ECSO
EUROPEAN CYBER SECURITY ORGANISATION

ECSO'S STRATEGIC VISION

EUROPEAN CYBERSECURITY 2030

UNLOCKING **GROWTH** BOOSTING **RESILIENCE** AFFIRMING **LEADERSHIP**

DISCLAIMER

COPYRIGHT NOTICE

Our vision at a glance

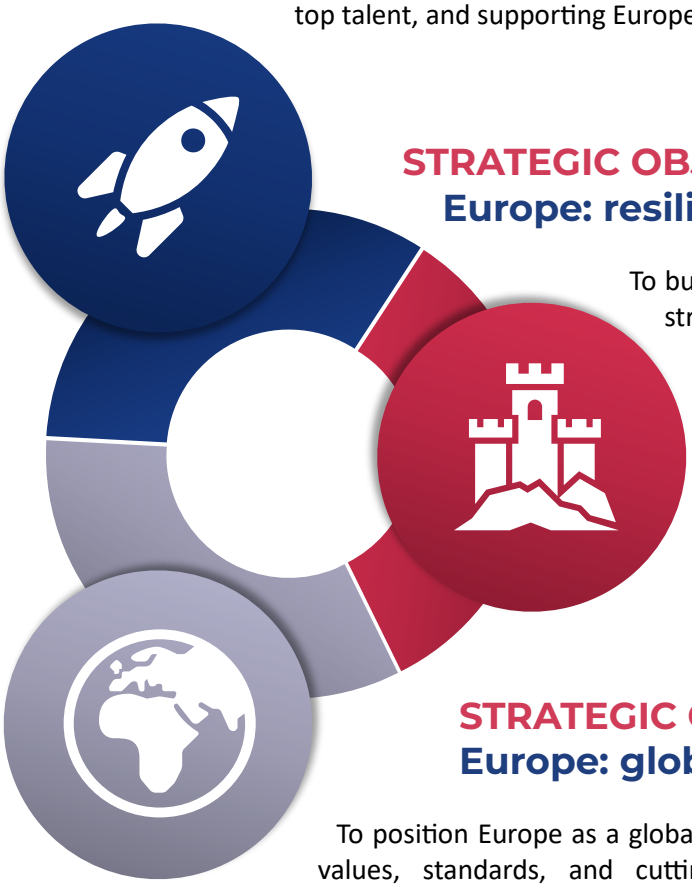
In alignment with Europe's new cybersecurity era, the European Cyber Security Organisation (ECSO), a pan-European, **private-public federation** that unites diverse cybersecurity stakeholders across the continent, confirms their commitment to shaping and executing together a bold, actionable vision for Europe's cyber future. Five core values will guide our work:

1. European strength
2. Public-private collaboration
3. Community empowerment
4. Proactive approach
5. Human-centric cybersecurity

Looking ahead, ECSO's strategic efforts will be structured around three **concrete pillars** reflecting our overarching ambition to drive economic growth, reinforce systemic resilience, and elevate Europe's leadership in the global digital landscape. Each pillar is translated into **concrete objectives:**

STRATEGIC OBJECTIVE 1
Europe: hallmark of competitiveness

To strengthen Europe's strategic digital autonomy by reinforcing its cybersecurity industry, driving research and innovation, enhancing market effectiveness, attracting top talent, and supporting European businesses.



STRATEGIC OBJECTIVE 2
Europe: resilient stronghold

To build a cyber-resilient Europe that enhances its strategic security and defence, by protecting critical infrastructure, securing supply chains, developing advanced dual-use capabilities, and bringing together different communities, including European cybersecurity leaders and civil-military exchanges.

STRATEGIC OBJECTIVE 3
Europe: global shaper

To position Europe as a global cybersecurity shaper, actively projecting its values, standards, and cutting-edge capabilities internationally, while fostering economic growth for European technologies and expertise through dialogue, cooperation, and robust private sector engagement.

Message from ECSO Chairperson

Dear Members of the European Cybersecurity Community,

It is with great pride and responsibility that I endorse and present to you ECSO's Strategic Vision: European cybersecurity 2030. As Europe navigates a defining moment, confronting unprecedented technological and geopolitical challenges, this vision sets the essential direction for our future.

I strongly believe that cybersecurity must be the foundation of Europe's strategic autonomy, digital sovereignty, economic competitiveness and societal resilience. The global race for technological leadership, rapidly accelerated by artificial intelligence and emerging innovations, demands that Europe act decisively and cohesively.

As Chairperson, my focus will be on accelerating ECSO's impact across businesses, enhancing competitiveness and strengthening European policymaking. Our ambition is clear: to position Europe as a strong and trusted global leader in the secure digital economy. Overcoming the fragmentation that still defines the current landscape is essential to drive a tangible impact.

Today, more than ever, we need a unifying force, representative of multiple public and private stakeholders, like ECSO to ensure that Europe's cybersecurity ecosystem comes together and thrives.

I once again sincerely thank the Board for their trust and confidence.

I invite all stakeholders to embrace this vision and work together to transform ambition into reality.

Yours sincerely,

Andrea Campora
Chairperson
European Cyber Security Organisation (ECSO)

Message from ECSO Secretary General

Dear Members of the European Cybersecurity Community,

It is my privilege to share with you ECSO's Strategic Vision: European cybersecurity 2030.

Our vision is built around three core objectives: Europe as a Hallmark of Competitiveness, a Resilient Stronghold, and a Global Shaper. Each of these pillars is translated into concrete initiatives that reflect ECSO's enduring commitment to operational excellence and collaborative progress.

What makes this document truly unique is that it was co-created with the stakeholders who form the ECSO community. It brings together a rich diversity of voices and perspectives, transforming them into a holistic and actionable guide designed to empower and advance Europe's cybersecurity capabilities.

At ECSO, we believe that success is rooted in engagement. Every actor has a unique and essential role in building a trusted and innovative cybersecurity ecosystem. Guided by our core values, we will continue to provide a platform for dialogue, knowledge exchange, and joint action.

I warmly invite you to contribute your expertise and energy to this mission. Together, we can ensure that Europe not only responds to challenges but actively shapes the future of cybersecurity worldwide.

Yours faithfully,

Dr Joanna Świątkowska
Secretary General
European Cyber Security Organisation (ECSO)

What is ECSO?

The European Cyber Security Organisation (ECSO) is the **pan-European**, private-public federation (**non-profit**) focused on empowering European cybersecurity communities.

Established in 2016 as the European Commission's contractual partner for the **Public-Private Partnership in Cybersecurity** (2016-2020), we have built on the successes of that partnership to strengthen European cybersecurity by providing a platform for cooperation, community advocacy, public-private collaboration, and more.

Today, we build on the trusted relationships already built with the key institutions shaping the European cybersecurity architecture: the European Investment Fund (EIF), the European Commission (EC), particularly DG CONNECT, DG GROW, and DG DEFIS, the European Cybersecurity Competence Centre (ECCC), the European Parliament (EP), the Council of the EU, the European Union Agency for Cybersecurity (ENISA), the European Defence Agency (EDA), the European Space Agency (ESA), and the AI Office. Together, we are laying the foundations for a resilient and innovative European cybersecurity ecosystem.

EMPOWERING EUROPEAN CYBERSECURITY COMMUNITIES

Why now: strategic context

As Europe stands at the halfway point of its Digital Decade[1], cybersecurity is no longer a supporting component - it is the foundation upon which our strategic digital autonomy, economic competitiveness, collective security, and resilience depend. It is the whole-of-society enabler securing critical services and unlocking opportunities.

