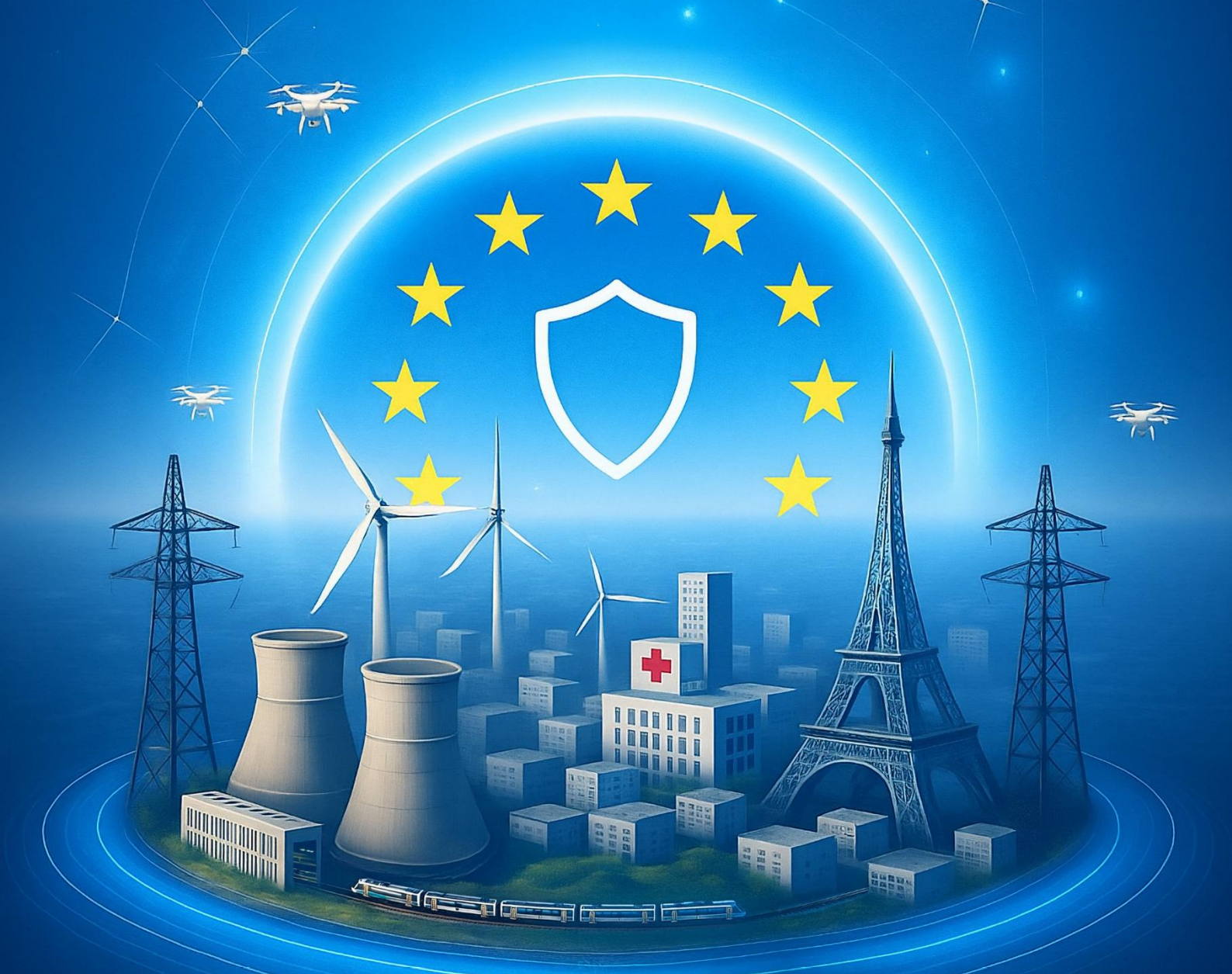
FORTIFYING EUROPE

THE COPENHAGEN PROJECT

ONE MARKET, ONE SHIELD, ONE MISSION
TO PROTECT CRITICAL INFRASTRUCTURE



DIGITALEUROPE

October 2025

Fortifying Europe: The Copenhagen Project

One mission, One Shield, One market
Securing the Future of Europe's Critical Infrastructure

