THE DIGITAL FRONT LINE

15 actions to boost Europe's Digital Resilience

DIGITALEUROPE

FOREWORD

The Ukraine war is the first hybrid war blurring the lines between physical and non-physical threats.

What role will digital technology play in this striking paradigm shift? And how vital is it for our societies to be digitally resilient?

Digital resilience emerged as a new central societal concept during the Covid 19 pandemic, and it has become even more critical following the Russian invasion of Ukraine and the recent heart-breaking earthquakes in Turkey and Syria.

> **Digital Resilience refers to our ability as a society to use digital technologies to prevent and face crises like pandemics, natural disasters, cyberattacks and hybrid wars, while sustaining our financial and security assets.**

Digital Resilience is highly reliant on the close collaboration between the private tech sector and the public sector. While the latter holds the institutional decision-making process for common good, the private sector holds the key to most of today's tech innovation and the digital infrastructure required to swiftly face and recover from any severe disruption.

At a time of rising hybrid threats, Europe's security is heavily dependent on its ability to foster a strong public/private partnership while providing the appropriate conditions for digital companies to scale up and grow in Europe.

In this paper we will look at four pillars of Digital Resilience:

1. **Cybersecurity and cyber governance**
2. **Digital Infrastructure**
3. **Supply Chain resilience**
4. **Agile procurement mechanisms for Emerging and Disruptive Tech (EDTs)**

If you are a policy maker or a professional in the digital resilience domain, looking for some actionable ideas on how to collaborate with the private sector, please read on. Or if you are a start-up or a scale-up wondering about ways to navigate the complex routes of EU and NATO procurement, we have you covered.

And lastly, if you are a citizen interested in the role of the digital sector in shielding our societies from the rising hybrid threats, this publication is for you.

Over a
40%
INCREASE IN CYBERATTACKS
in 2022

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

TABLE OF CONTENTS

WHAT IS Digital Resilience?

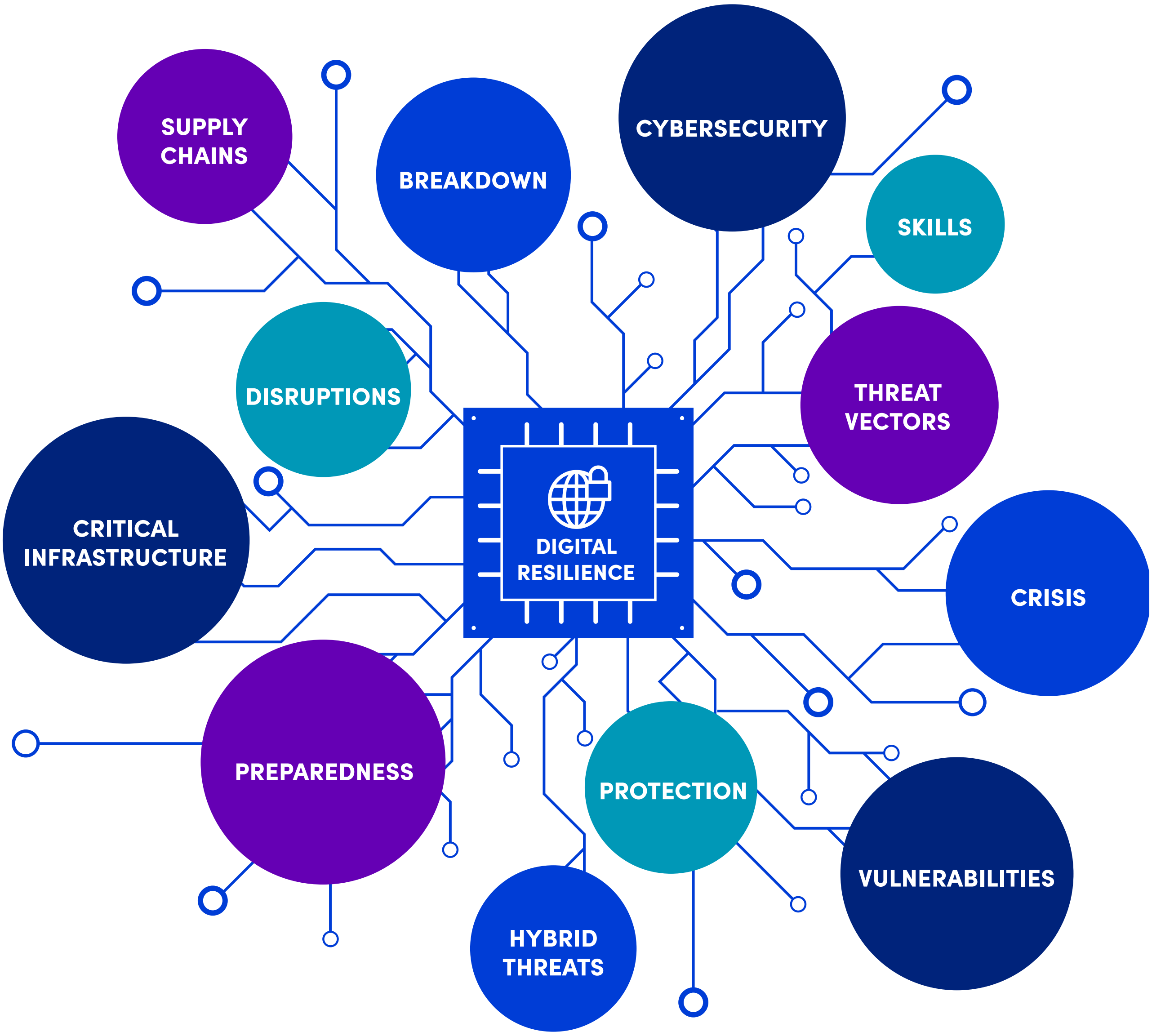
In the words of the NATO Deputy Secretary General Mircea Geoană: "We live in a world where digital borders matter as much as physical ones."

