strategy&
Part of the PwC network

Towards resilient ecosystems

A proactive approach for securing European Critical Infrastructure

strategyand.pwc.com/it

Contents

Executive Summary

The **Russian invasion of Ukraine in 2022** marked a turning point in Europe's approach to **critical infrastructure security**. While the battlefield remains geographically defined, the threat landscape does not. **Hybrid warfare** - characterized by a blend of sabotage, disinformation, cyberattacks, and covert operations - has proven capable of reaching far **beyond the borders of active conflicts**. European nations not directly involved in hostilities have nonetheless become targets, as evidenced by the **sabotage of the Nord Stream pipelines**, damage to subsea cables and pipelines in the **Baltic Sea**, and unexplained disruptions to energy and communication networks across the continent.

These incidents underscore a strategic shift: **critical infrastructures are now a frontline**, **regardless of geography or political alignment**. The goal of hybrid actors is not only to disrupt services, but to sow uncertainty, weaken public trust, and **fragment European cohesion**. In this context, **no country can consider itself immune** - neutrality or distance from conflict zones offers no protection from the systemic vulnerabilities that hybrid threats exploit.

Recognizing this, the **European Union has launched a series of initiatives** to bolster resilience and coordination across member states. Key actions include:

- **Critical Entities Resilience** (CER) Directive (December 2022), which mandates risk assessments and resilience planning for operators of essential services
- The **European Commission's guidance on countering drone-based threats** (October 2023), reflecting the growing risk posed by unmanned systems
- The **proposed Directive on Submarine Cable Security** (February 2025), aimed at protecting the physical backbone of Europe's digital infrastructure.

Following the provisions of the CER Directive, a **clear division of responsibilities has emerged between public and private sectors** regarding the security of critical infrastructure. While the public sector retains its primary role in defending the nation against acts of war, the responsibility for **addressing all other forms of hostile "non-war" activity falls to private operators**.

As a result, private entities managing critical infrastructure must **reassess and enhance their existing security frameworks** to align with increasingly complex and volatile threat scenarios. Consequently, **infrastructure protection is now a shared duty**: the public sector safeguards against warfare, while the private sector ensures resilience against non-military hybrid threats.

As a result, **infrastructure security is now demanded directly to operators** who must **anticipate and withstand hybrid threats** that are increasingly sophisticated, transnational, and persistent, evolving **from static protection to dynamic resilience**.

To address such challenges and based on our **direct hands-on experience** in such an environment, **our main recommendations are**:

1. **Map critical infrastructures** by industry sector for each European country, in accordance with **CER directive requirements**.
2. **Assess current security assets and infrastructure preparedness** (i.e. readiness level) to face potential **multi-domain threats** (air, land, above and below water, cyber, space).
3. **Devise comprehensive and integrated security ecosystems** to increase overall critical infrastructure security.

In an era where geopolitical tensions and technological risks converge, **safeguarding infrastructure is no longer a matter of national defense** - it becomes a **shared European imperative**.

About the authors – PwC Strategy& Italy

Critical Infrastructure Security Task Force

Cesare Battaglia is a Partner at PwC Strategy& and EMEA AD&S Leader based in Italy, with over 25 years of experience in the aerospace, defense, and security sectors. He specializes in business strategy, corporate planning, and transformation programs for leading AD&S players, and has held senior roles both in industry and consulting. Cesare has deep expertise in defense procurement, economic impact analysis, and post-merger integration, and is the ideator and founder of the Critical Infrastructure Security Task Force of PwC Italy.

Contact: cesare.battaglia@pwc.com

Giovanni Maver is a Senior Manager at PwC Strategy& in Italy with 9+ years of international experience in aerospace, defence, security, and automotive sector. He focuses on physical security strategies for critical infrastructures, business planning, and commercial due diligence. Giovanni has experience in steering security ecosystem development end-to-end projects for critical infrastructures around Europe and the Mediterranean area, managing operating team and acting as single point of reference for senior clients' members.

Contact: giovanni.g.maver@pwc.com

Gabriele Capomasi is a Partner at PwC Strategy& in Italy, specializing in Aerospace, Defence, and Security, with over 18 years of international experience. He focuses on strategy and implementation of technological solutions for physical security, business plan development, and impact analysis for leading defence and security players. Gabriele has deep expertise in security frameworks, unmanned systems, and digital transformation, and has led projects on risk mitigation, safety ecosystems, and strategic supervision for major European clients.

Contact: gabriele.capomasi@pwc.com

Gianmarco Polito is a Senior Associate at PwC Strategy& based in Milan. He has experience in the aerospace, defence, security, and energy sector, with a focus on physical security strategies for critical infrastructure operator, managing all the operating end-to-end activities, from ecosystem development to technologies implementation. He developed security ecosystems for critical infrastructures around Europe and the Mediterranean area, including risk assessment, supplier interviews, and supporting the implementation of technologies. Gianmarco holds a particularly strong knowledge of security technologies and associated suppliers around Western Countries.

Luca Colombo is a Partner at PwC Strategy& based in Italy, leading the Gas, Power & Utilities sector. He has over 20 years of international experience in management and strategy consulting, focusing on transformation strategies, process reengineering, and innovation for major energy and utilities clients. Luca specializes in physical security for critical infrastructures and has led projects on operational efficiency, contract management, and post-merger integration for leading industry players.

