# Cybersecurity - Annex

**Vision: "Cybersecurity Europe by 2030"**

A common vision for the cybersecurity in Europe by 2030 was discussed and developed jointly during the first Workshop. This common vision can serve as a guide for formulating, prioritising and coordinating recommendations for actions. The various suggestions have been clustered in the following Vision points.

V1. **Market share** → EU is to become a net exporter of cybersecurity solutions

- The EU, as a whole, imports 5.3% of its Cybersecurity products and services from non-EU sources. However, if one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the 'effective' imports from international companies headquartered outside the EU are between 26-30% of demand in 2016.
- We should stop losing ground on cybersecurity and aim to become a net exporter of cybersecurity solutions by 2030 for cybersecurity products, services and infrastructure solutions.
- This corresponds to a market share growth of 1.5%~2%/year over 2020→2030.
- For meeting above targets: EU should have a real-time cybersecurity market data available for agile decision-making in order to meet KPIs

V2. **Protection** → EU is to increase levels of protection with appropriate cybersecurity solutions

- Many EU consumers, politicians and organisations are not aware of cybersecurity risks, and users not adequately protected.
- EU enterprises have high risk to lose their valuable IPRs (particularly, trade secrets and confidential business information) due to insufficient cybersecurity preparedness
- Our aim should be to raise awareness and ensure adequate solutions are deployed for all users in the EU.
- The EU should promote general awareness with a shared cybersecurity taxonomy and ontology, also multi-language (EU official supported languages). We need to make sure that progress in this matter can be measured, with KPIs captured by an observatory.
- We need to increase resilience: detect and response more jointly, with high level of detection points in networks at EU-level (for states, companies, etc.).
- Cybersecurity does not exist and cannot be trusted by default. We need to consider cybersecurity and resilience by design to mitigate risk.
- The European Cybersecurity Certification Framework, due to enter into force by mid-2019, will create increased awareness and will help raise levels of cybersecurity for ICT products and services in the market, while at the same time reducing fragmentation of cybersecurity certification schemes at national level. We need to ensure its success.

V3. **Independence** → EU to increase its autonomy and digital sovereignty in cybersecurity

- We need competitive and state of the art, and "Made in Europe" solutions, for products and services across the cybersecurity value chain.
- Increasing the competitiveness both of the European market and industry, also means including the local and regional levels through a variety of measures to ensure they can adopt and profit from the use and development of standards, compliance programmes, certification, procurement rules and investments.

- For acceleration of growth, EU need to make full use of public procurement programmes to boost growth and market share
- Create a trusting environment to encourage pre-competitive collaboration between EU players.
- Stimulate the growth of SMEs and create incentives for existing players to collaborate/consolidate.
- It is essential to involve European operators and final users for the identification of needs and requirements. European Cybersecurity suppliers (especially SW companies) need to gain more traction accelerate in scale, and grow faster.

V4. **Leadership** → EU to achieve global leadership in key areas of cybersecurity

- Fragmentation and internal competition can be a source of weakness when facing foreign global giants. Pay special emphasis of deployment of H2020 and future MFF projects to stimulate market uptake. Europe has to become a global player that brings solutions to the market.
- We need to coordinate our efforts, especially efforts of various SME, research organisations, and governments, and to encourage collaboration and in some cases consolidation (individual SMEs are sometimes too small to compete with foreign players). A European cybersecurity industry should talk with a united voice and take common actions proactively.
- This could lead to the emergence of European **global leaders in innovation** that will be world leaders in their respective fields. This will require focusing investment on competitive advantages for the market uptake of European demand-oriented solutions.
- There should be selected leading edge cybersecurity research areas for showing European cybersecurity leadership in the technology. Each research organization should nominate their specific strategic focus areas for the cybersecurity and research organizations should be encouraged to collaborate with each other.
- Similarly, European solutions, standards, technologies and certifications should become **global standards**.
- As a global leader, Europe should attract, develop and retain top talent, especially in the public sector.

# SWOT Analysis

The following SWOT is a summary of task force members' contributions to the SWOT analysis. These items can serve as a basis for your recommendations. For ease of reference each items were given a unique number. For more information on each SWOT item, please refer to the Analytical Report.