The year 2025 marks five years since the launch of *the EU Cybersecurity Strategy*[2] and coincides with the release of the *State of the Digital Decade 2025* report[3] - a moment not only for reflection, but more

1 Digital Decade Policy Programme 2030. For further information, see https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030

2 The EU's Cybersecurity Strategy for the Digital Decade. For further information, see https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

3 State of the Digital Decade 2025 report. For further information, see https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report

importantly, for acceleration. The global technological race, intensified by the surge of artificial intelligence (AI), is moving at an unprecedented pace, and this is the last moment for Europe to build its position. In this context, cybersecurity, must be recognised as a key driver of Europe's competitiveness and economic growth. It is time to develop a comprehensive European Cybersecurity Industrial Policy - one that unlocks innovation and positions Europe as a global leader in the secure digital economy.

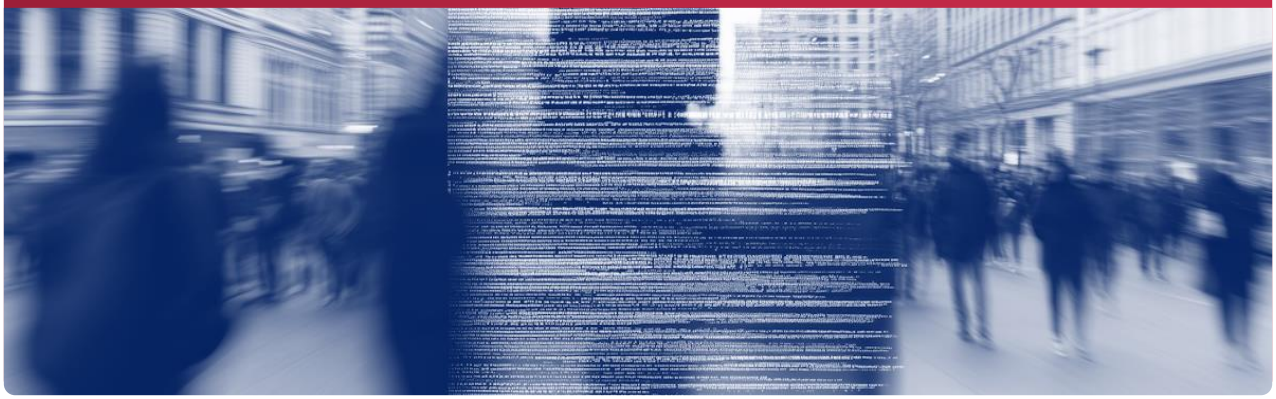
This pivotal moment is shaped not only by digital transformation but also by the complex geopolitical landscape. The ongoing war on the European continent - and conflicts elsewhere - resonate strongly in cyberspace, reinforcing the urgent need for coordinated action and strategic resilience. In response to the evolving security landscape, the European Union has launched the ProtectEU Internal Security Strategy[4] - clearly recognising cybersecurity as an essential pillar of Europe's internal security and crisis preparedness.

At the same time, the EU is extending its digital leadership globally, as reflected in the recently announced International Digital Strategy. This dual momentum - internal and external - highlights Europe's ambition to shape a secure, open, and resilient digital future, both at home and on the world stage.

This convergence of milestones and challenges is more than symbolic — it is a clear call to action. The next five years will determine whether Europe will lead the world in trusted digital innovation or risk being sidelined in an increasingly competitive digital landscape shaped by technological rivalry and complex cyber threat environments.

The European Cyber Security Organisation (ECSO) rises to this challenge with determination.

As a pan-European, private-public federation that unites diverse cybersecurity stakeholders across the continent, ECSO is dedicated to co-shaping and implementing a bold, actionable vision for Europe's cyber future - one that fuels economic growth, reinforces systemic resilience, and strengthens Europe's leadership in the global digital arena.



4 ProtectEU Internal Security Strategy. For further information, see https://home-affairs.ec.europa.eu/news/commission-presents-protecteu-internal-security-strategy-2025-04-01_en

Our core values

In these times of rapid change and challenges, we are renewing our commitment at ECSO by reinforcing the core values that have shaped who we are today.

European strength

ECSO's primary commitment is to support the development of Europe's capabilities and competitiveness in the cybersecurity domain, ensuring its leading global standing, reducing dependencies while working with trustworthy partners.

Public-private collaboration

ECSO believes that effective cybersecurity, cyberdefence, and market growth require strong partnerships and active engagement between the public and private sectors.

Community empowerment

ECSO is committed to fostering strong and trustworthy cybersecurity communities, collaborating across Europe, and recognising their vital role in collectively building and advancing European cybersecurity capabilities. Cybersecurity leaders, hands-on practitioners with deep subject matter expertise, are actively involved in advancing Europe's cybersecurity ecosystem.

Proactive approach

ECSO promotes a proactive cybersecurity approach, where security and resilience are embedded from the outset of all digital initiatives and strategic endeavours. Foresight activities anticipating emerging threats and opportunities support critical infrastructure and member states to adapt to future threats.

Human-centric cybersecurity

ECSO is dedicated to making cybersecurity a societal enabler for all citizens, not just a market driver. Through inclusive collaboration with citizens, youth, and local organisations, ECSO promotes a human-centric approach whereby secure digital services are trusted, secure, and available to all members of society, and backed by fundamental human values and rights.

Our strategic objectives

Our vision for *European cybersecurity 2030* is built upon **three concrete pillars**, which together forge the path to Europe's digital future.

I. Europe: hallmark of competitiveness

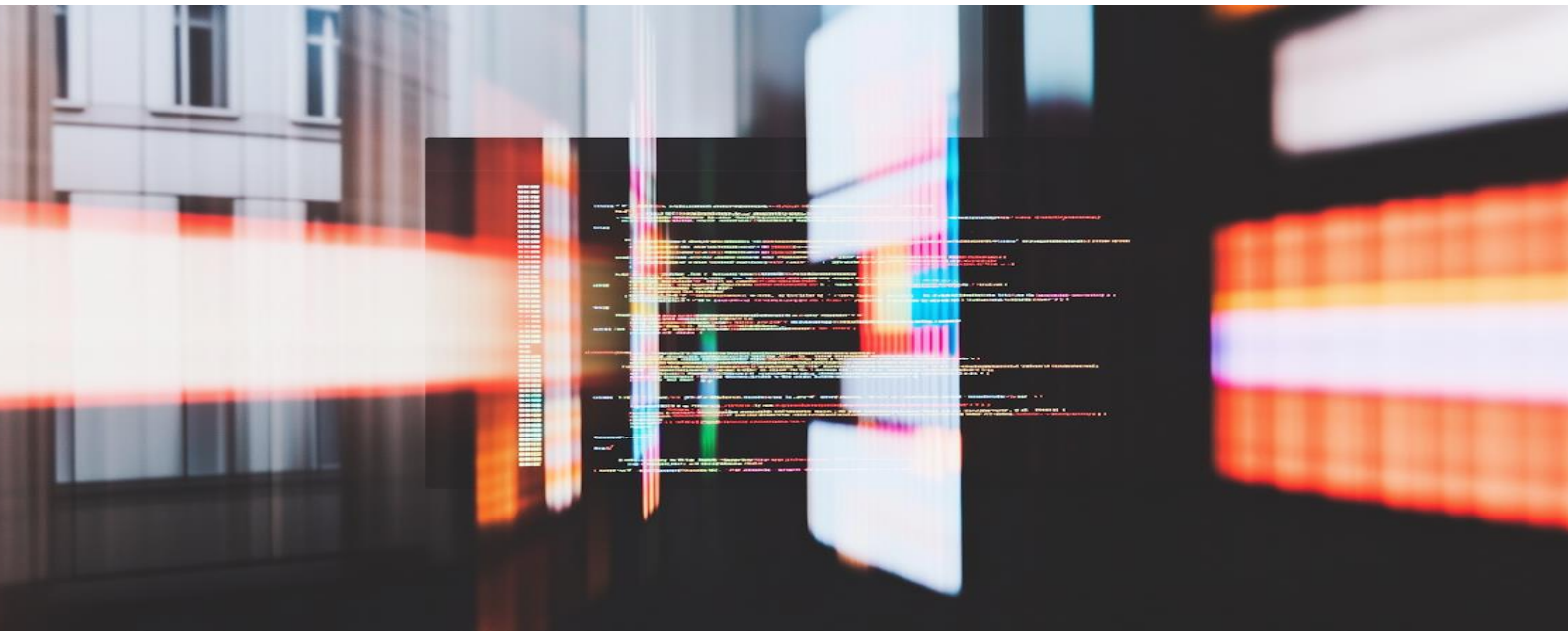
To strengthen Europe's strategic digital autonomy by reinforcing its cybersecurity industry, driving research and innovation, enhancing market effectiveness, attracting top talent, and supporting European businesses.

