Cybersecurity

Vision

Cybersecurity is a vast and often poorly understood topic. With the growing digitization of our world, it will continue to have an ever greater importance in all aspects of our life: from the economy to defence and the health of our democracies.

Cybersecurity covers a wide range of topics: encryption, monitoring, identity authentication, endpoints (devices) and digital services. It encompasses hardware, software and services. Because of its breadth and complexity, it is both difficult and necessary to have a holistic and integrated approach to Cybersecurity, and to do so at a European level in order to reach critical mass and levels of excellence need to strengthen the cybersecurity value chain, both for the benefit of its suppliers and its users.

The Cybersecurity Task Force developed a common vision for the "Cybersecurity in Europe by 2030", serving as a guide for formulating, prioritizing and coordinating recommendations for actions. This vision can be summarized as follows:

- **Market share**: EU is to grow its market share and become a net exporter of cybersecurity solutions
- **Protection**: EU is to increase levels of protection with appropriate cybersecurity solutions
- **Independence**: EU to increase its autonomy and digital sovereignty in cybersecurity
- **Leadership**: EU to achieve global leadership in key areas of cybersecurity
- **Stronger and more competitive European cybersecurity industry by 2030**

The digital transformation, Internet of Things, Artificial Intelligence and 5G mean that also the interface for cyber attacks is growing. There are more and more digital devices connected to the internet, and anything smart means they are also vulnerable. Digitalization has made cybersecurity everyone's concern.

The public and private sector, EU institutions, governments and business should join their forces to protect societies, critical infrastructure, data and privacy of its citizens. It is of utmost importance that Europe has key cybersecurity capabilities at its disposal and that it supports and strengthens its own European essential service providers and cybersecurity industry.

The main challenge for the European cybersecurity industry is that, in some sectors, the biggest players and service providers are non-European. If European cybersecurity market is 26% of the global market and only 5% are provided by the European providers, there is a problem. Another challenge is that European cybersecurity companies are small compared to the global giants. Therefore, Europe needs a different approach and understanding on how to build effective cybersecurity ecosystems.

Another challenge is the skills gap. Europe will be competing on a global scale for the best cybersecurity talent. The skills gap for cybersecurity professionals working in the industry in Europe is predicted to be 350 000 by 2022, and globally 1.8 million. The public sector has an additional challenge to compete with the private sector.

EU to grow its global cybersecurity market share

In the next few years, the global cybersecurity market is expected to grow at a double-digit compound annual growth rate. The cybersecurity market is globally a 600 Bln € market that is expected to grow in the next five years on average by approximately 17% in terms of sales, number of companies and employment.

The European Union has been losing its global market share in cybersecurity in the last six years from 13% down to 5%. The size of the European cybersecurity market is 26 %, however, only 5 - 7% are produced by actual European vendors and service providers.

The biggest challenge for European cybersecurity industry is to reverse this market trend and start regaining a bigger share of the global market. A real test for success is how Europe manages to achieve the common vision for EU in 2030 gaining back 1 - 1.5% of the global cybersecurity market every year.

The question is which market segments to focus on.

EU as a global leader in key areas of cybersecurity

In the cybersecurity discussions there seem to be two separate streams and even silos:

- "Civil" areas (consumers, businesses, administrations and public services) on the other hand.
- "Non-Civil" areas (police, homeland security, defence and intelligence) on the one hand, and

Whereas the first is considered as a high priority topic, with historically strong state financing and other proactive measures for protecting national players and technologies, the latter is left to open free competition with a more *laisser-faire* philosophy. Cybersecurity should be looked at more holistically as a matter of security, both for civil and non-civil areas.

Greater awareness about cybersecurity

Many EU consumers, politicians or organizations are not even aware of cybersecurity risks, and hence users are not adequately protected. EU enterprises have high risk of losing their valuable Intellectual Property (IP) due to insufficient cybersecurity preparedness and resilience.

Cybersecurity is, therefore, a strategic question and must become an integral part of any business strategy. Cybersecurity should, for example, be discussed in the boardrooms of international organizations, governments, corporations and SMEs. It is important that cybersecurity is discussed not only in technical terms, but also in relation to (international) law, ethics, privacy and governance in order to provide sufficient context. EU needs to contribute in raising awareness and ensuring that adequate solutions are deployed across the Union. And the focus should not be put on one-shot protective technologies but continuous response through technologies, processes and skills. Europe is strong and has world-class expertise in detection and response capabilities.

Europe needs to develop competitive and state-of-the-art European solutions for products and services across the cybersecurity value chain. Increasing competitiveness of the European market and industry means also including the local and regional levels through a variety of measures. It is also important that smaller companies can adopt and profit from the use and development of standards, certification, procurement and investments. Public procurement and understanding the need and role of actual European solutions play a critical role in the development of the market and key capabilities.