Digital resilience is about building our capacity as a society to use the powerful potential of digital technologies to prepare for and protect ourselves against a range of present and future challenges and threats. This could include cyber-attacks, disinformation campaigns, natural disasters, emerging infectious diseases or – as we have seen in the last year – war.

No government can build digital resilience on their own. This requires developing a strong and inclusive governance model involving the private tech sector and adopting strategies and practices that promote safety, citizens' awareness, and the use of the latest digital tools to stay ahead of bad actors.

> "DIGITAL RESILIENCE MUST BE SEEN AS AN INTEGRAL PART OF EUROPEAN SECURITY."

It involves:



WHY does it matter?

61%

The healthcare sector remains a prime target for cyber attacks, with a 61% increase in reported incidents in 2021

(Source: ENISA)

38%

increase in global cyberattacks in 2022

(Source: Check Point Research)

1 M

It is estimated that Europe lacks around a million of cybersecurity professionals

(Source: International Association of Information Technology Asset Managers (IAITAM))

17%

Attacks on supply chains represented 17% of intrusions in 2021

(Source: European Council)

17%

The value of the EU cybersecurity market is estimated at more than €130 billion and it is growing at a rate of 17% a year

(Source: ENISA)

€4.4 M

In 2021, the average cost of a data breach in Europe was €4.4 million

(Source: IBM)

102%

Ransomware attacks increased by 102% in Europe in the first half of 2021, with an average demand of $570,000 per incident

(Source: Check Point Research)

Only **48%** of European organizations believe they can prevent a ransomware attack, and only 32% have a cybersecurity insurance policy

(Source: Hiscox)

28%

of European SMEs experienced at least one type of cybercrime in 2021

(Source: Eurobarometer)

660

The EU has more than 60. 000 cybersecurity companies and more than 660 centres of cybersecurity expertise

(Source: European Research Executive Agency)

15%

As of June 2022, 15% of the internet infrastructure in Ukraine has been destroyed by Russia

(Source: European Council)

The infographic shows the extent to which hybrid threats have risen in the past year. However, instead of panicking, we should use it as an opportunity to prepare ourselves. Why? Because:

1 **Hybrid threats are difficult to detect:** Hybrid threats often involve multiple tactics and techniques, making them hard to detect and defend against.

2 **Hybrid threats can cause significant damage:** Hybrid threats can have a wide-ranging impact, from financial losses to damage to critical infrastructure, loss of sensitive data, and more. They can also be used to disrupt society, sow discord, and undermine trust in institutions and governments.

3 **Preparation is key:** To effectively defend against hybrid threats, we need to be prepared with a comprehensive approach that includes people, processes, and technology.

> **“Being prepared for hybrid threats is vital. The private sector as a creator of innovation should be strongly involved so that we can stay ahead of the game.”**

HOW can we boost Europe's digital resilience?

The answer is comprised of four pillars. We need:

1

A strong and inclusive cybersecurity and cyber governance:

The ability to react swiftly and in a unified way to cyber threats.

2

A solid and reliable critical infrastructure:

The ability to create and utilise critical platforms and tools needed to detect and handle hybrid threats.

3

Resilient supply chains:

The ability to access the components and materials needed for a digital society to function.

4

Fast-track procurement for critical Emerging & Disruptive Technologies (EDTs):

The ability for Europe and its allies to encourage innovation and stay one step ahead of its adversaries.

Inclusive cybersecurity and cyber governance

Today, the concept of digital resilience has taken on a new dimension with a soaring level of global threats caused by the Russian invasion of Ukraine. There has been **over a 40% increase** in cyberattacks in 2022 compared to 2021 globally. The healthcare sector was the most targeted industry for ransomware during the third quarter of 2022, **with one in 42 organisations impacted by ransomware**.

