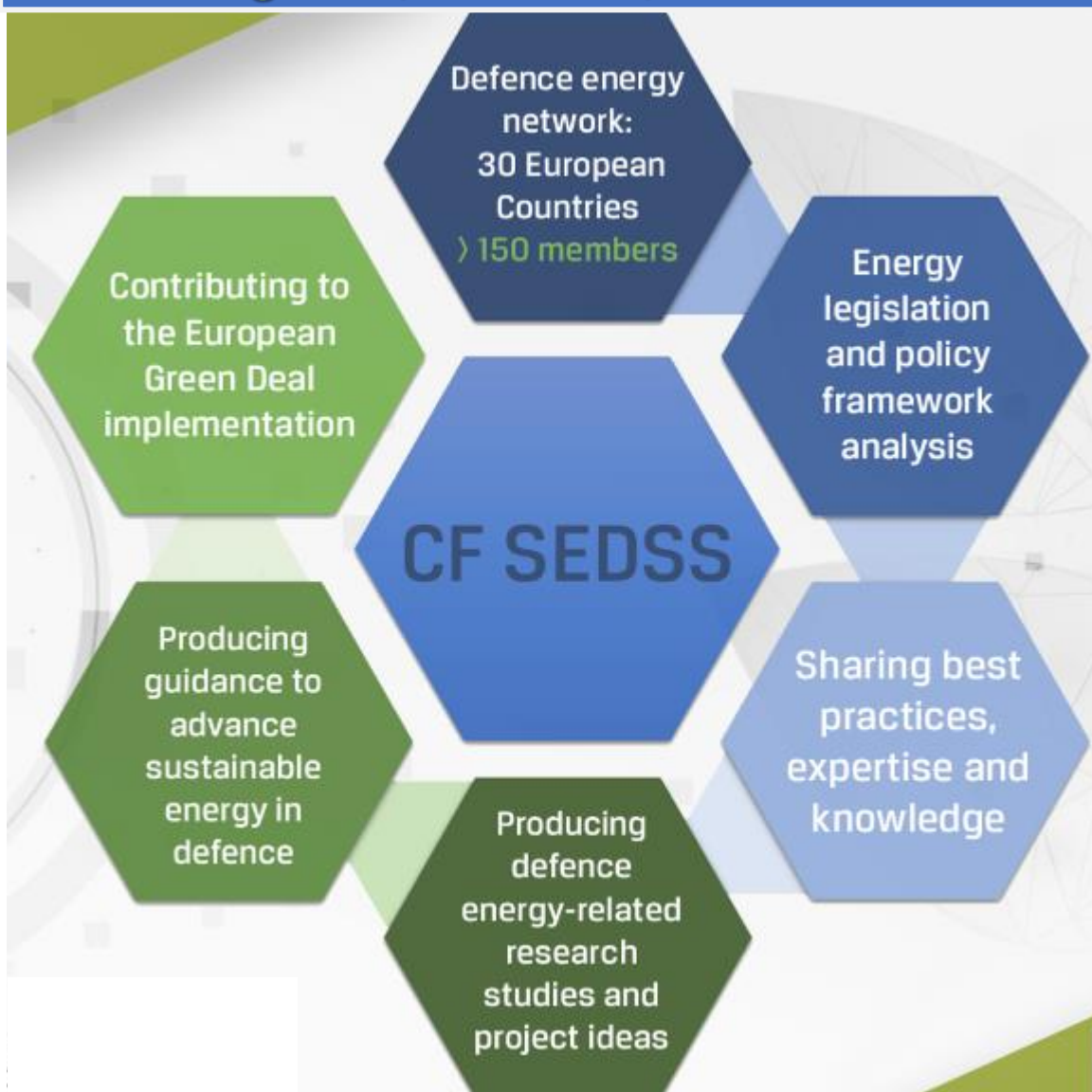
**Incubation Forum for Circular Economy in European Defence**  
**IF CEED LIFE- LU**



**cross-cutting**

# Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) – since 2015 (3.2 million Euro)

*a European Commission initiative managed by EDA to assist the EU MoDs to move towards green, resilient, and efficient energy models*



# CF-SEDSS / WG-3 Activities

## Scope

- strengthen the **resilience of defence-related critical energy infrastructure and identify related hybrid and asymmetrical threats.**

## Activities

- Pandemics' Impact on CEI
- Climate Change Impact on CEI
- Finance, markets and infrastructure ownership impact
- Offshore critical energy infrastructure beyond national sovereignty( study and ad-hoc meeting)
- TTX on Hybrid
- Network defence-energy stakeholders**

## Specific Objectives:



Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF-SEDSS) – Phase III

### Working Group 3 – Protection of Critical Energy Infrastructure

What	How
<p>As one of the four working groups of the third phase of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF-SEDSS III), working group 3 (WG-3) on protection of critical energy infrastructure (CEI) aims at <b>strengthening the research on the resilience and protection of defence-related critical energy infrastructure and identifying related hybrid and asymmetrical threats.</b></p> <p>Critical infrastructures do not operate as isolated systems and the continuity of their services is dependent on the proper operations of other networks. Challenges are associated with protecting national critical energy infrastructure from threats – including cyber, terrorist attacks or natural disasters – and how to maintain the energy supply chain and operational resilience in the energy domain. These threats may create significant risks, as an increased exposure to incidents potentially jeopardises the security of energy supply.</p> <p>In this context, WG-3 explores opportunities that derive from the implementation of the EU legislation on energy security, and in particular the European Critical Infrastructures Directive (ECI), the Regulation on Security of Gas Supply and the Regulation of Risk Preparedness in the Electricity Sector.</p> <p>Although national authorities are predominantly responsible for the protection of critical infrastructure, related disruptions can have a negative impact across national borders, thus requiring an EU dimension.</p>	<p>By providing a platform for discussion and sharing of expertise among MoDs, academia, industry, research and technology organisations, WG-3 will address the following objectives:</p> <ul style="list-style-type: none"> <li><b>Explore</b> how to contribute in preventing and managing crises at a cross-border level with regard to the security of gas supply;</li> <li><b>Explore</b> actions to enhance the risk preparedness in the electricity sector;</li> <li><b>Explore</b> means to boost the resilience of the energy network, infrastructure, which is relevant to the armed forces;</li> <li><b>Identify</b> how PCI contributes to securing energy strategic autonomy for the European defence and security sector;</li> <li><b>Contribute</b> to the research and sharing of best practices on the protection of defence energy-related CEI from natural disasters, terrorist, cyber attacks, environmental risks and climate change;</li> <li><b>Develop</b> guidelines for raising awareness and increase knowledge on the significance of the PCI in the EU defence and security sector;</li> <li><b>Generate</b> defence energy-related projects and best practices, including dual-use synergies within the defence and civilian markets.</li> </ul>



# CF SEDSS III – Table-top Exercise-Background

- **CF-SEDSS/WG3 (PCEI) flagship activity**
- **1<sup>st</sup> CF SEDSS III WG3 Hybrid Threats Table-top Exercise (TTX) in Sofia (BG) On 25<sup>th</sup>-26<sup>th</sup> of MAY 2023**



26 MAY 2023

Tabletop exercise and new study focus on protecting critical energy infrastructure

in [t](#) [f](#) [m](#)