For policymakers and legislators is essential to understand that no technology on its own is good or bad, hence when regulating it is important to look at and regulate its applications, not the technology itself. Therefore, it is necessary to bring technical, social sciences and ethics expertise to those tables where policies are developed in order to fully understand the consequences. Cybersecurity companies are competing globally, hence the EU should not regulate the European companies out of the global competition.

Stronger cybersecurity players

European cybersecurity industry's aspiration is to become a global player that brings valuable solutions to the market. However, the European market is too fragmented and too much internal competition weakens Europe in challenging existing global giants. The EU needs to coordinate its efforts, especially those of various SMEs, research institutions and governments, and encourage collaboration and, where feasible, consolidation. Small European SMEs are often too small to compete alone with global players. Often promising European SMEs are easy targets for non-European based buyouts.

The European Commission plans to launch in 2019 a pilot scheme within the COSME Loan Guarantee Facility (2014-2020) to support the financing of digitalisation projects including in the area of cybersecurity. European cybersecurity industry needs to talk with a united voice and take coordinated actions. This could lead to the emergence of European 2~3 leading players in each market segments that will be world-class players in their respective fields. This requires focusing investment on the competitive advantages of the European cybersecurity market. There is a lack of knowledge on cybersecurity among investors, which results in a lack of EU investments in cybersecurity companies/start-ups.

Action levers

To achieve the vision for EU in 2030, and in order to become stronger and more competitive in the global cybersecurity industry as well as becoming a net exporter of cybersecurity solutions, there are certain key action levers relevant for achieving the vision. This requires significant and bold decision and Europe should adopt some good practices from Israeli success model.

- **Investments**: coordinated strategic investments for technology deployment, new funding sources or modes.
- **Collaboration**: enhanced collaboration between public and private, as well as European, national and local players.
- **Procurement**: public and private procurement rules, guidelines and programs.
- **Technology**: research, development, innovation, proof of concept and technology deployment.
- **Skills**: attract, develop, retain, deploy skills and build a career path.
- **SME**: stimulate and facilitate the move from research and innovation to market, grow start-ups into SMEs, and SMEs into large corporations and global players.
- **Standards and Norms**: regulation, standardization, certification and interoperability.

Specific recommendations

Considering the complexity of the cybersecurity value chain, the Cybersecurity Task Force participants have proposed a large number of detailed recommendations (the full list of which can be found in the Annex). These have been grouped into:

- **Coordinated Investments** : which includes proposals for coordinated investments in 5 areas. This is supported by a total of 40 industry stakeholders, of which 31 industrial players and 9 other players (industry associations, governments and RTOs).

- **Related supporting recommendations** : which includes another 5 areas of actions that would be required and useful to support the development of the CCAV value chain?

Coordinated investments
1. Secure 5G for cybersecurity innovation and services

2. Sharing and exploiting information on threats, vulnerability and incidents
3. Secure highly critical applications and infrastructure: electricity, gas, water, vehicles…
4. Develop and deploy end-to-end data protection solutions using advanced cryptography
5. European Data Space: create a framework and infrastructure for secure data communication, storage and handling
Related supporting actions
6. Create a European Cybersecurity Investment Fund to support the European cybersecurity ecosystem
7. Create the next generation EU framework for PKI infrastructure and European DNS management for critical infrastructure
8. Leverage public procurement to enhance Cybersecurity environment in Europe
9. Accelerate implementation of the harmonisation process across the EU
10. Develop a comprehensive EU strategy to support EU players in critical cybersecurity areas
11. Secure Europe against emerging threats by supporting development and deployment of Key Enabling Technologies (KET)
12. Develop and strengthen a highly skilled workforce in all parts of the cybersecurity value chain

1. Secure 5G for cybersecurity innovation and services

5G provides a secure and capable platform, moving beyond today's consumer-oriented mobile broadband towards a more enterprise-oriented network where automation, critical systems and cyber-physical systems represent new constituents. According to GSMAi 5G alone is forecast to create $2.2 trillion of economic value by 2034. A telecommunications generation last approximately 10 years and as such this investment has a future-proofed market.

5G is the first generation of mobile telecommunications that allows: Network exposure functions (allowing more services to make use of the mobile network), Cloud services, Secured by design practices to be managed between networks. The 5G standards, defined by 3GPP, outline what will be secured but not how; this is being defined at present and will result in numerous opportunities that could be exploited within Europe.

Concrete actions

- Create favourable conditions for 5G networks and for its usage in the endpoints through various embedded systems like for vehicles, utilities, healthcare, and manufacturing.
- Support start-ups, scale-ups and research that has a focus on securing strategic 5G services.
- Identify key technologies and service requirements for secure-5G and provide funding to accelerate these deliverables.
- Support software development that relates to new technology identified for 5G networks, such as secured APIs for service interaction between the 5G network and strategic verticals.
- Support hardware development for securing 5G technology, such as embedded systems and new appliances introduced in the standards.
- The EU should adopt a common position regarding the (political) discussion about foreign suppliers' involvement in the implementation of 5G. This is important if the EU wants to act as a unit on the global cybersecurity market.