The picture of who or what is responsible for Europe's cybersecurity is complex. Many different overlapping institutions govern individual aspects, from strategy to skills to crisis response (see figure below). Within the EU, cybersecurity is also divided 27 times – with different bodies per member state – and into civil and military camps. Cooperation with international partners and the private sector adds an extra layer of complexity onto an already tangled picture of governance.

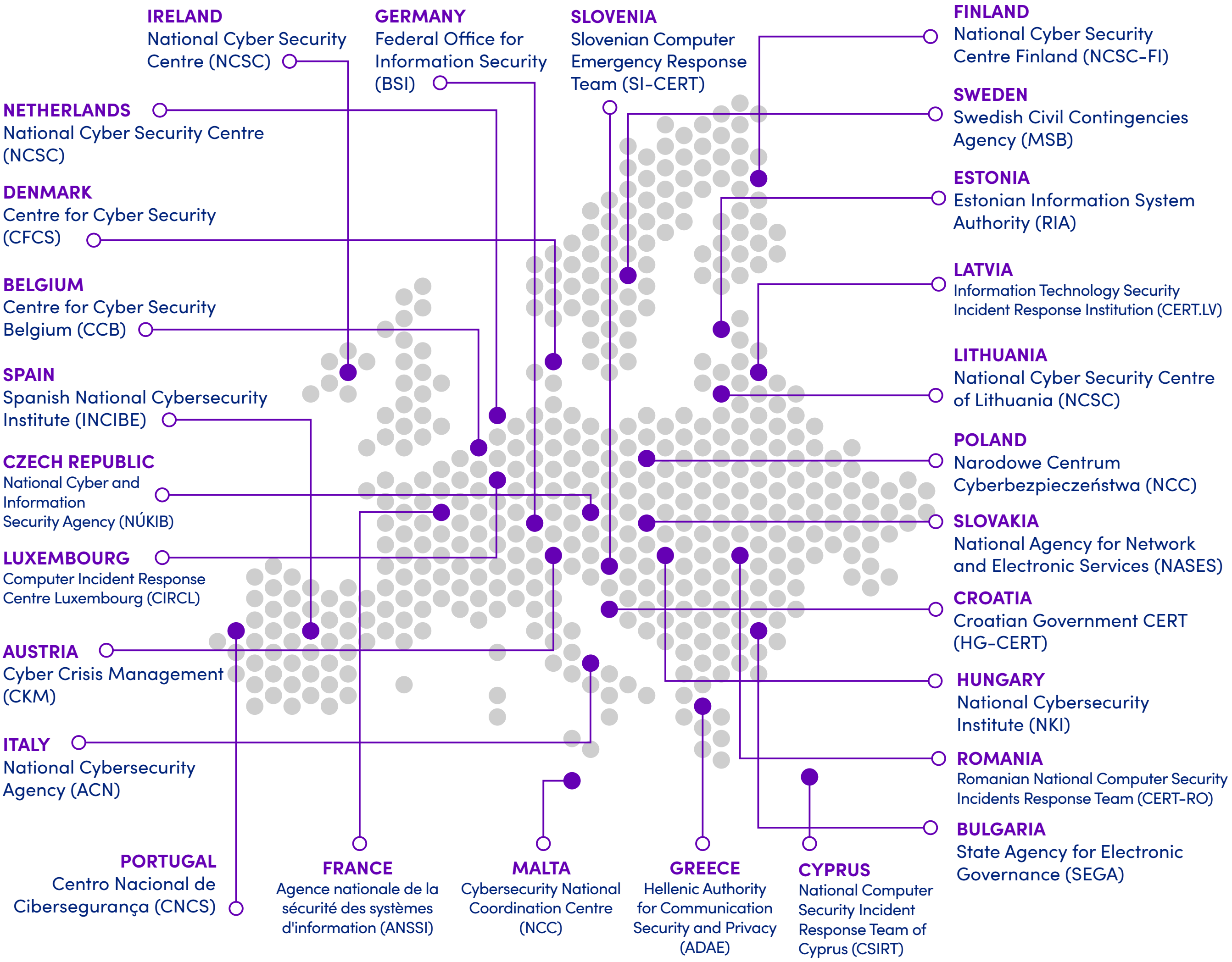
It begs the question, who is in charge if a large-scale attack occurs?

The EU recently put forward its new Cyber Defence Policy, which aims to pull together these different strands. We need to find a way to collectively act quickly when attacked, through a clear chain of command.