This initiative builds on the pioneering **Danish model**, originally designed to **rapidly deliver weapons to Ukraine by funding its defence industry**. Adopted by the EU and partners as an effective **government-to-government-to-business mechanism**, it proved how resources could be channelled at speed and scale. The **Copenhagen Project** expands this model to the civil sector, investing in the **protection of Europe's critical infrastructure with cutting-edge dual-use and digital technologies**, and as a result, building the future European digital defence capability in peacetime.

"There is no doubt: Europe's eastern flank keeps all of Europe safe. From the Baltic Sea to the Black Sea. This is why we must invest in supporting it through an Eastern Flank Watch. We must heed the call of our Baltic friends and build a drone wall."

Ursula von der Leyen

European Commission President

Executive summary

- Europe has entered a decisive moment. The Union's decision to extend its funding programmes to defence and dual-use technologies marks a turning point, creating, for the first time, a coordinated framework to co-finance and deploy capabilities that strengthen resilience and competitiveness across civilian and defence domains. This momentum aligns with the forthcoming **EU Defence Readiness Roadmap 2030** and **Defence Transformation Roadmap**, which together will steer Europe's evolution towards a more innovative, agile, and technology-driven defence ecosystem. The **Copenhagen Project** anticipates these ambitions, providing a framework to turn strategic vision into operational reality through the deployment of dual-use digital technologies across vital infrastructures.
- Across Europe, technology companies are already developing world-leading systems that can safeguard our societies: **AI-enabled grids, autonomous drones, radars, jammers, quantum optimisation, secure connectivity, and energy-resilient networks.** Yet despite this strength, Europe still lacks the coordination to transform innovation into protection. **Procurement remains fragmented across 27 national markets, which prevents companies from scaling outside Europe** and results in slow deployment and weakened competitiveness.
- Meanwhile, **hybrid warfare has shifted from the battlefield to Europe's second front, the homeland.** Energy networks, ports, hospitals, and data centres are increasingly targeted through cyber and physical attacks designed to paralyse societies and trigger cascading effects across sectors.

Protecting these systems has become inseparable from Europe's defence— the first line of defence against hybrid and cyber threats.

- The **Copenhagen Project** provides a concrete answer. Conceived as a **pan-European digital resilience and defence infrastructure programme**, it will scale dual-use technologies that protect critical networks in peacetime and enable rapid mobilisation in crisis. By aligning EU and national resources, it will enable trusted European and allied providers to deliver **interoperable, market-ready solutions** on a large scale. In doing so, it will enhance Europe's capacity to act, strengthen its industrial base, and lay the foundations of a truly **digital defence industry**, one capable of protecting citizens and preserving Europe's freedom to operate in an age of permanent disruption.

"In the struggle between democracy and autocracy, the digital sphere is not a sideshow: it is the frontline."

Ursula von der Leyen

European Commission President

Context and rationale

- Europe faces a rapidly evolving security environment in which **hybrid, cyber, and kinetic threats** increasingly target the backbone of our societies, our critical infrastructure. **Such hybrid tactics are among the most cost-effective forms of conflict:** coordinated attacks that cut power, water, and connectivity, stall hospitals and airports, and disable payment systems can immobilise a country within hours. Recent crises confirm that disruption is now deliberately employed to demoralise populations and undermine democratic stability.

- Ukraine has shown how innovation, AI, drones, and cyber tools can be mobilised at unprecedented speed when digital resilience becomes a matter of national survival. Its experience reveals that the same technologies protecting soldiers on the battlefield are those required to secure citizens at home. From GPS jamming and subsea cable sabotage to drone incursions over airports and cyberattacks on hospitals and data networks, **Europe is facing an unprecedented escalation of hybrid activity on its own territory**.