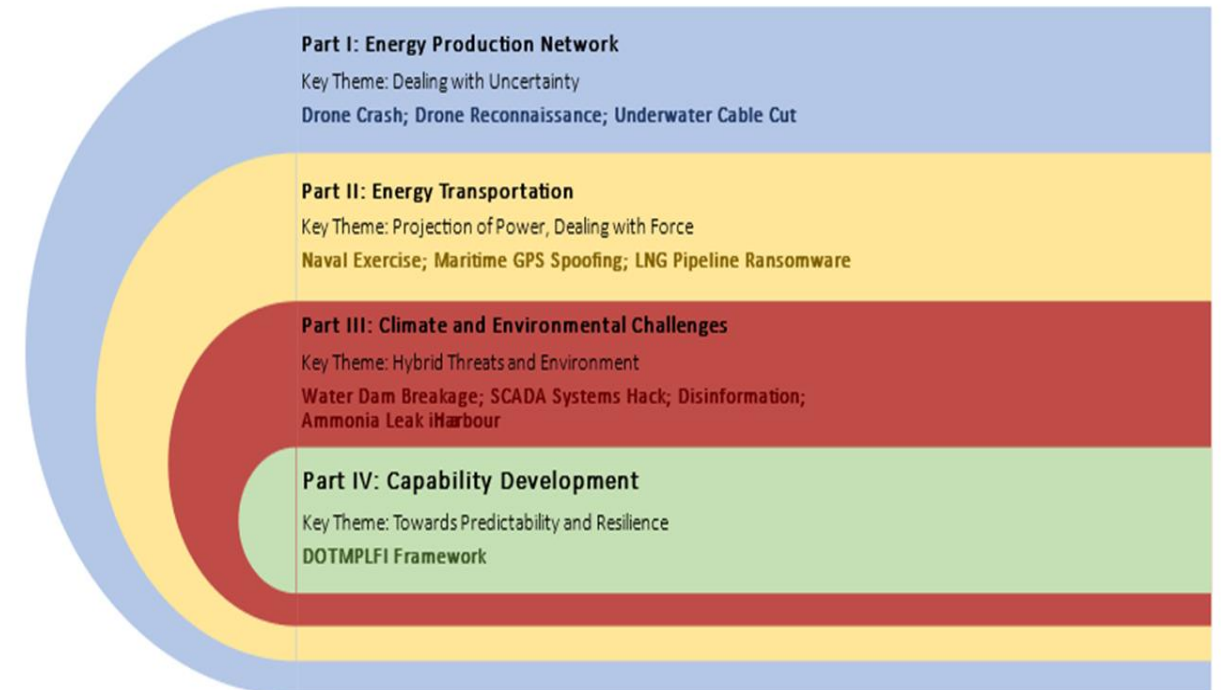
OEEDA



What should the European Union and its Member States do if its energy production and transport infrastructure were attacked by hostile groups in a region where like-minded, democratic countries coexisted with unfriendly authoritarian regimes? What if vulnerable critical energy infrastructure was essential for defence?

# CF SEDSS III – Table-top Exercise - Methodology

- **Cyber-attacks and/or physical** (e.g., terrorist) attacks against one/multiple defence-related CEI assets;
- **Disinformation campaigns** (e.g., fake news, social media, deception operation, etc.) combined with physical public demonstrations near a defence-related CEI;
- **Political divisions within the country's government** (possibly linked with the disinformation campaigns) and economic coercion from another country (e.g., sanctions, taxation, tariffs), resulting in riots and social disorder or confusion;
- **Natural phenomena/disasters due to climate change cascading effects** (e.g., major floods, extreme cold, etc.).
- **No right and wrong answers-No intention to evaluate/test**





# CF SEDSS III –TTX-Target Audience

- **Group A:** Defence
  - **Group B:** Government
  - **Group C:** Distribution and Transmission System Operators (DSO and TSO)
  - **Group D:** Civil society, industry and academia
- 
- In total, there were more than **60 participants** from **20 countries** alongside representatives of the European Commission and European External Action Service.

# CF-SEDSSIII-TTX-Aim and Objectives

- Identify the issue- explore the dependencies (EU level)
- Raise awareness (EU-National level)
- Initiate a dialogue between stake-holders (National level)
- Draw conclusions for designing similar future activities (CF-SEDSS level)
- Goal:
  - Develop security culture within a multistakeholder realistic modern model
  - Civil military cooperation


# CF-SEDDS III/TTX-Key conclusions

- Big variances on responses among groups
- Importance of SOPs
- Decision making processes:
  - in Civil-military cooperation
  - Under uncertainty
- StratCom in crises
- Develop a common security culture that facilitates the institutional interactions
- *Common request from all: interaction among groups*

# CF-SEDDS III/TTX-Way Ahead

- *Positive feedback*
- *Recommendations to MoDs*
- *Decision to proceed with further TTX within CF-SEDDS/P.4*

# CF-SEDSS/WG3 HYBRID THREATS TABLE-TOP EXERCISE



**Thank you for  
your attention!!**

**Workshop on Data Exchange & Cybersecurity  
in the energy sector  
17-18 Oct 2023**

Ioannis CHATZIALEXANDRIS

Project Officer Energy & Environment Systems  
[Ioannis.Chatzalexandris@eda.europa.eu](mailto:Ioannis.Chatzalexandris@eda.europa.eu)

## 12. Awareness: Introduction to the ENISA awareness package

Dr. Alexandris Zacharis - ENISA  
Dr. Georgia Bafoutsou - ENISA



# AR-IN-A-BOX

## How to Build your Custom Awareness Program

By Alex Zacharis  
(ARET,TREX,CBU)

BE THE STRONGEST LINK  
BREAK THE KILLCHAIN



EUROPEAN  
UNION AGENCY  
FOR CYBERSECURITY



# CONTENT

- What is a Cyber Awareness Program
- Why have one?
- What is AR-in-a-Box
- Roles
- Building Blocks
- Games/Quizzes





# CYBER AWARENESS PROGRAM

*“An (internal) marketing strategy designed to raise **cyber security awareness**.”*

- ✓ Teaches employees **how to mitigate the impact of cyber threats**.
  - ✓ A plan encompassing multiple awareness-raising activities over a long period of time following the organisation’s strategy for cybersecurity.
  - ✓ It can include one or more internal or external campaigns, focused on a common cybersecurity topic or target group.

# WHY HAVE ONE?

- New threats are emerging.
- Organizations can no longer just rely on their technological defenses to be safe.
- Cybercriminals use sophisticated social engineering techniques to by-pass defenses.
- All it takes is one employee to click on a malicious link and it's game over!
- Your employees are your first line of defense.

**A comprehensive Cyber Security Awareness program is the best way to educate staff and create a security-first culture.**

# STILL NOT SURE?

## ISO 27001/2 & Information Security Awareness Training

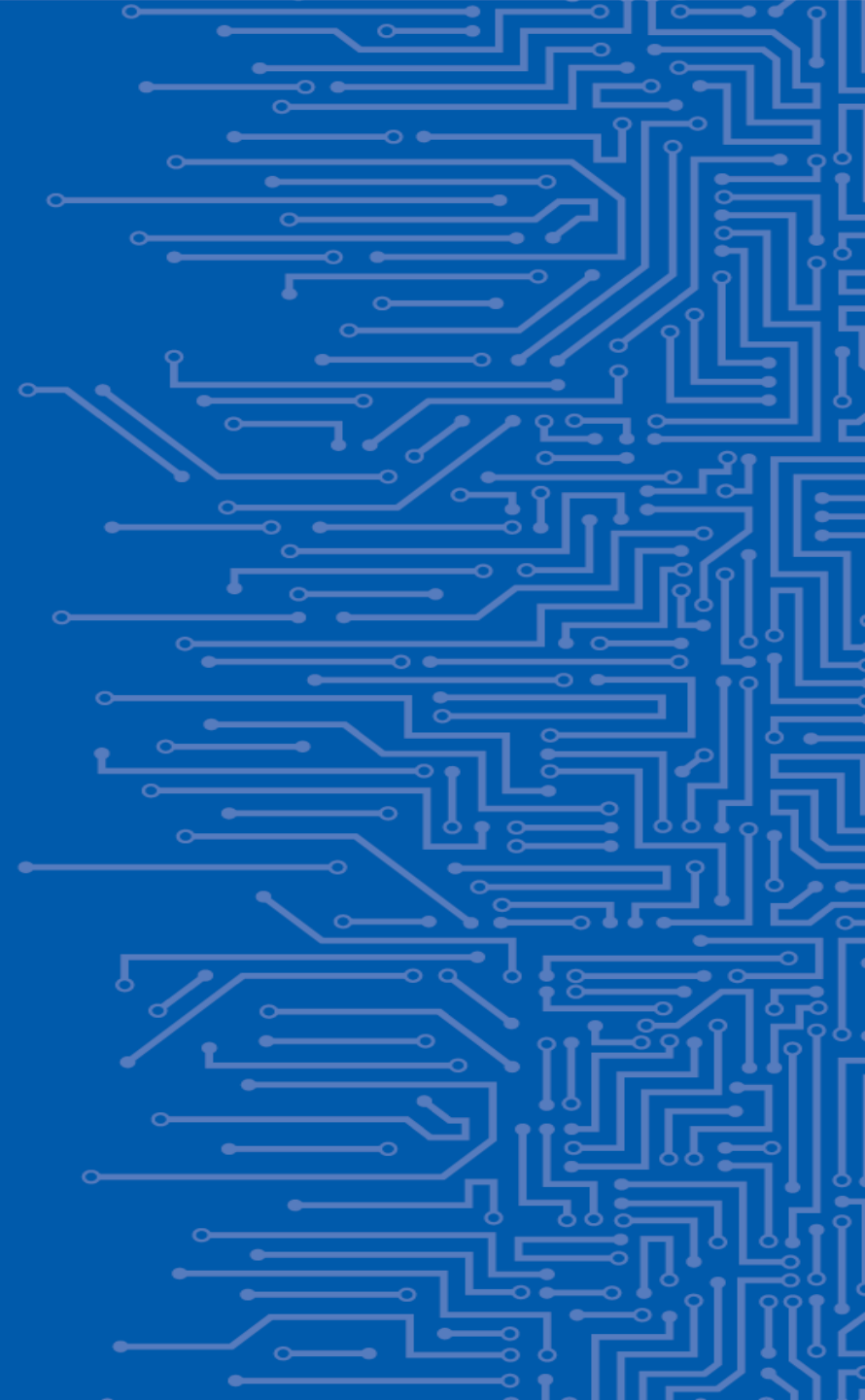
For ISO 27001 compliance, it is essential to comply with **clause 7.2.2**.

