



Acting as the voice of the **security industry**

Confederation of European Security Services



## WHITE PAPER

Shaping the Future of **Critical Infrastructure Security**  
and Resilience through **Public-Private Collaboration**



4 June 2025

#### Copyright:

Unless stated to the contrary, all materials and information are copyrighted materials owned by CoESS (Confederation of European Security Services). All rights are reserved. Duplication or sale of all or any part of it is not permitted. Permission for any other use must be obtained from CoESS. Any unauthorised use of any materials may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes. To the fullest extent possible at law we (and all our sister, parent, subsidiary and member companies and organisations) exclude all liability for any loss or damage (including direct, indirect, economic or consequential loss or damage) suffered by you as a result of using the contents of this manual.

#### Disclaimer:

Our liability—to the fullest extent possible at law we (and all our sister, parent, subsidiary and member companies and organisations) exclude all liability for any loss or damage (including direct, indirect, economic, or consequential loss or damage) suffered by you because of using the contents of this document.

#### Design & graphics:

<https://blog.acapella.be/>

#### Photo credits:

© AdobeStock: 1032234778\*: Johannes, 1243637290\*: Itsaree, 856511461\*:

Curioposs, 546319561\*: NongAsimo, 588772865: NicoElNino, 104034637:

Rawpixel.com

\* Generated with AI

© iStock: 1567221653: Jacob Wackerhausen, 1446655450: ko\_orn, 1340413200:

zhaojiankang, 506815322: artJazz, 697909418: Tero Vesalainen, 1053936332:

BrianAJackson, 1197313322: aerogondo, 1465589487: LeManna, 2024514092:

SweetBunFactory, 184413917: kapukdodds, 500873134: MartinLisner

© Shutterstock: 2319013245: Aree\_S, 1588653481: FOTOGRIIN

#### About CoESS:

The **Confederation of European Security Services (CoESS)** acts as the voice of the private security industry, covering **23 countries** in Europe and representing **45,000 companies** with **2 million security officers**. Private security services provide a wide range of services, both for private and public clients, ranging from Critical Infrastructure to public spaces, supply chains and government facilities. CoESS is recognised by the European Commission as the European employers' organisation representative. We are actively involved in European Sectoral Social Dialogue and multiple EU Expert Groups – including SAGAS, SAGMAS, LANDSEC, the EU Operators Forum for the Protection of Public Spaces and the EU Ports Alliance.

**EU Transparency Register Number: 61991787780-18**

#### Publisher:

**Catherine Piana**

Director General

CoESS aisbl

56 Avenue des Arts

1000 Brussels

Belgium

[catherine@coess.eu](mailto:catherine@coess.eu)

[www.coess.eu](http://www.coess.eu)

# TABLE OF CONTENTS

<b>PREAMBLE</b>	<b>4</b>
<b>FOREWORD</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
<b>Chapter I</b> Strengthening Critical Infrastructure: The Strategic Role of Private Security	<b>7</b>
<b>Chapter II</b> Defining Critical Infrastructure	<b>10</b>
<b>Chapter III</b> Analyzing the New EU Framework for Critical Entities Resilience	<b>12</b>
<b>Chapter IV</b> Threats and Vulnerabilities and Avenues for Thought	<b>14</b>
<b>Chapter V</b> The Role and Objectives of Standards: the EN 17483 Standard System	<b>22</b>
<b>Chapter VI</b> Best Practices in Critical Infrastructure Protection	<b>23</b>
<b>Chapter VII</b> Conclusions and Recommendations from Best Practice	<b>36</b>

# PREAMBLE



In a time of increasing geopolitical tension and hybrid threats, the resilience of Europe's Critical Infrastructure (CI) has become a strategic imperative. From energy and transport to digital networks and healthcare systems, our societies depend on a constellation of vital services whose disruption can have catastrophic consequences. The adoption of the Critical Entities Resilience (CER) Directive represents a crucial step forward, establishing a common European framework to strengthen the physical protection of CI in an era marked by unpredictable risk.

Critical infrastructures are strategic targets not only in times of war, but also in times of geopolitical crisis. They are subject to targeted attacks from digital space directly piloted or sponsored by opposing states. The interconnection between infrastructures across sectors and borders means that no entity exists in isolation. A successful attack on one critical node can rapidly cascade through the system, affecting entire regions or industries.

This reality compels us to rethink security in holistic terms, integrating public and private actors in structured and trustworthy partnerships. Public-Private Partnerships (PPPs) are not an option but a necessity—

offering the agility, expertise, and operational reach required to face complex and evolving threats.

At national level, no Member State can bear the burden of CI protection alone. Police and public security forces, though essential, lack the capacity to protect all infrastructures around the clock. Certified Private Security Companies (PSCs), when properly regulated and integrated, can assume key roles that complement public efforts—freeing up law enforcement to focus on core missions.

This White Paper makes a compelling case for a pragmatic, forward-looking security model: one that builds on best practices, fosters trust across sectors, and offers concrete recommendations to operationalise PPPs. In doing so, it contributes meaningfully to shaping Europe's collective resilience strategy at a time when it is needed most.

**LtG Christophe Gomart**  
French Member of the European Parliament  
Vice-Chair of the Committee on Security  
and Defence



**Vinz Van Es**  
CoESS Chairman



**Lt-col. (R) Jean-Philippe Béryllon**  
CoESS CIP Committee Chairman

# FOREWORD

In an era marked by unprecedented global turbulence, the protection of Europe's Critical Infrastructure (CI) has never been more vital. The convergence of geopolitical instability, terrorism and rapidly advancing technology, and increasingly sophisticated hybrid threats underscores the urgent need for robust, adaptive security measures. From cyberattacks targeting essential services to physical sabotage of energy infrastructure, the evolving threat landscape demands a new level of vigilance and collaboration.

At the heart of this protective framework lies a resource too often underestimated: Private Security Companies (PSCs). Operating security on a wide range of CI, and first line of defense, PSCs have become indispensable partners in safeguarding Europe's essential services and critical infrastructure. Their role extends beyond traditional security functions; they bring specialized expertise, operational flexibility, and innovative approaches that complement public authorities and law enforcement and allow states' and cities' security forces to focus on the higher end of the threat spectrum. In doing so, they help create a layered security network capable of withstanding both conventional and emerging threats.

The recognition of PSCs as strategic partners is now reflected in significant legislative progress. The adoption of the **Critical Entities Resilience (CER) Directive** is a major milestone, acknowledging the value of private security in fortifying Europe's infrastructure. This legislative shift, coupled with the development of CEN standards for private security services protecting critical infrastructure, has set the foundation for a more cohesive and effective security ecosystem.

Yet, legislation and standards are only as effective as their implementation. True resilience requires not just compliance but a shared commitment from all stakeholders—public and private—to foster collaboration, exchange intelligence, and build mutual trust. **The synergy between PSCs, national authorities,**

**and CI operators must become the cornerstone of Europe's security framework.**

This White Paper serves as both an analysis and a call to action. It reflects the insights gained from in-depth interviews, real-world case studies, and the collective expertise of industry leaders and policymakers. Our aim is to highlight best practices, identify gaps, and offer actionable recommendations that can elevate the security posture of Europe's critical infrastructure.

Drawing from the best practices gathered and the in-depth interviews conducted with a diverse range of stakeholders, we have identified key success factors, challenges, gaps, and corresponding recommendations. These insights aim to strengthen the protection and resilience of Critical Infrastructure (CI).

However, one fundamental element emerges—less tangible, yet vital—and that is the cooperative mindset. This mindset must be embedded within authorities and their representatives, permeating all levels of the hierarchy. Achieving this requires a genuine recognition of the added value that Private Security Companies (PSCs) bring to the table—their unique competencies, expertise, and operational capabilities. Only by treating PSCs as true partners can this collaboration reach its full potential.

At a time when Europe faces an unprecedented convergence of political instability, shifting geopolitical dynamics, a persistent terrorist threat, societal pressures, and rapid technological advancement—coupled with increasingly easy access to disruptive tools by ill-intentioned actors—there is no room for complacency. Whether authorities acknowledge the analysis and recommendations presented here, and take decisive action, will determine our ability to elevate Critical Infrastructure Protection (CIP) to the next level and ensure resilience against the evolving challenges and threats ahead.

# Introduction

Since the last edition of this White Paper in 2016, **two major developments** have reshaped Critical Infrastructure Protection (CIP) in Europe. First, the adoption of the **Critical Entities Resilience (CER) Directive**, and second, the establishment of a **CEN Standard System for Private Security Companies (PSCs)** protecting Critical Infrastructure. This system includes three unanimously adopted standards by the 34 European Standards Institutes.

Most significantly, the Directive explicitly references private security, emphasizes quality standards in training, and encourages Member States to integrate relevant standards into their CI Protection frameworks. This is the outcome of several years of advocating in favour of quality for any type of private security services, but even more so for Critical Infrastructure Protection.

However, this is merely a starting point. The real challenge lies in ensuring that these quality and standardization references are not just recommendations but become binding obligations through national transposition.

The national legal acts transposing the CER Directive's provisions should have entered into force latest in October 2024 but at the time of writing (mid-April), only 10 out of 27 Member States have adopted their national acts. The geopolitical context, namely the War in Ukraine, and acts of sabotage against energy and transport infrastructure, is making this transposition even more crucial, as it has been reminded by the Council in a Recommendation to the Member States<sup>1</sup> and in the recently published Commission "ProtectEU: a European Internal Security Strategy"<sup>2</sup>.

It is therefore also timely to publish not just an update of the 2016 paper, but rather a new document exploring the situation 9 years after the previous one.