II. Europe: resilient stronghold

To build a cyber-resilient Europe that enhances its strategic security and defence, by protecting critical infrastructure, securing supply chains, developing advanced dual-use capabilities, and bringing together different communities, including European cybersecurity leaders and civil-military exchanges.

III. Europe: global shaper

To position Europe as a global cybersecurity shaper, actively projecting its values, standards, and cutting-edge capabilities internationally, while fostering economic growth for European technologies and expertise through dialogue, cooperation, and robust private sector engagement.



1. Europe: hallmark of competitiveness

1. Europe: hallmark of competitiveness

The ambition to strengthen Europe's cybersecurity capabilities lies at the heart of its pursuit of strategic digital autonomy. Achieving this goal requires cultivating a robust cybersecurity ecosystem - one that stimulates a dynamic, integrated digital single market, drives innovation, and enhances Europe's technological competitiveness. Crucially, it is also essential for attracting and retaining top talent, reducing external dependencies, and ensuring long-term prosperity.

All of that requires a bold European Cybersecurity Industrial Policy. Despite this strategic imperative, given the current situation, Europe is currently losing the technological race, and its cybersecurity landscape remains fragmented. While the continent hosts a vibrant community of small and medium-sized cybersecurity companies, and several emerging leaders have begun to stand out, Europe still lacks the critical mass of globally competitive players necessary to anchor its strategic digital autonomy. Europe can offer a market of 450 million consumers[5], yet structural barriers, including limited access to investment and scale-up opportunities, continue to hinder the growth of promising ventures and are not sufficiently offset by market-driven mechanisms.

Furthermore, European cybersecurity solutions often struggle to gain traction within domestic markets. The insufficient adoption and purchasing of homegrown technologies hamper their ability to scale, innovate, and compete globally - exposing a disconnect between political ambition and economic execution. Frequently, these solutions are overlooked not due to lack of quality, but because of limited visibility and insufficient market recognition.

This dynamic leads to the point where Europe is overdependent on third-party providers dominating the European market. It also contributes to a brain drain, as a growing number of skilled professionals seek opportunities abroad, further weakening Europe's cybersecurity strength.

ECSO believes this must change.

We are committed to reinforcing Europe's cybersecurity industrial base by combating fragmentation, advancing scale-up pathways, facilitating investment, promoting a Buy-European mindset, elevating European competitiveness, and ensuring that Europe remains an attractive environment for cybersecurity talent and innovation. We call for the creation and implementation of the **European Cybersecurity Industrial Policy** — an overarching framework designed to coordinate strategic initiatives that ECSO is ready to support:

- Closing the investment gap
- Stimulating demand for European solutions
- Accelerating R&D and innovative technologies
- Winning the talent race
- Building a business-enabling environment
- Supporting data-driven strategic decisions

[5] Eurostat, March 2023. Population projects in the EU. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=682006

1.1. Closing the investment gap

A persistent high-risk investment gap is one of the most critical barriers to building a strong European cybersecurity ecosystem. Addressing this challenge requires more than capital - it demands smart investment, guided by deep sectoral expertise, mentorship, and long-term commitment. ECSO's approach focuses on mobilising both private and public capital, while creating the conditions for sustainable growth and talent retention.

"ECSO will strive to co-develop a fund-of-funds mechanism. It will empower venture capital firms with greater resources to invest in cutting-edge European cybersecurity startups and scale-ups."

ECSO contribution areas

1.1.1 European cybersecurity investment capital

In collaboration with the European Investment Fund, ECSO will strive to co-develop a fund-of-funds mechanism. It will empower venture capital firms with greater resources to invest in cutting-edge European cybersecurity startups and scale-ups.

1.1.2 Investment ecosystem growth

ECSO will continue to foster a vibrant investment ecosystem through targeted matchmaking events (i.e., Cyber Investor Days and Cyber Solution Days), pitching sessions that connect innovators with investors and potential buyers who understand the sector and share a vision for European leadership. These events will support startups with access to finance and business opportunities across Europe. Additionally, ECSO will continue providing curated networking opportunities for VCs and Limited Partners.

1.1.3 European strategic funding for cybersecurity

ECSO will advocate for increased and strategically planned public spending in the cybersecurity area, ensuring that investments in programmes such as DEP, Horizon Europe, and other cybersecurity-relevant initiatives like the European Defence Fund are well-funded and targeted to deliver the greatest possible impact, fostering European strategic digital autonomy. ECSO will also raise awareness of European funding opportunities related to the cybersecurity domain, facilitating synergies between actors and supporting project development, targeting SMEs specifically. See also 1.4.1 and 0 for further information.

1.2. Stimulating demand for European solutions

To build a true European cybersecurity powerhouse, both public and private entities must significantly increase their adoption and purchasing of European cybersecurity products and services. Public procurement, in particular, plays a pivotal role. Besides funding research and innovation, it does so by translating that investment into tangible impact by purchasing the cybersecurity services and solutions developed. The purchasing power of public administrations is a strategic leverage to support European providers and strengthen the market. Likewise, private sector purchasing decisions are equally strategic and essential.

Many European cybersecurity solutions are robust and competitive. Where gaps exist, targeted efforts must be made to close them. This approach will not only strengthen Europe's strategic digital autonomy but also stimulate growth and innovation within its domestic industry.

This push comes at a timely moment, coinciding with the ongoing revision of the EU Directives on Public Procurement[6] - a unique opportunity to embed stronger cybersecurity considerations into procurement frameworks.

ECSO contribution areas

1.2.1 Essential cybersecurity procurement requirements

ECSO will advocate for cybersecurity to be treated as a core criterion in procurement decisions, beyond compliance and cost. It must be recognised as a strategic enabler of resilience, trust, and long-term value.

1.2.2 'Buy European' mindset

ECSO will collaborate with policymakers and industry leaders to promote procurement strategies that ensure European solutions are considered in bidding processes, streamline procedures to align with SME timelines, and foster market consolidation along with the formation of consortia that integrate diverse stakeholders. This approach will also enhance supply chain cybersecurity and contribute to highlighting Europe's technological needs to European organisations.

6 Specifically, Directive 2014/23/EU on the award of concession contracts; Directive 2014/24/EU on public procurement and repealing Directive 2004/18/EC; Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC [2014] OJ L94/243.