Sections with more details in the annex:

- Secure 5G for cybersecurity innovation and services – R12.

2. Sharing and exploiting information on threats, vulnerability and incidents

Cybersecurity incidents are a reality and attacks are becoming more and more sophisticated. It is difficult for the industrial sector to maintain a permanent up-to-date protection level. An expert and legitimate authority at EU level able to keep track of security incidents will help to understand better the threats, impacts and vulnerabilities. A centralised data collection point, where information is stored in a standard/normalized way, will lead to better and faster reaction for the community to provide appropriate countermeasures. This body will act as an advisor and could help in certain circumstance to offer complete advisory information and/or services for investigations.

European policymakers have acknowledged the value of voluntary information sharing to understand threats, protection, information and networks, and how to prevent cyber-attacks. Under the NIS Directive and GDPR, it is now mandatory for Operators of Essential Services and Digital Service Providers (controllers, processors) to inform relevant authorities of a Data Breach and/ or incident. However, this is considered after the fact, after an incident and/or breach.

Concrete actions

- Implement and optimize existing rules, guidelines and framework for disclosure and information sharing on incidents/breach reporting and for vulnerabilities detection.
- Make the most out of initiatives around "Cybersecurity Information Sharing Sector-Based Networks" where parties can join on a voluntary basis, and adhere to specific information sharing rules.
- Examine possibility of mandatory disclosure in certain areas/cases.
- Create a Cyber Security Ontology and Taxonomy on a specific language and across languages. So, putting human/domain expert know-how into a cognitive computing engine (based on either Semantics or Machine learning)
- Create (manually or automatically) the semantic rules in order to apply categorization, entities/relations extraction and consequent terms normalization automatic activities
- Build a horizontal network (instead of vertical from organization, to decentral, to national, to EU institution). Such a flat network stimulates sharing information and collaboration, without imposing fines. This creates trust and more transparency who experienced, what, when, why. Creating a feedback loop between those who report and the regulator/entity receiving notifications is crucial.
- Strengthen the role of trusted intermediary parties (as in the case of the MISP).
- Promote a culture of (in-house) ethical hacking.
- Define an ISAC standard (guidelines, requirements) paper in cooperation with CEN CENELEC JTC13 (cybersecurity TC) covering the ISAC information management, processes etc. (see ENISA's study). Thus establishing a harmonized environment which will facilitate collaboration among all European Standards, as well as information sharing among regional/national/sectorial ISACs themselves throughout the EUSupport the cybersecurity analysis of emerging technologies (Artificial intelligence, quantum, cognitive technologies…) and their use in innovative protection products, services and processes (see the recent call for tender the ISACs Facilities manager).

Sections with more details in the annex:

- Promote greater sharing of cyber threats, vulnerability and incident information – R6.
- Develop and maintain European excellence in cyber threat understanding and hunting – R7.

- Support to the development of European breakthrough technologies applied to cybersecurity – R10.
- Risk Information Sharing Platform: Collaboration in risk management towards informed governance – R71.
- Shared Database for AI development in cybersecurity – R21.

3. Secure highly critical applications and infrastructure: electricity, gas, water, vehicles…

Critical infrastructures, such as energy infrastructure (including electricity, oil and gas, water and nuclear) are very complex, as other sectors depend on them. We need to improve the cyber resilience in the highly critical infrastructures to avoid as much as possible the unavailability of the essential services supply system. This will provide Europe with a network of critical infrastructures with a high degree of resilience that are supported by a network of European suppliers that meet the highest security requirements established by international standards and norms. To this, we need to build and set-up a European-level cybersecurity regulation for critical infrastructures that allows the provision of essential services for the EU.

The project will work in three directions:

- Increasing the protection level of the infrastructure assets against cyberattacks.
- Developing advanced mechanism of early cyberattacks detecting and prevention systems.
- Restoring the system in the fastest way when a cyberattack has succeeded.

Concrete actions

- To set up an alliance integrating stakeholders of highly critical infrastructure sector (network operators, technology suppliers, cybersecurity solution providers, standard and certification bodies, etc.) for defining cybersecurity standards and test procedure (see the call for tender for enhancing EU cooperation under the NIS Directive).
- To foster the development of specific cybersecurity solutions that satisfy functional and performance requirements coming from critical sectors.
- To support investment in R&D, since new technology could be needed, and R&D projects can help in the development and validation of new solutions.
- To create a specific Computer Emergency Response Team (CERT) for high critical infrastructure sector at EU level.
- Support hardware development for securing embedded systems and automation architectures.
- Support development of Scada systems secured by design.
- Support development of a detection system adapted to industrial protocols and fieldbus.
- Identify key technologies and service requirements for automation and provide funding to accelerate these deliverables
- Support the establishment of relevant partnerships between automation actors and cybersecurity firms to enhance the protection of installations
- Develop new equipment to prepare Industry 4.0 to be resilient on the basis of certification and approval systems.
- Launch a European coordinated action to develop security, governance and security certification for sector-specific applications.