The ISO 27001/2 clause 7.2.2 states:

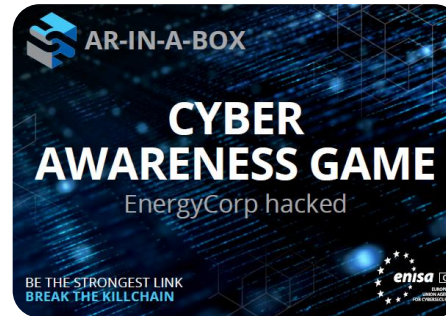
*'Information security awareness, education and training - All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function'.*



# AR-IN-A-BOX PREVIEW



# AR-IN-A-BOX CONTENT

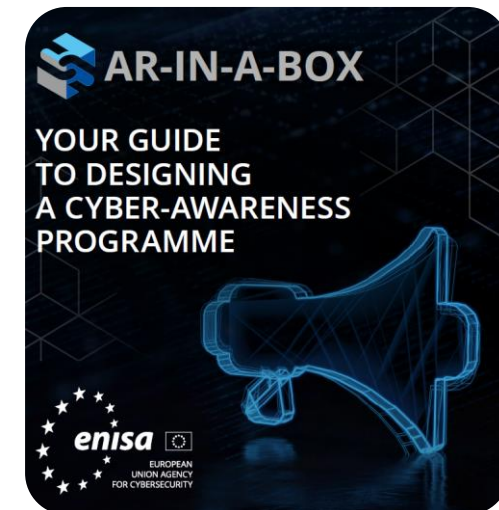


WHICH TYPE OF CYBER-ATTACK IS COMMONLY PERFORMED THROUGH EMAIL?

- A Phishing
- B Smishing
- C Vishing
- D Ransomware



# DESIGNING A CYBER-AWARENESS PROGRAMME



# SETTING OBJECTIVES



Overall goals for awareness and learning

Definition of SMART awareness objectives

Selection of specific material, tools, methods

**Awareness-raising objectives stem from the risk assessment of the organization and help:**

- ✓ To promote cybersecurity education and culture
- ✓ To be prepared for incidents.
- ✓ To develop an understanding of emerging cybersecurity threats and landscape
- ✓ To promote cybersecurity culture and hygiene
- ✓ To test policies and procedures

# HERE IS AN EXAMPLE

Objective	Indicative implementation timeline
<p><b>1. Raise awareness on the cyber threat of phishing.</b></p> <ul style="list-style-type: none"><li>• Provide a custom training on the topic, informative material and a hands-on quiz to evaluate progress.</li><li>• Utilize a phishing simulation campaign to capture before and after results.</li><li>• 100 % of staff should participate in the activity.</li></ul>	6 months
<p><b>2. Promote cybersecurity education and culture.</b></p> <ul style="list-style-type: none"><li>• Provide a custom training, a reporting process in the event of an incident and a hands-on table-top exercise to evaluate lessons learned.</li><li>• 80 % of the staff should participate in the activity.</li></ul>	1 year
<p><b>3. Improve preparedness in the event of an incident.</b></p> <ul style="list-style-type: none"><li>• 100 % of ICT personnel should participate in the activity.</li><li>• Provide training and a hands-on technical exercise to evaluate lessons learned.</li><li>• Test escalation procedures in place and identify gaps.</li></ul>	6 months



# FINANCIAL RESOURCES



## MANAGEMENT:

- Plays a critical role.
- Make sure they are involved in the design and the objectives-setting phase of the awareness programme from an early stage.
- Budget allocation depends on their support.

## TIPS:

- ✓ Try to identify the must-do topics of your programme and the must-train employees who will minimise the risk for your organisation when trained.
- ✓ Reuse or update existing material or resources.
- ✓ Select open-source material or create it in-house.
- ✓ Exploit synergies in the community where available.

# HUMAN RESOURCES



- ✓ **Management**
- ✓ **Cyber Security Officer**
- ✓ **Public Relations & Communications**
- ✓ **ICT**
- ✓ **HR**
- ✓ **DPO / Legal**
- ✓ **Content Developers**
- ✓ **Instructors**



# TARGET GROUPS



**Table 1. Employee target groups**

Audience groups		Clustered audiences
1	Generic employee	Generic employee
2	Contractor	
3	HR	
4	Communications and marketing	
5	Legal	
6	Operations and research and development	C-level, decision-makers, handling budgets
7	Finance and procurement	
8	Managers, officers	
9	Heads of unit, directors	
10	Cybersecurity professionals	Professionals / horizontal implementors of cybersecurity measures and users of cybersecurity solutions, working for organisations and/or individuals
11	Information technology (ICT) professionals	

# SELECTING THE RIGHT TOOLS

5



Choose the right means



## Infographics - Posters

Easy to deploy physically, e.g. in elevators, common spaces



## Ads - Videos

Able to hold and convey a lot of information



## TOOLS FOR AWARENESS RAISING



## Puzzles - Quizzes

Ensure and test understanding of concepts



## Live presentations

Direct interactions with participants

# SELECTING THE RIGHT TOOLS FOR THE RIGHT AUDIENCE



- **Aware – proficiency level 1 (PL1)**
- **Trained – proficiency level 2 (PL2)**
- **Experienced – proficiency level 3 (PL3)**

PL drop down per audience group and topic category	Audience groups			
	Generic employee	C-level	ICT and security professionals	
Topic categories	Cyberbullying	PL1		
	Online gaming	PL1		
	Online pornography	PL1		
	Safe internet	PL1	PL1	
	Sexting	PL1		
	Fake news	PL1		
	Privacy and data protection	PL1	PL1	
	Financial scams	PL1		
	Mobile banking	PL1		
	Device safety	PL1	PL1	
	Email spam	PL1	PL1	
	Business email compromise fraud	PL1	PL1	
	Password attacks	PL1	PL1	
	Data breach	PL1	PL1	PL2
	Malware	PL1	PL1	PL2
	Phishing	PL1	PL1	
	Ransomware	PL1	PL1	PL2
Cyber upskilling	PL1		PL2	
Cyberterrorism		PL1		
Certifications			PL2	

# EXAMPLE

Target audience	Channels and delivery methods
<b>Generic employee, contractor HR, communications and marketing, legal, operations and research and development</b>	<ul style="list-style-type: none"><li>• Social media websites, portals</li><li>• Online games and quizzes</li><li>• Gamification (e.g. role playing, escape rooms, mock attacks)</li><li>• Awareness kits (posters, background, screensavers, infographics, customised Windows login pages)</li><li>• Helplines / hotlines / chat boxes</li><li>• Video tutorials</li><li>• Discussion groups / forums</li></ul>
<b>Finance and procurement, managers, officers, heads of unit, directors</b>	<ul style="list-style-type: none"><li>• Newsletters</li><li>• Awareness kits (posters, background, screensavers, infographics, customised Windows login pages)</li><li>• Videos</li><li>• Webinars/workshops</li><li>• e-learning / online courses</li><li>• Publications</li><li>• Conferences/events</li></ul>
<b>ICT professionals, cybersecurity professionals, cyber knowledgeable</b>	<ul style="list-style-type: none"><li>• Real-time courses (face to face or online)</li><li>• Videos</li><li>• Webinars/workshops</li><li>• e-learning / online courses</li><li>• Training labs</li><li>• Certifications/diplomas</li><li>• Publications</li><li>• Networking events / conferences</li></ul>

# HEALTHCARE SECTOR CAMPAIGN

## Cyber Health Week 2022

Welcome to the official page of the Cybersecurity Healthcare Week 2022!