1.2.3 European market promotion

ECSO will systematically increase the visibility and adoption of competitive European cybersecurity technologies. This is enabled through The Cyberhive EUROPE, Europe's first pan-European cybersecurity marketplace, and The Cyberhive Matrix, Europe's first quadrant for cybersecurity solutions, along with the Cybersecurity Made in Europe Label, a regional identifier for cybersecurity companies. Overall, ECSO European market promotion goes beyond marketing or analytical efforts in establishing a European benchmark. It is meant to build trust among the European ecosystem.

1.3. Building a business-enabling environment

Europe's fragmented cybersecurity landscape continues to constrain market growth, stifle innovation, and undermine overall resilience. To unleash the full potential of the European cybersecurity ecosystem, a more coherent and business-friendly regulatory environment is essential - one that streamlines compliance for both providers and users.

"To unleash the full potential of the European cybersecurity ecosystem, a more coherent and business-friendly regulatory environment is essential — one that streamlines compliance for both providers and users."

This means moving beyond a patchwork of national rules toward a truly harmonised European framework. A key priority is the swift and consistent implementation of pivotal legislation, including the NIS2 Directive, the Cyber Resilience Act, the revised Cybersecurity Act, and other key regulations. ECSO will advocate for clear, practical guidance and consistent interpretation across Member States, fully aligned with the EU's *Competitiveness Compass*[7] objective of simplifying cybersecurity legislation. Similarly, it will also follow very carefully the development of the *Digital Omnibus*[8] package, for what concerns cybersecurity simplifications aspects.

Furthermore, Europe's diverse markets, business cultures, and languages provide further challenges to European companies trying to grow across the Common Market. Europe's strength lies in its unity. A federated and bottom-up collaboration at the European, national, and regional/local level and between the public and private sector, is needed to facilitate the introduction and growth of different cybersecurity providers across EU markets.

7 A Competitiveness Compass for the EU. For further information, see https://commission.europa.eu/topics/eu-competitiveness/competitiveness-compass_en

8 2025 State of the Digital Decade package, see 2025 State of the Digital Decade package | Shaping Europe's digital future

ECSO contribution areas

1.3.1 EU policy for a unified market

ECSO will engage in strategic policy dialogues and contribute with targeted feedback to broader EU initiatives addressing market fragmentation, such as the 28th Regime, the EU-INC movement, and following adopted initiatives for which ECSO has provided feedback, such as the EU Startup and Scaleup Strategy. In promoting a cybersecurity perspective within these cross-sectoral efforts, ECSO helps ensure cybersecurity remains central to Europe's digital competitiveness agenda.

1.3.2 Regulatory streamlining

ECSO will continue analysing national divergences in cybersecurity policies and promote harmonised approaches, to build a European cybersecurity ecosystem, where organisations and professionals can take advantage of economies of scale and cross-border collaboration. This will contribute to a more efficient, innovation-friendly, and competitive European cybersecurity landscape.

1.4. Accelerating R&D and innovative technologies

Cybersecurity is a foundational enabler of Europe's digital transformation. As the continent advances in technologies like AI, quantum computing, advanced connectivity, cloud, edge, and IoT, through initiatives such as the AI Continent Action Plan and Quantum Strategy, cybersecurity must be embedded from the outset and evolve alongside these innovations.

"Greater uptake of homegrown technologies is essential. Where individual players lack scale, a federated approach is key to delivering robust, integrated European solutions."

Th Europe already offers competitive solutions, but adoption remains limited. Greater uptake of homegrown technologies is essential. Where individual players lack scale, a federated approach - pooling resources and fostering collaboration - is key to delivering robust, integrated European solutions. Technological interoperability across cybersecurity solutions and platforms is essential to enable this federated innovation model, ensuring that diverse technologies can integrate, scale, and evolve cohesively across Europe.

A strong cybersecurity ecosystem also depends on research and development. Europe's R&D capabilities are a major asset, but they must be continuously strengthened and better aligned with market needs. Strategic collaboration between academia and industry is vital to steer research toward high-impact areas and ensure breakthroughs lead to real-world innovation.

To succeed, Europe needs a pan-European perspective that promotes synergies, avoids duplication, and supports joint research. Commercialisation and scaling of innovations should be supported through federated accelerator programmes, ensuring that cybersecurity advances reach the market and reinforce Europe's digital resilience.

ECSO contribution areas

1.4.1 Technological trends and strategic innovation

ECSO will monitor technological trends and emerging technologies, with a particular focus on AI. It will identify areas of European leadership, flag critical gaps requiring strategic investment, and assess the impact of disruptive innovations. A core principle will be advocating for "cybersecurity and resilience by design" to be embedded from the earliest stages of all digital initiatives.

It will also develop and promote a dynamic Strategic Research and Innovation Agenda (SRIA) to guide EU funding programmes such as Horizon Europe and Digital Europe. This agenda will prioritize key areas essential to Europe's digital competitiveness, and long-term resilience.

1.4.2 Innovation synergies

ECSO will champion a federated approach by fostering strong synergies among diverse stakeholders. Advancing technological interoperability across cybersecurity solutions and platforms.

Through dedicated knowledge sharing meetings and brokerage events, ECSO will promote direct cooperation between researchers and industry, ensuring that R&D efforts are both market-driven and commercially viable. Last, ECSO will leverage professional expertise and its market promotion toolbox to analyse and communicate ECSO will facilitate community-driven activities and supporting key institutions such as the ECCC, NCCs, and EDIHs.

1.4.3 European accelerator federation

ECSO aims to build a federation of accelerators and enrich their offerings with input from European communities (investors, CISOs, founders). This network will be linked with innovators and startups. These efforts will help startups to position themselves in different EU markets, attracting investment, and improving the quality of their products. Facilitating market access throughout European countries will support creation of competitive EU champions.

1.5. Winning the talent race

Europe's ambition to lead in cybersecurity must be matched by its ability to retain homegrown talent and attract global experts. In a time of increasing geopolitical tension and digital threats, the stakes are too high to allow a continued brain drain. The departure of skilled professionals to more competitive markets threatens Europe's strategic digital autonomy and its ability to build resilient cyber capabilities.

"To counter this, Europe must position itself not just as a place to work, but as a destination of choice for cybersecurity professionals worldwide."

To counter this, Europe must position itself not just as a place to work, but as a destination of choice for cybersecurity professionals worldwide. The current tightening of immigration policies worldwide presents a unique opportunity for Europe to step up and offer a compelling alternative. By creating an environment where talent can thrive, Europe can become a magnet for global cyber expertise.

This requires a multi-layered strategy. To retain European talent, Europe must offer competitive compensation packages aligned with global benchmarks, ensure clear career progression and leadership pathways, and foster a culture rooted in innovation, purpose, and impact. It is equally important to invest in lifelong learning and internal mobility to keep professionals engaged and evolving, while embedding mentorship and coaching as core pillars of talent development.

Attracting foreign talent calls for decisive measures such as introducing fast-track visa schemes for cybersecurity professionals, recognising international qualifications, and streamlining relocation processes. Europe should also provide targeted tax incentives and relocation support, while promoting its unique value proposition: stability, diversity, and purpose-driven work.

Sustainable talent cultivation begins with embedding cybersecurity into national education systems from an early age and strengthening partnerships between academia, industry, and governments. It also requires expanding vocational training, internships, and hands-on learning opportunities, prioritising inclusion to tap into underrepresented talent pools, including women and minorities, and supporting initiatives like Women4Cyber to empower women in cybersecurity through mentorship, visibility, and community-building. All these efforts must now integrate an AI perspective, to navigate and leverage this transformative technology.