Unlike traditional defence, the private sector is both the supplier of technology but also the first line of defence. Any cyber defence governance should reflect this fact and embed private sector experts into the process, moving beyond traditional concerns about information sharing. Again, the Ukraine war has shown more agile ways of public-private cooperation, but also the limitations of an ad-hoc approach where individual companies were sought for help without a proper structure in place.

Who is involved? The state of play

NATIONAL



IRELAND
National Cyber Security Centre (NCSC)

GERMANY
Federal Office for Information Security (BSI)

SLOVENIA
Slovenian Computer Emergency Response Team (SI-CERT)

NETHERLANDS
National Cyber Security Centre (NCSC)

DENMARK
Centre for Cyber Security (CFCS)

BELGIUM
Centre for Cyber Security Belgium (CCB)

SPAIN
Spanish National Cybersecurity Institute (INCIBE)

CZECH REPUBLIC
National Cyber and Information Security Agency (NÚKIB)

LUXEMBOURG
Computer Incident Response Centre Luxembourg (CIRCL)

AUSTRIA
Cyber Crisis Management (CKM)

ITALY
National Cybersecurity Agency (ACN)

PORTUGAL
Centro Nacional de Cibersegurança (CNCS)

FRANCE
Agence nationale de la sécurité des systèmes d'information (ANSSI)

MALTA
Cybersecurity National Coordination Centre (NCC)

GREECE
Hellenic Authority for Communication Security and Privacy (ADAE)

CYPRUS
National Computer Security Incident Response Team of Cyprus (CSIRT)

FINLAND
National Cyber Security Centre Finland (NCSC-FI)

SWEDEN
Swedish Civil Contingencies Agency (MSB)

ESTONIA
Estonian Information System Authority (RIA)

LATVIA
Information Technology Security Incident Response Institution (CERT.LV)

LITHUANIA
National Cyber Security Centre of Lithuania (NCSC)

POLAND
Narodowe Centrum Cyberbezpieczeństwa (NCC)

SLOVAKIA
National Agency for Network and Electronic Services (NASES)

CROATIA
Croatian Government CERT (HG-CERT)

HUNGARY
National Cybersecurity Institute (NKI)

ROMANIA
Romanian National Computer Security Incidents Response Team (CERT-RO)

BULGARIA
State Agency for Electronic Governance (SEGA)

EU LEVEL

- **European Defence Agency** (EDA)
- **European Cybersecurity Competence Centre** (ECCC)
- **European Union Agency for Cybersecurity** (ENISA)
- **European Union External Action Service** (EEAS)
- **EU CyberNet**
- **Computer Emergency Response Team for the EU Institutions, bodies and agencies** (CERT-EU)
- **National Computer Security Incident Response Teams** (CSIRTs)
- **EU Cyber Crisis Liaison Organisation Network** (CyCLONe)
- **Security Operation Centres** (SOC)
- **The European Cybercrime Centre** ('EC3')
- **Defence Permanent Structured Cooperation** (PESCO)

INTERNATIONAL TRANSATLANTIC

- **North-Atlantic Treaty Organisation** (NATO): Brussels, Belgium
- **NATO Cooperative Cyber Defence Centre of Excellence** (CCDCOE)
- **EU-US Cyber Dialogue**

The above diagram maps out the many agencies, departments and other actors involved in Europe's cyber defence. It is far from being a comprehensive list and yet we can make the following conclusions:

- The network of involved players is extremely wide and complex, which makes it hard to shape a straightforward and inclusive cyber governance model.
- There is no representation of the private sector in the current cyber defence bodies, which could undermine the relevance and impact of cyber policies.
- There is an urgent need to streamline the network of stakeholders to avoid losing a clear sense of direction and slowing down action due to a lack of proper coordination.

EU-NATO collaboration

For the EU, NATO and the democratic world to face and defeat current and imminent hybrid threats, they need to perceive the private sector as a critical partner that can play a key role in responding to cyber-attacks and promoting rapid recovery.

The EU and NATO bolstered their strategic partnership in January 2023 by signing the 3rd declaration on EU-NATO cooperation which demonstrated the vital importance of a strong transatlantic bond.

The Russian invasion of Ukraine has deepened dialogue between the two institutions and has opened new avenues of cooperation.

We believe an impactful EU-NATO partnership should be built on:

- A strong push for the development of cutting-edge emerging and disruptive technologies
- Alignment on cybersecurity and other technical standards to cut down on red tape and reduce bureaucracy.
- Alignment on procurement standards: the EU and NATO should co-establish a clear and efficient procurement framework to enable companies, especially SMEs, to access public tenders and benefit from a fair competition.

Skills gap

Whoever has the skills, has the power. Skills are crucial to building our society's digital resilience. Despite the current rising hybrid treats, there has been very little focus on sourcing critical security talent. Both the public and private sectors report difficulties in finding people with the right skill set.