Contact: luca.colombo@pwc.com

Other relevant contributors: Todd Bradshaw (CEE), Bernat Figueras Comas (ESP), Pekka V. Pesonen (FIN), Tuomas Kotilainen (FIN)

Frame of reference

Introduction

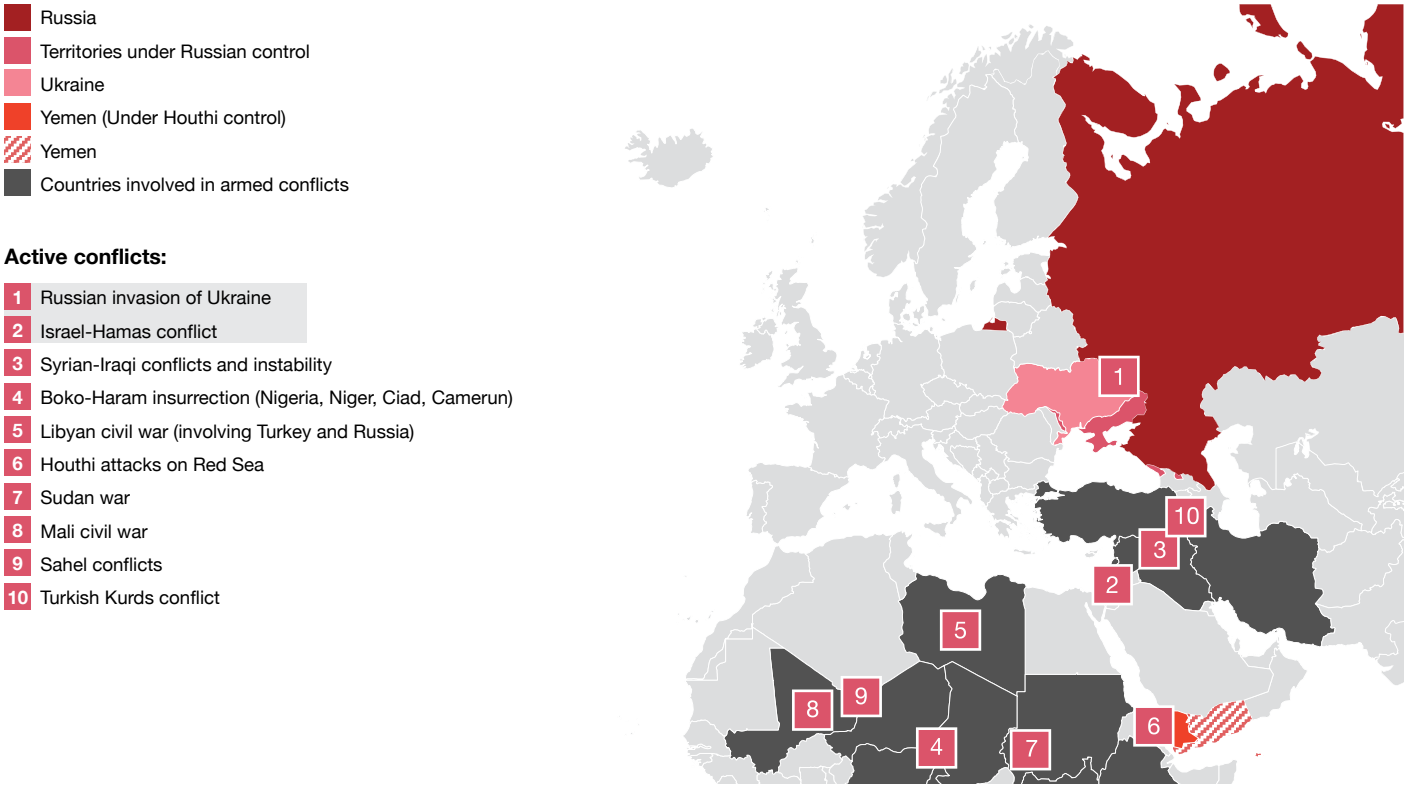
Since the **war in Ukraine**, **tensions** have **risen** along **Europe's borders**, marking a new era of **geopolitical instability**. The conflict between **Russia** and **Ukraine** stands as the most significant threat to **European security**, with direct consequences for **energy supplies**, the **economy**, and collective **defense**. At the same time, the war between **Israel** and **Hamas** in the Middle East has **reignited regional tensions**, drawing in international actors and increasing the risk of escalation.

These crises are part of a broader confrontation between **East and West**, with **NATO** and **Russia** once again **positioned** as **opposing blocs**. The renewed rivalry is not limited to military posturing but extends to **economic**, **technological**, and **informational domains**, making the European continent a central stage for global competition.

Other conflicts, such as the civil **war in Libya**, instability in **Syria and Iraq**, **Houthi attacks in the Red Sea**, and crises in the **Sahel and Sudan**, further contribute to a landscape of growing uncertainty (**see Figure 1**). While these crises differ in nature and intensity, they all have direct or indirect implications for Europe, particularly regarding **security**, **migration flows**, and **the protection** of **strategic trade routes** and i**nfrastructures of national significance**.

In this context, traditional military threats are increasingly accompanied by **new forms** of confrontation. The preferred **method** of **warfare** is no **longer limited** to **conventional** means: **hybrid warfare**, **combining military**, **cyber**, **economic**, and **informational tactics**, has become a **defining feature** of the c**urrent security environment**.

Figure 1: Main actual conflicts around Europe (2025)



Concept note – Critical infrastructures

In 2008, the European Critical Infrastructure Directive (2008/114/EC) defined **critical infrastructure** as "an element, facility, equipment, network, system, or part thereof necessary for the provision of a service essential to the maintenance of vital societal functions, economic activities, public health and safety, or the environment." In other words, critical infrastructures encompass both **physical and digital systems that enable essential functions and services** supporting the most basic social, economic, environmental, and political systems.