In this new edition, we are including a section on the new Directive and its implications, provide an outlook on the evolution of threats against CI, introduce the new CEN Standard System and explore some best practices in CIP, on the basis of which we conclude the document with recommendations to Authorities and, in particular, the EU Critical Entities Resilience Group chaired by the Commission. This edition also introduces emerging systemic risks—such as disinformation campaigns and digital sovereignty concerns—that increasingly affect the resilience of Critical Infrastructure.

<sup>1</sup> <https://data.consilium.europa.eu/doc/document/ST-15623-2022-INIT/en/pdf>

<sup>2</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0148>

# Chapter I

## Strengthening Critical Infrastructure: The Strategic Role of Private Security



Critical Infrastructure in Europe is owned, operated and protected by a mixture of public and private organisations. It is a fact that Private Security Companies (PSCs) increasingly provide security services to CI, either on their own or on behalf of and in cooperation with state and law enforcement authorities. Some CI have their own in-house security services, which may or may not be subject to the same obligations as outsourced security services.

For years, CoESS has championed best-value procurement practices, producing key resources such as a manual on purchasing quality private security services<sup>3</sup>, White Papers on Public-Private Partnerships, Cyber and Physical Security in CI, and Best Practices in Transport Security<sup>4</sup>. CoESS has been advocating for many years in favour of best value procurement and, with decades of collective experience in CI protection, CoESS and its members are well-positioned to define the essential criteria for PSCs operating in these environments.

In a wider context, CoESS has been highlighting the common sense elements that need to be in place in order to ensure that the values that underpin all its actions, namely quality, safety, compliance and trust, are translated into actions in the protection and resilience of CI.

These elements break down into 5 areas:

### 1. Adequate legislation

It is crucial that legislation includes high quality criteria for the PSCs protecting CI. In its previous CIP White Paper, published in 2016, CoESS called for a revision of Directive 2008/114 and asked for:

- Enforcing best value procurement practices when hiring security services
- Using Standards as criteria for potential PSCs protecting CI

In 2018, CoESS was invited to contribute to the Report of the European Parliament's Special Committee on Terrorism<sup>5</sup>. The Rapporteur took over the points made by CoESS:

- It promotes quality certification of security services in CIP (Recommendation 175).
- It recommends enforcing specific quality criteria for the procurement of security services in CIP (Recital DW).

Meanwhile, CoESS became more active than ever before in European Standardisation and led the set up and development of a Standards System for PSCs protecting CIP (see Chapter V for more details and useful links).

A few years ago, in a time where CI were particularly exposed to terrorist attacks, the Commission started working on a revision of the EU Directive 2008/114 on European Critical Infrastructure. CoESS was an active contributor and commentator at every stage of the decision-making process and, at the end of 2022, the CER

<sup>3</sup> <https://www.securebestvalue.org/>

<sup>4</sup> <https://www.coess.org/newsroom.php?page=white-papers>

<sup>5</sup> [https://www.europarl.europa.eu/doceo/document/TA-8-2018-0512\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-8-2018-0512_EN.html)

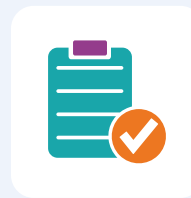
Directive was adopted by the EU Council and Parliament. While the Directive's transposition deadline was 17 October 2024, at the time of writing this White Paper (mid-April 2025), only 10 Member States have published the corresponding legislative texts.

The Directive is a huge improvement in comparison with the “old” CIP Directive (2008/114). It is the first EU legal instrument that recommends to operators of so-called “Critical Entities” quality control of private security services, including with the help of existing Standards.

## 2. Good procurement practices

Best value practices and quality have been at the heart of the CoESS activities since its inception in 1989. While it may seem self-evident, security procurement for Critical Infrastructure is still too often driven by cost considerations rather than quality—even among public sector buyers. This approach is never acceptable, especially given that the threat of terrorist attacks has remained high for over a decade. With the added risks of sabotage, espionage, and cyberattacks—particularly in the context of the War in Ukraine—it is even more incomprehensible. Our goal is to equip CI operators with the necessary guidance to procure high-quality security services, ensuring that responsible and credible providers are selected over those prioritizing cost-cutting measures. In 2014, together with its Social Partner UNI Europa, CoESS led an EU-funded project (DG EMPL), which resulted in the publication in 15 languages of a hands-on manual entitled “Buying Quality Private Security Services<sup>6</sup>”. The guide was published shortly after the publication of the Public Procurement Directive and includes practical advice on selection and awarding criteria, as well as what should constitute exclusion criteria.

<sup>6</sup> <https://www.securebestvalue.org/>



## 3. The use of Standards

Private security services are regulated at the national level, as the EU has no direct competence in this area. However, standards play a crucial role in complementing and addressing gaps in national legislation. They are based on common sense practices and experience acquired between CI operators and security contractors. For Critical Infrastructure Protection, and with the new Directive, the reference to standards is particularly useful, in particular to determine the criteria that private security companies should meet in order to be selected for CIP. With this objective in mind, CoESS was at the basis of setting up a dedicated CEN Technical Committee, TC 439, to deal with “Private Security Services”. Established in 2015, the TC has been producing the 3 first standards of a series, defining the general requirements (EN 17483-1:2021) and specific ones for Aviation Security (EN 17483-2:2023) and Maritime and Port Security (EN 17483-3:2023). Work is currently progressing on defining the requirements for Energy infrastructure. Future areas of focus will include water distribution, healthcare infrastructure, and other sectors identified as requiring enhanced protection.

Ideally, the national transposition of the CER Directive would mention the use of standards to protect Critical Entities and, even better, mention the standard series EN 17483 and require that companies that are selected be certified to the relevant standards. This would mean, for example, that a company working in airport environments would have to be certified to both EN 17483-1 and EN 17483-2.

The contents of the standards are presented in more detail in Chapter V.

**“Security procurement for Critical Infrastructure is still too often driven by cost considerations rather than quality”**

## 4. Public-Private Partnerships

The protection of CI may be subject to partnerships between private and public players. In its latest White Paper on “Public-Private Partnerships: Unlocking the Potential of Enhanced Security”<sup>7</sup>, CoESS draws recommendations and guidelines from PPP best practices in several countries.

*Below is a summary of the recommendations made to the main PPP stakeholders*



Specific best practices in several CI sectors are analysed more in detail in Chapter VI.

## 5. Capacity building

In several areas, CoESS has contributed to training curricula, such as:

- A Training manual for security staff in Maritime and Port Security<sup>8</sup>, implementing the ISPS code in concrete terms.
- CoESS coordinated an EU-funded project with Securitas and DHL on the Insider Threat, which led to the set-up of an e-learning platform called Help2Protect<sup>9</sup> (now a commercial enterprise).

<sup>7</sup> <https://www.coess.org/newsroom.php?page=white-papers>

<sup>8</sup> <https://www.coess.org/newsroom.php?page=white-papers>

<sup>9</sup> <https://www.help2protect.info/>

## Chapter II

# Defining Critical Infrastructure



Definitions and categories of Critical Infrastructure (CI) vary across countries, with some distinguishing between *critical* and *sensitive* infrastructure. Additionally, certain activities, though not critical on their own, can significantly impact the functioning of CI. In today's interconnected and complex world, these interdependencies must be taken into account when defining what constitutes Critical Infrastructure.

In the Directive on Critical Entities Resilience, the EU leaves to the Member States the mission of identifying its Critical Entities on the following criteria:

- The entity provides one or more essential services;
- The entity operates, and its critical infrastructure is located, on the territory of that Member State; and
- An incident would have significant disruptive effects, as determined in accordance with article 7 (1) on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services.

The Directive lists disruptive effects, including among others:

- The number of users affected;
- The effect on sectors and subsectors;
- The impact (in degree and duration) on economic and societal activities, the environment, public safety and security, or the health of the population;
- The affected entity's market share in the market concerned;
- The geographical area affected;
- The availability of alternative means for the provision of the essential service affected.

The CER Directive lists the sectors, subsectors and categories of entities in its Annex<sup>10</sup>. The 11 sectors are:

1. Energy
2. Transport
3. Banking
4. Financial Market Infrastructure
5. Health
6. Drinking Water
7. Wastewater
8. Digital Infrastructure
9. Public administration
10. Space
11. Production, processing and distribution of food


<sup>10</sup><https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557>



Interestingly, the chemical sector is not part of the list, while it is considered CI in several Member States. The nuclear sector being addressed in separate EU legislation, it is excluded from the scope of the EU Directive. Nevertheless, in many European countries,

the internal security of nuclear power plants is ensured by PSCs working in close collaboration with government security forces, which are responsible for external security and response in the event of an incident or an attack.





## Chapter III

# Analyzing the New EU Framework for Critical Entities Resilience

### EU Legislation on Critical Infrastructure Protection

The European Commission has in the past years proposed a whole package of EU legislation aiming at better protecting Critical Infrastructure and the European economy at large. The mere activity at EU level shows the importance of the matter, because the primary responsibility for ensuring the protection of Critical Infrastructure usually rests with the Member States. But obvious vulnerabilities of supply chains and Critical Infrastructure, as well as impacts on the European internal market, which became evident in the past years, made increased coordination at EU level important.

The EU legislation's main texts are the EU Directive on the Resilience of Critical Entities (CER) and the EU Directive on measures for a high common level of cybersecurity across the Union (NIS2), forcing Member States to put in place legislation that ensures respectively a better physical (CER) and cyber (NIS2) protection of Critical Infrastructure. Both have been adopted in December 2022

and had to be transposed into national law by October 2024. As indicated previously, at the time of writing this White Paper, only 10 Member States have done so.

In this chapter we take a particular look at the CER Directive and its relevance for the security services industry.