Europe lacks between 350,000 and one million cyber specialists, for example. In addition, most children leave school without basic computer science knowledge, in contrast to other regions around the world.

To fill this gap, it will require the companies, governments, schools, and universities to work together. What better time to start than 2023, the European Year of Skills.

Actions

1. A joint EU Rapid Reaction Team including the private sector

Recently, great progress has been made coordinating the work of the various Computer Emergency Response Teams (CERTs) across Europe. The creation of the Joint Cyber Unit to improve coordination and speed of response is a great step in the right direction.

The next step is to move beyond coordination and introduce more specific obligations for information sharing and a clear chain of command. Private sector CISOs should also play a stronger role in the event of an attack.

2. A Joint Public-Private Expert Unit embedded in the EU's cyber defence policy

The Unit would be comprised of CISOs of leading companies operating in Europe and would provide strategic input on cooperation and preparedness prior to an attack, as well as advise on certification, the 'cyber reserve' of trusted providers, and the priorities for the Cyber Skills Academy.

3. Interoperability based on common standards

Interoperability will be crucial for our cyber defence. We cannot cooperate with likeminded partners if our shields don't fit together.

The Unit mentioned above should liaise regularly with the EU's High Level Forum on European standardisation, and be used to cooperate in standards-setting bodies. NATO can also play an important role as a standards adopter, as is the case for military hardware.

4. A network of cyber campuses and compulsory computer science on every curriculum

The recently established Campus Cyber in France is a best practice that should be used at the EU level. DIGITALEUROPE is looking to expand the cyber campus initiative based on the French model, using our network of 41 national organisations. This will be fully plugged into the EU Cyber Skills Academy and aims to align closely with Europe's overall cybersecurity preparedness, e.g. the new regional SOCs.

The Commission should support and coordinate this network. In addition, a pan-European live fire cyber defence exercise modelled on NATO's Locked Shields would help participants hone their skills and teach them to work together.

Finally, all member states should put computer science on the primary and secondary curricula, and the Commission should explore ways to incentivise this.

Critical infrastructure

Infrastructure has always been a crucial factor for the prosperity and security of societies. After World War II, Europe experienced a period of growth and peace thanks to the Marshall Plan, which supported the rebuilding of roads, airports, and rail tracks. Today, digital infrastructure, such as satellites, 5G, and 6G, has become just as important. President Ursula Von der Leyen's Commission aims to expand democratic and trade relations with the Global Gateway initiative, but competing initiatives, such as China's Belt and Road, are also investing in infrastructure across Southeast Asia and Africa.

The Commission has addressed critical infrastructure network security with the NIS directive, however there has been wide divergence among Member States with regard to scope, security and incident reporting obligations, as well as supervision and enforcement. The new NIS2 Directive, which will apply as of Oct. 2024, aims to solve these issues.

The illegal war in Ukraine highlighted the importance of digital infrastructure, as it has been a key target for the Russian army, making communication with endangered civilians and refugees difficult. Private-public collaboration has been crucial in addressing this issue. Today, DIGITALEUROPE and the European Commission are collaborating with the Ukrainian Digital Ministry **to collect over 300,000 laptops and handheld devices for schools and hospitals in Ukraine** to ensure that society can continue to function. In a historic first, the EU agreed to expand the scope of its civil protection mechanism (used to respond to emergencies) to include the delivery of ICT devices and components. The safety of our digital infrastructure is essential, and it has become a key component in the resilience and security of societies.

Actions

5. Boost connectivity:

The EU is home to strong players in connectivity. Boosting 5G and 6G connectivity is crucial for enhancing digital resilience as it enables faster and more reliable communication between devices, networks, and systems. The availability of high-speed and low-latency networks is essential for maintaining digital operations and ensuring continuity in times of crisis.

6. All member states to implement the NIS2 Directive as soon as possible.

7. Accelerate adoption of the Cloud:

Cloud computing is the cornerstone of digital transformation, and it is the foundation of innovative products and services such as IoTs and AI-powered devices. However, less than 50% of EU enterprises used cloud computing in 2021 which is slowing down the EU's cloud adoption rate and makes it lag behind other regions.

8. Governments should embrace the new innovative concept of "data embassies":

Estonia is leading the way with its data embassy initiative in Luxembourg, allowing it to set up part of its government's server resources in Luxembourg, following the highest levels of cybersecurity. This defines the idea of storing state information within specific physical boundaries, which boosts digital resilience in the event of a large attack.

A recent example of this is the war in Ukraine, where the government with the help of the private sector was able to move its essential data out of the country and into more secure locations.

9. Investment in secure and back up digital infrastructure:

Governments must now realise that digital infrastructure is as crucial to our security as traditional defence industries, and a resilient supply chain of critical components like cables, servers, phone masts, devices and screens is essential for our security.