- These realities mark the emergence of a **"second front",** not on distant battlefields, but within Europe's borders. In response, the **EU Preparedness Union Strategy**, the **European Defence Readiness Omnibus**, and the **April 2025 Commission proposal**, which extends EU funding programmes to defence and dual-use technologies, all point towards a more integrated approach to resilience and capability planning. The **June 2025 European Council conclusions** further called for embedding dual-use considerations across infrastructure investment and capability development to strengthen civil-military readiness. Together, these steps mark the beginning of a **European investment mandate linking digital innovation directly with operational protection**.

- In parallel, at the **June 2025 NATO Summit**, Allies committed to investing **5% of GDP annually by 2035** in defence and security-related spending, including **up to 1.5%** for protecting critical infrastructure,

defending networks, enhancing civil preparedness, supporting innovation, and strengthening the defence industrial base.

- Yet despite this strong political momentum, **Europe still lacks a unified operational framework to coordinate investments**, scale dual-use solutions, and protect essential networks across borders. To close this gap, **DIGITALEUROPE proposes the Copenhagen Project,** a flagship initiative first introduced at the **GLOBSEC 2025 Forum** and welcomed by key strategic stakeholders. Building on DIGITALEUROPE's recognised leadership in **defence digitalisation**, including contributions to the **EU White Paper on Defence**, the **Defence Readiness Omnibus**, and **NATO's Industrial Blueprint for the Rapid Adoption Action Plan**, the project aims to translate Europe's digital ambition into tangible resilience and readiness.

Fragmentation and strategic gap

- Europe's innovation ecosystem remains globally competitive, with world-class capabilities in fields such as **AI, quantum technologies, secure communications, and digital engineering**. Across the continent, companies — large and small — are developing solutions that can strengthen both civilian resilience and defence capabilities. Yet these advances rarely reach operational deployment across borders.
- **The problem is not innovation, but fragmentation.** Europe's industrial capacity remains dispersed across **27 national procurement systems**, each too small to sustain global competitiveness or keep pace with technological change. While national frameworks protect domestic priorities, they collectively constrain Europe's ability to consolidate demand, attract investment, and create the scale-ups needed to compete internationally. The **NIS2 Directive** establishes a common baseline for protecting essential entities, but it remains primarily a compliance instrument rather than a driver of industrial leadership and investment
- As innovation cycles in critical technologies now evolve in months rather than years, the **window for commercialisation and operational deployment is closing faster than Europe can act**. Other global players are scaling through consolidation, mergers, and strategic investment; Europe, by contrast, continues to **regulate and fund in silos**. Without a coherent mechanism linking innovation, procurement, and deployment, **Europe risks remaining an R&D powerhouse but a deployment follower.**
- The **Defence Readiness Omnibus** introduces welcome regulatory simplifications but falls short of establishing a **pan-European framework for deploying dual-use digital technologies across critical infrastructure**. This strategic and operational gap has also been highlighted by **Estonia, Latvia, and Lithuania**, which jointly called for infrastructure protection to become a priority in the next **Multiannual Financial Framework (MFF)**. Yet no EU programme currently exists to deliver on this ambition.
- Existing EU instruments, such as the **European Defence Fund (EDF)**, **Digital Europe Programme**, **Horizon Europe**, and **Secure Action for Europe (SAFE),** alongside regulatory frameworks like the **Critical Entities Resilience (CER) Directive**, **NIS2**, and the **Cyber Resilience Act**, remain **disconnected from operational realities**. There is still no dedicated EU mechanism linking Europe's R&D investments with concrete deployment needs, resilience risks, or battlefield-tested insights, nor one capable of scaling dual-use technologies for infrastructure protection.