Initially applicable to the **energy and transport sectors**, this directive has been revisited since 2022, leading to the publication and enforcement of the Critical Entities Resilience (CER) Directive, which extends coverage to **twelve sectors**, including banking, healthcare, food supply, etc. The establishment of a common European standard was the first step towards creating a collaborative framework and encouraging self-assessment of protection levels for continuous improvement. Furthermore, it declares that the ultimate responsibility for protecting European critical infrastructures lies with the member states and their respective operators.

In this context, **public administrations and private operators must coordinate efforts to protect critical infrastructures**, as they now share the responsibility of enhancing security and resilience in response to a new and heightened global risk landscape.

Central to the success of this cooperation is the collaboration of three key stakeholders:

1. **Governments** – They play a crucial role in developing and implementing initiatives to protect critical infrastructures and ensure essential services operate smoothly.
2. **Public Security Institutions** – These public bodies (Gendarmerie, Navy, Air Force, etc.) are responsible for supporting industries in adopting security measures as dictated by protection laws, promoting awareness, and facilitating compliance.
3. **Critical Infrastructure Operators** – Operators aim to keep their infrastructures secure and operational, though regulatory requirements may sometimes conflict with business strategies.

This strategic cooperation between such key stakeholders will be **further supported by NATO's commitment — and that of its member states — to allocate 5% of their annual GDP** to core defence and security-related spending by 2035. Of this, **up to 1.5% of GDP annually will be dedicated to protecting critical infrastructure**, defending networks, ensuring civil preparedness and resilience, fostering innovation, and strengthening the defence industrial base.

Hybrid warfare

Hybrid warfare represents a profound shift from the **total wars** of the **twentieth century**, blending **conventional military operations** with a wide array of **non-military tactics** such as **cyberattacks**, **disinformation**, **economic pressure**, **sabotage**, **and the use of proxy forces**. This approach **deliberately blurs** the **lines between war** and **peace**, **state** and **non-state actors**, and **military** and **civilian targets**, exploiting ambiguity to complicate detection and response. Unlike traditional conflicts, **hybrid warfare** is **designed** to **operate below** the **threshold** of **open confrontation**, leveraging multiple domains such as military, cyber, economic, and informational simultaneously to destabilize adversaries and undermine their resilience.

A defining feature of hybrid strategies is the systematic targeting of **critical infrastructures**, including **energy grids**, **telecommunications**, **transport networks**, **and financial systems**. These assets are increasingly exposed to **cyber intrusions**, **physical sabotage**, and coordinated influence operations. Such tactics have become **integral** to the **conflicts** in **Ukraine** and the **Middle East**, where **hybrid warfare** is used to disrupt essential services, erode public trust, and weaken the ability of societies to respond effectively. As a result, **hybrid threats** now **represent** a **persistent** and **complex challenge** for **European security**, **demanding coordinated** and **adaptive responses** across all sectors.

PwC Strategy& continuously and **systematically monitors** current **conflicts** and **terrorist attacks** all around the world. This mapping activity is based on the detailed **collection** of **data** regarding different types of attacks, with a particular focus on the **attacks** on **civilian** and **critical infrastructure** such as **energy networks**, **transport** and **logistic hubs** and **communications** facilities.

Some of the most **recent episodes of maritime drone use cases are highlighted** in the **Black Sea** and in the **Red Sea** (**see Figure 2**), where Unmanned Surface Vehicles were used to attack both military and civilian targets. In particular, in the Ukrainian war, the USV Magura V5 has been used to damage the Crimean Bridge, while the Houthi utilized the Toofan to sink oil tankers. This approach enables the **anticipation** of **emerging trends**, the **assessment** of **system vulnerabilities**, and **supports clients** in **defining resilience** and **response strategies,** thereby **strengthening** the **security** of **infrastructures** throughout **Europe**.

Current conflicts have highlighted the **efficacy of drones** as a threat not only to **military** and **naval** targets, but also to **civilian critical infrastructures**. In the Ukrainian war, both sides have **systematically deployed** aerial, maritime, and underwater drones to target critical infrastructures.