Mentorship is a particularly powerful lever, not only for developing technical and leadership skills, but also for building confidence, networks, and a sense of belonging. Initiatives like Women4Cyber are already demonstrating the impact of structured mentorship in diversifying and strengthening Europe's cyber workforce. By investing in people, removing barriers, and promoting meaningful careers, Europe can secure its digital future and lead by example. Cyber skills and the development of a robust cyber workforce must be recognised as a strategic priority for Europe, as they form the cornerstone of cyber resilience. This imperative should be clearly reflected and reinforced in policy-making at all levels.

ECSO contribution areas

1.5.1 Career pathways development

ECSO's flagship skills initiative, Road2Cyber, is emerging as the central European platform bridging the gap between education, training, and employment in cybersecurity. It offers a comprehensive ecosystem: job listings, training opportunities, a curated talent pool, recruitment tools for employers, and access to initiatives like Youth4Cyber, Women4Cyber, and immersive environments such as cyber ranges.

Through its collaboration with Women4Cyber, Road2Cyber also champions inclusive career development, offering mentorship, visibility, and support to women in cybersecurity. Together, these initiatives are laying the foundation for a competitive, sustainable, and diverse European cyber workforce.

1.5.2 Retention incentives

To prevent the outflow of skilled professionals and make Europe a globally attractive destination for cybersecurity talent, ECSO will work closely with EU and national policymakers to advocate for a comprehensive package of retention and attraction incentives. These include:

- Targeted tax relief for cybersecurity professionals and employers investing in training
- Streamlined immigration and visa pathways for non-EU cyber experts
- Recognition of international qualifications to ease mobility
- Support for relocation and family integration, especially for high-demand roles

1.5.3 Skills foresight

To stay ahead of the curve, ECSO will launch the Foresight Council on the Future of Cybersecurity Skills in Europe, a strategic body tasked with anticipating the skills and roles needed in the next 5–10 years. The Council will analyse:

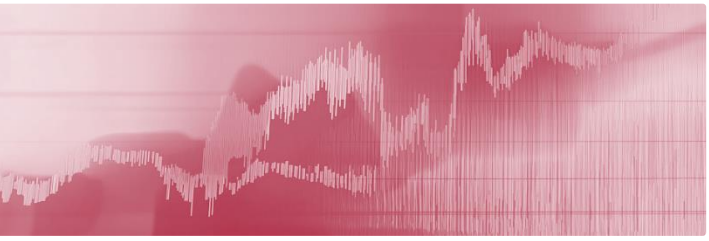
- The impact of emerging technologies (e.g. AI, quantum, IoT)
- Geopolitical and regulatory shifts affecting the cyber workforce
- Demographic and labour market trends
- The evolution of cyber threats and defence capabilities

Its insights will guide education reform, workforce planning, and investment priorities, ensuring that Europe's talent strategies are future-proof, agile, and aligned with its strategic digital autonomy goals.

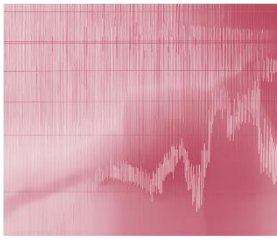
In addition to strategic foresight, the Council will tackle key problem statements facing the future of cyber skills in Europe, in close collaboration with the European Institutions, Agencies, and Member States, in order to propose tangible solutions that feed into key cybersecurity regulations and initiatives.

1.6. Supporting data-driven strategic decisions

Effective strategic decisions in cybersecurity require accurate, timely, and comprehensive data to navigate a complex and rapidly evolving landscape. A robust, data-driven European Cybersecurity Industrial Policy enables policymakers and industry leaders to identify emerging trends, allocate resources efficiently, and strengthen Europe's position in the global cybersecurity market. By leveraging in-depth market intelligence and analytical insights, Europe can foster innovation, support promising ventures, and build a more resilient and competitive cybersecurity ecosystem.



"Effective strategic decisions in cybersecurity require accurate, timely, and comprehensive data to navigate a complex and rapidly evolving landscape."



ECSO contribution areas

1.6.1 Cybersecurity investment analysis

ECSO will monitor and analyse key market trends, including investment flows, mergers, and acquisitions, to inform strategic decision-making in priority, high-impact investments, and informed policymaking.

1.6.2 European cybersecurity market mapping and analysis

ECSO will analyse the European cybersecurity market, among others by mapping of the European cybersecurity landscape, analysing research and innovation activities to provide an overview of capabilities, helping identify leading actors and areas requiring targeted support.

Europe: resilient stronghold

2.

2. Europe: resilient stronghold

In today's volatile geopolitical landscape - shaped by ongoing conflicts within and beyond Europe and increasingly intertwined with cyber threats - strengthening cybersecurity is an existential imperative and a fundamental element of national security.

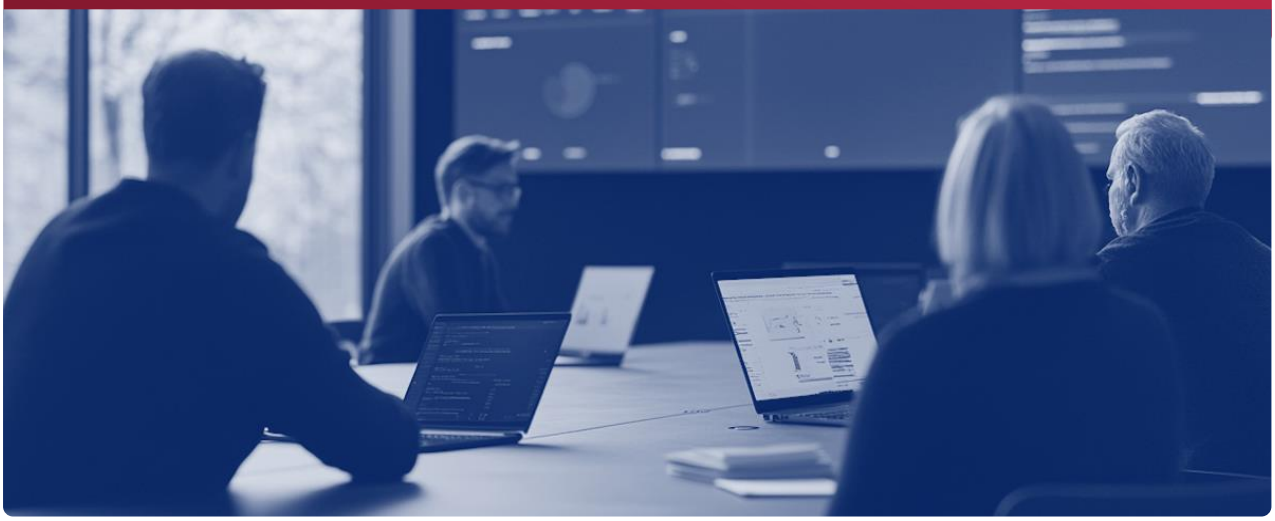
The escalating threat environment underscores the urgent need for a resilient digital infrastructure - one capable of withstanding state-sponsored attacks, cybercrime, and hybrid warfare tactics. This imperative is clearly articulated in strategic frameworks such as *ProtectEU: A European Internal Security Strategy* and the *REArm EU initiative*, both of which call for a decisive strengthening of Europe's collective security and defence capabilities, extending deep into the cyber domain.

Building this Cyber Resilient Europe is a complex and continuous endeavour. It requires not only the development of advanced defensive capabilities, but also efficient applications and consistently effective and proven outcomes. This culture must permeate every layer of society - from critical infrastructure and public services to businesses and individual citizens - ensuring that resilience is not just a technical standard, but a shared European value.

It is equally crucial that Europe's cybersecurity leaders engage actively in key strategic processes.