Resilient supply chains

Europe's digital resilience is heavily reliant on certain components and raw materials from outside of its borders. The pandemic and the war in Ukraine have brought this into sharp focus, with shortages affecting our economy and ability to defend ourselves. Recent EU proposals such as the EU Chips Act and Critical Raw Materials Act aim to make us more resilient.

At home, several barriers stand in the way. Obtaining environmental permits for chip fabrication plants in the EU can take up to an excessively long period of 12 months.

Sweden's bedrock contains more than half of the substances in the EU's list of critical raw materials, but none is being mined due to current regulations. In Europe we also lack the skills necessary in advanced chip manufacturing or to refine raw materials. Finally, both the volume of regulation and fragmented nature of national laws are a serious brake to boosting capacity in Europe.

In addition to grow production capacity in Europe we must also grow our trade with likeminded partners and look for new opportunities. Chips, digital infrastructure components and raw materials are examples of global by nature industries.

Actions

10. Ease permit procedures and provide tax incentives

Europe can quickly increase production of vital components like chips and speed up the extraction of critical raw materials by easing permitting procedures and the regulatory reporting burden. Tax incentives and tailored university programmes with private sector involvement also have a role to play to close the skills gap.

11. Friend-shoring and building a global network of trade partners

The EU-US Technology and Trade Council has all the elements to become a blueprint for new models of global governmental engagement. On chips, for example, it offers the opportunity to align on public support measures to keep up with high expected demand and deepen common EU-US understanding of market dynamics.

On raw materials, recent EU strategic partnerships with Namibia and Greenland can point to the way forward for trade diversification. They can also mitigate the EU's overreliance on geographically concentrated regions.

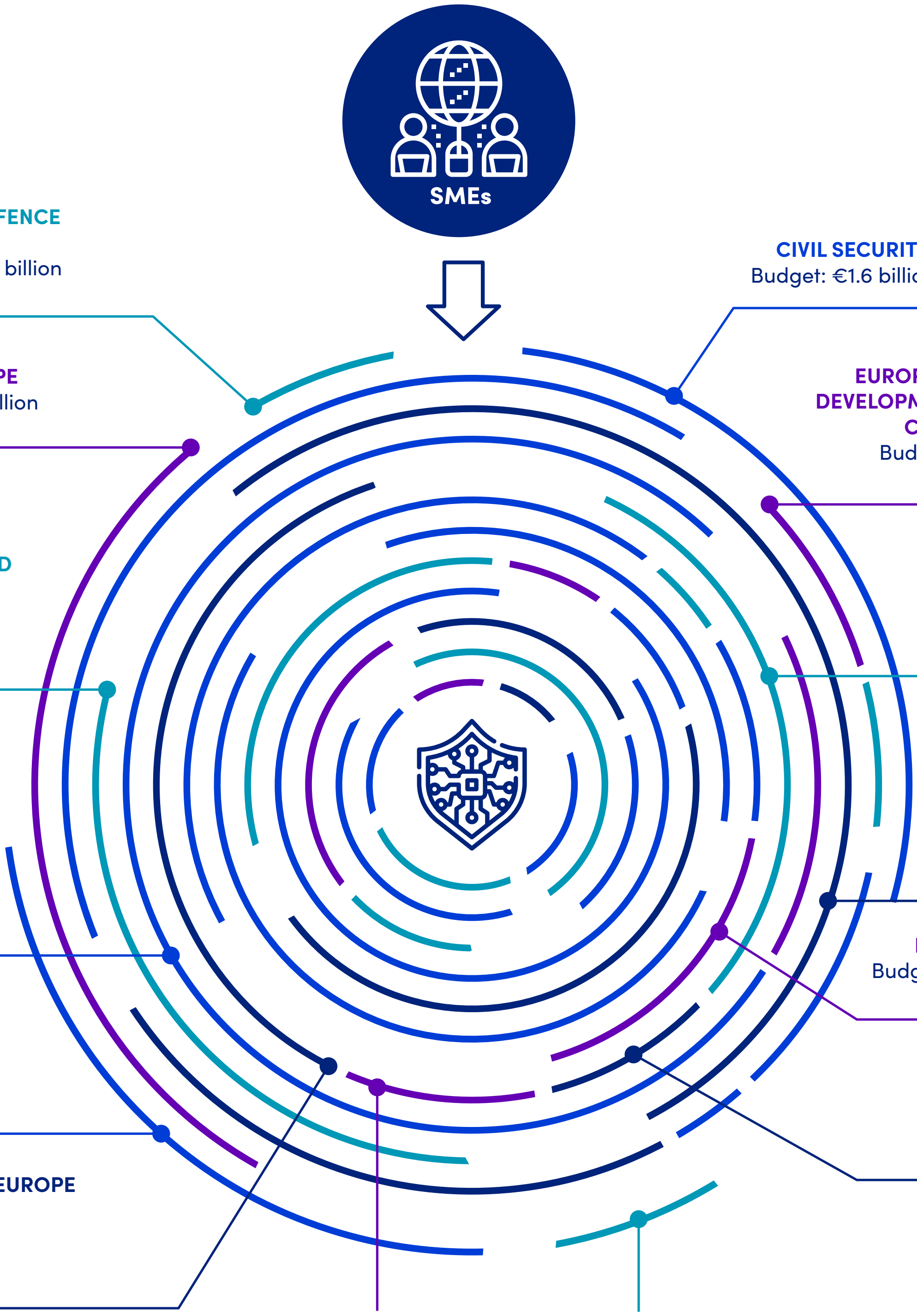
Fast-track procurement for critical Emerging & Disruptive Technologies (EDTs)