In addition to CER and NIS, the EU has also adopted in October 2024 the Cyber Resilience Act, which sets in place strict cybersecurity requirements for providers of connected products.

The EU Artificial Intelligence Act, adopted in May 2024, establishes a common regulatory and legal framework for AI and puts emphasis on cyber resilience.

#### The EU Directive on the Resilience of Critical Entities: An important milestone

The CER Directive, which was adopted in December 2022, must be seen in the context of the COVID-19 pandemic and Russia's war against Ukraine which laid bare the vulnerability of essential supply chains and Critical Infrastructure. As the war in Ukraine persists, the threat to Europe's Critical Infrastructure from physical and cyber-attacks continues to escalate, particularly from nation-state proxies. Incidents such as the Nord Stream pipeline sabotage and repeated attacks on underwater infrastructure underscore the vulnerability of essential services and the risk of significant cross-border disruptions, posing serious consequences for EU citizens, economies, and national security.

This growing threat landscape has also been acknowledged, as is shown by the adoption by the Council of a Recommendation on a Union-wide coordinated approach to strengthen the resilience of

Critical Infrastructure, which accompanied the CER Directive, explicitly recognizing these risks. In the Recommendation, national governments affirm the urgent need for action as follows:

“It is in the interests of all Member States and the Union as a whole to clearly identify and protect relevant critical infrastructure that provides essential services within that market. (...) In view of the fast-evolving threat landscape, resilience-enhancing measures should be taken as a matter of priority in key sectors (...) Member States should (...) use all available tools to move forward and help strengthen physical and cyber resilience. (...) Member States are invited to accelerate preparatory work for the transposition and application of the new legal framework applicable to critical entities and of the reinforced legal framework for cybersecurity.”

This is where the CER Directive comes in. At its core, the Directive establishes a process for EU Member States to identify “critical entities” in 11 sectors. These entities must then take appropriate and proportionate technical, security and organizational measures to ensure their resilience to physical threats, according to Article 13 of the Directive – for example by using standards, according to Article 16.

In Recital 34, the CER Directive recommends that there might be situations in which it is appropriate to require compliance with specific Standards, and that Member States should encourage the use of European and international Standards relevant to the security and resilience measures outlined in Article 13.

### Relevance of the CER Directive for the security services industry

The Directive goes on to recommend what such measures should look like in concrete terms – and this is where things get extremely interesting for the security services industry.

After all, security companies and security personnel are an integral part of Critical Infrastructure Protection and corresponding measures in many countries. Especially when it comes to protecting Critical Infrastructure, security services must meet the highest quality standards. However, this is often not reflected in the procurement practices of operators – a problem that CoESS, together with its Social Partner UNI Europa, have been pointing out for years. It should be self-evident, for example, that authorities and operators only use security companies with sufficiently trained, equipped and qualified security personnel to protect these facilities, which are important for the functioning of our societies and economies.

The CER Directive that has now been adopted addresses precisely this issue: It is the first EU law to recommend quality control of personnel protecting Critical Infrastructure, including external service providers, using standards. In concrete terms, this means that the aforementioned Article 13 recommends operators to control the quality of, for example, security service providers and their personnel on the basis of existing industry standards such as the EN 17483 Standard system, on Private Security Services Protecting Critical Infrastructure, in particular EN17483-1:2021 (Private Security Services – CIP – General requirements), EN17483-2:2023 (Private Security Services – CIP – Aviation Security) and EN17483-3:2023 (Private Security Services – CIP – Maritime and Port Security).

On the one hand, these provisions in the Directive respond to demands made by the EU Parliament in 2018 for a revision of the EU Directive on the Identification of European Infrastructures (which has now been done with the CER Directive) and specific quality criteria for the procurement of security services for Critical Infrastructure Protection. On the other hand, the Directive ties in with two initiatives of the European Private Security Services industry:

- In the wake of the 2014 EU Public Procurement Directive, CoESS, together with our Social Partner UNI Europa and with the help of EU funding, has developed a guide for procurement procedures based on the “best value principle” (“Purchasing Quality Private Security Services” available in 15 languages at [www.securebestvalue.org](http://www.securebestvalue.org)).
- For years, CoESS has been actively involved in the development of European standards for the security industry, including the Terminology standard EN 15602:2021, and the above-mentioned standards on Private Security Services protecting CI.

### Next steps: Transposition at national level by October 2024

Member States should have transposed the requirements and recommendations of the CER Directive by October 2024 through national law. While this major legislative exercise is still in progress, they will need to reflect these recommendations in their national legislation, and introduce more stringent requirements. Policymakers should therefore ensure the implementation of the text in line with the adopted version and enforce quality control of security service providers protecting Critical Infrastructure in an efficient, and legally binding way based on existing standards.

## Chapter IV

# Threats and Vulnerabilities and Avenues for Thought



### General context

As stated in the 2024 EUROPOL TE-SAT<sup>11</sup>, which is the reference on major developments and trends in the terrorism landscape in the EU in 2023, terrorism continued to pose a serious threat to EU Member States. Detailed figures are published in the report: in 2023, a total of 120 terrorist attacks (98 completed, 9 failed and 13 foiled) were carried out in 7 EU Member States, an increase compared to previous years. The highest number of terrorist attacks were perpetrated by left-wing and anarchist actors (32, of which 23 completed). There were 14 Jihadist terrorist attacks of which 5 completed. Two right-wing terrorist attacks were foiled. Jihadist terrorist attacks were the most lethal – resulting in six victims killed and twelve injured.

Over the same period, 426 individuals were arrested by EU Member States' law enforcement authorities for terrorism-related offences (compared to 380 in 2022).

Although the specific figures for terrorist attacks in Europe for the entirety of 2024 are not available, several attacks occurred in the past year, including:

- **March 2024:** A major Islamist attack in Moscow, Russia, killed at least 144 people and injured nearly 550.
- **June 2024:** Another Islamist attack in Dagestan, Russia, resulted in around 20 deaths and 40 injuries.
- **August 2024:** A suspected member of the Islamic State (IS/ISIS) carried out an attack in Solingen, Germany, killing 3 people and injuring 8.
- **September 2024:** A Syrian national drove his van into a shop and threatened people with a knife and machete, injuring 31 people, several of them children, in Essen, Germany. There is no credible evidence or official statement linking the perpetrator to terrorist organizations or Islamist extremism in this case.

Several planned attacks were thwarted by authorities, including:

- A plot against the 2024 Olympics and Paralympics in Paris.
- A planned attack on a Taylor Swift concert in Vienna, Austria.

<sup>11</sup> <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat>

- An intended attack on the Israeli embassy in Germany.

France remained the European country most affected by Islamist terrorism, with 85 attacks committed on its soil between 1979 and April 2024<sup>12</sup>.

The use of artificial intelligence and other technological innovations by terrorists and violent extremists increased in 2023, a trend likely continuing into 2024<sup>13</sup>.

**EUROPOL** identifies several types of terrorism:

- Jihadist terrorism, a key security concern for the EU, as it had the most harmful direct impact on victims in 2023. The jihadist threat comes from foreign terrorist groups, online networks and individual actors.
- The right-wing terrorist lone actors or small groups, often motivated by accelerationist ideas, pose the highest threat. New right-wing violent extremist groups are emerging online and seeking to act in real life.
- Left-wing and anarchist terrorist and violent extremist groups continued to coalesce around anti-state, anti-capitalism, anti-fascism, anti-racism, anti-militarism and climate-related narratives.
- Ethno-nationalist and separatist terrorist groups remain active in the EU, mainly Corsican groups and the PKK.

The following conditions and circumstances make the current climate prone to violent extremism and terrorism:

- A world that is uncertain and volatile;
- A polarizing context resulting from the Israël – Hamas conflict;
- An increasing number of young adults and minors being involved in planning attacks or producing propaganda;
- The capabilities offered by the digital world;
- The availability of online training material and instruction manuals for all types of means and equipment (3-D weapons, bombs, drones, chemical weapons).

## The evolving threat against Critical Infrastructure

- As highlighted by the Centre for European Reform in its paper “Protecting Europe’s critical infrastructure from Russian hybrid threats<sup>14</sup>” by Helmi Pillai (April 2023), “European policy-makers have become increasingly concerned about Moscow’s use of hybrid attacks and the threat these pose to critical infrastructure. Suspicious incidents, such as the disruption of railways in Germany, the sabotage of communication cables in France and the GPS disturbances in Finland have all increased worries about the dangers posed by Russia’s hybrid attacks. Reports of Russian surveillance of energy infrastructure in Norway, the Netherlands and Belgium have further added to these concerns”.

The likely impact of a disruption of the energy production and transmission would have significant cascading effects throughout Europe and, therefore, it has never been as important and crucial for the good functioning of our democracies to protect Critical Infrastructure and ensure their resilience.

Energy and transport infrastructure are directly targeted by attacks, and therefore require additional attention, as does the healthcare sector. Ultimately, all types of CI are potential targets, because of the consequences on the functioning of states. In particular, “hybrid” or “blended threats” with a cyber and physical component, and potentially an insider facilitating the attack, are worrisome. The use of drones, as shown in Norway, where these were used to fly over an offshore energy platform, has increased. The threat from CBRNe, in particular chemicals, is also on the rise. Finally, CI and those in charge of their protection need to be prepared for increased breaches of perimeter by activists.