**6 - 12 JUNE IS**  
 Cybersecurity Healthcare Week 2022  
 #CyberHealthWeek  
 #BoostYourCyberVitals

Join us for CyberHealthWeek  
 #BoostYourCyberVitals

**Ensure the continuity of clinical services – Information availability:**

Make your healthcare organisation resilient to cyber incidents

In other words, make sure your clinical services are always available and patients have continuous access to them!

But, how?

By having a recovery plan that will help you:

- Respond swiftly
- Deliver services in abnormal circumstances
- Quickly get back to business as usual

A cybertip a day keeps the hackers away!

#BoostYourCyberVitals

**Don't take the bite!**

Immunise yourself from phishing infections!

**THE THREAT**

Fraudulent attempts to steal user data are usually launched through e-mail, appearing to be sent from a reputable source, with the intention of persuading the user to open a malicious attachment or follow a fraudulent URL.

**SOME PHISHING FACTS**

**OVERALL OVERVIEW**

Number of phishing attacks has **TRIPLED** since post from early 2020  
 Phishing attacks hit an **ALL TIME HIGH** in 2021  
 Phishing accounts for **90%** of data breaches

**HEALTHCARE SECTOR OVERVIEW**

Cyberattacks on healthcare sector saw a **71%** increase in 2021

**PHISHING MADE IT TO THE RANKS**

Phishing is found as the most common significant security incident and the most common initial point of compromise

Good news is I have a prescription for phishing immunity.

Let's make some checks looking for a pathogen pattern!

Cyber-hygiene: a set of simple routines to minimise the risk of cyberthreats and information leaks.

**PROTECT YOUR HEALTH DATA**

To prevent information leaks and unauthorised access to your devices you must never leave sensitive information unattended. The moment you are not on your workstation, devices, must be locked, and papers must be safely stored. Also, back up your data regularly.

**BROWSE SAFELY**

At work, browse only secured websites (https) related to your duties and never download unauthorised software.

**KEEP YOUR SYSTEMS UP TO DATE**

To keep yourself fully protected, use an anti-malware solution on all your devices and implement all available updates as soon as possible.

**KEEP YOUR DEVICES SECURED**

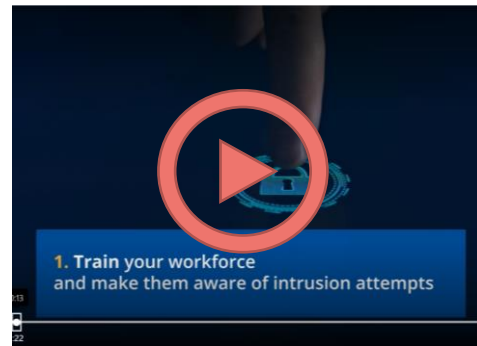
Choose strong passwords, keep them secret and unique for each service, change them regularly and use a password manager. Use an extra step when you log-in, such as a code sent to your phone or a fingerprint scan (two-factor authentication).

**CONNECT SAFELY OVER PUBLIC WI-FI**

Avoid connecting to public Wi-Fi networks. If you have no choice, verify the network, keep your antivirus enabled, avoid entering credentials or performing financial transactions and ask the IT personnel for Access through VPN.

#BoostYourCyberVitals

# ENERGY CAMPAIGN TO TRANSMISSION SYSTEM OPERATORS



## Electricity operators, it is your time!

We need **you** to help us **power up cybersecurity knowledge** in your sector!

Together let's lead all your employees into the light! Give them the tools they need to **deal with** the top cyberthreat... **Ransomware!**

...and find ways to **establish cyber-secure relations** with third parties **protecting** the entire **supply chain!**

Become a cybersecurity conductor and transmit the message, be the light of our cybersecurity community!

**#PowerYourCyber**

### Focus your energy, prepare for ransomware!

Become a human circuit breaker

**RANSOM... WHAT?**

Ransomware is a type of malware where threat actors lock or encrypt your data and demand a ransom to get the data back or to stop the encryption.

Ransomware core actions: LEES	Ransomware Life Cycle
<ul style="list-style-type: none"> <li><b>L</b>ockdown: Ransomware encrypts files and folders on the infected system.</li> <li><b>E</b>xact: Ransomware demands a ransom for the decryption key.</li> <li><b>E</b>xecution: Ransomware spreads to other systems on the network.</li> <li><b>S</b>teal: Ransomware steals sensitive data.</li> </ul>	<ul style="list-style-type: none"> <li><b>1. Infection:</b> Ransomware enters the system via a vulnerability or phishing.</li> <li><b>2. Execution:</b> Ransomware starts running and begins to encrypt files.</li> <li><b>3. Lateral movement:</b> Ransomware spreads to other systems on the network.</li> <li><b>4. Ransom demand:</b> Ransomware demands a ransom for the decryption key.</li> <li><b>5. Payment:</b> The victim pays the ransom, and the attacker provides the decryption key.</li> <li><b>6. Decryption:</b> The victim uses the decryption key to decrypt their files.</li> <li><b>7. Recovery:</b> The victim recovers their data and systems.</li> </ul>

**Ransomware attacks footprint**

The ransomware footprint is the set of artifacts left behind by ransomware on a system.

**Checklist:**

- Check for ransomware on your system.
- Check for ransomware on your network.
- Check for ransomware on your cloud services.
- Check for ransomware on your mobile devices.
- Check for ransomware on your IoT devices.

**Do not pay the ransom!** Paying the ransom does not guarantee that your data will be restored and may encourage further attacks.

**#PowerYourCyber**

## Be the cybersecurity transmitter!

Stay safe from ransomware

Did you know that ransomware can affect our company both directly and indirectly? You heard it! Your organization can be directly targeted by an attack, but it can also be the lateral victim of an attack to a third-party provider, particularly a Supply Chain attack. Let's take a look at both cases...

### Your company could be under attack

Your company could be the **direct victim** of an attack aimed against your assets

The main entry vectors exploited are **remote services and phishing**

So... may the entry points be cybersealed... How can you protect your company?

- **Reduce the attack surface**
  - Apply **Awareness Training Plans**
- **Protect your perimeter:** Run security software, maintain strict security awareness, security policies, and privacy protection policies up to date keeping personal data encrypted according to the GDPR.
- **Restrict administrative privileges** according to the PLOP (Principle of Least Privilege)
- **Stick to good practices** (pay special attention to backup policies)
- **Have a continuity plan**

### A third party is under attack

Your company could be affected by an **attack against a third party**

Your organisation is breached through **vulnerabilities in its supply chain**, meaning DSOs or other partnering companies. The attack has affected a supplier, rendering its operations unusable, with **direct repercussions on the services they provide to you**. Or suppliers are used as **stepping stones** to spread the attack.

By building cyber-secure relations with third parties:

- **Evaluate security policies** of third parties (requiring a minimum level of security requirements)
  - Apply **Awareness Training Plans**
- **Define obligations** of suppliers regarding protection of assets, sharing of information, audit rights, business continuity
- **Include** all obligations and requirements **in contracts**, e.g., GDPR
- **Restrict administrative privileges** according to PLOP (Principle of Least Privilege)
- **Monitor service performance** and perform **routine security audits**

**In case of suspicion always REPORT to the corresponding IT Department! if you suffer a ransomware attack...**

- Quarantine affected systems to contain the infection and stop the spread
- Lock down access to backup systems until after the infection gets removed
- Contact the national cybersecurity authorities or law enforcement on how to handle and deal with ransomware
- Visit the **No More Ransom Project**, a European initiative that can decrypt variants of ransomware
- Do not pay the ransom and do not negotiate with the threat actors

**#PowerYourCyber**



# HOW TO DO IT?



# SOME TIPS (1/2)



## WHAT DO YOU WANT TO ACHIEVE?

## OBJECTIVES

1. Generate awareness about cybersecurity issues and practices.
2. Raise awareness about the impact of different types of attacks, especially when they involve companies and businesses.