Sections with more details in the annex:

- Secure highly critical applications and infrastructure: electricity, gas, water, vehicles – R18,
- Coordinated EU cybersecurity strategy and governance for the smart grid / Smart charging – R25,

- Develop cybersecurity solutions for connected and autonomous vehicles (V2X) and related infrastructure – R73,
- Build policies on existing industry security measures, including investments towards industrial cybersecurity solutions – R72,
- Development of Industrial cybersecurity building on Europe's strong industrial base – R32,
- Certifiable secure firmware on open hardware for Europe – R65,
- Provide funding for and set up an EU driven community for open source security software and hardware – R65.

4. Develop and deploy end-to-end data protection solutions using advanced cryptography

In parallel to efforts toward creating secure environments, it is necessary to develop the capabilities to operate safely in a (foreign) unsecured environment – this is the objective of this initiative. Cryptography is the key technology to secure digital applications. Europe has a strong background in theoretical and mathematical basis of cryptography, and innovative schemes development should be encouraged, supported and pushed to proof of concept and standardization.

Homomorphic encryption is the cloud privacy game-changer to come, enabling the use of untrusted cloud services, Identity and attribute-based encryption (IBE, ABE) enabling global secure solutions with massively interconnected objects are technologies to support. Homomorphic encryption is a form of encryption that allows correct computation using ciphertexts only without revealing the plaintext. Therefore, homomorphic algorithms can protect the privacy of data in hostile environments (e.g. in a foreign cloud) out of reach of laws like the American Cloud Act of March 2018.

Concrete actions

- Develop ad-hoc advanced encryption algorithm to support European regulation (GDPR, NIS, eIDAS, …), and deploy these solutions to allow safe transmission, storage and exploitation of this data in insecure environments
- Develop algorithms in the following domains: ABE attribute-based encryption, IBE identification-based encryption, homomorphic encryption, anonymization, zero knowledge, blockchain, quantum safe cryptography
- Develop adequate architecture to support this.
- Support technology from fundamental research to operational proof of concept in advanced cryptographic.
- Define EU policy and guidelines on cryptography (there is no such thing for the moment)
- Provide funding to encourage the 6~7 EU start-up companies that have development specified niche solutions to team up to develop more comprehensive solutions for cryptography

Sections with more details in the annex:

- Develop and deploy end-to-end data protection solutions using advanced cryptography – R8.
- Develop homomorphic encryption – R64.

5. European Data Space: create a framework and infrastructure for secure data communication, storage and handling

We already have dedicated, European-wide, communication frameworks and infrastructures for secure data sharing in some sectors: banking, personal identification, health, social security and pension data. We also have such infrastructure at national levels and are currently trying to develop new ones for dedicated

sectors (energy, transport). As more and more sectors become digital and connected, secure communication will become more and more important in new sectors: connected cars, intelligent houses, and health data.

Europe needs to develop a harmonised communication framework for such infrastructure, and a coordinated approach to develop, finance and operate them. Here the inherent capabilities (e.g. latency, slicing) and security functionality of 5G provides a foundation for such secure infrastructures. The aim is notably to facilitate communication within industries and knowledge sharing and trust between key EU players.

The objective is to create a European environment where users can securely communicate, store and handle their data, with high levels of security and confidentiality. This framework and supporting infrastructure may include securing communication networks with appropriate levels of cybersecurity, developing European cloud services solutions as well as governance-related issues.

Concrete actions

- Develop a cloud framework with a high level of authentication and secure data lake.
- Enable secure and privacy-enhancing end-to-end communication between devices, individuals and legal entities for pan-national and pan-sector specific use
- Create a dedicated European-wide harmonised communication framework and infrastructure for secure data sharing
- Support the cybersecurity analysis of emerging technologies (artificial intelligence, quantum, cognitive technologies…) and their use in innovative protection products, services and processes

Sections with more details in the annex:

- Create dedicated European-wide harmonised communication framework and infrastructure for secure data sharing – R34.
- Support emergence of a European cloud service that can provide the highest levels of security and functionalities, and can compete internationally – R22.
- Digital Trusted Attestation model – R9.
- Implementing a secure European Operating System – R23
- Shared Database for AI development in cybersecurity – R21
- Market data availability and awareness – R59

6. Create a European Cybersecurity Investment Fund to support the European cybersecurity ecosystem

Europe is lacking a venture capital market with similar scale as in the US and markets. The EU should develop an industry-specific investment fund for cybersecurity to encourage and leverage private investors. Investments are needed to scale cybersecurity companies to grow globally. Europe should model global leaders and success stories and apply those best practices in Europe on how best to structure such funds.

The EU should develop a platform providing better visibility for European cybersecurity players and more and better opportunities for venture capitalists and industrial investors to find potential deals in Europe. In order to develop the European market, it is essential to increase and open new funding opportunities for cybersecurity start-ups and SMEs to grow in Europe, instead of selling too early usually to the US.