**“In particular, “hybrid” or “blended threats” with a cyber and physical component, and potentially an insider facilitating the attack, are worrisome”**

<sup>12</sup> <https://www.fondapol.org/en/study/islamist-terrorist-attacks-in-the-world-1979-2024/>

<sup>13</sup> <https://eucri.eu/news/europol-te-sat-2024/>

<sup>14</sup> <https://www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid>

Attacks against critical infrastructure in Europe increased significantly in 2023-2024, with both cyber and physical threats posing major challenges:

#### Cyber Attacks (sources<sup>15 16</sup>)

- Surge in incidents: Europe became the most impacted region globally, with 4,618 cyberattacks recorded in 2023 of which:
  - ♦ DDoS attacks: 2,525 cases
  - ♦ Ransomware attacks: 1,066 cases
  - ♦ Malware attacks: 44% of global share, highest worldwide
- Targeted sectors:
  - ♦ Finance and energy were hardest hit, representing 37% and 43% of global attack distribution respectively.
  - ♦ Healthcare: Ransomware attacks affected hospitals in Romania, Spain, and Belgium in 2023-2024.
  - ♦ Transportation: Attacks on railways in Baltic countries and Romania; Eurocontrol reported an ongoing cyberattack by pro-Russian hackers in April 2023.
- Geopolitical factors: Baltic States experienced the highest incidence of cyberattacks per population in 2023, likely due to their strategic importance.

#### Physical Attacks (sources<sup>17 18</sup>)

- Nord Stream pipeline sabotage: This incident in October 2023 highlighted vulnerabilities in undersea infrastructure.
- Energy grid: In August 2024, an “ethical hacker” demonstrated the ability to take control of 4 million smart solar arrays across the EU, exposing potential weaknesses in Europe’s energy infrastructure.

#### Trends and Impacts (sources<sup>19 20</sup>)

- Increased frequency: Disruptive cyber-attacks nearly doubled from Q4 2023 to Q1 2024, according to the EU cybersecurity chief.
- Russia-linked attacks: Many disruptive attacks were traced to Russia-backed groups, extending physical aggression into the digital realm.

 in 2023

4,618 cyberattacks



43%



37%



- AI-enabled threats: EU cybersecurity agencies identified AI-powered manipulation as a significant emerging threat.
- Critical sectors at risk: Food production, satellite management, and self-driving vehicles were identified as areas requiring increased cybersecurity attention.

These attacks underscore the urgent need for enhanced protection of critical infrastructure across Europe, with both cyber and physical resilience becoming increasingly crucial for national and regional security.

### The gap between cyber-physical security equation

The blurring of the limits between cybersecurity and physical security is well described in the recent White Paper on Cyber-Physical Security in Critical Infrastructure<sup>21</sup> published jointly by the International Security Ligue (ISL) and CoESS.

The reason why we decided to address this issue is that vulnerabilities exist due to the blurring of cyber and physical security limits. Connected systems underpin much of the critical infrastructure (CI) that keeps nations running, including energy grids, financial services, and more. Isolating cyber and physical systems from one another misses opportunities but also creates

<sup>15</sup> <https://www.diis.dk/en/research/protecting-eus-critical-infrastructure-the-fight-intensifies-in-the-cyber-realm>

<sup>16</sup> <https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en&center=europe>

<sup>17</sup> <https://post.parliament.uk/critical-infrastructure-readiness-resilience-and-security/>

<sup>18</sup> <https://xage.com/blog/cyber-attack-news-2024-attacks-on-critical-infrastructure/>

<sup>19</sup> <https://www.euronews.com/next/2024/05/29/disruptive-attacks-double-in-eu-in-recent-months-cybersecurity-chief-says>

<sup>20</sup> <https://www.diis.dk/en/research/protecting-eus-critical-infrastructure-the-fight-intensifies-in-the-cyber-realm>

<sup>21</sup> <https://www.coess.org/newsroom.php?page=white-papers>

vulnerabilities for malicious players. With the IoT (Internet of Things), billions of sensors, platforms, and devices are interconnected, increasing the potential for harm.

Computers and other technologies are now integrated into the design and function of physical infrastructure, such as “smart grid” technology in energy networks, and automated traffic control in transportation systems. This progress will accelerate with 5G and AI. The separation between computer networks and physical systems is diminishing, resulting in a complex mesh of cyber-physical systems.

Connectivity extends threat surfaces outside secure locations, linking critical operational and physical systems. Extremist groups and activists are exploiting these vulnerabilities, targeting vital CI systems. Real-world examples include the 2017 virus that disrupted global shipping and a 2019 attack that caused a power grid outage. Red Team exercises show how quickly systems can be compromised.

Most CI operators are unsure if they have experienced physical breaches leading to network attacks or vice versa. Often, attackers go undetected for weeks before causing real-world damage. CI operators must adopt a joint physical-cyber security approach for strategic alignment and risk reduction.

A unified framework for physical and cybersecurity coordination is crucial and Corporate Security Directors are naturally called upon to embrace this new organizational vision. Addressing hybrid threats requires breaking down security siloes and improving coordination, thus ensuring better protection for critical infrastructure in a world of interdependent risks.

**“Isolating cyber and physical systems from one another misses opportunities but also creates vulnerabilities for malicious players”**



## The Insider Threat

While the Insider Threat is not specific to Critical Infrastructure, it can be particularly damaging to them and have severe consequences on a whole country and even beyond. An Insider Threat is any individual with inside knowledge or access to an organisation and who thereby has the potential to harm the organisation and its people. Insiders may have malicious intent, but they can also contribute to threats by negligence or accident.

Insiders may therefore be existing or former employees, but also consultants, temporary workers, sub-contractors, etc. It is important to note that over 2/3 of Insider incidents are caused by accidents or negligence (cutting corners with security rules). A small proportion of incidents are caused by malicious Insiders but can have highly damaging consequences, in many different forms, affecting people and the organisation.

Insider incidents include all types of acts and behaviours that are in breach of rules, regulations and/or the law. They include physical and cyber incidents, among others theft, fraud, sabotage, activism, workplace violence, organised crime, terrorism.

Insider Threats are not new, but they are increasing. According to the Ponemon 2022 report<sup>22</sup> on the matter, “Insider Threats have increased in both frequency and cost over the past two years. Credential thefts, for example, have almost doubled in number since 2020. However despite insider threats having increased across all three insider threat profiles, those caused by careless or negligent employees are the most prevalent. According to the findings, 56% of incidents experienced by organizations represented in this research were due to negligence, and the average annual cost to remediate the incident was \$6.6million.”

<sup>22</sup><https://static.poder360.com.br/2022/01/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf>

This upward trend is reinforced by several factors:

- The rise of teleworking: it is more difficult to prevent Insider Threats when people are in remote locations. It is also more difficult to create cohesion within teams, and this has an impact on security culture.
- As previously mentioned, the blurring frontier between physical and cyber objects creates vulnerabilities, which can be used by malicious insiders and by people who will seek to use employee's credentials. Credential theft accounts for 18% of all Insider incidents, according to the above-mentioned Ponemon 2022 report on the Insider threat.
- The war in Ukraine has increased the number of sabotage incidents and attempts, as well as espionage, mainly on transport and energy infrastructure but the health sector and hospitals are also being targeted. Ultimately, all types of Critical Infrastructure may be targeted and need to strengthen their level of protection against both outsiders and insiders.
- More recently, the Israël-Hamas war has had a polarizing effect, which may trigger malicious attacks, such as sabotage or workplace violence.

**“Meanwhile, only one third of companies report that they have robust Insider Threat programmes in place, even though over 70% of them recognize that this is a major source of concern”**

Meanwhile, only one third of companies report that they have robust Insider Threat detection and prevention programmes in place, even though over 70% of them recognize that this is a major source of concern. Legislation does not oblige organisations to have Insider Threat policies in place, except EU legislation on aviation security. The latest CER Directive only creates obligations regarding the background checks, which is of course an important element in Insider Threats, but certainly not the only one and far from being the panacea. It has no impact on negligent and accidental cases, which are the majority of incidents.



## Drones

Unmanned Aerial Systems (UAS), as they are referred to by European Legislation, or drones, have already been used in other regions of the world to commit attacks with explosives. But they are also used to disturb the functioning of Critical Infrastructure, to transport prohibited goods such as drugs, or even carry out hostile surveillance and reconnaissance, as recent incidents show:

- **Challenge to aviation:** Traffic at European airports, but also worldwide, has repeatedly been disrupted by drones, leading to severe costs and posing already a real threat to safety and security of civil aviation.
- **Threats to maritime infrastructure:** European ports see a drastic increase of drug traffic and organised crime, for which also drones can be used. Also, offshore platforms are sensitive infrastructure subject to drone threats and espionage, as witnessed in 2022 in Norway where numerous drone sightings were reported near offshore oil and gas platforms and other infrastructure. There are also Unmanned Maritime Systems, which can be a threat to ships and ports and used to carry out illegal activities. For over a decade, Explosive Unmanned Surface Vessels (e-USVs) have been used by the Houthis (Yemen) to target ships in the Gulf of Aden and other objects in Saudi Arabia.
- **Attacks on energy infrastructure:** not only since the war against Ukraine, European energy infrastructure, including pipelines and solar panel facilities, are a high potential target of attacks – as showcased with the sabotage of the Nord Stream Pipeline in 2022. Such attacks can also be conducted with the help of unmanned vehicles, air-, land- and sea-borne.
- **Espionage of other Critical Infrastructure and military sites:** drones can be used for cyber and physical attacks, but also espionage on Critical Infrastructure and military sites. For example, drones were sighted last year over multiple Swedish nuclear plants, or over military training camps for Ukrainian soldiers in Germany.

What is particularly worrying is that, when a UAS is detected in a place where it should not be flying, time is of the essence to verify its identity, if it is a threat and, if so, in what way, and, finally, counter it safely and securely. At present, there is no uniform approach across the EU Member States on how or who is capable and legally allowed to carry out anything beyond the mere detection of a drone around Critical Infrastructure. Anything that goes further than “passive” radio frequency detection, including verification of the identity of the drone, localisation of the pilot or even taking over the drone, is in many countries legally not possible for private stakeholders, but only for law enforcement agencies.