Awareness



3. Provide detailed information on how to react in the event of phishing and ransomware attacks.
4. Inform potential attack targets of what happens before, during and after a ransomware attack.

Information



5. Prompt the target audience to act and to eventually spread the word on what they learned from you.

Engagement



6. Promote the safer use of the internet for end users and the practice of basic cyber hygiene.
7. Promote existing cybersecurity recommendations and best practices to prevent cyberattacks.

Promotion



8. Provide users with resources to protect themselves online and prevent attacks.
9. Make people become 'human firewalls' by empowering them to play their part in preventing attacks.

Empowerment



# SOME TIPS (2/2)



Table 3. Activities matrix

No	Activity	Category	Target audience			Occurrence	Delivery method	Expected level of impact	Measurability	Resources (people)
			General	Specific	Target group					
1	Videos	Media	X	X	Young adults (including students)	Ad hoc, on request	Online	2	1	2
2	Webinar/ seminar	Training	X			Annual, on request	Online, instructor led	2	3	3
3	Communication calendar	Material	X	X	National awareness-raising authorities, SMEs, large organisations	Annual	Online	2	2	1
4	Workshop	Training	X			On request	Instructor led, online	3	3	3
5	Cybersecurity in a box	Material	X	X	National awareness-raising authorities	On request	Online	3	2	3
6	Surveys/quizzes	Training	X			Annual	Online	2	3	1
7	Social media	Media		X	Young adults (including students), employees, cyber ignorant, cyber knowledgeable	Annual	Online	2	3	1
8	Computer-based training (CBT)	Training		X	Employees, SMEs, large organisations	On request	Online	2	3	2
9	Physical material	Material	X			Annual	Conventional	2	1	1
10	One-day campaign	Event	X			On request	Conventional	2	2	3
<b>Advanced suggestions</b>										
11	Gamification	Training		X	Young adults (including students), employees, C-level management	On request	Game based	2	2	2
12	Lunch and learn	Event		x	Civil servants, employees, cyber ignorant	Ad hoc, on request	Conventional	3	1	2
13	Role play simulations	Training		X	Employees	On request	Instructor led	3	2	3

continued

# PLANNING

6



Create  
a timeplan

January	February	March	April
 Baseline quiz	 Training topic	 Videos and dissemination material	 Videos and dissemination material
May	June	July	August
 Training topic 2	 Simulation exercise	HOLIDAYS	HOLIDAYS
September	October	November	December
 Back-to-school training	 Games/test/quiz	 <u>Insights</u> collections	 Report to management

# IMPLEMENTATION



## **Cybersecurity training is an ongoing process.**

Ensure that your security posture is as mature as it can be, even as your company and the cybersecurity landscape grows and evolves.

Three periods are considered relevant for delivering cybersecurity-awareness training to your employees:

- ✓ When they join the organisation as part of the induction process
- ✓ After an incident, in order to indicate the procedures, roles and responsibilities in place;
- ✓ At regular intervals throughout the year (see calendar)

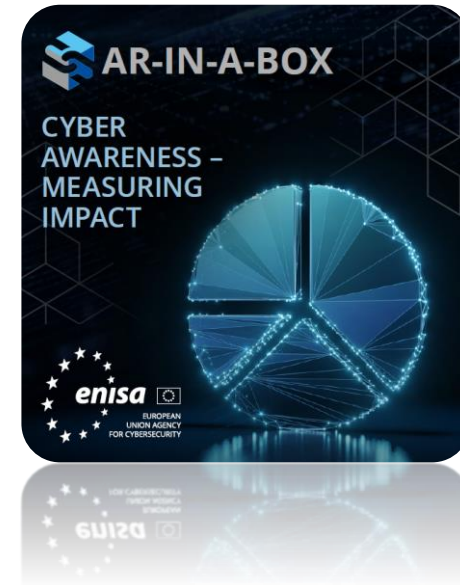
# EVALUATION



**A KPI is a value that measures a component of an awareness-raising campaign or programme.**

**There are five reasons why KPIs fail to improve performance:**

1. the KPIs are poorly defined;
2. they lack accountability;
3. they are not achievable;
4. they are not specific enough;
5. they are too hard to measure.



# CYBER AWARENESS GAMES

## Gamification helps!

- ✓ Determine how your team will react to a theoretical cyber attack and how effective your plan is.
- ✓ Identify flaws or gaps in the organization's response and make adjustments
- ✓ Testing consequences in a safe environment
- ✓ Coordination between different departments
- ✓ Save money



# QUIZZES



EUROPEAN UNION AGENCY FOR CYBERSECURITY

Which type of cyber-attack is commonly performed through email?

- Phishing
- Smishing
- Vishing
- Ransomware



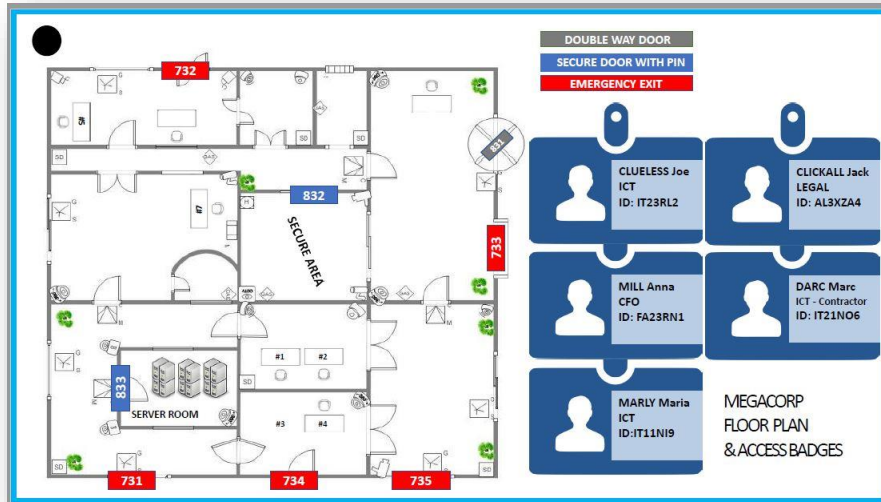
## Phishing

**CORRECT!** The term 'phishing' is used to describe a social engineering based cyber-attack that arrives mainly by email. Though email phishing is the most popular kind of phishing, other variants of this attacks can arrive by SMS (smishing), phone calls (vishing) or ransomware (digital kidnapping).

Other choices: **INCORRECT**



# TABLE-TOP GAMES



## SCENARIO - MEGACORP HACKED

MegaCorp, a leader in online retail has been hacked based on information leaked on the public internet.

Attackers appeared to have gained initial access via a successful **PHISHING ATTACK**.

To make matters worse **UNAUTHORISED ACCESS** has been detected in MegaCorp headquarters and a **RANSOMWARE** hit the company the same day.

You are the lead Cyber Security Investigator recruited to provide answers on who is behind the hack and try to stop him/her before its too late.

We gathered as much evidence as possible. Analyze them quickly.

You have 30 minutes left before all our data are wiped out.

**GOOD LUCK!**

## ANSWER SHEET

What is the name of the first known victim of the PHISHING ATTACK?  
 (Name Surname as seen in the Badge with space\*)

Which Badge ID was used to performed unauthorized access?

ENCIPHERMENT KEY

What is the filename of the decrypted file?

# AR-IN-A-BOX: METHODS OF DELIVERY

## 1 Training-at-your-own-pace

**Set Up:** Online access to Material  
**Content:** [AR-in-a-Box — ENISA \(europa.eu\)](#)



## 2 Virtual or Physical Workshop

**Set Up:** 1-2 days Workshop  
**Content:**

- Theory of building an Awareness Raising Program
- Use of Communications dept in real life
- How ENISA supporting tools can be best utilized to deal with cyber crisis.