The objective is to create an EU Investment Fund, with public and private funds, dedicated to supporting the development of the Cybersecurity value chain. In parallel, develop the cybersecurity ecosystem with dedicate platforms and networks to encourage development, collaboration and consolidation between EU

players. The Fund would coordinate its investments with/through the platforms and networks with a clear mandate to support the development of the cybersecurity industry. The first fund would be an encouragement for the coming years to create cybersecurity-related investment funds across the EU.

Concrete actions

- Create a dedicated fund and the related managing structure for Cybersecurity within the European Fund for Strategic Investments
- Design and implement a specific platform aiming to facilitate the meeting between cybersecurity companies and private investors
- Create a "Cybersecurity Accelerator" network of regional technology clusters ("Cybersecurity Valleys")

Sections with more details in the annex:

- European Cybersecurity Fund & Private Investment Portal – R61,
- Create a "Cybersecurity Accelerator" network of industry players and regional technology clusters – R50,
- Cybersecurity SME Hub: a unique platform supporting the "Cybersecurity Made in Europe" – R31,
- Create a mapping of the European cyber-industry value chain or industry, which includes SMEs and end-users, to complement the one already developed by the JRC, based on a common taxonomy – R59.

7. Create the next generation EU framework for PKI infrastructure and European DNS management for critical infrastructure

Public Key Infrastructures (PKI) and the Domain Name System (DNS) are two extremely relevant enabling elements to create and maintain a trustworthy and reliable European Digital Society. Today's PKI and DNS are managed by foreign (private) organisations and date back to the early days of the internet age. Europe needs to develop an innovative and EU-managed PKI and DNS for infrastructure, to improve both its functionalities and its governance.

Enable secure, interoperable and privacy-enhancing end-to-end communication between devices, individuals and legal entities for pan-national and pan-sector specific use defining an EU Public Key Infrastructure common harmonisation framework.

Ensure the establishment of a DNS fit for the challenges of the full EU digitalisation: a common EU effort is needed to ensure the DNS ability to address the reliability and security requirements to satisfy the needs of a fully digitalised Europe. This action implies on a side a harmonisation action for what concerns security requirements for the existing DNS infrastructure and on the other the opening of an R&D and standardisation debate with the relevant stakeholders and MS to plan the design and governance of a DNS fit for the next Internet generation.

Concrete actions

- EU common harmonisation and standardisation action (potentially supported by the JRC and ENISA). This action would imply to place a new work item by a European Standardisation Organization (ESO) to create a harmonised PKI standard. It would aim at the definition of a common trustworthy Authentication Framework.
- Enable the secure and privacy-enhancing end-to-end communication between devices, individuals and legal entities for pan-national and pan-sector specific use through the implementation of the identified PKI standard across all the digital sectors. The future European Cybersecurity

Competence Centre could tackle this point based on the above-referenced Authentication Framework by including MSP, JRC and ENISA inputs with the involvement of stakeholders.
- Establish an international debate and negotiation on the governance of the DNS with the involvement of ICAAN, ITU, the Member States and the technical support of JRC and ENISA, aiming at guaranteeing the protection of European interests, security and autonomy in the governance of the DNS
- Ensure the establishment of a DNS fit for the challenges of the full EU digitalisation: a common EU effort is needed to ensure the DNS ability to address the reliability and security requirements to satisfy the needs of a fully digitalised Europe. This action implies on a side a harmonisation action for what concerns security requirements for the existing DNS infrastructure and on the other the opening of an R&D and standardisation effort with the relevant stakeholders and MS to plan the design of an European DNS fit for the next Internet generation (with the technical support of JRC and ENISA).
- Establish an additional infrastructural layer of DNS targeting more specifically ICT critical access (i.e. Smart-Grids, intelligent transport systems, eID solutions, eHealth, e-government…)

Sections with more details in the annex:

- EU mutualised framework for PKI infrastructure and European DNS management – R66.

8. Leverage public procurement to enhance Cybersecurity environment in Europe

Europe needs to look at cybersecurity public procurement from a new perspective and through a more holistical lense as a matter of security, both for civil and non-civil areas. This means treating cybersecurity not just as any other commercial product, but as an essential vector in defending European sovereignty and interests. Not only in the sensitive "non-civil" domains (military, intelligence, internal security) but also in all the other "civil" domains where protection of sensitive information (personal privacy, intellectual properperty, financial data...) is also in Europe's vital interests. In a context of growing geopolical uncertainty, a certain level of European independence, with competitive and state-of-the-art European solutions in key areas, is crucial. The guiding principle in European public procurement should be taking into account European security considerations. Europe should not rely solely on solutions and providers from third countries but have at least some strategic layers from European providers where possible. This is key for end-to-end trusted services: the orchestration of multiple solutions, as providers will be required by large companies and SME as well (outsourcing their IT).