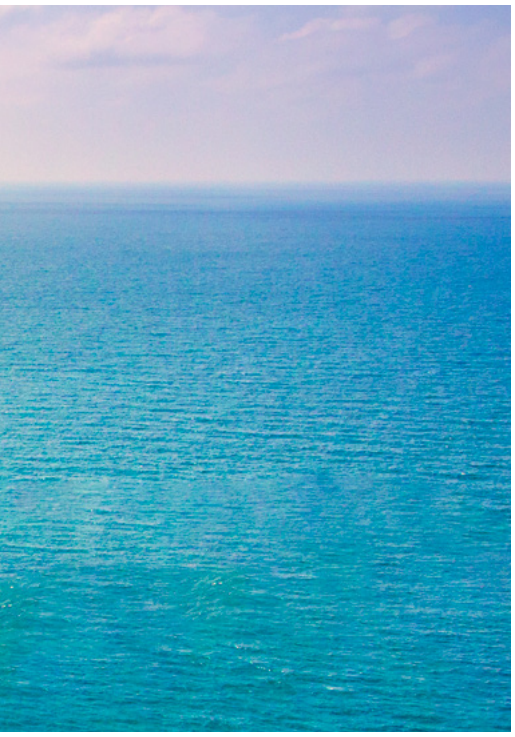
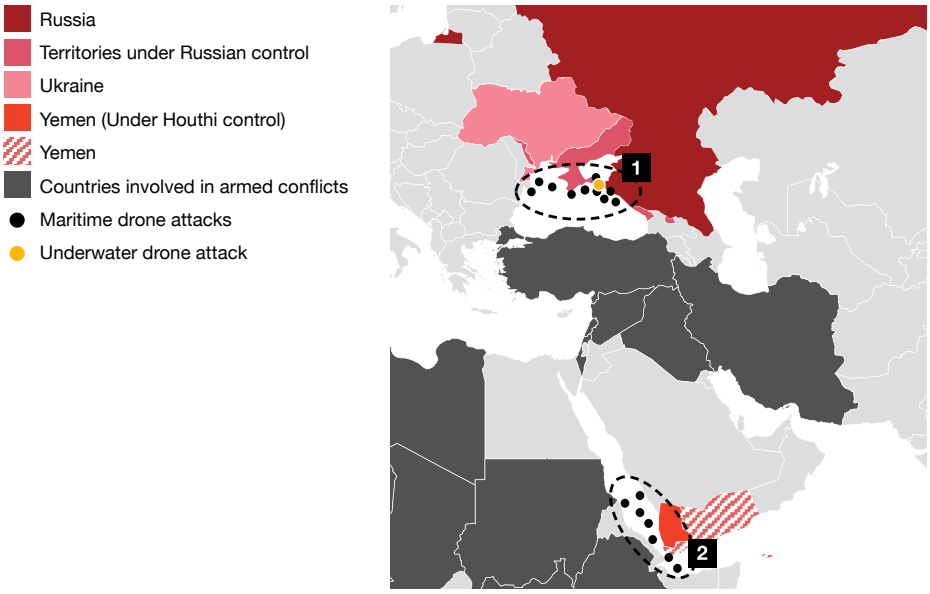


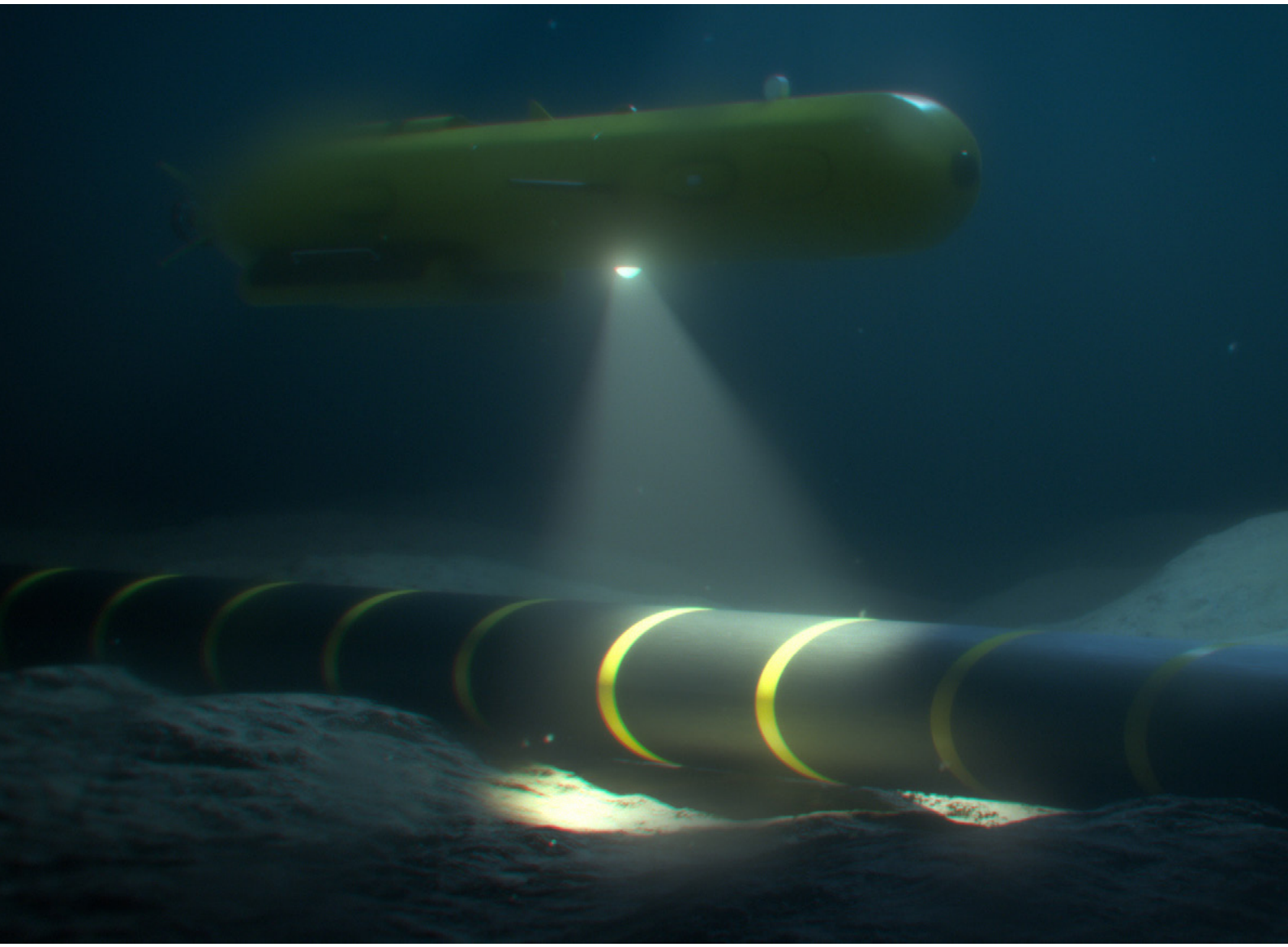
Figure 2: Maritime and underwater drone use cases in Ukraine war and in Houthi attacks



Cheap aerial drones with low skilled personnel have been used to target strategic industrial complexes. The attacks on the Crimean Bridge have shown how unmanned systems can inflict significant damage on vital infrastructure with relatively low investment. Indeed, the USV Magura V5 and the UUV Marichka casued several critical damages with minor upfront investments (cost < 500k€). In a nutshell, in the Ukrainian war drones proved to be crucial given their ability to perform **low-cost**, **high-impact** and **risk-free missions** with relatively low **skilled personnel**.