In a situation where response time is key to prevent an incident at Critical Infrastructure with potentially disastrous consequences, the absence of legal certainty, rapidly available C-UAS capabilities as well as clear procedures, roles and responsibilities in C-UAS is currently a real challenge. CoESS therefore believes that a legal basis is required to enforce no-fly zones and to better protect Critical Infrastructure in Europe from unknown drones.

**“What is particularly worrying is that, when a UAS is detected in a place where it should not be flying, time is of the essence to verify if it is a threat and, if so, counter it safely and securely”**



## CBRNe

The acronym ‘CBRN’ defines chemical, biological, radiological and nuclear materials and agents that could potentially harm the society through their accidental or deliberate release, dissemination, or impacts. The letter “e” stands for explosives.

The use of IEDs (improvised explosive devices) and IIDs (improvised incendiary devices) and fire accelerators is frequent in terrorist attacks. The Europol report TE-SAT 2023 indicates that these were more prominent in the right-wing and left-wing terrorist and violent extremist circles, while bladed weapons were mainly used in the jihadist context. Firearms featured both in right-wing and jihadist foiled attacks. While Aviation is at the forefront of using equipment to detect such products, other types of CI do not necessarily and systematically seek to detect them. It is worth noting that terrorists and violent extremists continue to disseminate online manuals and tutorials for the manufacture of homemade explosives (HMEs) and IEDs. The report further highlights that terrorists and violent extremists remain apt in evading restrictive measures and monitoring related to explosive precursors in the EU. For instance, a pro-IS group released a document on a cloud-based instant messaging platform, suggesting the use of alternative precursors for HMEs, to circumvent the controls on precursors without raising suspicion.

The Europol report TE-SAT 2023 indicates that no terrorist attacks were perpetrated with CBRN materials in 2022. However, online propaganda concerning the recourse to such materials is available and shows the interest for these products among extremists and terrorists across the ideological spectrum. TE-SAT mentions one example of online right-wing extremist magazine that published an article on a do-it-yourself (DIY) method to produce a radiological dispersal device, also known as “dirty bomb”, by combining explosives and nuclear material. Such material could be smuggled into the EU from the Russian/Ukraine war zone.

The United Nations Investigative Team to Promote Accountability for Crimes Committed by Da’esh/Islamic State in Iraq and the Levant (UNITAD) reported evidence of ISIL using and testing biological and chemical agents on prisoners, and some of these products having been deployed against civilian populations between 2014 and 2016.<sup>23</sup> The potential risk of chemicals and biological agents needs to be considered.

<sup>23</sup>[https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s\\_2021\\_419.pdf](https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_419.pdf)

## Environmental Extremism and Activism

According to Europol’s TE-SAT, there has been an increase in environmental activism in the EU. Environmental extremism is not new and has seen varying levels of activity over the past decades. In 2022, many actions by environmental activists caused damage to public and private property and disrupted public order. Notable incidents included activists damaging artworks in museums by throwing liquids on them and gluing themselves to different locations. Several critical infrastructures, such as energy companies, public institutions, and airports, were impacted by the occupation of environmental activists.

**“In 2022, several critical infrastructures, such as energy companies, public institutions, and airports, were impacted by the occupation of environmental activists”**

The actors and groups within this movement are connected at a global level, and the TE-SAT indicates that there is an overlap with other extremism phenomena, predominantly with left-wing and anarchist extremists. Additionally, there is a connection with animal rights activists and extremists, which impacts meat and dairy production and distribution centres. Some Member States are concerned that certain groups may become further radicalized and potentially engage in acts of violence and terrorism.

Critical infrastructure in various sectors, including transportation, energy production and transmission, chemical plants, and government buildings and agencies, may be potential targets for activist activities.

## Disinformation, Digital Propaganda and Geopolitical Influence Operations

In an age where perception is weaponised, disinformation and fake news campaigns represent a potent and under-recognised threat to Critical

Infrastructure (CI). By undermining trust in institutions, destabilising democratic consensus, and amplifying extremist narratives, such campaigns erode the very governance structures upon which infrastructure security depends.

A prominent example is the Russian “DoppelGänger” campaign<sup>24</sup>, which used AI-generated content and cloned news websites—including cloned versions of *The Guardian* and *Bild*—to spread pro-Russian narratives, destabilize European unity, and manipulate perceptions of the Ukraine conflict. These tactics aim not only to influence public opinion, but to fragment societal cohesion, weaken support for resilience measures, and delegitimise government and EU-level actions related to CIP.

The scale of these operations is staggering. Investigations in 2024 uncovered over 500 interconnected fake news websites, often linked to the so-called “Portal Kombat” network, which targeted countries such as Germany, Poland, and Ukraine. These sites repackage Kremlin-state media content (e.g., RT, TASS) and support their reach through bot-driven amplification across Telegram, Facebook, and other platforms. Forged documents—including fake diplomatic correspondence—have been disseminated to lend credibility to fabricated claims, further muddying the information environment<sup>25</sup>.

The impact is measurable: 70% of EU citizens encounter fake news weekly, and 80% consider it a threat to democracy. False news spreads significantly faster than factual news, particularly on social media. In such an environment, public support for security interventions, PPPs, and investment in resilience can be distorted or delayed by deliberate digital manipulation.

## Strategic Dependencies and Digital Sovereignty: Risks of Overreliance on U.S. Platforms

A further strategic concern lies in Europe’s dependency on foreign-owned IT infrastructure, particularly U.S.-based cloud platforms such as AWS, Google Cloud, and Microsoft Azure. Over 90% of European governments rely on these services, despite the legal implications of the U.S. CLOUD Act, which allows American authorities to access data stored on foreign soil. This raises substantial sovereignty and privacy concerns—especially in scenarios where transatlantic political alignment weakens.<sup>26 27</sup>

<sup>24</sup> <https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelganger-unmasked-a-web-of-deception/>

<sup>25</sup> [https://www.lemonde.fr/en/pixels/article/2024/02/12/france-uncovers-vast-network-of-russian-disinformation-sites\\_6518362\\_13.html](https://www.lemonde.fr/en/pixels/article/2024/02/12/france-uncovers-vast-network-of-russian-disinformation-sites_6518362_13.html)

<sup>26</sup> <https://dev.ua/en/news/v-ievropi-podumuiut-vidmovytsia-vid-amerykanskoj-khmary-1742907334/>

<sup>27</sup> <https://www.euronews.com/next/2025/02/27/is-overreliance-on-us-big-tech-a-threat-to-europe-the-netherlands-may-soon-find-out>

The 2025 removal of over 8,000 U.S. government webpages (including public health and environmental datasets) under Trump-era executive orders illustrated how political shifts can have sudden and disruptive impacts on digital continuity. Such actions affected global access to CDC data, climate modelling tools, and pandemic preparedness resources—vital for infrastructure planning.<sup>28</sup>

A scenario in which a future U.S. administration imposes restrictions on the export or operation of these platforms in Europe, or prioritises domestic access under an “America First” policy, would have significant implications for CI operators, public services, and cyber resilience. This possibility underscores the urgency of investing in European-based alternatives, and bolstering regulatory and contingency frameworks.

Notably, initiatives such as GAIA-X<sup>29</sup>—a decentralised, EU-funded sovereign cloud infrastructure—have gained momentum as part of efforts to reduce strategic dependencies and ensure operational continuity in times of geopolitical uncertainty.

## The threat in the future

The TE-SAT 2023 and 2024 reports give an outlook on potential developments in terrorism and violent extremism in the EU, as follows:

- Thinning delineations between different types of terrorism and convergence between groups that share topics of common interest, as well as targets and tactics.
- Right-wing, left-wing and environmentally inspired terrorism and violent extremism are expected to gain further prominence. As indicated above, the convergence of several groups with similar agendas is already taking place, as is the infiltration by violent extremists in protests.
- Geo-political developments outside the EU: terrorists will continue to “import” or use issues taking place in other geographical areas to fuel their narratives. The Russian war of aggression against Ukraine is already being used and will continue to be used to polarize opinions. The Hamas terrorist attack and Israeli military response highlighted several lines of convergence between supporters and sympathisers of the jihadist, right-wing and left-wing and anarchist terrorism and violent extremism scenes.

→ As in past conflicts, the war is used as an opportunity to divert weapons and explosives outside battlefields by firearms traffickers.

→ The online environment is used as a channel for terrorist propaganda and different trends can be observed: a widening of themes that are used to build terrorist narratives and thus of the potential supporters and recruits. Emerging technologies or ecosystems, such as the metaverse, might be used to disseminate propaganda, recruit supporters, plan, or coordinate actions. The use of drones and other types of unmanned devices would allow terrorists to perpetrate attacks remotely, as well as in combination with various weapons, potentially including radioactive or biological material. The Internet of Things (IoT) and artificial intelligence (AI), including the use of deep fakes, augmented reality and conversational AI also offer opportunities to commit attacks. These new technologies can be used to reach a wider audience more quickly, expand the narrative and train people virtually, fund terrorism via digital currencies and the trade of NFTs.

→ Lone (but not unconnected) actors are expected to perpetrate most of the terrorist attacks in the EU, as the online content is widely available and thus more vulnerable individuals are exposed to radical content and ideas.

→ In 2023, young adults and minors were increasingly involved in planning attacks, producing terrorist propaganda, and inciting violence—a concerning trend across all ideological spectrums, highlighting their vulnerability to exploitation by terrorists. Many of those arrested were connected through online platforms, sharing propaganda, training materials, and resources to facilitate attacks. These (self)-radicalised individuals often acted independently of formal groups but were embedded in virtual communities fostering extremism.



