Cybersecurity, regional networks and resilience

Italy Smart Grids Study Tour

Luigi Ballarano, Head of Cyber Security - CISO Group
Alessandro Marasco, Head of Cyber Defence Center
Alberto Della Ratta, Head of Cyber Security Governance Strategy & Awareness

22 MAGGIO 2026

ISC - Uso INTERNO / INTERNAL Use

Sommario

Cyber Security Landscape	3
Cyber Security in Terna	9
Zero Trust Approach	20
Supply Chain	23
Cyber Security Challenges	25

Cyber Security Landscape

Main Cyber Threats 1/2

«Technology has ceased to be merely innovation and has become the driving force of change, as well as one of the main factors impacting national security. We are living through a historical phase marked by a profound and ongoing transformation, capable of structurally affecting strategic balances, economic stability, and social cohesion».
(2026 Annual Report on Information Security Policy, "Sistema di informazione per la Sicurezza della Repubblica")

68% **of cyber attacks in 2025 targeted public entities or strategic infrastructures**

+18 **percentage points compared to the previous year in pressure targeting public entities or strategic infrastructures**

Source: "2026 Annual Report on information Security Policy" - Dipartimento delle informazioni per la Sicurezza (DIS)

53,7% of the total number of recorded incidents involved essential entities (according to NIS2 definition).

Source: ENISA Threat Landascape 2025

Technological and Cybersecurity Landscape

- Attack surface expansion to be monitored
- Technological complexity and legacy systems
- Remote access and distributed management
- Supply chain technology

Cybersecurity challenges driven by the digital and energy transition

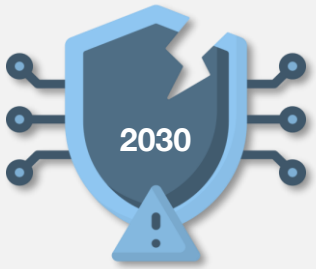
- Cyber threats evolution
- Regulatory pression and compliance
- Disruptive technologies
- Complex geopolitical landscape

ISC - Uso INTERNO / INTERNAL Use

Main Cyber Threats 2/2

The **Global Cybersecurity Outlook 2026*** (January 2026) identified the following future threat vectors:

While **artificial intelligence** continues to dominate the cybersecurity landscape, a number of emerging technologies and threat vectors are quietly gaining ground and are expected to **increase their influence by 2030**



Autonomous systems and robotics

Developments in this field will give rise to new cyber-physical risks, where decisions made by machines can affect security and the services provided within seconds, significantly reducing detection and response times.

Digital currencies

With the evolution of virtual identities and AI-based fraud, digital currencies are increasingly becoming a critical infrastructure, the security of which underpins economic and social stability.

Space technology and submarine cables

Satellite communications and submarine cables will form the backbone of emergency services, cloud infrastructure and international data exchange. As AI-based operations grow, the consequences of disruptions will become more severe, with repercussions for entire digital ecosystems.

Natural disasters and climate change

In the future, the climate could act as a catalyst for cyber risk, increasing recovery times and blurring the line between environmental and digital resilience. Extreme weather conditions can cause disruptions to electricity, IT and logistics networks, and AI-based coordination systems for energy, water and emergency response networks can introduce new attack surfaces.