**Delivery upon Request**

## 3

**PRACTICE MAKES PERFECT**

# THE FUTURE -2023



- ✓ **Crisis Communications guide**
- ✓ **Sector agnostic, editable, customizable material for an AR campaign on phishing and cyber-hygiene (leaflets, posters, videos, quizzes, etc)**
- ✓ **Expansion packs for Game including other kinds of threats/incidents (e.g. BYOD, DDOS)**
- ✓ **Online version of the Game**
- ✓ **Translations**

**GIVE US SOME  
FEEDBACK!**



[EUSurvey - Survey  
\(europa.eu\)](https://europa.eu)



**AR-IN-A-BOX**

**Thank you**



www

**BE THE STRONGEST LINK  
BREAK THE KILLCHAIN**



## 13. Awareness: Desktop exercises with ENISA

Dr. Alexandris Zacharis - ENISA  
Dr. Georgia Bafoutsou - ENISA



EUROPEAN  
UNION AGENCY  
FOR CYBERSECURITY

# How to Build your Custom Awareness Program

By Alex Zacharis & Georgia Bafoutsou  
(ARET)

BE THE STRONGEST LINK  
BREAK THE KILLCHAIN



# CONTENT

- What is a Cyber Awareness Program
- Why have one?
- What is AR-in-a-Box
- Roles
- Building Blocks
- Games/Quizzes



# CYBER AWARENESS PROGRAM

*“An (internal) marketing strategy designed to raise **cyber security awareness**.”*

- ✓ Teaches employees **how to mitigate the impact of cyber threats**.
  - ✓ A plan encompassing multiple awareness-raising activities over a long period of time following the organisation’s strategy for cybersecurity.
  - ✓ It can include one or more internal or external campaigns, focused on a common cybersecurity topic or target group.



# WHY HAVE ONE?

- New threats are emerging.
- Organizations can no longer just rely on their technological defenses to be safe.
- Cybercriminals use sophisticated social engineering techniques to by-pass defenses.
- All it takes is one employee to click on a malicious link and it's game over!
- Your employees are your first line of defense.

**A comprehensive Cyber Security Awareness program is the best way to educate staff and create a security-first culture.**

# STILL NOT SURE? WHAT ABOUT COMPLIANCE?

## ISO 27001/2 & Information Security Awareness Training

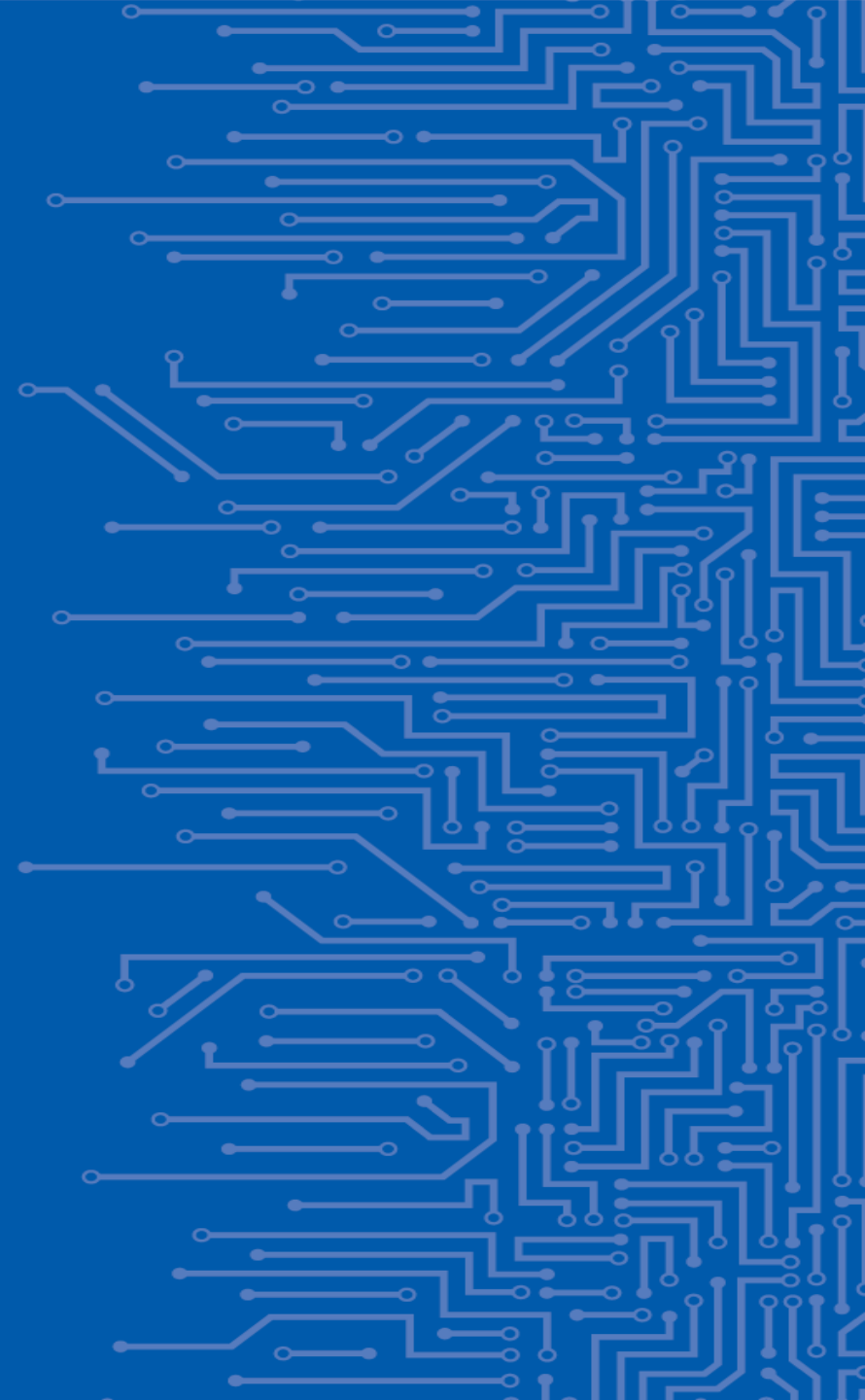
For ISO 27001 compliance, it is essential to comply with **clause 7.2.2**.

The ISO 27001/2 clause 7.2.2 states:

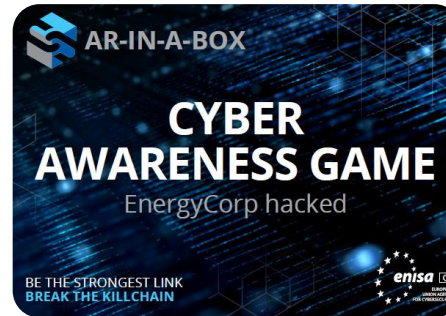
*'Information security awareness, education and training - All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.'*



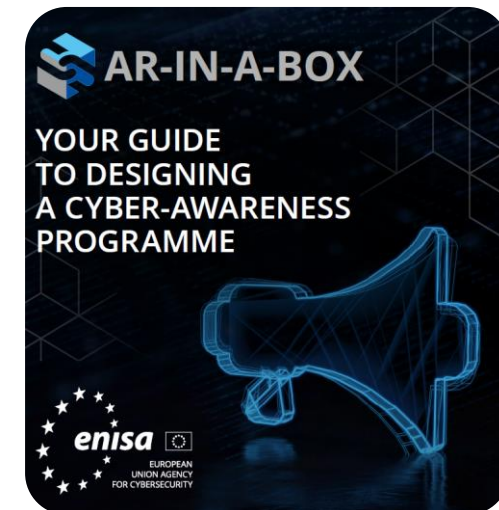
# AR-IN-A-BOX PREVIEW



# AR-IN-A-BOX CONTENT



# DESIGNING A CYBER-AWARENESS PROGRAMME



# SETTING OBJECTIVES



Overall goals for  
awareness and  
learning

Definition of  
SMART awareness  
objectives

Selection of  
specific material,  
tools, methods

**Awareness-raising objectives stem from the risk assessment of the organization and help:**

- ✓ To promote cybersecurity education and culture
- ✓ To be prepared for incidents.
- ✓ To develop an understanding of emerging cybersecurity threats and landscape
- ✓ To promote cybersecurity culture and hygiene
- ✓ To test policies and procedures

# FINANCIAL RESOURCES



## MANAGEMENT:

- Plays a critical role.
- Make sure they are involved in the design and the objectives-setting phase of the awareness programme from an early stage.
- Budget allocation depends on their support.