A crucial evolution in recent years is that drones are no longer the exclusive domain of national armies. Their **low cost and accessibility** - thanks to commercial off-the-shelf technologies - have enabled not only state actors, but also **terrorist organizations**, **militias**, **and subversive groups** to deploy them effectively. For example, rebel forces in **Myanmar** such as the Karenni Nationalities Defence Force are using **commercial technology** like inexpensive drones, 3D printers, and agricultural drone components from China to create homemade **attack drones**. These tools have become crucial in **their fight against** the **military junta** that took power in **2021**.

Another example is the **Houthi** usage of **unmanned surface vehicles** (USV) to **disrupt shipping** in the **Red Sea**, **threatening global supply chains**. This **democratization** of



drone technology has **dramatically expanded** the **threat landscape**, making it possible for a wide range of actors to conduct **low-cost**, **high-impact**, **and risk-free missions**.

In the **evolving landscape** of **hybrid warfare** and **terrorism**, **drones** have **emerged** as a **strategic enabler** due to their ability to **execute low-cost**, **high-impact operations** with **minimal risk** and **limited personnel** training. **Unlike conventional warfare**, where force projection and visibility are often part of the calculus, **asymmetric** and **terrorist actors prioritize anonymity** and **non-attribution**. The **capacity** of **drones** to **deliver precision strikes**, **conduct surveillance**, or **disrupt infrastructure without exposing the operator makes them uniquely suited to these environments**. **Their risk-free deployment profile** not only **reduces operational liabilities** but also **aligns perfectly** with the **tactical imperatives** of **deniability** and **stealth** that define **modern hybrid war operations**.

Incidents to critical infrastructures

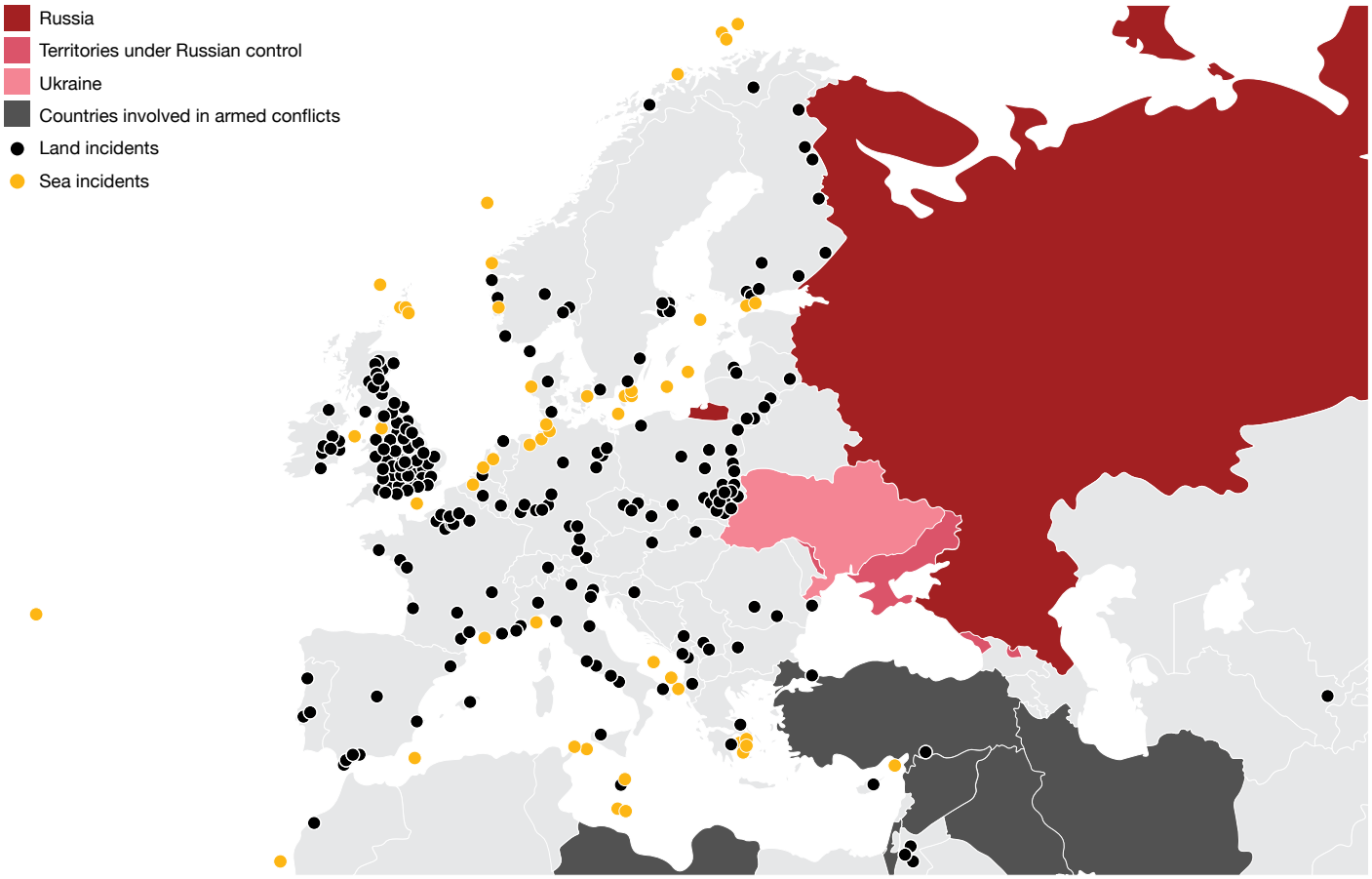
Geospatial distribution of incidents to critical infrastructures