Especially those that shape strategic and business decision-making. Their participation is vital to building a resilient Europe that is prepared to withstand systemic risks. ECSO stands ready to operationalise Europe's protection ambitions, by supporting the following six initiatives:

- Empowering cybersecurity leaders
- Making compliance seamless
- Protecting critical infrastructure
- Securing digital supply chains
- Promote effective standards and certification
- Bolstering strategic cyber defence capabilities



2.1. Empowering cybersecurity leaders

Europe must shift its approach to cybersecurity leadership and start acting united. Chief Information Security Officers (CISOs) and other cybersecurity leaders must be empowered and fully integrated into strategic business decision-making processes. They are increasingly held liable for cybersecurity incidents while they lack financial, human and operational resources to design and implement effective strategies. The size of challenge, on one hand, and the efforts poured into it by cybersecurity leaders should be acknowledged. To address this, cybersecurity must evolve from a technical afterthought into a core pillar of business strategy, embedded from the outset in every major initiative.

"Europe must shift its approach to cybersecurity leadership and start acting united. Chief Information Security Officers (CISOs) and other cybersecurity leaders must be empowered and fully integrated into strategic business decision-making processes."

At the same time, cybersecurity leaders must embrace a proactive approach. To achieve this, they need actionable insights that enable informed, timely decisions. This is where Cyber Threat Intelligence (CTI) becomes an indispensable cornerstone of organisational resilience enabling companies to anticipate and neutralise threats before they materialise. Automated, timely, and relevant CTI, enhanced by AI, can no longer remain a privilege of large enterprises. It must be accessible to all. Effective intelligence sharing depends on trusted platforms and participants, ensuring secure, real-time information exchange across sectors and borders.

Building a strong, connected European professional ecosystem is essential to achieving these goals. Cybersecurity specialists need structured opportunities to learn from one another, exchange critical insights, and collaborate on threat mitigation. ECSO is committed to fostering a truly European collaborative ecosystem that strengthens Europe's collective resilience against evolving cyber threats.

ECSO contribution areas

2.1.1 ECSO CISO Community

ECSO will actively support and leverage and further grow its dynamic CISO network, currently comprising over 650 European professionals. This network extends even further through nine national chapters of the ECSO CISO Community and 5 strategic partnerships with leading national CISO organisations across Europe, broadening our network impact to reach over 1000 professionals indirectly.

This vibrant community serves as a trusted forum for peer exchange, knowledge sharing, and collaborative problem-solving, supported through targeted activities, events, an annual conference, and strategic dialogue.

2.1.2 Cyber Threat Intelligence

ECSO will create an information sharing environment, in collaboration with its Members, where cybersecurity professionals can collectively assess emerging threats, share mitigation strategies, and develop coordinated response measures.

2.2. Making compliance seamless

As cybersecurity regulations across Europe continue to evolve, organisations face increasing pressure to navigate complex compliance landscapes while maintaining operational resilience. Effective cybersecurity governance is no longer optional. If Europe wants to protect their vital organisations, helping stakeholders interpret, implement, and align with regulatory frameworks is mandatory.

"Organisations face increasing pressure to navigate complex compliance landscapes while maintaining operational resilience. Effective cybersecurity governance is no longer optional."

This includes both fostering collaboration between public authorities, industry leaders, and solution providers as well as relying on automation, AI, and machine-readable products. By promoting structured knowledge exchange and practical support, Europe can build a more coherent, innovation-friendly cybersecurity ecosystem that empowers organisations to meet compliance obligations confidently and efficiently.

ECSO contribution areas

2.2.1 Public policy orientation

ECSO will monitor the implementation of EU cybersecurity legislation across Member States, ensuring strategic oversight and providing practical support. This includes identifying gaps and inconsistencies, and equipping stakeholders with the resources needed to meet regulatory requirements effectively. To this end, ECSO will also identify and promote policy measures that reduce compliance burdens and foster a more agile, efficient, and effective European cybersecurity market. Legislative piloting and sandboxes can be used to test new legislative frameworks in controlled environments before full-scale adoption, ensuring that rules are practical, innovation-friendly, and aligned with market realities.

2.2.2 Cybersecurity governance knowledge exchange

ECSO will foster mutual understanding and collaboration through targeted knowledge-sharing sessions and structured peer-to-peer dialogues on cybersecurity governance and compliance. These engagements will connect public authorities, solution providers, and industry stakeholders to share insights, best practices, and practical approaches to regulatory compliance.

2.2.3 Compliance efficiency

ECSO will investigate the development and adoption of standardised schemes and frameworks designed to facilitate, and eventually automate, interoperability between frameworks and standards. By simplifying regulatory mapping, automating control assessments, and enhancing transparency across cybersecurity compliance processes, ECSO aims to improve compliance processes for end-users, third-party providers, and national authorities through time savings and efficiency gains. This initiative will help organisations reduce manual overhead and reallocate resources from costly assessment practices to actually improving protection.

2.3. Protecting critical infrastructure

Europe's critical infrastructure forms the backbone of our digital society. Protecting it requires tailored cybersecurity approaches that address each sector's unique operational challenges and regulatory requirements while maintaining shared resilience standards. As sector-specific legislation continues to proliferate, ECSO will support operationalisation of these policies, ensuring they adequately address sectoral requirements without redundancy and with a focus on the critical infrastructure and sectors already highlighted in EU frameworks.

ECSO contribution areas

2.3.1 Risk management support

ECSO will support the creation of resources for risk management frameworks to help organisations implement requirements of EU cybersecurity policies.

2.3.2 Sectoral policy analysis

ECSO will monitor and analyse critical sector cybersecurity policies, such as DORA, the EU Space Act, and the Healthcare Cybersecurity Action Plan.

2.4. Securing digital supply chains

Securing digital supply chains must become a top priority for Europe's cybersecurity agenda. As highlighted in key regulatory frameworks such as NIS2, DORA, and the Cyber Resilience Act (CRA), cybersecurity requirements must be deeply and effectively embedded across the entire supply chain ecosystem.

However, this cannot be reduced to a theoretical exercise or a checkbox compliance activity. It must translate into real, measurable improvements in cybersecurity. At the same time, these efforts must be proportional and practical, avoiding undue burdens on businesses - especially SMEs - while ensuring meaningful protection.

The well-known principle of risk-based security must be further developed to facilitate implementation. This includes establishing baseline requirements and segmenting actions according to risk profiles. Moreover, it is vital to ensure that European cybersecurity solutions capable of meeting these regulatory demands gain visibility and traction in the market.

ECSO contribution areas

2.4.1 Harmonised supply chain cybersecurity

ECSO will develop a unified approach to streamline and replace fragmented, burdensome practices with a more effective and scalable model for securing digital supply chains.

2.4.2 Mutual recognition agreements

ECSO will support the establishment of mutual recognition mechanisms for cybersecurity frameworks, standards and certification, such as conformity assessment for CRA-compliant products, enabling secure and seamless cross-border operations.

2.5. Promote effective standards and certification

Europe has a longstanding tradition and experience in product certification and assurance. As cybersecurity legislation expands, standardisation and certification have a large impact on raising cybersecurity maturity. In addition, a robust standardisation and certification ecosystem will also create a level playing field for SMEs to enter the market and enhance the competitiveness of European solutions by providing clear, trusted assurance to customers and partners worldwide.

However, certification, and in general compliance with policies and legislations, entails costs in terms of time to market and budget. Leveraging certified components and international standards require robust models and approaches, such as composition-based conformity, to accelerate time-to-market and reduce fragmentation. ECSO is ready to raise awareness and provide guidelines for an ecosystem that is efficient, scalable, and aligned with Europe's strategic objectives.