<sup>28</sup> <https://fedscoop.com/cdc-data-site-goes-dark-as-agency-complies-with-trump-gender-ideology-order/>

<sup>29</sup> <https://gaia-x.eu/>

# Chapter V

## The Role and Objectives of Standards: the EN 17483 Standard System



In the complex landscape of Critical Infrastructure Protection (CIP), bridging the gap between legislation and operational needs and realities is essential for ensuring both compliance and effectiveness. **Standards serve as a vital tool in this regard, offering clear, measurable benchmarks for operational quality.** While most standards are voluntary, they become essential when driven by client expectations and regulatory incentives.

Aligning with established standards not only enhances security outcomes but also helps identify legitimate, professional organisations capable of meeting the specific demands of protecting critical infrastructure.

This is why CoESS has been a strong supporter of combining the CER Directive's recommendation to use standards, with the quality criteria established in CEN standards. Within the CEN Technical Committee (TC) 439 "Private Security Services"<sup>30</sup>, CoESS experts have been working since 2016 on creating a whole "standards system". With this system, CEN establishes the quality criteria for private security companies that protect CI. The first standard, which is the foundation of the system is EN 17483-1:2021 "Private Security

Services – Critical Infrastructure Protection – General Requirements"<sup>31</sup>. It covers the criteria for the provider, contracts, staff, and service delivery. The next standards will cover, one by one, all sectors of CI that require it, starting with the adopted standards EN17483-2:2023 for Aviation and Airports, EN17483-3:2023 for Maritime and Ports Security and the future EN17483-4 for Energy Production and Transmission.

Companies wishing to deliver security services, for example in an Airport, will have to be compliant (or better still, certified) to both the General Requirements EN 17483-1 and the aviation-specific standard EN 17483-2. The sector-specific standards mainly cover training requirements and quality control.

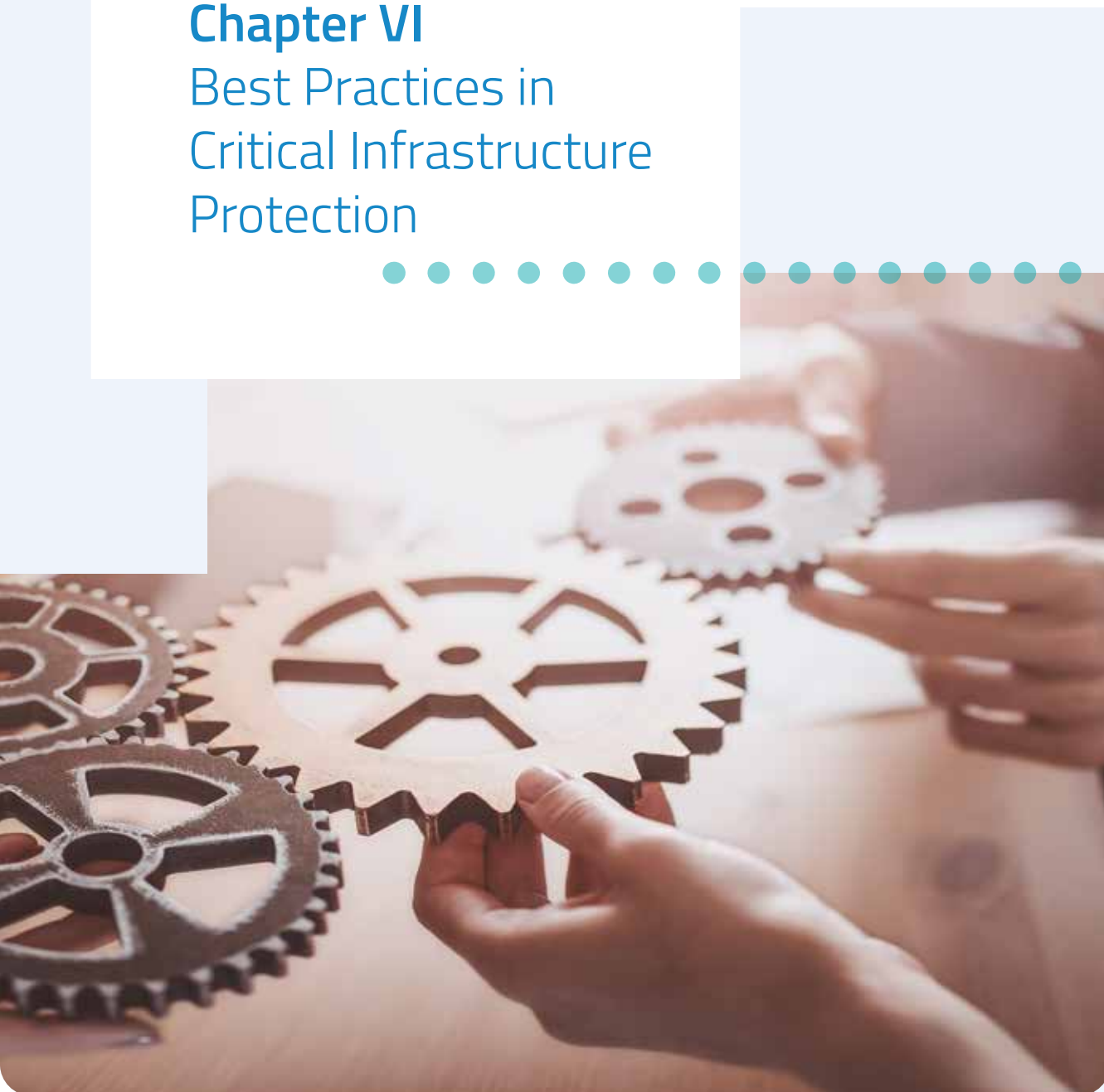
CoESS recommends therefore that Operators of Critical Infrastructure select companies that comply with the objective and measurable criteria set out in the standards, as this gives a certain level of trust that they operate in an efficient and effective manner. In today's context, with the threats listed above, CI Operators and Owners would take a significant risk if they were selecting companies based on the lowest price with no consideration for quality.

<sup>30</sup> [https://standards.cencenelec.eu/dyn/www/f?p=205:7:0:::FSP\\_ORG\\_ID:1969247&cs=1C2C0D4C4CB14B5549C367FB7A2F697EA](https://standards.cencenelec.eu/dyn/www/f?p=205:7:0:::FSP_ORG_ID:1969247&cs=1C2C0D4C4CB14B5549C367FB7A2F697EA)

<sup>31</sup> [https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP\\_PROJECT:66899&cs=145C45D445C53F6244FF0A6692EB6E984](https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:66899&cs=145C45D445C53F6244FF0A6692EB6E984)

## Chapter VI

### Best Practices in Critical Infrastructure Protection



**This section is based on deep-dive interviews and visits to Critical Infrastructure across Europe. In agreement with the CI Operators, the name of the company and country are not mentioned.**



## I. Joint Training Against Infiltration in a Seaport

### 1. Context and Security Challenges

This case study focuses on a major European seaport, a vital hub for international trade and logistics. Like many large ports, this facility faces significant security challenges, with **drug trafficking** emerging as a primary concern. Organized criminal groups often target ports for smuggling operations and attempt to infiltrate various stakeholders, including **Private Security Companies (PSCs)**, which are key players in securing port infrastructure.

Port employees and security personnel are susceptible to manipulation or coercion by criminal networks. To address this issue, a **Public-Private Partnership (PPP)** was initiated, aimed at strengthening cooperation between law enforcement and private security providers. The goal was to enhance awareness of infiltration risks, develop preventive strategies, and improve response capabilities.

### 2. Stakeholders Involved

The initiative was built on close collaboration between public authorities and private sector actors:

#### → Public Actors:

- ✓ Specialized **law enforcement units** focused on drug trafficking within ports.
- ✓ A dedicated police team addressing **human trafficking**.

#### → Private Actors:

- ✓ A **Private Security Company (PSC)** tasked with securing port infrastructure.

This partnership fostered a collaborative environment where roles and responsibilities were clearly defined, encouraging seamless cooperation.

### 3. Security Measures and Initiatives

To counter infiltration risks effectively, a **joint training program** was developed by law enforcement in collaboration with the PSC. The training aimed to raise awareness among security personnel of the methods used by criminal organizations, delivering a strong message: **“If you get involved with criminals, there is no way back.”** The training included real-life examples illustrating how criminal networks target individuals’ vulnerabilities, including the exploitation of family connections.

In addition to drug trafficking, the training covered **human trafficking** threats, drawing on the expertise of specialized police units. While law enforcement developed the training content, delivery was handled by a PSC trainer with a background in policing, fostering peer-to-peer trust and enhancing the program’s effectiveness.

The initiative also incorporated practical tools to support learning and response capabilities:

- A **PowerPoint presentation** featuring **QR codes** that link to specific response procedures for various security incidents.

# SEAPORT

- A dedicated **hotline** allowing PSC staff to report suspicious activities directly to law enforcement.
- **Anonymous reporting channels**, encouraging security personnel to share information without fear of retaliation.

This combination of training, practical resources, and enhanced communication channels established a comprehensive framework for reinforcing security measures at the port.

## 4. Operational Impact

The partnership between law enforcement and private security significantly improved operational effectiveness, particularly in communication, information-sharing, and fostering mutual trust. Notable impacts include:

- **Improved Information Flow:**
  - ✓ Law enforcement authorities now actively seek intelligence from PSC personnel, resulting in a more dynamic and responsive exchange of information.
- **Strengthened Mutual Trust:**
  - ✓ Regular engagement between PSC staff and police officers has built stronger working relationships, leading to better coordination during security operations.
- **Enhanced Security Awareness:**
  - ✓ Private security personnel are now better equipped to recognize and respond to potential infiltration attempts, contributing to a safer operational environment.