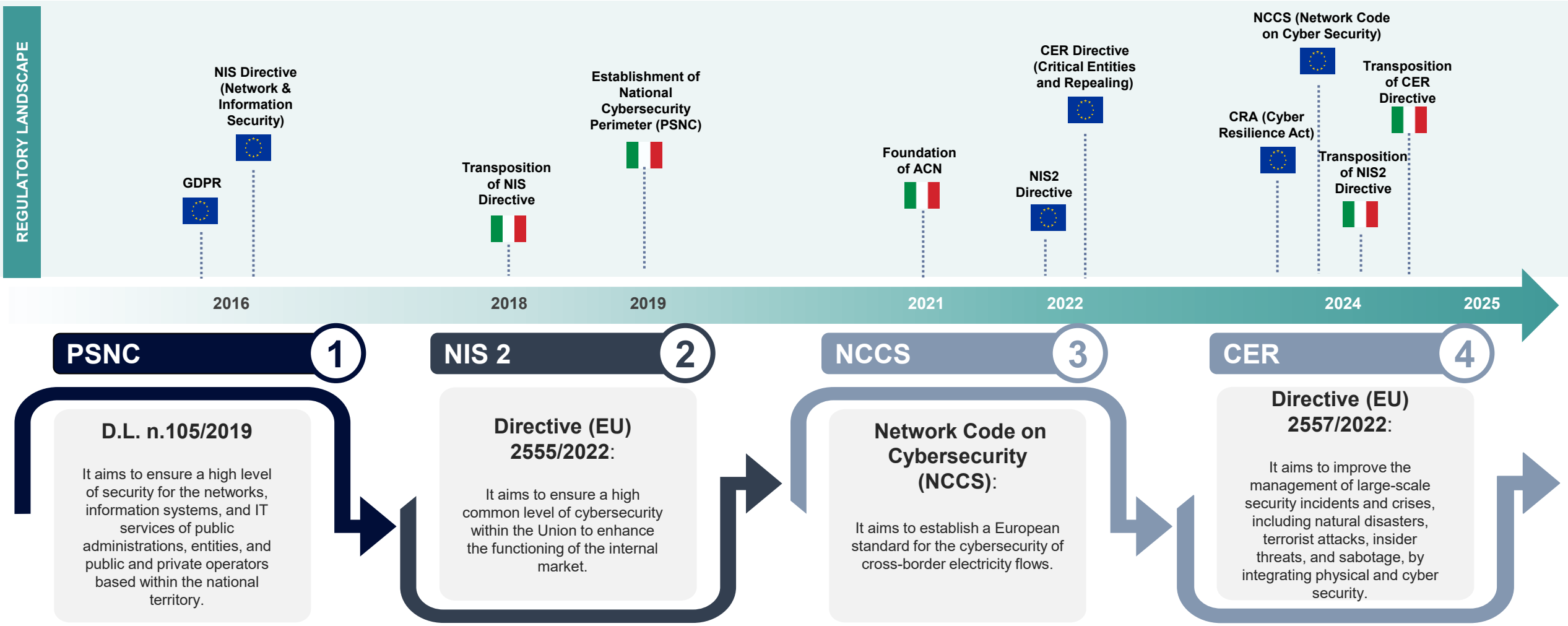
Quantum technologies

Quantum technology will increasingly pose a real threat to cryptography. However, this technology also serves as a tool to support cyber defence: the processes of analysis and anomaly detection can be enhanced through its use.