ECSO contribution areas

2.5.1 Standards and certification awareness

ECSO will raise awareness of and guide the adoption of cybersecurity standards and certification schemes that validate the security of components and services, reinforcing trust and transparency across the ecosystem. ECSO will build on existing collaboration with relevant standardisation bodies and institutions.

2.5.2 Composition-based conformity approach

ECSO will propose practical summaries and examples of composition beyond Common Criteria and EUCC, exploring re-usability of previous assessments in other contexts, such as the CRA. In particular, ECSO will look into how the process of designing and making complex products available to the market can benefit from its underlying pre-assessed base of components.

2.5.3 Community engagement for standardisation

Through initiatives such as Cyberstand.eu, ECSO will support European experts and coordinate communities to ensure strong, unified participation in international cybersecurity standardisation efforts and global technical working groups.

2.6. Bolstering strategic cyber defence capabilities

Europe must prioritise the development of strategic cybersecurity capabilities to protect its most vital assets - from critical infrastructure and military systems to the rapidly expanding domain of space technologies. This imperative comes at a pivotal moment, as NATO agreed to raise defence spending to 5% of GDP (with 1.5% dedicated to innovation), and the European Union prepares a strategic plan to mobilise approximately €800 billion in defence investments over the coming years[9].

To ensure these investments deliver maximum impact, Europe must adopt a coordinated approach that avoids fragmentation and redundancy, while enabling seamless interoperability across national and sectoral boundaries.

Strategic cybersecurity investments will not only strengthen Europe's security posture but also drive strategic competitiveness by fostering innovation and leadership in cutting-edge defence and dual-use technologies. Including startups delivering the most innovative cybersecurity solutions must be integral to these efforts, serving as engines of agility, technological progress, and disruptive capability within Europe's evolving security ecosystem.

"Europe must anticipate and neutralise threats before they materialise. This requires continuous investment in threat intelligence exchange, scenario-based planning, and the development of threat-driven strategies that keep pace with an evolving and increasingly complex threat landscape."

Equally important is a shift in mindset: from reactive to proactive cybersecurity. Europe must anticipate and neutralise threats before they materialise. This requires continuous investment in threat intelligence exchange, scenario-based planning, and the development of threat-driven strategies that keep pace with an evolving and increasingly complex threat landscape.

[9] 'The Hague Summit Declaration'. For further information, see https://www.nato.int/cps/en/natohq/official_texts_236705.htm

ReArm Europe Plan/Readiness 2030. For further information, see https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en

ECSO contribution areas

2.6.1 Dual-use technologies

ECSO will actively contribute to the development of a roadmap for dual-use cybersecurity technologies for civil, defence, and space, and promote existing European capabilities.

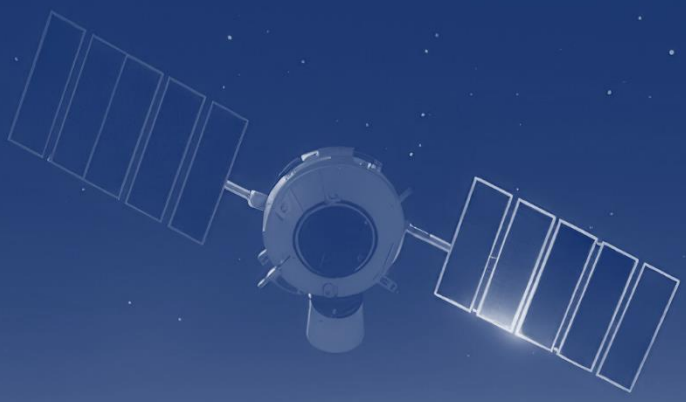
2.6.2 Cybersecurity for space

ECSO will contribute to Europe's cybersecurity strategy for space applications, highlighting their dual-use nature and supporting decision-makers in navigating this emerging challenge.

2.6.3 Civil-military cooperation

ECSO will contribute to building specialised communities and facilitate dialogues among expert networks from both the civilian and military sectors, enabling knowledge exchange, collaboration, and strategic foresight

Europe: global shaper



3.

3. Europe: global shaper

Europe's ambition must extend beyond its borders, toward actively shaping the global cybersecurity landscape. This vision aligns with the principles set out in *An International Digital Strategy for the EU*, and represents a strategic opportunity to project Europe's values, standards, and capabilities on the world stage.

By exporting its high cybersecurity standards - rooted in trust, transparency, and fundamental rights - Europe can help shape a more secure and open digital world. At the same time, this global engagement, leveraging initiatives like the Global Gateway, offers a powerful lever for economic growth, enabling European technologies, services, and expertise to thrive in international markets.

Europe plans to continue to lead through dialogue and cooperation with like-minded partners, engaging from a position of equal partnership. It must not only offer its best practices and regulatory leadership, but also its cutting-edge technologies and exceptional talent.

Crucially, the private sector must be at the heart of this global effort.

European companies - from startups to global providers - are essential ambassadors of Europe's cybersecurity excellence and must be empowered to contribute to shaping global norms, standards, and innovation. ECSO stands ready to support this global engagement, through its strategic initiative on Advancing Europe's international role.

3.1. Advancing Europe's international role

Europe's leadership in cybersecurity depends on its ability to shape global standards and governance frameworks. This requires sustained engagement in international bodies, strategic partnerships, and alignment with like-minded partners. Europe's voice must be coordinated, inclusive, and values-driven. Mobilising a broad coalition, including industry, academia, and civil society, is essential to ensure that European priorities and technical excellence are reflected in global frameworks. At the same time, fostering regulatory alignment and mutual recognition with international partners will simplify cross-border operations and promote a more cohesive global digital environment.

In this context, we must also actively support global expansion, strengthen recognition of European businesses, and showcase our solutions capabilities. That is why ECSO stands ready to actively support flagship initiatives such as the European Tech Business Offer and the Global Gateway, promoting trusted and competitive European solutions on the global stage.

ECSO contribution areas

3.1.1 International regulatory cooperation and knowledge transfer

ECSO will act as a platform for structured dialogue between European experts and international partners, helping translate EU cybersecurity regulations and their related technical standards (e.g. NIS2, CRA, and DORA) into actionable guidance for global adoption. This includes supporting regulatory alignment and capacity building in partner countries, such as Ukraine and Moldova, through dedicated projects and expert engagement.

3.1.2 European solutions on the global stage

ECSO will promote the integration of European cybersecurity solutions in global digital development, particularly within EU-led infrastructure investments abroad. This will strengthen global cybersecurity resilience and expand market opportunities for European providers.

ECSO will also engage international stakeholders through strategic dialogues, Digital Partnerships, and commercial missions. It will support European trade delegations to major global conferences, helping startups and scale-ups access non-European markets. These efforts will showcase European technologies, foster innovation, and stimulate cross-border cooperation and investment.

What's Next?

The cybersecurity landscape is constantly changing, like everyone loves saying. For this reason, our *Strategic Vision for European Cybersecurity* should be seen as a living document, reviewed and updated regularly. In the meantime, we welcome any feedback the European cybersecurity community may have. In line with ECSO's nature, we will continue to continuously engage with all stakeholders, listening to and giving space to all voices of the cybersecurity ecosystem.

EMPOWERING EUROPEAN CYBERSECURITY COMMUNITIES

Acknowledgements

We would like to express our sincere gratitude to the Members of the ECSO Board of Directors and the Chairpersons of ECSO's Working Groups and Workstreams for their invaluable contributions to the development of this vision.