These developments represent a significant step forward in securing the port environment and highlight the importance of strong partnerships in countering organized crime.

## KEY LESSONS

This case underscores the importance of proactive collaboration between public and private actors to counter organized crime. The structured partnership enabled a mutual understanding of roles and improved information-sharing, which is vital for early detection of infiltration attempts.

## RECOMMENDATIONS

CI Operators should institutionalize structured partnerships with law enforcement and PSCs to foster trust and facilitate regular information-sharing. PSCs should invest in specialized training focused on infiltration risks, leveraging peer-to-peer approaches to enhance operational effectiveness.



## II. Pharmaceutical Facility: Strengthening Security Through Internal-External Collaboration

### 1. Context and Security Challenges

This case focuses on a major pharmaceutical facility located on the outskirts of a European capital city. The site hosts over 9,000 people daily, including employees, contractors, and visitors. Security threats include **theft of materials, sabotage, and inappropriate behaviour** toward service staff. Ongoing construction projects and the high-value nature of the site increase its vulnerability to both internal and external threats. To mitigate these risks, a **Public-Private Partnership (PPP)** was initiated to strengthen collaboration between the company's internal security team, law enforcement, and a contracted PSC.

### 2. Stakeholders Involved

- **Public Actors:** Local police forces responsible for external coordination and crime prevention.
- **Private Actors:** The pharmaceutical company's security department, a contracted PSC for infrastructure protection, and an internal licensed private detective focusing on internal investigations.

### 3. Security Measures and Initiatives

The company has implemented a comprehensive security strategy combining physical measures, advanced technology, and procedural controls:

- **Access Control:** Includes biometric identification and advanced visitor screening procedures, with strict entry requirements for visitors and subcontractors.
- **Internal Investigations:** Managed by an internal licensed private detective, who works closely with human resources and the PSC to investigate reports of insider threats, ensuring swift action against potential risks.
- **Training Programs:** Specialized courses for PSC staff cover emergency procedures, including responding to potential AMOK situations, and are tailored to the specific operational environment of the pharmaceutical facility.
- **Integrated Security Operations:** A strong collaboration framework ensures PSC personnel feel embedded within the company's internal security ecosystem, contributing to low staff turnover and high operational consistency.

# PHARMACEUTICAL FACILITY

## 4. Operational Impact

- **Enhanced Security Culture:** PSC personnel are well-integrated with the company's security operations, fostering strong collaboration and shared responsibility.
- **Improved Intelligence-Sharing:** Informal exchanges with law enforcement have led to better detection of thefts and suspicious behaviours.
- **Increased Preparedness:** Specialized training ensures that personnel are equipped with the knowledge to handle emergencies effectively.
- **Proactive Risk Mitigation:** Regular assessments and internal audits enhance early detection of potential threats.

### KEY LESSONS

This case highlights the value of integrating internal security teams with external PSCs and law enforcement for a layered security approach. The inclusion of an internal licensed detective illustrates the need for thorough internal threat detection mechanisms.

### RECOMMENDATIONS

CI Operators should implement robust internal threat detection systems, supported by close coordination with PSCs.



### III. Telecom Headquarters: Bridging Physical and Cybersecurity Gaps

#### 1. Context and Security Challenges

This case examines the headquarters of a leading telecom company, responsible for managing service nodes and data centers across 15 critical buildings. The facility faces significant threats, including **insider sabotage, cyber espionage, and activist-driven attacks** related to infrastructure developments like 5G. A strategic **Public-Private Partnership (PPP)** was formed, complemented by a private-private collaboration with the energy sector to coordinate security measures across interconnected infrastructures.

#### 2. Stakeholders Involved

- **Public Actors:** National police and intelligence services, providing threat analysis and security assessments.
- **Private Actors:** The telecom company's internal security department and a contracted PSC overseeing physical security operations.

#### 3. Security Measures and Initiatives

The security framework incorporates integrated technological and operational measures:

- **Centralized Monitoring:** A control room, operated by PSC staff, monitors security across all sites 24/7.
- **Access Control:** Strict monitoring of service nodes and data centers with regular vetting and background checks for personnel.
- **Threat Analysis:** Ongoing collaboration with national intelligence services ensures real-time monitoring and analysis of potential threats.
- **Cybersecurity Integration:** A dedicated internal C-SERT (Cyber-Security Emergency Response Team) works closely with physical security teams to address evolving cyber-physical threats.

# TELECOM HEADQUARTERS

## 4. Operational Impact

- **Improved Threat Detection:** Close cooperation with national authorities has enhanced detection capabilities for both physical and cyber threats.
- **Strengthened Collaboration:** Integrated efforts between PSC personnel and the company's cybersecurity teams ensure comprehensive risk management.
- **Enhanced Surveillance:** The centralized monitoring center improves response times and situational awareness.
- **Proactive Risk Mitigation:** Regular security reviews ensure that emerging threats are swiftly addressed.

### KEY LESSONS

The integration of cyber and physical security operations, coupled with real-time collaboration with national authorities, proved essential for safeguarding sensitive data infrastructure. The proactive approach to hybrid threats through coordinated internal teams is a model for CI protection.

### RECOMMENDATIONS

CI Operators must prioritize the integration of cybersecurity and physical security functions. PSCs should consider enhancing their technological capabilities to support cyber-physical security convergence and regularly engage in joint training with internal cybersecurity teams.



## IV. Airport: Strengthening Security Through Coordinated Partnerships

### 1. Context and Security Challenges

This case study focuses on a large international airport serving as a major transport hub with connections to national and international destinations. The airport faces complex security challenges, including **drug trafficking, human trafficking, theft of valuable cargo, and potential terrorist threats**. A structured **Public-Private Partnership (PPP)** platform was established to foster collaboration between public authorities and private stakeholders, ensuring proactive risk mitigation and effective incident response.

### 2. Stakeholders Involved

- **Public Actors:** Ministries of Transport, Justice, Home Affairs, Customs, Secret Service, Police, and the National Counter Terrorism Authority.
- **Private Actors:** Airport leadership, Airports Association, PSCs, Cargo Association, Airlines, and the Pilots Association.

### 3. Security Measures and Initiatives

The PPP platform was established following a major criminal incident, leading to the implementation of structured collaboration frameworks:

- **Steering Committee:** Meets 2-3 times annually, bringing together high-level decision-makers for strategic discussions.
- **Core Team:** Meets 3-4 times a year to address operational security challenges and coordinate responses.
- **Information-Sharing Channels:** Real-time communication through a dedicated hotline, integrated into the national Critical Infrastructure Protection Plan.
- **Awareness Campaign:** Comprehensive communication strategy encouraging all airport employees to report suspicious activities through various channels, including QR codes and a dedicated security website.

# AIRPORT

## 4. Operational Impact

- **Improved Situational Awareness:** Enhanced coordination has led to faster incident reporting and response.
- **Enhanced Trust:** Regular meetings have fostered strong partnerships among stakeholders, encouraging open communication and collaboration.
- **Broad Staff Engagement:** The awareness campaign has cultivated a proactive security culture across all levels of airport operations.
- **Enhanced Preparedness:** Regular exchanges between stakeholders ensure that both airside and landside threats are effectively monitored and addressed.

### KEY LESSONS

This case demonstrates the power of structured PPP platforms to foster a comprehensive and proactive security culture across diverse stakeholders. Regular communication and awareness campaigns are pivotal for enhancing situational awareness.

### RECOMMENDATIONS

CI Operators should establish regular coordination platforms that involve all relevant public and private actors. PSCs should actively participate in these forums, contributing to awareness campaigns and integrating feedback into operational procedures.



## V. Refinery: Coordinated Security Operations in a High-Risk Industrial Environment

### 1. Context and Security Challenges

This case examines a large refinery located within a major port, exposed to significant security threats due to its proximity to illicit trafficking activities and the handling of hazardous materials. The facility faces challenges such as **contraband smuggling, sabotage, and cybersecurity risks**. Given the complexity of its operations, close coordination between private security, the refinery operator, and law enforcement is essential.

### 2. Stakeholders Involved

- **Public Actors:** Law enforcement and national security agencies responsible for critical infrastructure protection.
- **Private Actors:** Refinery operator and PSC overseeing physical security operations.

### 3. Security Measures and Initiatives

- **Access Control:** A two-layer system with biometric verification, ensuring stringent perimeter security.
- **Centralized Security Management:** A single PSC manages all security functions, including patrols, access control, and control room operations.
- **Risk Assessment:** Regular evaluations of security protocols and emergency preparedness, carried out in partnership with law enforcement and national authorities.

# REFINERY

## 4. Operational Impact

- **Enhanced Coordination:** Effective collaboration between the refinery operator and PSC ensures seamless threat detection and response.
- **Improved Risk Management:** Regular security assessments and joint emergency response exercises enhance preparedness.
- **Integrated Security Framework:** Cyber and physical security measures are increasingly aligned to address modern hybrid threats.
- **Operational Efficiency:** A unified security structure contributes to streamlined processes.

### KEY LESSONS

The refinery's two-layered access control and centralized management highlight the importance of a unified security strategy in high-risk environments. Regular risk assessments and emergency preparedness exercises strengthen overall resilience.

### RECOMMENDATIONS

CI Operators should implement layered access control systems and conduct regular joint risk assessments. PSCs must offer comprehensive security management solutions tailored to high-risk industrial environments.



## VI. Nuclear Power Plant: Managing Complex Security Ecosystems in High-Sensitivity Environments

### 1. Context and Security Challenges

This case involves a **nuclear power plant (NPP)** that operates under strict regulatory oversight due to the sensitive nature of its infrastructure. Key security threats include **terrorist attacks, insider threats, and unauthorized drone activity**. Given the plant's importance to national energy security, a robust collaboration framework between public and private entities was established.