Source: Global Cybersecurity Outlook 2026 | World Economic Forum

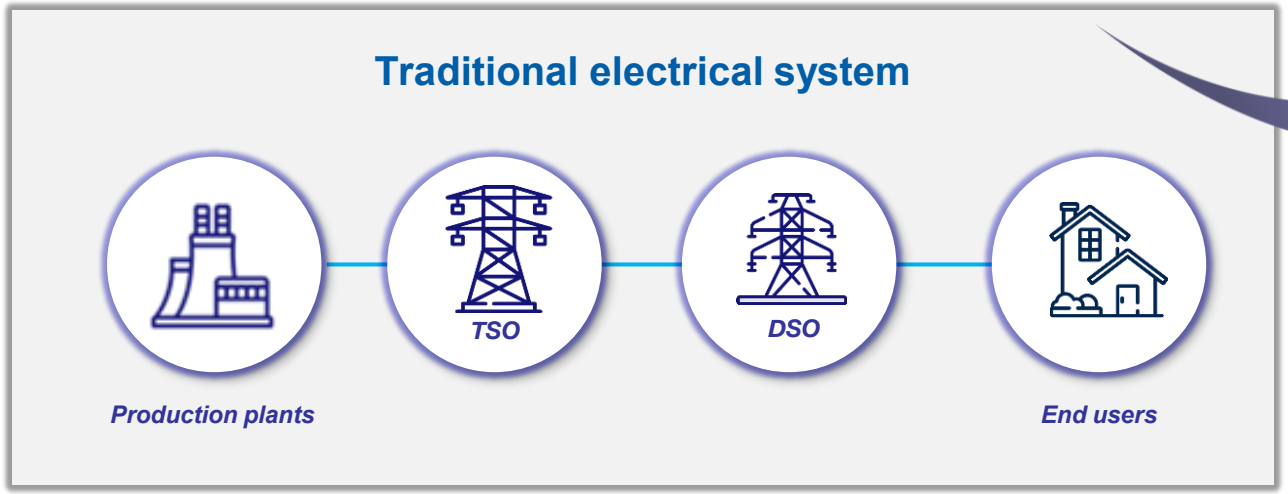
Evolution of the regulatory context

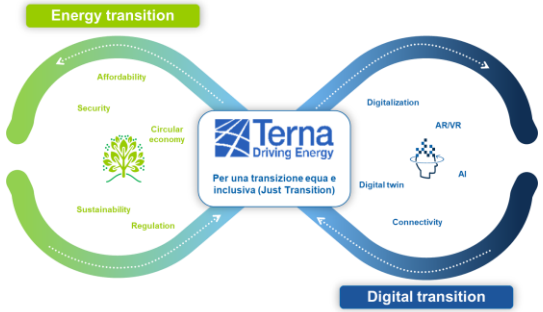
The regulatory context in the cyber field is progressively evolving, with the introduction of new constraints and the requirement to implement increasingly higher security standards.



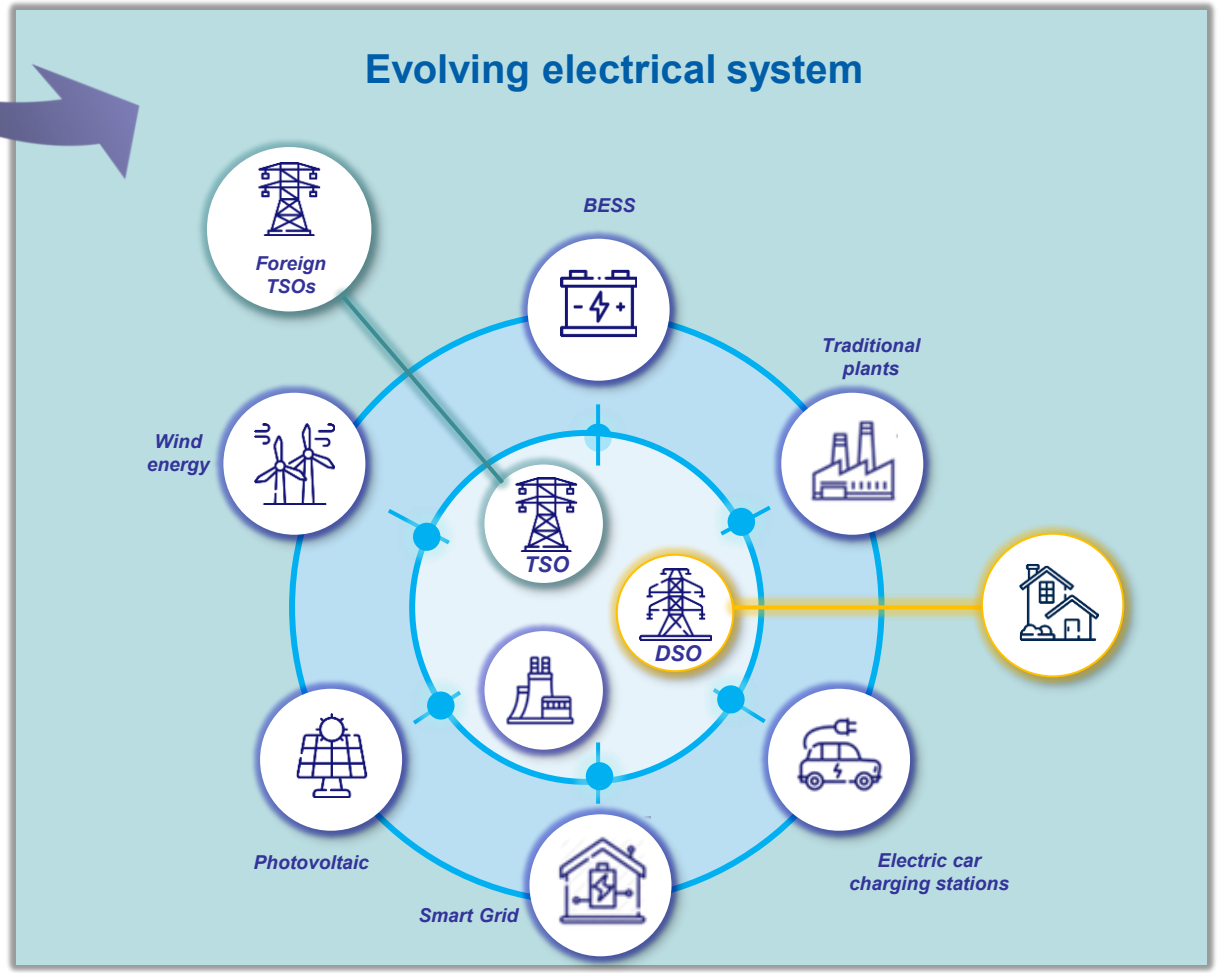
Evolution of the National electrical grid – main Cyber impacts