ECSO Board of Directors

Associations
Arnaud Dechoux (Alliance pour la Confiance Numérique (ACN))
Xabier Mixelena (AEI Ciberseguridad)
Frank Van Caenegem (CESIN)
Paolo Grassia (CONNECT EUROPE)
Willi Mannheims (Eurobits)
Juha Remes (North European Cybersecurity Cluster)
Alexander Schellong (TeleTrusT – IT Security Association Germany)

Investors
François Lavaste (Tikehau Ace Capital)

Large Companies
Thierry Racaud (Airbus)
Günter Koinegg (Atos)
Andy Garth (ESET)
Aldo Sebastiani (Leonardo)
Jean-Michel Brun (Schneider Electric)
Gerd Müller (Secunet Security Networks AG)
José Lucio González Jiménez (SGS Group)
Karim Asser Nassim (Sopra Steria)
Alexis Caurette (Thales)
Tiina Sarhimaa (WithSecure)

National Public Administrations
Luca Nicoletti (Agenzia per la Cybersicurezza Nazionale (IT))
Marek Zeman (Cyber Security Competence and Certification Centre (SK))
Märt Hiietamm (Information System Authority, Republic of Estonia (RIA) (EE))
Miguel Ángel Cañada (Instituto Nacional de Ciberseguridad (INCIBE), Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), Centro para el Desarrollo Tecnológico y la Innovación (CDTI) (ES))
Michal Pukaluk (Ministry of Digital Affairs of Poland (PL))
Krzysztof Szubert (National Institute of Telecommunications (PL))
Dan Cimpean (Romanian National Cyber Security Directorate (RO))

Regional Public Administrations
Javier Dieguez (CYBERZAINTZA (ES))

Research and Technology Organisations (RTOs) and Universities
Nizar Touleimat (Commissariat à l'Energie Atomique et aux Energies (CEA))
Fabio Martinelli (Consiglio Nazionale delle Ricerche (CNR))
Ana Ayerbe (Fundación Tecnalia Research & Innovation)
Kai Rannenberg (Goethe Universität)

Small and Medium Enterprises (SMEs)
Anett Madi-Nator (CyEx)
Sebastiano Taffaletti (European Digital SME Alliance)
Michel Bosco (Nexova)
Miguel A. Juan Bello (S2 Grupo)

Users and Operators
Matthias Muhlert (Die Oetker Gruppe)
Giorgio Cusma Lorenzo (Intesa San Paolo)
Alessandro Menna (Italgas)

ECSO Working Group on Trusted Supply Chains

Working Group
Costantinos Tsiourtos (KINEAS)
Roland Atoui (Red Alert Labs)
Mario Jardim (Schneider Electric)

Workstream for Preparing Members for CRA Implementation
Shadi A Razak (Angoka)
Patricia Shields (Cyber Cert Labs)
Mariano J Benito (GMV)

Workstream on Compliance & Implementation of Legislation
Marta Przywała (SAP)

Workstream on Trusted Supply Chain Implementation
Thomas Stubbings (KSO)

ECSO Working Group on Market Development

Workstream on Investments
Carlos Moreira da Silva (33N Ventures)
Carlos Alberto Silva (33N Ventures)
Willi Mannheims (eCAPITAL)
Elisabetta Vesconi (Planven)
François Lavaste (Tikehau Capital)
Michael Lucassen (TIN Capital)

Workstream on Regional Approaches
Aude Ollivier-Cadoret (Bretagne)
Mònica Espinosa Garcés (Catalonia Region)
Kayle Giroud (Global Cyber Alliance)
Kiril Grigorov (Union for Private Economic Enterprise (UPEE))
Gianluca Vannuccini (Tuscany Region)

Workstream on SME2Market
Eoin Byrne (Cyber Ireland)
Jörg Audörsch (ESCRA)
Pierre Calais (PRCONSEIL/NEOSMOS)
Régis Cazenave (S2 Grupo)
Ignacio Sbampato (Whalebone)

ECSO Working Group on Cyber Threat Management

ECSO CISO Community Workstream
Paul Bayle (Atos)
Matthias Muhlert (Die Oetker Gruppe)
Olivier Caleff (Erium)
Frank Van Caenegem (Schneider Electric)
Stephane Lenco (Thales)

Workstream on Risk Management Policies Implementation
Mariano Benito, Cybersecurity (GMV)
Dr Ali Mabrouk (Sama Partners)

ECSO Working Group on Skills and Human Factors

Working Group
Almerindo Graziano (CYBER RANGES)
Csaba Virag (CYBER RANGES)
Solveig Walsøe Pettersen (Secure Practice)
Gabriele Lenzini (University of Luxembourg)

Skills & Job Workstream
Jacqueline Kehoe (Cyber Ireland)
Manuel Avramescu (ISC2)
Vanessa Lewis (Nexova Group)

Training & Cyber Ranges Workstream
Donna O'Shea (Cyber Ireland)
Csaba Virag (CYBER RANGES)
Almerindo Graziano (CYBER RANGES)
Gustavo Frega (ISACA)
Artūrs Filatovs (LIKTA)

Education & Awareness Workstream
Deborah White (Cyber Ireland)
Marcello Hinxman-Allegri (CYBER RANGES)
Stewart James Kowalski (NTNU - Norwegian University of Science and Technology)
Christine Petr (Université Bretagne Sud)

ECSO Working Group on Research and Innovation for European Cybersecurity

Working Group
Fabio Martinelli (CNR)
Fabio Cocurullo (Leonardo)
Volkmar Lotz (SAP)
Ana Ayerbe (Tecnalia)

Workstream on Ecosystem
Cristian Petrollini (RHEA Group)
Ana Ayerbe (TECNALIA)

Workstream on Digital Transformation in Verticals
Adriana Frejtas (APWG.EU)
Mònica Espinosa Garcés (Cybersecurity Agency of Catalonia)
Paolo Roccetti (Engineering)

Workstream on Data & Economy
Manel Medina (APWG.EU)
Evangelos Markatos (FORTH - Foundation for Research and Technology – Hellas)
Herve Debar (IMT - Institut Mines-Télécom)

Workstream on Basic & Disruptive Technologies
Patricia Mouy (CEA)
Matthias Hiller (Fraunhofer)
Javier Lopez (University of Malaga)

Workstream on Strategic Roadmap and Foresight to Competitiveness
Adriana Freitas (APWG.eu)
Paolo Roccetti (Engineering)
Evangelos Markatos (FORTH - Foundation for Research and Technology - Hellas)
Herve Debar (IMT - Institut Mines-Télécom)
Javier Lopez (University of Malaga)

Workstream on Dual-use Cyber Technologies for Defence
Anett Madi-Nator (Cyex)
Angel Gavin (GMV)
Matteo Merialdo (RHEA Group)
Adrien Becue (Thales)

Workstream on Cybersecurity for Space Applications
Shadi A Razak (Angoka)
Marios Thoma (Cyberecocul)
Julio Vivero (GMV)
Matteo Merialdo (Nexova)

ECSO Secretariat

Leadership Team
Joanna Świątkowska
Roberto Cascella
Nina Olesen
Emilie Jonckheere
Cristian Tracci

Working Group Management Team
Sebastijan Čutura
Matteo Molé
Francisco Andrade e Silva
Arnaud de Vibraye
Guillermo Ferrer Hernáez
Anne-Sophie Van Vaerenbergh
Simona Kaneva
Daniele Dionisi
Tomasz Michałowski
Aistė Merfeldaitė
Angèle Billaud
Claudia Comandini

Outreach Team
Victoria Cristiano
Pablo Robles Hernández
Matteo Nicolussi
Patrick Vandewalle
Vasiliki Lada

HR
Chloe Peirce

Avenue des Arts 46, 1000, Brussels (Belgium)
secretariat@ecs-org.eu
www.ecs-org.eu