There exist a significant number of **geographically spread hybrid incidents across Europe**. A **notable concentration** is observed in the **United Kingdom** and along the borders with Russia and Belarus. This pattern **correlates strongly** with the **deployment** of **advanced detection technologies** in these regions, which enable the **identification** of **threats** that may remain invisible elsewhere.

For example, **airports equipped** with **drone detection radars** report a **significantly higher number** of **incidents compared** to **rural** or **maritime zones lacking** such **capabilities**.
This disparity underscores the importance of technological readiness in threat recognition and response.

The data also shows that, in the context of hybrid warfare, attacks can be directed even at countries **not formally involved in conflicts**, using tools such as spy, saboteurs, drones, and countries not formally involved in conflicts, using tools such as spy, saboteurs, drones, and other hybrid agents. Importantly, these incidents are not limited to deliberate attacks designed to cause physical damage. They also include **collisions or near-collisions**, **espionage**, **harassment**, **and smuggling**, which - while less overtly destructive - still pose serious risks to operational stability and strategic resilience.

Figure 3: Incidents on critical infrastructures in Europe in non-belligerent countries from 2022 to 2025 (up to date)



European institutions response

Regulatory initiatives by EU institutions

In recent years, the European Union has significantly strengthened its regulatory framework for the protection of critical infrastructures, acknowledging the growing threat posed by hybrid warfare and multi-domain attacks. The EU's approach is based on an integrated strategy that combines operational resilience, cross-border cooperation, and stringent obligations for operators of essential services. The most important legislative and regulatory initiatives include:

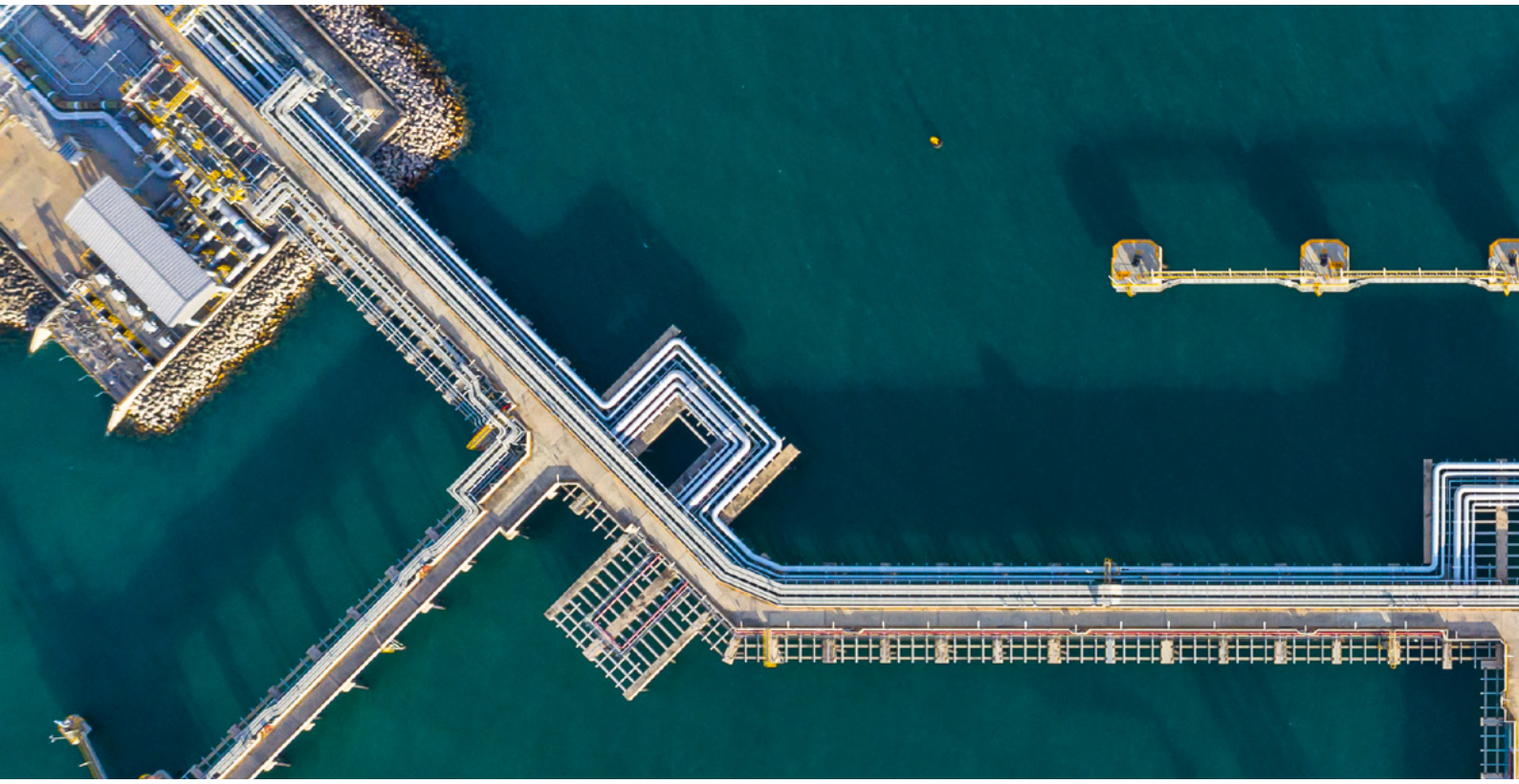
- **Council Directive 2008/114/EC**, the first EU legislation for identifying and designating European Critical Infrastructures (ECI), aimed at improving their physical protection;
- **Directive (EU) 2016/1148 (NIS Directive)**, which introduced a common level of security for network and information systems, requiring Member States to adopt national strategies, establish cooperation groups, and designate competent authorities;
- **Directive (EU) 2022/2555 (NIS2 Directive)**, which strengthens and updates the previous NIS Directive by expanding the scope to more sectors and entities, imposing risk management and supply chain security obligations, enhancing cooperation among national authorities, introducing stricter sanctions for non-compliance, harmonizing incident notification and crisis management procedures, and repealing Directive 2016/1148;
- **Directive (EU) 2022/2557 (CER – Critical Entities Resilience Directive)**, which establishes a framework for the resilience of critical entities across 11 strategic sectors such as energy, transport, health, digital, water, finance, space, and food, requiring mandatory risk and threat assessments—including hybrid and cross-border threats—adoption of resilience plans and technical or organizational measures to prevent, mitigate, respond to, and recover from disruptive incidents, incident notification obligations, administrative fines up to €125,000 (tripled in case of repeated non-compliance), and oversight by designated national authorities and inter-ministerial task forces;
- **EU Guidance on Countering Unmanned Aircraft Systems (UAS)** from October 2023, which recognizes the increasing risk posed by unmanned systems and promotes detection, neutralization, and enhanced coordination among Member States;
- **Proposed Directive on Submarine Cable Security** from February 2025, which aims to strengthen the protection of the physical backbone of Europe's digital networks with specific obligations for operators and Member States;
- **European Union's Action Plan on Cable Security**, presented in early 2025, which proposes the adoption of **SMART cable technologies**—equipped with sensors for temperature, pressure, and acceleration—to enhance seabed monitoring and early threat detection. However, this initiative faces **legal and geopolitical obstacles**, particularly in regions like the Mediterranean and the Arctic, where sovereignty claims and military interests complicate sensor deployment. Some states fear that such technologies could be used for **anti-submarine warfare**, raising concerns about data collection and strategic exposure.