The national electrical system is transforming from a centralized model to an integrated and distributed one: today there are approximately 2.1 million electricity production plants in Italy (compared to about 160,000 in 2010).





The **energy transition** and the concurrent **digital transition** of the electrical sector involve the expansion and the evolution of the National Electric System from a technological perspective.



Evolution of the National electrical grid – new cyber scenarios

To mitigate the risks associated with the increase in the attack surface, it is essential to implement adequate cybersecurity measures to prevent threats across the entire National Electrical Sector.

Connected devices: with the adoption of IoT technologies and the connection of systems to monitoring and control networks, the number of connected devices increases significantly, and as a result, the **potential access points exploitable by cyber attackers also rise**.

System complexity: the increase in the complexity of the software used in devices and systems associated with plants can lead to a greater number of potential vulnerabilities, which **can be exploited by attackers to gain unauthorized access or compromise the stability of the system**.

System interconnections: plants are generally integrated into larger energy networks. Therefore, a potential attack on one component could have **cascading effects on other interconnected systems**, directly or indirectly interconnected to the infrastructure managed by Terna.

Remote access: the need to monitor and manage plants remotely may involve the configuration of remote access points. These additional access points, if not properly secured, **can pose a security risk**.

The attack surface exploitable by cyber attackers is increasing

Cyber Security in Terna

ISC - Uso INTERNO / INTERNAL Use

Cyber Security in Terna

Organizational structure and main services