- The result is a widening **strategic gap** between Europe's technological potential and its ability to protect, mobilise, and defend. The continent remains **over-reliant on external providers** for critical technologies, while its own companies face regulatory complexity, limited financing, and a lack of anchor customers for dual-use solutions.
- The **Copenhagen Project** seeks to close this gap. It proposes an **integrated European mechanism** to scale and deploy dual-use digital technologies for critical infrastructure protection, **transforming Europe's technological excellence into a shared shield** that connects innovation with procurement, and industry with operational readiness.

Objectives and key actions of the Copenhagen project

- The **Copenhagen Project**, conceptualised by DIGITALEUROPE, is a strategic initiative to establish a **pan-European digital defence infrastructure programme**. It aims to protect Europe's most vital sectors, **energy, water, ports, hospitals, communication networks, and data centres,** as well as trusted partners, such as Ukraine, from hybrid, cyber, and kinetic threats. Drawing on battlefield lessons from Ukraine and other crisis zones, it calls for a more cohesive, mission-driven use of dual-use technologies across the EU.
- The project establishes a framework aimed to align EU and national funds directly into trusted European, Ukrainian, and, where appropriate, transatlantic providers, ensuring both solidarity and resilience. This approach will deliver **rapid, interoperable, and sustainable deployments** to strengthen critical entities against hybrid attacks. By enabling Ukrainian firms to **co-produce** within EU and EFTA territories, the initiative will deepen defence industrial integration, diversify supply chains, and accelerate the adaptation of battlefield-tested innovations to Europe's resilience needs.
- To move at the required pace, the **Copenhagen Project calls for the rapid mobilisation of unspent or reallocated EU budget lines**, complemented where possible by national contributions, as a bridge while in parallel preparing a **dedicated funding envelope under the next MFF** to secure structural, long-term support. In this context, **DIGITALEUROPE proposes** that the **European Commission**, in coordination with relevant EU institutions, including the **European Investment Bank** (EIB) and the **European Defence Agency** (EDA), as well as **Member States**, **industry**, and **trusted partners**, jointly pursue the following actions:
    - **Deploy flagship pilot projects across critical sectors**: Roll out cross-border demonstration pilots based on the five infrastructure domains outlined in the following thematic section to test and validate dual-use technologies under real or simulated operational conditions. These deployments will help identify scalable, interoperable, and resilient solutions aligned with the infrastructure operators' needs. Using the Copenhagen Project, pilots can be rapidly contracted and funded, ensuring deployment at scale within a three-year implementation horizon.
    - **Accelerate industrial scale-up and broaden supplier participation**: Expand access for SMEs, mid-sized companies, and established suppliers through simplified procedures, fast-track evaluations, and phased deployment models. Prioritise the uptake of market-ready technologies that strengthen infrastructure resilience, leveraging trusted European and allied providers, cross-border consortia, and, where appropriate, co-development with Ukraine and other strategic

partners, integrating battlefield-tested insights and supporting interoperability. The Copenhagen Project will act as the anchor mechanism to channel funds directly to these providers, reducing delays and de-risking investment while enabling rapid industrial consolidation.

- **Establish a coordinated governance structure and pilot an "anchor-customer" procurement model for digital technologies:** Create a joint platform under EU leadership, involving Member States, relevant institutions and agencies (European Commission, EDA, EIB), industry associations such as DIGITALEUROPE, and, where appropriate, NATO and strategic partners. Under this model, the EU would act as an "anchor customer," guaranteeing early strategic demand, similar to the joint vaccine and ammunition procurement mechanisms, to de-risk private investment, allowing vendors to retain IP, and applying light-touch technical requirements. The governance framework will steer priorities, align funding streams, prevent duplication, and ensure transparency and coherence across Member States through the Copenhagen Project.

Thematic priorities and sectoral focus

- The **Copenhagen Project** identifies infrastructure domains where dual-use digital technologies can deliver the most significant strategic and operational impact. The table below outlines priority sectors, the enabling technologies, and their intended effects.