To boost Europe's digital resilience, companies and especially small and medium-sized Enterprises (SMEs) should be provided with enough research and innovation support. Investing in research and innovation in the security sector is Europe's best chance to maintain its technological edge over potential adversaries.

It is also crucial to revisit current procurement practices in security and defence and set up a fast-track path for SMEs to offer their latest technological innovations, especially when it comes to Emerging and Disruptive Technologies (EDTs).

DIGITAL
RESILIENCE
ROUNDTABLES
A SERIES OF EVENTS FOCUSING ON DIGITAL RESILIENCE & CYBER GOVERNANCE

Existing funding programmes:



EUROPEAN DEFENCE FUND (EDF)
Budget: €7.953 billion for 2021-2027

DIGITAL EUROPE
Budget: €7.5 billion for 2021-2027

INTERNAL SECURITY FUND (ISF)
Budget: €1.93 billion for 2021-2027

ASYLUM AND MIGRATION FUND (AMF)
Budget: €9.882 billion for 2021-2027

EUROPEAN DEFENCE AGENCY GRANTS

CONNECTING EUROPE FACILITY (CEF)
Budget: €33.71 billion for 2021-2027

CIVIL SECURITY FOR SOCIETY
Budget: €1.6 billion for 2021-2027

EUROPEAN REGIONAL DEVELOPMENT FUND AND COHESION FUND
Budget: €243 billion for 2021-2027

HORIZON EUROPE
Budget: €95.5 billion for 2021-2027

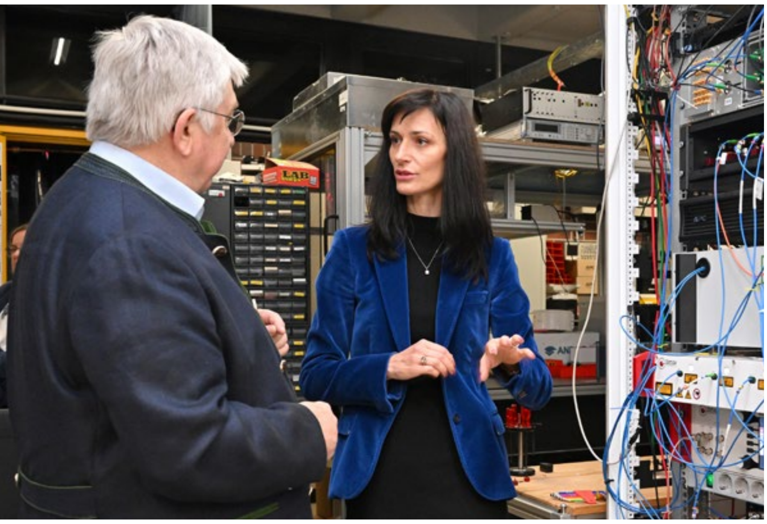
EUROPEAN PEACE FACILITY (EPF)
Budget: €5 billion for 2021-2027

INVESTEU FUND
Budget: €26.2 billion for 2021-2027

EU SPACE PROGRAMME
Budget: €14.88 billion for 2021-2027

NEXTGENERATIONEU – RECOVERY AND RESILIENCE FACILITY (RRF)
Budget: €672.5 billion for 2021-2026

EUROPEAN DEFENCE INDUSTRY REINFORCEMENT THROUGH COMMON PROCUREMENT ACT (EDIRPA)
Budget: €500 million for 2022-2024



Although these are just a few examples of the many funding programmes available to SMEs in the defence sector, we can conclude the following:

- There is a plethora of funding opportunities in the area of digital resilience, however many of them are little known to SMEs or hidden in a jungle of too much information.
- The application process to EU funding opportunities especially is typically lengthy, complex and requires key resources such as bid-writing personnel.
- There is a lack of alignment between EU funding opportunities and NATO-funded programmes.