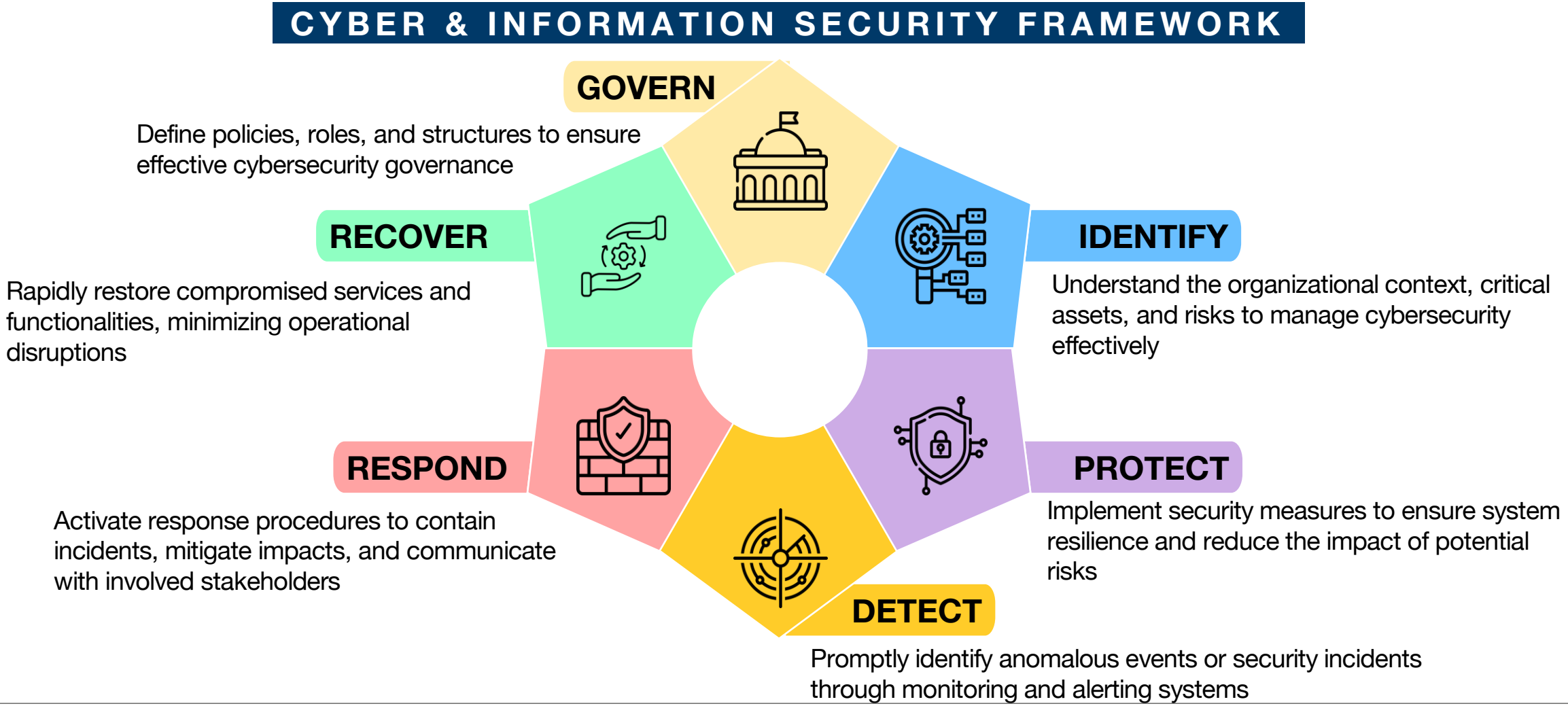
Cyber Security

Cyber Security Governance, Strategy & Awareness | **Cyber Security Architectures & Engineering** | **Cyber Risk Management & Policies** | **Cyber Defence Center** | **Security Platform**

MAIN SERVICES

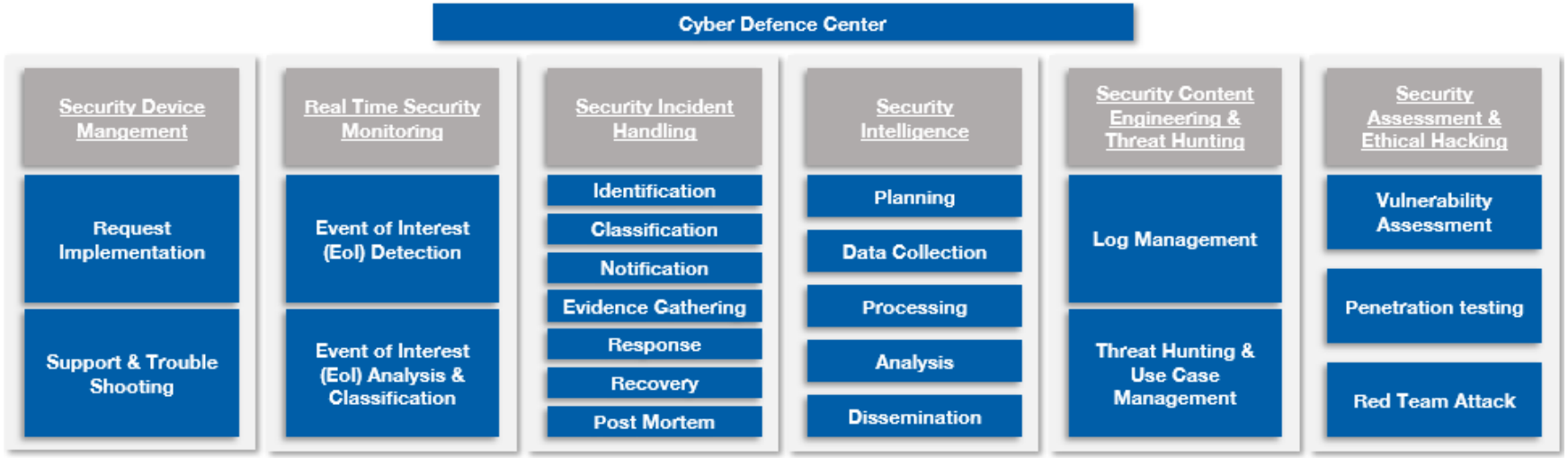
- Definition and implementation of the **Group Cyber Security strategy** through the development **of metrics and monitoring processes**
- Definition and review of **Information Security policies, operating procedures and guidelines**
- Design, development and acquisition of **solutions and architectures** for active and passive defence, and support for **Cyber Security by Design**
- Planning and execution of **Technical Assurance activities (e.g. Vulnerability Assessment / Penetration Test / Red Team Attack)**
- Implementation of the **OT Security program** to strengthen the **cyber security posture of digital electrical substations**
- Design, implementation and promotion of corporate **Cyber Security Awareness** initiatives
- **Real-time monitoring** of security events, Threat Intelligence analysis, and management and coordination of information security incidents
- Development and management of **internal/external digital identity tools** for the Group
- Design and implementation of **Zero Trust** architectures and **Digital Protection** solutions, including encryption of corporate communication channels and documents
- Cyber risk governance, regulatory compliance, **Third-Party Cyber Risk Management and Cyber Assurance**
- **Cryptography management,** including PKI and cryptographic key lifecycle management
- Monitoring the evolution of cryptographic solutions, **developing quantum-safe and post-quantum technologies**
- Definition and coordination of **Cyber Resilience, Business Continuity** and **Disaster Recovery** strategies
- **Operations of Cyber Security platforms** and dedicated **Data Center**