## TIPS:

- ✓ Try to identify the must-do topics of your programme and the must-train employees who will minimise the risk for your organisation when trained.
- ✓ Reuse or update existing material or resources.
- ✓ Select open-source material or create it in-house.
- ✓ Exploit synergies in the community where available.

# HUMAN RESOURCES



- ✓ **Management**
- ✓ **Cyber Security Officer**
- ✓ **Public Relations & Communications**
- ✓ **ICT**
- ✓ **HR**
- ✓ **DPO / Legal**
- ✓ **Content Developers**
- ✓ **Instructors**





# TARGET GROUPS



**Table 1. Employee target groups**

Audience groups		Clustered audiences
1	Generic employee	Generic employee
2	Contractor	
3	HR	
4	Communications and marketing	
5	Legal	
6	Operations and research and development	C-level, decision-makers, handling budgets
7	Finance and procurement	
8	Managers, officers	
9	Heads of unit, directors	
10	Cybersecurity professionals	Professionals / horizontal implementors of cybersecurity measures and users of cybersecurity solutions, working for organisations and/or individuals
11	Information technology (ICT) professionals	

# SELECTING THE RIGHT TOOLS

5



Choose the right means



## Infographics - Posters

Easy to deploy physically, e.g. in elevators, common spaces



## Ads - Videos

Able to hold and convey a lot of information



## TOOLS FOR AWARENESS RAISING



## Puzzles - Quizzes

Ensure and test understanding of concepts



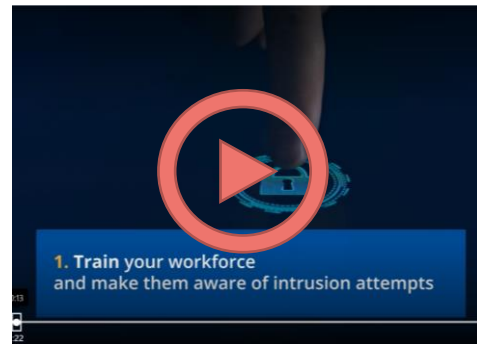
## Live presentations

Direct interactions with participants

# EXAMPLE

Target audience	Channels and delivery methods
<b>Generic employee, contractor HR, communications and marketing, legal, operations and research and development</b>	<ul style="list-style-type: none"><li>• Social media websites, portals</li><li>• Online games and quizzes</li><li>• Gamification (e.g. role playing, escape rooms, mock attacks)</li><li>• Awareness kits (posters, background, screensavers, infographics, customised Windows login pages)</li><li>• Helplines / hotlines / chat boxes</li><li>• Video tutorials</li><li>• Discussion groups / forums</li></ul>
<b>Finance and procurement, managers, officers, heads of unit, directors</b>	<ul style="list-style-type: none"><li>• Newsletters</li><li>• Awareness kits (posters, background, screensavers, infographics, customised Windows login pages)</li><li>• Videos</li><li>• Webinars/workshops</li><li>• e-learning / online courses</li><li>• Publications</li><li>• Conferences/events</li></ul>
<b>ICT professionals, cybersecurity professionals, cyber knowledgeable</b>	<ul style="list-style-type: none"><li>• Real-time courses (face to face or online)</li><li>• Videos</li><li>• Webinars/workshops</li><li>• e-learning / online courses</li><li>• Training labs</li><li>• Certifications/diplomas</li><li>• Publications</li><li>• Networking events / conferences</li></ul>

# ENERGY CAMPAIGN TO TRANSMISSION SYSTEM OPERATORS



## Electricity operators, it is your time!

We need **you** to help us **power up cybersecurity knowledge** in your sector!

Together let's lead all your employees into the light! Give them the tools they need to **deal with** the top cyberthreat... **Ransomware!**

...and find ways to **establish cyber-secure relations** with third parties **protecting** the entire **supply chain!**

Become a cybersecurity conductor and transmit the message, be the light of our cybersecurity community!

**#PowerYourCyber**

### Focus your energy, prepare for ransomware!

Become a human circuit breaker

**RANSOM... WHAT?**

Ransomware is a type of malware where threat actors lock a computer system and demand a certain amount of money in exchange for restoring the system's usability and functionality.

**Ransomware core actions: LEES**

- Lockdown:** Ransomware locks the system, preventing access to data and systems.
- Extortion:** Threat actors demand a ransom payment to restore access to the system.
- Elimination:** Threat actors delete or destroy data and systems.
- Steal:** Threat actors steal sensitive data and systems.

**Ransomware Life Cycle**

- Initial access:** Threat actors gain access to the system through various means, such as phishing, remote access, or vulnerabilities.
- Establish persistence:** Threat actors establish persistence on the system to ensure they can return if they are removed.
- Access to objectives:** Threat actors gain access to the system's data and systems.
- Payment:** Threat actors demand a ransom payment to restore access to the system.
- Remote eradication:** Threat actors remove themselves from the system.
- Ransom payment:** Threat actors receive the ransom payment.

**Ransomware attack footprint**

The ransomware attacker leaves behind several attack artifacts, such as:

- **Log files:** Threat actors may log system activity to track their progress.
- **Registry entries:** Threat actors may create registry entries to maintain persistence.
- **Files:** Threat actors may create files on the system, such as ransom notes or scripts.

**#PowerYourCyber**

## Be the cybersecurity transmitter!

Stay safe from ransomware

Did you know that ransomware can affect our company both directly and indirectly? You heard it! Your organization can be directly targeted by an attack, but it can also be the lateral victim of an attack to a third-party provider, particularly a Supply Chain attack. Let's take a look at both cases...

### Your company could be under attack

Your company could be the **direct victim** of an attack aimed against your assets

The main entry vectors exploited are **remote services and phishing**

So... may the entry points be cybersealed... How can you protect your company?

- **Reduce the attack surface**
  - Apply Awareness Training Plans
- **Protect your perimeter:** Run security software, maintain strict security awareness, security policies, and privacy protection policies up to date keeping personal data encrypted according to the GDPR
- **Restrict administrative privileges** according to the PLOP (Principle of Least Privilege)
  - Stick to **good practices** (pay special attention to backup policies)
  - Have a **continuity plan**

### A third party is under attack

Your company could be affected by an **attack against a third party**

Your organisation is breached through **vulnerabilities in its supply chain**, meaning DSOs or other partnering companies. The attack has affected a supplier, rendering its operations unusable, with **direct repercussions on the services they provide to you**. Or suppliers are used as **stepping stones** to spread the attack.

By building cyber-secure relations with third parties:

- **Evaluate security policies** of third parties (requiring a minimum level of security requirements)
  - Apply **Awareness Training Plans**
- **Define obligations** of suppliers regarding protection of assets, sharing of information, audit rights, business continuity
- **Include** all obligations and requirements **in contracts**, e.g., GDPR
- **Restrict administrative privileges** according to PLOP (Principle of Least Privilege)
- **Monitor service performance** and perform **routine security audits**

**In case of suspicion always REPORT to the corresponding IT Department! if you suffer a ransomware attack...**

- Quarantine affected systems to contain the infection and stop the spread
- Lock down access to backup systems until after the infection gets removed
- Contact the national cybersecurity authorities or law enforcement on how to handle and deal with ransomware
- Visit the **No More Ransom Project**, a European initiative that can decrypt variants of ransomware
- Do not pay the ransom and do not negotiate with the threat actors

**#PowerYourCyber**


# GAS SECTOR CAMPAIGN

## Blocking the manipulation of social engineering: The quote collection

#FuelForCyber

<p><b>RUSH/HURRY</b></p> <p><b>Haste and speed are rarely Good</b> Nothing is that urgent.</p> 	<p><b>FEAR</b></p> <p><b>The fear of war is worse than war itself</b> Never act out of fear.</p> 	<p><b>DIFFICULTY TO REFUSE</b></p> <p><b>He who refuses nothing will soon have nothing to refuse</b> Don't let them get you, don't be afraid to say no.</p> 	<p><b>WORSHIP</b></p> <p><b>Worship changes the worshiper into the image of the One worshiped</b> Don't fall for it, flattery is the best persuader of people.</p> 
<p><b>CURIOSITY</b></p> <p><b>Curiosity killed the cat</b> Be wary of the unexpected, don't bite.</p> 	<p><b>TRUST</b></p> <p><b>Never take anything at face value</b> Don't take anything for granted.</p> 	<p><b>WE LIKE TO HELP OUT</b></p> <p><b>He who helps everybody, helps nobody</b> Don't empathise with the fraudster, don't let them fool you.</p> 	<p><b>IMPRESSIVE OFFERS</b></p> <p><b>Cheap has its price</b> Bare in mind, if it is too good to be true, it probably isn't.</p> 

**READ BETWEEN THE LIES  
DON'T LET THEM FOOL YOU**



## Phishing

Aims at gaining access to systems via impersonation and deception to the user.