Challenges facing SMEs:

A. Information overload

SMEs often simply don't have the time to look for all the different calls on often opaque and difficult-to-navigate web platforms. Each time a new authority sets up a new funding mechanism, it requires them to start from scratch.

B. Too big, too small

European streams like the European Defence Fund are difficult to access for SMEs because the EU prefers big consortia of companies and academia, which are very challenging for smaller companies to bring together.

> **“SMEs never have enough resources to apply for different EU programs (like Horizon Europe). The diligent process is necessary but the heavy paperwork throughout the whole process from application up to the audit can be human resource intensive.”**
>
> **Rainer Saks**
> Member of
> The Management
> Board at
> CybExer Technologies

> **“SMEs are usually not capable to apply for projects unless they join partners from minimum two different countries. That makes the paperwork in such cooperation a huge burden.”**
>
> **Rainer Saks**
> Member of The Management
> Board at CybExer Technologies

C. 27 different countries, 27 different sets of rules

The fragmentation of rules is a longstanding complaint for many SMEs. Instead of growing across borders within Europe, many decide it is easier to move elsewhere to scale. One example is access to data: the development of innovative cybersecurity or artificial intelligence tools require vast amounts of data, but shopping around different EU member states is too cumbersome.

> Any modernization of our European cyber defences will imply collaboration with the private sector, and this brings up the challenge of procurement. Procurement operating models, processes, and even tooling have rarely received the attention and funding they deserve: to be successful, any ambitious investment program should foresee specific funding for the modernizations and innovation in the procurement practices themselves. Procurement should not only be local, but also pan-European; and earmark dedicated funds for SMEs, as any successful involvement of young & dynamic SMEs requires specific procurement attention and techniques.

Vincent Defrenne
Director Cyber Strategy
& Architecture at NVISO

Actions

12. A simple Europe-wide funding application system similar to the DIANA model

Simplified procurement starts with reducing the bureaucracy. This would allow more non-traditional and smaller companies to access the growing pots of funding set aside for digital resilience. The Defence Innovation Accelerator for the North Atlantic (DIANA) is a model for how to set up funds that are accessible for SMEs.

13. Earmark funding for digital and cybersecurity technologies

Our benchmark is that 1% of GDP should be spent on emerging and disruptive technologies with civilian and military uses. Investment in technology is investment in tomorrow's defence.

14. Earmark 25% of defence funding to technology SMEs

Some of Europe's brightest minds work outside traditional defence contractors. We need to ensure that these innovators get a share of Europe's significant public funding available for digital resilience.

15. Break down digital barriers in the European Single Market

The most efficient way to support innovative companies to grow and be profitable in Europe is to reduce regulatory complexity in the EU and remove barriers. New regulation should prioritise harmonisation with fewer national derogations, and the Commission should look again at existing regulation with a view to tackling barriers to growth.

CONCLUSION

In conclusion, the 15 actions presented in this publication highlight the urgent need for a comprehensive approach to digital resilience. The increasing threat of cyberattacks, coupled with the growing energy, climate and supply chain crises, underscores the importance of boosting our societies' resilience. This will require a concerted effort to foster collaboration between the private and public sectors to ensure that responses to any potential threats are swift and unified.

Furthermore, we emphasize the critical role played by a solid and reliable critical infrastructure, as well as resilient supply chains, in supporting a digital society. Ensuring that Europe and its allies have access to the tools, components, and materials needed to function in a digital world is essential to maintaining the integrity and security of the digital ecosystem.

Finally, there is a crucial need for an enabling innovation ecosystem that can support the fast track procurement of critical digital technologies, with a focus on Emerging and Disruptive Technologies (EDTs). Encouraging innovation and staying one step ahead of adversaries will be critical to maintaining a competitive edge in the digital domain.

Overall, these actions provide a roadmap for ensuring that Europe and its allies are well-positioned to address the complex and evolving challenges of the hybrid era. By prioritizing cybersecurity, critical infrastructure, and innovation, we can build a stronger and more resilient society for all. We look forward to continuing the debate.

DIGITALEUROPE represents the voice of digitally transforming industries in Europe. We stand for a regulatory environment that enables businesses to grow and citizens to prosper from the use of digital technologies.

We wish Europe to develop, attract and sustain the world's best digital talents and technology companies.

DIGITALEUROPE's members include over 45,000 companies in Europe represented by 102 Corporate Members and 41 National Trade Associations.

www.digitaleurope.org

@DIGITALEUROPE

For more information please contact:
Chris Ruff, Director of Communications & Political Outreach
chris.ruff@digitaleurope.org
+32 485 55 22 54

DIGITALEUROPE
Rue de la Science, 14
B-1040 Brussels
Info@digitaleurope.org
+32 2 609 53 10

DIGITALEUROPE