Sector	Priority Dual-Use Technologies
Energy	AI-driven grid security, decentralised power backups, energy resilience microgrids, cyber-secure SCADA systems, digital twins, grid interconnectors, autonomous inspection drones, anti-drone equipment, 5G/6G connectivity, satellites, radar systems, AI platforms
Water	Autonomous water-air drones, emergency purification technologies, secure monitoring systems, robotics, cloud-based infrastructure, anti-drone equipment, IoT sensors, 5G/6G connectivity, satellites, radar systems, AI platforms
Ports	Maritime surveillance drones, integrated sensor networks, smart perimeter and access-control systems, autonomous logistics, anti-jamming communications, water-air drones, anti-drone equipment, 5G/6G connectivity, satellites, radar systems, AI platforms
Hospitals	Health data clouds, secure connectivity, mobile emergency networks, autonomous hospital logistics, protected medical device networks, edge computing, drones for rapid supply delivery, anti-drone protection, 5G/6G connectivity, satellites, radar systems, AI platforms
Comms & Data Centres	Quantum-secure communications, trusted cloud platforms, AI decision-support systems, advanced microelectronics, end-to-end encryption, secure data routing, anti-drone equipment, 5G/6G connectivity, satellites, radar systems, AI platforms

Political and industrial opportunity

- The **Copenhagen Project** comes at a pivotal moment for Europe's political and industrial agenda. As the EU prepares its next **MFF (2028–2034)**, Member States are calling for more substantial investment in infrastructure protection and dual-use innovation. While the **Defence Readiness Package** has improved alignment on funding and procurement, Europe still lacks a unified programme to deploy trusted technologies across borders and at scale.
- Europe's technological base is strong but fragmented. To remain competitive, the EU must move beyond innovation to **industrial scale,** turning its diversity into a strategic advantage through

coordinated procurement and shared standards. Regulatory, financial, and industrial policies must converge around one goal: deploying interoperable European technologies that enhance both **resilience and competitiveness**.

- **DIGITALEUROPE** calls for dedicating **at least 25% of EU defence funding** to digital and dual-use technologies, including **AI, cloud and edge computing, secure connectivity, and cybersecurity**. Funding instruments should be better coordinated—mobilising unspent EU resources now while preparing a dedicated MFF envelope to provide long-term, structural support. The **Copenhagen Project** offers a mechanism for this transition, linking **research, procurement, and deployment** under a single, coherent framework.
- Looking ahead, the **Copenhagen Project** will serve as a delivery vehicle for Europe's broader **defence transformation**, operationalising the ambitions of the forthcoming **Defence Readiness Roadmap 2030** and **Defence Transformation Roadmap**. By aligning with initiatives such as **BraveTech Europe** and the EU's **Readiness Flagships**, it will accelerate the integration of **AI, autonomy**, and **secure digital infrastructures** into Europe's defence architecture—positioning the Union as a **defence-tech powerhouse** built on speed, scale, and industrial agility.

Example – Delivering Europe's Digital Shield

Imagine a unified "**Airport and Border Digital Shield**" deployed across EU airports and borders: an integrated system that combines secure connectivity, radar and drone sensing, AI-driven threat analysis, electronic countermeasures, quantum-secure communications, and resilient energy and cloud operations.

Core systems would be protected by cybersecurity controls and run on 5G/6G edge infrastructure. These networks would fuse multi-domain sensor data into a common command-and-control (C2) layer, enabling real-time situational awareness and coordinated response across domains. The platform would enable local control from operations towers, remote operation under hybrid attacks, and uninterrupted functionality via decentralized energy resources.

Delivered by 5 to10 leading European suppliers, this model, based on **the Copenhagen Project**, would reinforce the EU's flagship initiatives such as the European Drone Wall, Eastern Flank Watch, Air Defence Shield, and Defence Space Shield, **by providing their shared digital backbone**. Interoperable across Member States and strategic partners, this solution would be **scalable through joint procurement**, and in times of a crisis, and it could be repurposed to support national defence as a civil capability reserve.