Transposition into Italian legislation

As an example of national implementation, **Italy transposed the CER Directive with Legislative Decree No. 134/2024**, introducing a comprehensive regulatory framework that:

- **Covers a wide range of sectors**, including energy, transport, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, and food production/ agriculture.
- **Imposes strict obligations** on both public and private entities, such as conducting regular risk assessments for infrastructures, implementing technical and security measures, and promptly notifying authorities of any incidents affecting critical infrastructure.
- **Establishes clear timelines**, with the decree entering into force on October 18th, 2024, the National Resilience Strategy to be adopted by July 17th, 2025, preliminary identification of critical entities by July 17th, 2026, and final notification by July 17th, 2027.
- **Provides for significant sanctions**, including administrative fines up to €125,000 for non-compliance with risk assessment and resilience measures, with fines tripled in case of repeated violations.
- **Defines a robust governance model**, with compliance monitored by a task force appointed by the Prime Minister's Office and supervised by the Sectoral Competent Authority (Autorità Settoriale Competente) through a Single Contact Point (Punto di Contatto Unico).

The EU's institutional response now represents an advanced model of critical infrastructure security governance, shifting from static protection to dynamic and adaptive resilience. Operators are required to integrate risk management into all operational phases, anticipating increasingly sophisticated and transnational hybrid threats, in line with the CER and NIS2 Directives and the latest EU initiatives.



Military support to maritime infrastructure security

In response to the growing threat landscape, **European naval forces have increasingly mobilized to protect critical underwater and maritime infrastructures**. Several countries have launched dedicated initiatives aimed at enhancing seabed surveillance, threat detection, and operational readiness.

Italy has taken a proactive role, starting with the **Sparkle–Marina Militare protocol** in July 2022, followed by the launch of **Operation "Fondali Sicuri"** and the establishment of the **National Hub for the Submarine Dimension** (Polo Nazionale della dimensione Subacquea, PNS). France has formalized its approach through the **Seabed Warfare Strategy**, which now includes **offensive capabilities for underwater conflict**. The United Kingdom has invested in the **MROSS program**, commissioning the **RFA Proteus** and deploying **deep-sea threat neutralization robotics**.

In the Baltic region, NATO has intensified its presence with the creation of the **Commander Task Force Baltic**, the launch of **Operation Baltic Sentry**, and the deployment of **autonomous Saildrones** by Denmark. These initiatives reflect a broader shift toward **multi-domain maritime defense**, where seabed control and infrastructure protection are becoming central to European security strategies.

PwC Strategy& recommendations

From sector mapping to integrated security ecosystems: a proactive response to multi-domain hybrid threats

To address the **growing complexity** of **hybrid threats** and the **evolving risk landscape**, we offer a set of **strategic recommendations grounded** in our direct, **hands-on experience across multiple geographies** and **operational domains**. These recommendations aim to support **critical infrastructure operators** in **enhancing resilience**, improving **situational awareness**, and **aligning** with **European regulatory frameworks** such as the Critical Entities Resilience (CER) directive.