Cyber Security Governance: Terna's Information Security Framework & NIST



Cyber Security in Terna

Cyber Defence Center Operating Model



The **Cyber Defence Centre (CDC)** operates 24 hours a day, 7 days a week, 365 days a year, and is organised as follows:

- **Computer Emergency Readiness Team**
- **Active Cyber Defence**
- **Cyber Security Assessment & Ethical Hacking**

Cyber Security in Terna

Cyber Defence Center Evolution

2021
- **CERT**
- **RTSMh24**

2022
- CERT
- RTSMh24
- **ACD**

2023
- CERT
- RTSMh24
- ACD
- **SDAMh24**

2024
- CERT
- RTSMh24
- ACD
- SDAMh24
- **CDCh24**

2025
- CERT
- RTSMh24
- ACD
- SDAMh24
- **CSAH**

2026
- **CDCh24 (Q2 2026)**

Enhanced response capabilities

Reduced response times

Main collaborations and stakeholders

Terna's Cyber network

Institutional authorities

Memorandum of understanding with several **institutional bodies**, including the **National Cybersecurity Agency (ACN)** and the **National Cybercrime Center for the Protection of Critical Infrastructures (CNAIPIC)**, with the aim of:

- **Preventing** and countering **attacks** or **damage** against Terna's infrastructures
- Promoting the **exchange of information**, knowledge, best practices, and risks, threats, and vulnerabilities analysis
- **Strengthening** the **Cyber security posture**

Universities & associations

Collaboration with **universities** in line with **measure #59 of the National Cybersecurity Strategy** promoted by ACN, which aims to strengthen the development of Cyber Security training programs.

TYRRHENIAN LAB: Second-level Master's degree in "Digitalization of the electricity system for the energy transition" – designed by Terna in collaboration with the Universities of Cagliari, Palermo and Salerno, as part of the Tyrrhenian Lab project.

Collaboration with **associations** aimed at **knowledge sharing** and the **sharing of experiences** with cross-sector players in order to **create a national and European cybersecurity ecosystem**.

External stakeholders

Collaboration with various **external stakeholders**:

Players operating in the **energy sector** for collaboration and the sharing of best practices

Associations supporting information sharing among the **CERTs** of major global organizations

Industry associations for cooperation among **European TSOs** with a view to **implementing EU energy policy** and achieving Europe's energy and climate policy objectives

Strategic sponsorships, such as the one with Fondazione MICO 2026.

Action Pillars

Cyber attack risk is consistently among the top risks identified by Terna, considering the continuous increase in cyber threats and the ongoing evolution of regulatory obligations.

Main Cyber Challanges

Ensuring a cyber resilience energy transition

The energy transition and the parallel digital transition lead to an **increased cyber attack surface**

Anticipating the evolution of cyber threats

The continuously evolving **cyber threat landscape** requires ongoing monitoring and the ability to minimize the impacts of cyber events

Making Cyber Security a strategic business partner

Cyber Security is a **key enabler** in business strategic processes, contributing to the achievement of corporate objectives.