The objective of this action is to use public procurement as a lever to:

- increase the level of resilience and autonomy against cybersecurity threats in Europe,
- boost the market for advanced, innovative and high quality cybersecurity solution,
- promote European standards and schemes on cybersecurity in public procurement
- support the European cybersecurity ecosystem.

Concrete actions

- Incorporate the cybersecurity certification framework (a standard) criteria with the common scheme into public sector procurement.
- Develop guidance for the contracting authorities on how to impose various security of information requirements within their procurement procedures for cybersecurity solutions.
- Develop guidance documents on security of information, on best European practices and on procurement levers for contracting authorities regarding cybersecurity procurement.

- Develop a new procurement institution/program to boost forerunner innovation in cybersecurity (ie: DARPA style).
- Facilitate and encourage cross-border procurement from other Member States (ie: to favour a common large EU cybersecurity market, and not a series a small national ones).
- Make a detailed mapping exercise to better understand the perimeter, structure and size of the cybersecurity market, especially in public procurement.

Sections with more details in the annex:

- Leverage public procurement to increase the overall levels of cybersecurity in Europe – R29.
- Increase innovative public procurement – R54.
- Create a network of experts to provide assistance and training to public procurement agencies for their cybersecurity procurement needs – R69.
- Incorporate the cybersecurity certification framework criteria into public sector procurement by default – R29.
- Build cybersecurity functionalities within existing Public Procurement Competence Centres – R51.

9. Accelerate implementation of the harmonisation process across the EU to achieve a common cybersecurity ecosystem by leveraging the existing EU initiatives (agencies, standards, regulation, certification)

Fragmentation is a key weakness in Europe, with different regulation and standards in different countries, and multiple agencies and regulators at different levels (national and European). This creates problems of interoperability, limited market size. Barriers between Member States should be removed (in particular removing those that impede SMEs to enter the market), while product criteria for entering the market should be kept.

Security is another major concern with a wide range of quality/security levels of cybersecurity solutions in the market. Regulation and certification is a way or raising the levels of cybersecurity protection, and supporting those companies that do meet the certification requirements. Guidance for companies on how to implement certification frameworks would be beneficial, linked to a clear image of threats.

Sections with more details in the annex:

- Clarify and raise awareness of the role of the various European bodies involved Cybersecurity: ENISA, ECSO, European Cybersecurity Competence Centre, regional authorities – R39, R59.
- Create a European optimized NIST-like framework – R39.
- Speed up the use of the EU Cybersecurity Certification Framework and support the SMEs to receive certification – R42.
- Align cybersecurity strategies of public institutions within the EU – R52.
- Assess the necessity for mandatory cybersecurity certification or general cybersecurity legislation for all IoT products – R36, R4,
- Standardization of cybersecurity protocols and languages for better interoperability, ergonomics and secure cybersecurity solutions – R3.
- Labelling of cybersecurity solutions in sensitive digital domains – R4, R11.
- Develop cyber-insurance in Europe – R68.
- Accelerate the adoption of the “International Procurement Instrument”, also for Cybersecurity, to ensure an appropriate response to non-reciprocity in public procurement by foreign countries – R2

- Setup a pan-European campaign to educate and raise awareness about cybercrime – R17, R33.

- Maintain high security and privacy standards for better user protection and support for EU players – R5.
- Launch a European coordinated action to develop cybersecurity and cybersecurity certification for sector-specific applications → see Cybersecurity Directive
    - connected/autonomous mobility, vehicle-grid communication – R18, R25, R40.
    - health, energy and manufacturing infrastructure – R19,
    - telecommunications (5G) – R12.

10. Develop a comprehensive EU strategy to support EU players in critical cybersecurity areas

European initiatives such as the creation of Airbus were driven both by innovation and by strategic considerations and the need to reach independence in areas that were considered critical from an economic and/or a military standpoint. They were successful before there was a strong political and public support for them. Such an initiative also helped develop the European aeronautics ecosystem.

Cybersecurity should be treated with the same level of importance. Europe should develop a strategy to actively support, with political support and public funding, cybersecurity players that have an innovative, value-added technology and have the potential to become global players. Having 2~3 EU world-class players, capable of competing globally, in each critical area of cybersecurity would help both to achieve EU independence and to improve EU competitivity.

For each identified critical areas of cybersecurity, a comprehensive strategy should be developed using all available forms of public support:

- Research funding (grants): Horizon Europe, Digital Europe,
- Public investments (debt, equity): InvestEU, European Investment Bank, European Strategic Fund, national Public Investment Banks, Sovereign Investment Funds,
- Public Procurement (revenues).

Sections with more details in the annex:

- Coordinated EU investment strategy to support EU cybersecurity players – R35,
- Create European world-class player for Firewall and Antivirus – R38,
- Support European cybersecurity hardware suppliers – R24,
- Enhance the use of AI (Artificial Intelligence) for cybersecurity – R20.