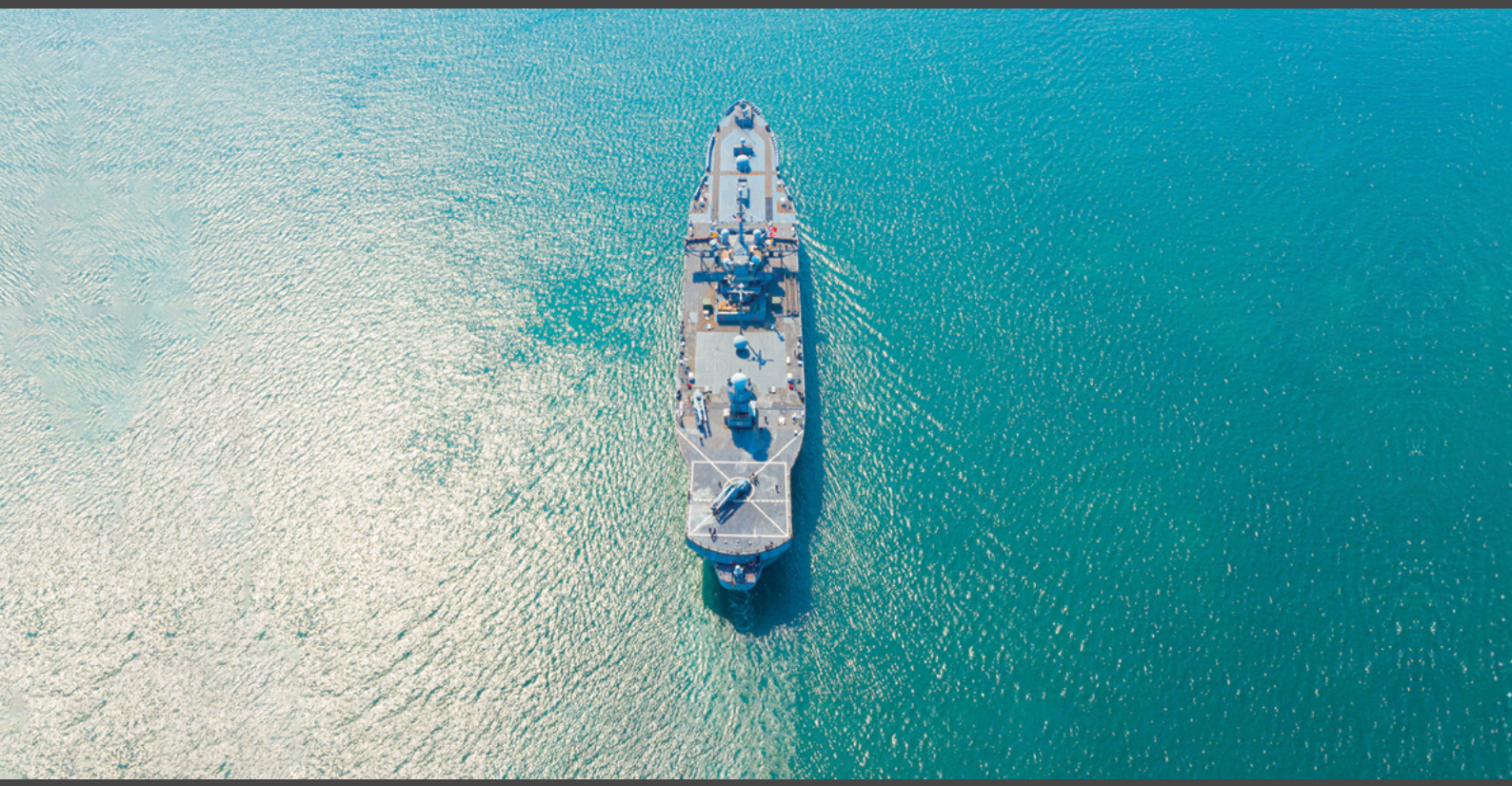
First, we recommend **conducting** a **comprehensive mapping** of **critical infrastructure** assets by **industry sector** across all **European countries**. This exercise should go beyond national inventories and incorporate cross-border dependencies, supply chain nodes, and sector-specific vulnerabilities.

The mapping should be **aligned** with **CER requirements** and **serve** as a foundational layer for risk prioritization and resource allocation.

Second, **operators should assess** the **current state** of **their security architecture** against multi-domain threats. This includes evaluating readiness to prevent, detect, identify and react to new threats.

Third, we advocate for the **design** and **implementation** of **integrated security ecosystems**. These should combine **physical security measures**, advanced **monitoring technologies**, and **intelligence-driven protocols** into a **cohesive operational framework**. **Integration across** domains and **stakeholders** - **public** and **private** - is **essential** to **ensure agility** and **coordinated response** in the face of complex, low-attribution threats.

In an era **where geopolitical tensions** and **technological risks increasingly converge**, safeguarding **critical infrastructure** is **no longer solely** a **matter of national security**. It has **become** a **shared European imperative** - one that demands collaboration, transparency, and strategic foresight. **Operators** must move **beyond reactive postures** and invest in **proactive**, **threat-informed resilience strategies** that **reflect** the **realities** of **today's hybrid operating environment**.



Contacts

Cesare Battaglia
Partner | PwC Italy
+39 340 469 7913
cesare.battaglia@pwc.com

Gabriele Capomasi
Partner | PwC Strategy&
+39 366 612 3428
gabriele.capomasi@pwc.com

Luca Colombo
Partner | PwC Italy
+39 335 774 6376
luca.colombo@pwc.com

Giovanni Maver
Senior Manager | PwC Strategy&
+39 334 684 7774
giovanni.g.maver@pwc.com

strategy&

Part of the PwC network

strategyand.pwc.com/it