Cyber Action Pillars

Ensuring full visibility of the corporate security perimeter and continuous monitoring of related threats

Protecting corporate technology domains, with particular focus on Operational Technology (OT), and mitigating risks arising from potential cyber threats

Responding promptly to potential cyber security events

ENABLING FACTORS

- Strengthening cooperation with **external stakeholders and national and international authorities**
- Developing **new capabilities in terms of skills and technologies**
- Adopting a **human-centric cyber approach**

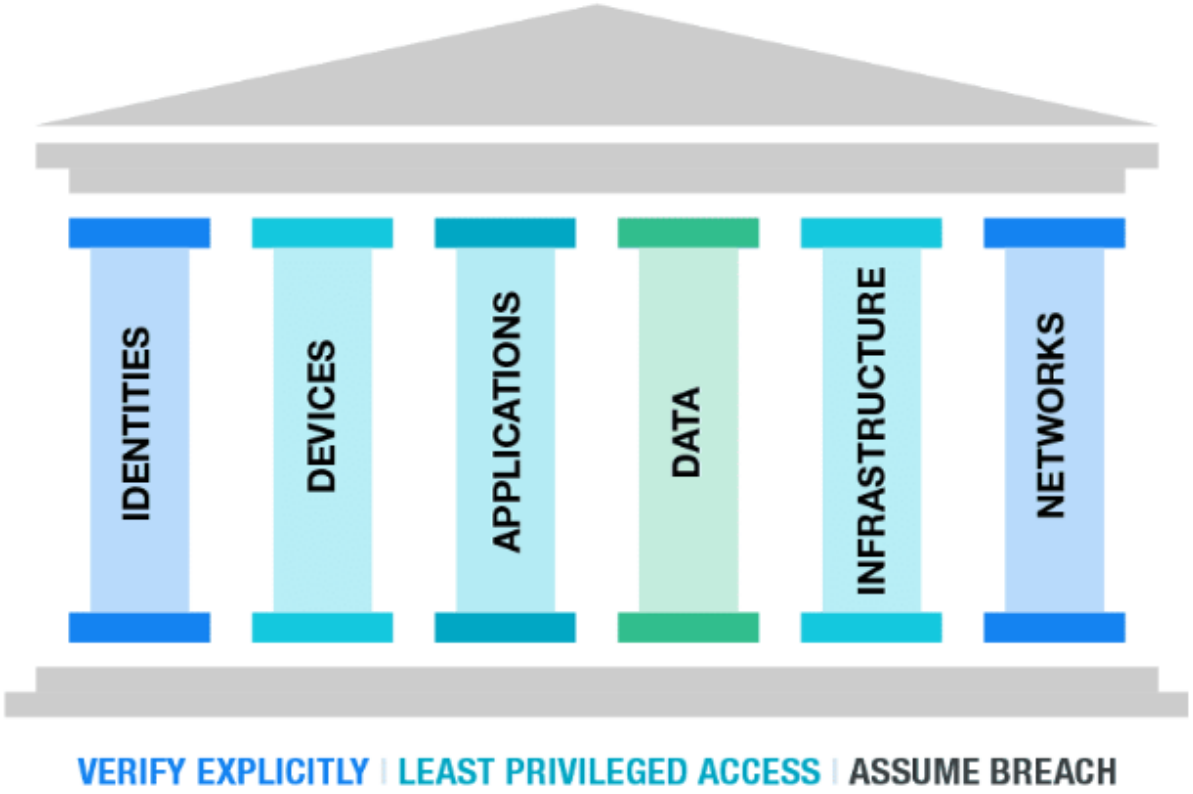
Zero Trust approach

Zero Trust overview

Zero Trust key pillars

Never Trust, Always Verify

The pillars of the Zero Trust model represent a **holistic approach to security**, focusing on the continuous protection of identities, devices, applications, data, infrastructure and networks. Each pillar works together to **ensure that every access attempt is verified, authorised and constantly monitored**, thereby reducing the risk of both internal and external threats.



Zero Trust – projects & benefits

Terna security evolution approach and benefits

Zero Trust projects in Terna

Implementation of a Zero Trust SASE solution for the entire workforce.
Designed to protect users, devices, applications and systems in hybrid work environments.
This ensures secure and fast access to corporate resources by implementing centralised security policies with a focus on continuous monitoring.