### 2. Stakeholders Involved

- **Public Actors:** Police station within the NPP, local police of the nearby town, National Agency for Nuclear Control, and international bodies like the International Atomic Energy Agency (IAEA).
- **Private Actors:** NPP operator, PSC, and specialized technology providers for anti-drone systems.

### 3. Security Measures and Initiatives

- **Specialized Security Staff:** A team of 100 guards and 15 firefighters with specialized training in nuclear safety and crisis response.
- **Comprehensive Access Control:** Stringent entry requirements, including biometric checks and metal detection for all employees and contractors.
- **Advanced Crisis Response Infrastructure:** Regular joint emergency exercises with law enforcement and dedicated crisis management teams.
- **Anti-Drone Systems:** Advanced detection and mitigation measures to address aerial threats.

# NUCLEAR POWER PLANT

## 4. Operational Impact


- **Enhanced Preparedness:** Regular training exercises improve crisis response capabilities across all security functions.
- **Strengthened Collaboration:** Close cooperation between PSCs, plant operators, and law enforcement fosters an effective security culture.
- **Operational Efficiency:** Comprehensive security measures contribute to increased operational effectiveness and cost savings.
- **Innovative Security Practices:** The NPP implements cutting-edge solutions to address evolving threats, particularly drone-related risks.

### KEY LESSONS

This case illustrates how specialized training and advanced technological measures, such as anti-drone systems, are essential for protecting highly sensitive infrastructure. Regular joint exercises enhance crisis preparedness. The exceptional relation between LEA and PSC, developed over several years, shows how the leadership can influence the attitude of the staff and inspire mutual trust.

### RECOMMENDATIONS

CI Operators should prioritize specialized training for security personnel and invest in advanced detection technologies. PSCs should continue to develop niche expertise in high-sensitivity environments and maintain close coordination with regulatory bodies and law enforcement.



## Chapter VII

# Conclusions and Recommendations from Best Practice

In an era marked by evolving and increasingly complex threats, Critical Infrastructure Operators and Private Security Companies must rise to the challenge by embracing innovation, collaboration, and quality standards. The examples and best practices highlighted in this White Paper demonstrate that true security resilience is built on cooperation, mutual trust, and a proactive mindset.

The legislative advancements, particularly the implementation of the CER Directive and the adoption of CEN standards, provide a solid foundation. Yet, their success hinges on more than formal compliance—it requires a commitment to operational excellence and cross-sector collaboration.

By fostering stronger partnerships, enhancing technological capabilities, and prioritizing quality over cost-driven procurement, both CI Operators and PSCs can build a robust defense framework.

The aim of PPPs is to optimize the effectiveness of the security measures to be implemented, with the number of security guards and security forces adapted to actual needs. The aim is to avoid deploying personnel who are not needed for the missions identified, to eliminate unjustified costs for CI operators and to deprive security forces of personnel needed for other missions. **Only through genuine collaboration, backed by actionable recommendations and a cooperative mindset, can Europe's critical infrastructure be effectively safeguarded against the threats of today—and those yet to come.** Finally, the growing influence of information warfare and strategic digital dependencies calls for new cross-sectoral responses that reinforce trust, resilience, and sovereignty in an interconnected security landscape.



## 1. Common Success Factors

Below are recurring elements that consistently contributed to effective protection across different infrastructures:

- Strong **Public-Private Partnerships (PPPs)**
- Trust-building through continuous engagement
- Comprehensive **training and awareness programs**
- Effective **communication channels** and intelligence-sharing
- Integration of **digital tools** and technological innovations

## 2. Key Challenges & Gaps

These were the most prevalent obstacles observed across all cases:

- Lack of joint exercises and drills
- Time and resource constraints for training
- Fragmented coordination between physical and cybersecurity functions
- Regulatory and legal barriers (e.g., GDPR limitations on background checks and use of biometric access control technology)

## 3. Policy and Strategic Recommendations

### European Legislator

- Revise the Public Procurement Legislation to guarantee bidders' compliance with Collective Agreements (where they exist) and to provide legal certainty for procurement authorities on the use of awarding criteria related to qualitative working conditions, adequate training, and innovative services.
- Re-affirm the risk-based approach as the guiding principle in the interpretation and application of the General Data Protection Regulation (GDPR), e.g. through a targeted European Commission evaluation of Articles' 6, 9 and 23 interpretations in national law and a constructive dialogue between the regulator, data protection authorities, and the industry.
- Produce guidelines and recommendations for PPPs drawing from the best practice described in the White Paper.

# “Only through genuine collaboration, backed by actionable recommendations and a cooperative mindset, can Europe’s critical infrastructure be effectively safeguarded against the threats of today—and those yet to come”

## National Legislators

- **Review Legislation:** Examine existing laws to ensure they support effective and lawful PPP operations, removing legal barriers to information sharing and collaboration.
- **Establish Clear Legal Frameworks:** Define the roles and responsibilities of both public and private sectors in PPPs to ensure clarity and compliance.
- **Promote Standardization,** in particular the EN Standard System EN 17483, especially designed for Private Security Companies protecting Critical Infrastructure.
- The complementarity of LEA and PSC staff should be reflected in their respective training curricula and bridges between the two should be made possible.

## Law Enforcement Agencies (LEAs)

- **Enhance Training and Integration:** Ensure that law enforcement personnel receive training on how to effectively collaborate with private security companies, including understanding the capabilities and limitations of private security.
- **Regular Evaluations:** Implement regular assessments of PPP effectiveness, adjusting as needed to improve outcomes and maintain public trust.
- **Information Sharing Protocols:** Develop protocols that allow for safe, secure, and efficient sharing of information between public and private entities without compromising data protection standards.

## Recommendations for Critical Infrastructure Operators

- **Prioritize Quality in Security Procurement:** Shift away from cost-driven procurement practices by implementing best-value criteria that emphasize quality, compliance with standards (such as EN 17483), and demonstrated operational excellence in security services.
- **Foster Public-Private Collaboration:** Establish regular communication channels and partnerships with both public authorities and PSCs to facilitate intelligence sharing, joint exercises, and rapid response coordination.
- **Integrate Cyber-Physical Security Strategies:** Develop unified security frameworks that bridge the gap between cybersecurity and physical security, ensuring that protection measures are comprehensive and mutually reinforcing.
- **Conduct Regular Risk Assessments and Drills:** Implement systematic security audits and joint emergency exercises with PSCs and public authorities to continuously assess vulnerabilities and refine response protocols.
- **Promote a Security Culture Across All Levels:** Cultivate a proactive security mindset within the organization through ongoing staff training, awareness campaigns, and clear reporting mechanisms for security incidents.

## Recommendations for Private Security Companies (PSCs)

- **Adhere to European Standards:** Ensure compliance with relevant CEN standards, particularly the EN 17483 series, and seek certification to demonstrate operational quality and professionalism in CI protection.

- **Invest in Specialized Training:** Provide ongoing, sector-specific training for security personnel, including modules on cybersecurity awareness, crisis response, and handling hybrid threats (e.g., drones, insider threats).
- **Strengthen Partnerships with Public Authorities:** Where possible, actively engage with law enforcement and regulatory bodies, participating in joint exercises, information-sharing initiatives, and sector-specific security forums.
- **Enhance Technological Capabilities:** Leverage advanced security technologies—such as surveillance systems, access control, and drone detection solutions—to stay ahead of evolving threats and improve incident response efficiency.
- **Promote a Professional Security Culture:** Foster a strong internal security culture by emphasizing ethical behaviour, operational excellence, and continuous improvement, while encouraging personnel to contribute actively to risk detection and mitigation efforts.

### Cross-Sector Recommendation: Countering Information Warfare and Ensuring Digital Sovereignty

As demonstrated in this White Paper, disinformation campaigns, digital propaganda, and geopolitical shifts increasingly intersect with Critical Infrastructure Protection (CIP). These factors can erode trust in institutions, disrupt access to essential data, and amplify polarisation—undermining resilience efforts across sectors. The risks associated with information warfare and digital sovereignty are not confined to one actor or domain; **they affect EU policymakers, national authorities, infrastructure operators, and private security companies alike.**

The following recommendation outlines measures to address these emerging challenges holistically.

**European policymakers and national legislators** should recognise disinformation campaigns and digital propaganda as critical threats to infrastructure resilience, and:

- Invest in counter-disinformation capabilities within CI sectors (e.g., dedicated monitoring units, staff awareness, response protocols);
- Support initiatives that improve public trust in security governance, including transparency mechanisms and strategic communications.

**National governments and CI operators** should assess and reduce dependencies on non-EU digital infrastructure by:

- Prioritising investment in sovereign or decentralised cloud services (e.g., GAIA-X);
- Developing contingency plans for platform withdrawal or restricted access to foreign-managed systems;
- Conducting regular stress tests on digital continuity and data access under extreme geopolitical scenarios.

**The European Commission** should accelerate coordination efforts to:

- Harmonise legal protections for data sovereignty;
- Encourage the integration of digital sovereignty principles in public procurement and Critical Infrastructure risk assessments;
- Facilitate cross-border collaboration to identify, attribute, and respond to information manipulation campaigns targeting CIP stakeholders.



Acting as the voice of the **security industry**

Confederation of European Security Services

**Private security services in Europe** provide a wide range of essential services, both for **private and public clients**, ranging from **Critical Infrastructure facilities** to **public spaces and supply chains**.

**coess.eu**

**Confederation of European Security Services**

Avenue des Arts 56

B-1000 Brussels

Belgium