#FuelForCyber

enisa  
EUROPEAN UNION AGENCY FOR CYBERSECURITY



# HOW TO DO IT?



# PLANNING

6



Create  
a timeplan

January	February	March	April
 Baseline quiz	 Training topic	 Videos and dissemination material	 Videos and dissemination material
May	June	July	August
 Training topic 2	 Simulation exercise	HOLIDAYS	HOLIDAYS
September	October	November	December
 Back-to-school training	 Games/test/quiz	 <u>Insights</u> collections	 Report to management

# IMPLEMENTATION



## **Cybersecurity training is an ongoing process.**

Ensure that your security posture is as mature as it can be, even as your company and the cybersecurity landscape grows and evolves.

Three periods are considered relevant for delivering cybersecurity-awareness training to your employees:

- ✓ When they join the organisation as part of the induction process
- ✓ After an incident, in order to indicate the procedures, roles and responsibilities in place;
- ✓ At regular intervals throughout the year (see calendar)



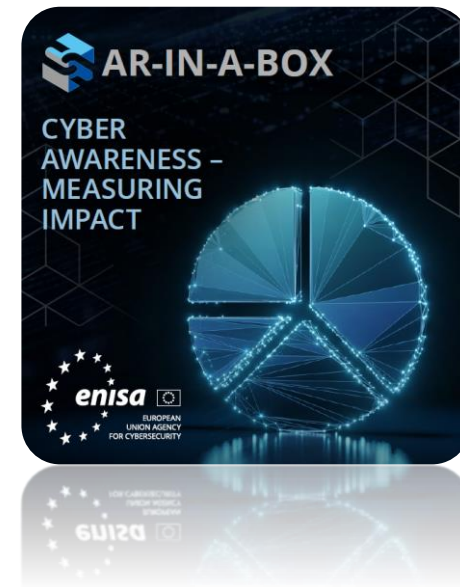
# EVALUATION



**A KPI is a value that measures a component of an awareness-raising campaign or programme.**

**There are five reasons why KPIs fail to improve performance:**

1. the KPIs are poorly defined;
2. they lack accountability;
3. they are not achievable;
4. they are not specific enough;
5. they are too hard to measure.



# CYBER AWARENESS GAMES

## Gamification helps!

- ✓ Determine how your team will react to a theoretical cyber attack and how effective your plan is.
- ✓ Identify flaws or gaps in the organization's response and make adjustments
- ✓ Testing consequences in a safe environment
- ✓ Coordination between different departments
- ✓ Save money



# QUIZZES

   
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Which type of cyber-attack is commonly performed through email?

- Phishing
- Smishing
- Vishing
- Ransomware

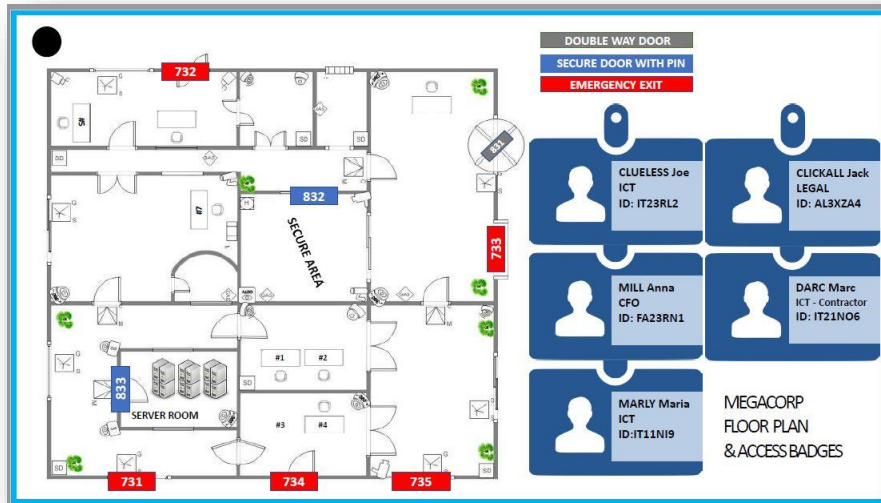


## Phishing

**CORRECT!** The term 'phishing' is used to describe a social engineering based cyber-attack that arrives mainly by email. Though email phishing is the most popular kind of phishing, other variants of this attacks can arrive by SMS (smishing), phone calls (vishing) or ransomware (digital kidnapping).

Other choices: **INCORRECT**

# TABLE-TOP GAMES



## SCENARIO - MEGACORP HACKED

MegaCorp, a leader in online retail has been hacked based on information leaked on the public internet. Attackers appeared to have gained initial access via a successful PHISHING ATTACK. To make matters worse UNAUTHORISED ACCESS has been detected in MegaCorp headquarters and a RANSOMWARE hit the company the same day. You are the lead Cyber Security Investigator recruited to provide answers on who is behind the hack and try to stop him/her before its too late. We gathered as much evidence as possible. Analyze them quickly. You have 30 minutes left before all our data are wiped out.

**GOOD LUCK!**

## ANSWER SHEET

What is the name of the first known victim of the PHISHING ATTACK?  
 (Name Surname as seen in the Badge with space!)

Which Badge ID was used to performed unauthorized access?

ENCRIPTION KEY

What is the filename of the decrypted file?

# AR-IN-A-BOX: METHODS OF DELIVERY

## 1 Training-at-your-own-pace

**Set Up:** Online access to Material  
**Content:** [AR-in-a-Box — ENISA \(europa.eu\)](#)



## 2 Virtual or Physical Workshop

**Set Up:** 1-2 days Workshop  
**Content:**

- Theory of building an Awareness Raising Program
- Use of Communications dept in real life
- How ENISA supporting tools can be best utilized to deal with cyber crisis.

**Delivery upon Request**

## 3

**PRACTICE MAKES PERFECT**

# UPDATE FOR 2023



- ✓ **Crisis Communications guide**
- ✓ **Sector agnostic, editable, customizable material for an AR campaign on phishing and cyber-hygiene (leaflets, posters, videos, quizzes, etc)**
- ✓ **Expansion packs for Game including other kinds of threats/incidents (e.g. BYOD, DDOS)**
- ✓ **Online version of the Game**
- ✓ **Translations**



**AR-IN-A-BOX**

**Thank you**



www

**BE THE STRONGEST LINK  
BREAK THE KILLCHAIN**



## 14. Q&A and goodbye



Douglas Walker Hill  
Interoperability & Data  
Exchange Adviser  
ENTSOG



A top-down view of a wooden table with various food items. On the left is a large pizza with toppings like broccoli, onions, and pickles. In the center are two burgers with sesame seed buns and a pile of fries. On the right is another pizza with arugula and prosciutto. At the bottom left is a sandwich with lettuce and tomatoes. At the bottom center is a bowl of oysters on ice. At the bottom right are a knife, a fork, and a small chocolate bun. The text "Enjoy your lunch And goodbye" is overlaid in the center in white, with a faint, mirrored version of the text below it.

Enjoy your lunch  
And goodbye

And goodbye



# Thank you for your attention & being an active part at this event

Douglas Walker Hill, Interoperability & Data Exchange Adviser

[douglas.hill@entsog.eu](mailto:douglas.hill@entsog.eu)

ENTSOG - European Network of Transmission System Operators for Gas

Avenue de Cortenbergh 100, 1000 Bruxelles

[www.entsog.eu](http://www.entsog.eu) | [info@entsog.eu](mailto:info@entsog.eu)