Implementation of a Zero Trust SASE solution for Terna's suppliers.
Aimed at removing site-to-site VPN connectivity and protecting corporate resources by reducing the granularity of access by users outside the company.

Definition and implementation of a secure application development process.
Automatically integrates security solutions during the design and coding phases - proactively detecting and resolving any vulnerabilities and threats.

Definition of guidelines and best practices regarding Strong Authentication, both at the user-to-machine and machine-to-machine levels. Guide the design of architectures supporting various business initiatives to natively incorporate this security requirement, thereby promoting the implementation of more secure and resilient systems.

BENEFITS

Improve **compliance** and **visibility** across **all flows** and **devices**, facilitating monitoring and control capabilities

Enhance protection against **well-known** and **zero-day threats** through continuous and granular control of vulnerabilities, access points, and exposed systems

Protect corporate assets in **distributed environments** involving both data and people (smart working, cloud)

Reduce the impact of potential breaches and business disruptions through segmentation and access control at the individual asset level

Simplify IT management through the automated application of security rules

Supply Chain

Third-Party Risk Management

Cyber Security Risk Assessment & Third-Party Cyber Risk Monitoring

Terna adopts a structured approach to manage and monitor cybersecurity risks related to its suppliers.

Terna carries out Cyber security risk assessment activities on a group of suppliers selected on a yearly basis. These activities include security questionnaires and an evaluation of the supplier's cyber risk using a defined methodology.

Terna continuously monitors the Cyber security posture of key suppliers through OSINT-based technology tools, which provide relevant contextual information.

Terna uses contractual documentation to set specific information security requirements for its suppliers. These requirements are regularly updated, also taking into account the evolution of the regulatory framework.

Cyber Security Challenges

ISC - Uso INTERNO / INTERNAL Use

Artificial Intelligence, Quantum Computing & Digital Sovereignty

Artificial Intelligence

- **Attacks automation & AI-enhanced phishing**

Cyber attacks are becoming more effective and scalable thanks to generative models capable of producing realistic and personalized emails, messages, and malicious code.

- **Deepfakes & advanced social engineering**

AI-generated fake audio and video are being used to impersonate executives, colleagues, or suppliers in order to gain unauthorized access or induce fraudulent money transfers.

- **Attack surface expansion and system opacity**

The widespread adoption of GenAI is leading to an exponential increase in access points and risk vectors, which are often difficult to monitor. In addition, the limited transparency ("black box" nature) of AI models makes it more difficult to detect errors or misuse.

- **Information manipulation**

Generative AI, in particular, introduces new risks related to cybersecurity and information manipulation

Quantum Computing

- **Compromise of current cryptography**

Once mature, quantum computers will be able to break additional algorithms (e.g, RSA, ECC), which currently underpin digital identities, VPNs, and secure communications.

- **Harvest now, decrypt later**

Malicious actors may intercept and store encrypted data today in order to decrypt in the future using quantum computing capabilities.

- **Impact on critical infrastructures and OT**

Industrial systems characterized by long life cycles and legacy technologies are particularly vulnerable to delayed cryptographic transition.

- **Risks related to the technology supply chain**

Dependence on suppliers that are not prepared for Post-Quantum Cryptography (PQC);
Complexity in ensuring interoperability and end-to-end security across distributed ecosystems

Digital Sovereignty

- **Complex geopolitical landscape** characterized **by tensions and technological dependencies**
- **Greater complexity in supply chain management**, including the assessment of supplier reliability, security and control.
- **Limited availability of mature European solutions** and need for long-term, structural investments to strengthen industrial capabilities, skills, and national and Eurepean innoviation

Against this backdrop, **regulatory measures** are being introduced to govern the **procurement of technologies intended to protect assets critical to national security.**
This framework is **based on preferential criteria** designed to promote cybersecurity technologies developed by Italian, European, NATO, or other trusted-country entities (**DPCM, 30 April 2025**).

Grazie

Luigi Ballarano, Head of Cyber Security - CISO Group
Alessandro Marasco, Head of Cyber Defence Center
Alberto Della Ratta, Head of Cyber Security Governance Strategy & Awareness

Terna
Driving Energy

ISC - Uso INTERNO / INTERNAL Use