11. Boost research, innovation and technology deployement in cybersecurity

Cybersecurity is a race between attackers and defenders. Change is constant and extremely fast-paced. Cybersecurity solutions and products are becoming obsolete fast. Hence, by definition, the cybersecurity industry needs to be dynamic and agile to be able to react to this constant change.

Current public cybersecurity investments in the EU are estimated to be between €1bn and €2bn per year. This is far behind the government investments in the US (€13.3bn per year) and China (€8.8bn).

The challenge with EU research and innovation funding instruments is that processes are often slow, projects take long and focus is on a more basic-level and academic research. As majority of European cybersecurity companies are relatively small, they might not have resources to identify relevant projects and participate in time-consuming and long research projects. The Commission has proposed a European cybersecurity competence network and centre. Together with industry players, Europea as a whol eshould

continue developing more agile innovation funding models to keep them attractive and relevant for the industry players.

The EU would also need to develop a new type of market test-bed-model. That would allow researchers to test the innovation on the market already in the early stage and get critical feedback. This would show early on if there is a real market interest and if there are opportunities for future success. The innovation could also be introduced to the investors at an earlier stage.

One indicator of European cybersecurity innovation is patents. On average, the EU owns less than 5% of cybersecurity-related patents (with cryptography being the only exception with the result of 21%), while patent filing is dominated by China, followed by the US.

In the EU, research and education are scattered across the Member States. There are a lot of research institutes and universities with a wide coverage of different academic fields. Cybersecurity is competing with other research areas over the limited resources. Research institutions should make choices and specialize on selected key success areas. With better focus and more coordinated resources, there will be significantly better outcomes and EU-based innovations.

Europe needs to make strategic choices when allocating European budget. It is necessary to pay special attention on the deployment of Digital Europe Program, Horizon Europe and other new financial instruments to benefit European industry and stimulate market growth to be more innovative in the future in order to match for dynamic industries like cybersecurity.

There should be a new type of support for SMEs' industrial accessto the global markets. EU has extensive network embassies all around the world. European based SMEs has challenges to find correct market information of partners, resellers and customers outside of EU. US, China and many other countries have an extensive network of trade counsellors located in their embassies enabling their industries to access new markets. EU could a part of Cybersecurity IPCEI establish cybersecurity industry related scheme to have trade counsellors for cybersecurity for balancing the score with competing countries.

Some key technologies need to be supported in a sustained with over an extended period, by multiple players, and in different forms, all along the process from fundamental research to large scale commercial deployment. While research programs are not the main focus of the Strategic Forum, the topics below were identified by Strategic Forum Members and invited experts as strategic issues, that will require research funding but also other forms of supports, including:

- funding proof of concept, demonstrators,
- funding start-up companies, in their creation and ramp up phases,
- funding scale-up processes for SMEs,
- introduction of new regulations/standards/certification support make certain technologies,
- introduce new procurement rules/guidelines to push market adoption by public/private players

Sections with more details in the annex::

- Boost European research funding for cybersecurity through DARPA-style research focusing goals and excellence – R43, R44.
- Focus funding on areas of specific EU excellence and critical needs by integrating existing expertise into the EU decision making processes – R60, R62, R63, R59.
- Create dedicated strategic funding programs to fund proofs of concepts (POC) and large-scale industrial deployment – R43, R26.
- Set test labs using critical infrastructure as a platform for testing innovative solutions – R67.

- Develop European key enabling technologies (KET) and key enabling platforms (KEP), which will help the development of other technologies:
    - Develop and make available to the community analysis tools to reduce vulnerabilities in software and hardware – R13, R11.
    - Advanced cryptography/homomorphic encryption to allow data privacy in hostile environments – R64, R8, and R43.
- Security of emerging technologies (AI) – R43.
- Methodology to certify complex systems, complex solutions and services – R11.

12. Develop and strengthen a highly skilled workforce in all parts of the cybersecurity value chain

There is a growing skill gap on cybersecurity experts globally. Industry, research and public sector (including defence) communities struggle to find skilled cybersecurity professionals for business and research purposes. The skills gap for cybersecurity professionals working in the industry in Europe is predicted to be 350 000 (globally 1.8 million) by 2022.

A particular focus should be placed on promoting entrepreneurial drive and innovation-oriented mind-sets in order to unlock personal potential, creativity and self-initiative. Europe needs joint efforts to foster competences in science, technology, engineering and mathematics (STEM) and motivate more young people to embark on a career in these fields.

As a global leader, Europe should attract, develop and retain top talent, both in the private and public sector. This requires joint efforts across the Union.

Raising awareness. Upgrade competences, all along the life. Life-long-learning. Becoming a digital citizen in a digital society. Similar to STEM, start early.

Concrete actions:

- Help universities and other education/ training institutions to build new degree courses in cooperation with industry for cybersecurity specialists. Cybersecurity is an area where experience and relevant certification may be more valuable than formal degrees. In order to develop new courses, teachers must be trained themselves, via knowledge transfer from technology experts to teachers.
- Encourage cybersecurity companies to be more involved in creating new courses together with Universities, to ensure that courses are in line with their needs.
- Establish cybersecurity apprenticeships: In the mid-term, develop a dedicated civil service fast track apprenticeship scheme that focuses on cybersecurity. Graduates will gain valuable cybersecurity experience as part of the broad curriculum and will be able to support governments' overall digital transformation efforts through their specialization. It is important to ensure that the focus of these schemes should not only be on technical cybersecurity skills, but on risk management and other organization aspects of cybersecurity. The EU could develop an apprenticeship scheme/toolbox that can be used by companies to set up their own apprenticeships at different levels and in different sectors.
- Map skills demand and create a blueprint for cybersecurity skills - as it was done for sectors such as Automotive (https://ec.europa.eu/social/main.jsp?catId=1415&langId=en). In the future the new initiative under Erasmus 2021-2027 on Centres of Vocational excellence could be relevant for the sector as it aims at developing comprehensive skills ecosystems
- Launch a sector skills alliance that will implement the Blueprint in Cybersecurity.
- Create an interoperable network of cyber ranges starting with the identification of gaps to be covered in the cyber range area at EU level from the analysis of the cyber ranges being identified in

ECSO and the ones that are part of the 4 pilot actions (SPARTA, CONCORDIA, CyberSec4Europe, ECHO), following with the creation of specific cyber ranges in sectors or areas of interest not covered by the existing ones and the connection among them.

Sections with more details in the annex::

- Develop and strengthen a highly skilled workforce in all parts of the cybersecurity value chain – R16,
- Develop a platform that provide insights into the current and needed skills capacity, per Member State – R28,
- Establish cybersecurity apprenticeships and training centres – R16, R30,
- Blueprint for cybersecurity skills – R16,
- Set up a special e-training program and professional certification in the cybersecurity – R41,
- Generalizing the cybersecurity risk management in safety analysis frameworks – R14, R15.

13. Support development, consolidations and growth of start-ups and SMEs into scale-ups that can compete globally

Facilitating cross-border collaboration and supporting SMEs

Encouraging cross border collaboration and dismantling practical trade barriers are essential for creating a true European Digital Single Market.

EU Member States have mainly small and local cybersecurity service and product suppliers. They may be well-established in one member state market, but expansion across the EU is not taking place. Often trade-barriers are invisible like differences in business culture, language, lack of trust. SMEs have often easier way to grow to non-EU markets than in the EU.

EU should develop programs where SME have opportunities to find new partners, distributors and solution integrators from the other member states. EU should encourage and facilitate SMEs build joint offerings together, and support the process all the way. Best practices and examples would lay the ground for further cooperation and joint projects.

The EU should also develop mechanisms and tools to support the European cybersecurity industry access and excel in the global markets. EU has an extensive network of EU delegations all around the world. In addition to the national efforts, also EU delegations could support European companies gaining access and visibility in the third country markets, and support access to the market data and networks (partners, resellers, and customers).

In order for the EU to develop and strengthen the European cybersecurity market, it is also important to have and maintain an understanding of the market. At the moment market data is not easily available. Detailed market studies are conducted and updated, but especially for smaller companies, it is almost impossible to find relevant market data. This is a task that could be done best on the EU-level, *i.e.* development of relevant indicators, information about different Member States, and also similar data from non-European markets. At same time, there should be an updated directory of all significant organizations operating in the EU in the field of cybersecurity.

Magnify the voice of the European cybersecurity community

As European cybersecurity market is scattered, industry voice might not be strong enough in Brussels. As there are a lot of start-ups and SMEs in cybersecurity, the public sector should support the existence of

forums and working groups for cybersecurity policy experts. Such a dynamic and critical business sector as cybersecurity requires continuous visibility to real economy and policy-making.

The EU in general needs stronger dialogue and connection between all the cybersecurity stakeholders, including the EU Commission, the Member States and the industrial players. We could set up an industrial advisory board to the EU Commission with relevant cybersecurity stakeholders, including companies of different sizes, to bring the best European expertise on the table. The advisory board would meet quarterly to provide advice, generate new ideas, consult European institutions and decision-makers and update real-time SWOT-analysis for Europe. This would also benefit the decision-makers to develop relevant policies and advocate for Europe in the international forums.

The cybersecurity advisory board would also be analysing and defining the must-win battles and policies keeping track of the European cybersecurity market, its strengths and potential gaps.

Sections with more details in the annex:

- Create dedicated strategic support and funding programs to help SMEs in Cybersecurity, in support of SME growth, SME collaboration and market consolidation in Europe –R55, R56, and R58.
- Introduce advisory services for European Business within the EU delegations network – R57.
- Create a dedicated information, training and funding program to help European SMEs obtain certification – R31
- Introduce specific rules/tools to support to simplify the participation of SMEs in EU-funded projects – R53.
- Reinforce and promote the use of the European “Small Business Act”– R31