**Strengths (What is the EU good at?)**

- S1. Common regulatory framework → regulation is useful for creating a single market and needs to be effectively implemented cross EU. The NIS Directive, the Cybersecurity Act, the Radio Equipment Directive (RED) and in future the European Competence Centre proposal have laid the regulatory framework in the area of cybersecurity.
- S2. Wide research base
- S3. Services → EU is strong in cybersecurity service offerings (downstream part of value chain)
- S4. Large internal market → The EU's internal market has proven to be the strongest one worldwide and currently is the strongest market for cybersecurity products and services
- S5. Cybersecurity ecosystem: many players, local clusters of expertise. Collaboration among players much better than in the US and APAC
- S6. NIS and some other areas very strong: Network and Information System Security (NIS), embedded security, cryptography, block chain, formal methods and privacy… large presence of European players in international top conferences and journals, start-ups, sectors

- S7. Certification and standardization → EU has tremendous knowledge to support global certification and standardization schemes, and these should be (or should become) global standards. For Cybersecurity, however, we are behind other continents. High standards of certification and standardization are strengths in terms of raising user protection levels, but they are a barrier to SMEs. They need to be accompanying measures to help EU start-ups and SMEs raise above these barriers.
- S8. Cybersecurity associations → The organisation of the sector in order to be able to speak and act with one voice through the existence of cybersecurity associations…
- S9. High expectations of security and privacy
- S10. Education → EU has high level of education
- S11. Strong industrial base → Industry in the EU has a core competence in the development on industrial security and embedded security

**Weaknesses (What is the EU not good at?)**

- W1. Lack of Global leaders → the EU lacks large innovating global market players
- W2. Underinvestment → underinvestment in developing and deploying cybersecurity solutions, misallocation or funds, lack of strategy and focus. Investment gap in the proof of concept (POC) and early stage industrialisation/commercialisation.
- W3. Fragmentation → the EU Digital Single Market in this area is not yet developed; different countries have for example developed different cybersecurity certification policies. The Cybersecuirty Act hopes to counter this. Regulatory differences between EU countries, compliance wields differences in export possibilities.
- W4. R&D Gaps → lack of research efforts in some cybersecurity sub-domains. Research institutes are working EU widely within generic topics with limited resources, instead focusing some selected technologies to become global leader within selected cybersecurity area.
- W5. Dependency for Hardware/Software → EU is weak in cybersecurity hardware and software (upstream part of value chain). We rely heavily on foreign players. Local players often lag behind other region-based competitors. In some areas, EU totally lacks local solutions.
- W6. Patenting → difficult to patent software in EU, this gives unfair competitive advantage to US and Chinese players.
- W7. Openness → EU gives open and unguarded access to foreigner to its IP, research, technologies, start-ups and SME. Our best assets are being acquired by foreign players. This them and weakens our local players. We are missing a vision about protecting EU technology. We are being too native.
- W8. Illiteracy → lack of awareness (public, politicians, organisations) about cybersecurity threats (including theft of trade secrets through cyber attacks/intrusions) and solutions, lack of skills
- W9. Dispersion → Many different, uncoordinated initiatives, institutions, efforts. Lack of structures to build collaboration or consolidation within European origin small and medium size cybersecurity companies
- W10. Lack of reliable cybersecurity data related to EU and Member States
- W11. No common vision for European Cybersecurity industry
- W12. Lack of public administrations support to EU cybersecurity products in public procurements
- W13. Lack of cybersecurity professionals

**Opportunities (What are the favourable external factors that could benefit the EU?)**

- O1. Digitalisation → Overall digitalisation, Internet of Things
- O2. Single Market → the EU Digital Single Market
- O3. Labour → Labour market growth
- O4. Unique assets → leveraging unique assets from across the EU
- O5. Differentiation → developing advanced and certified cybersecurity solutions, giving specific advantage to EU solution, especially in procurement criteria
- O6. Training → developing skills and creating cybersecurity ecosystem

- O7. Cooperation → greater cross-border cooperation, notably between research organization and universities networks
- O9. Innovation → promising new cybersecurity start-ups with creative business ideas
- O10. EU has possibilities to test and pilot in different types of regional markets with different types of conditions and languages, if pilot can be scaled cross EU, it is possible to scale globally.
- O11. Strong industrial base (automotive, machine tools, energy, industrial control systems, …) that could help develop a strongly specialized industrial cybersecurity offer for the international market.
- O12. Strong position in High Performance Computing (HPC) and Cryptography.

### Threats (What are unfavourable external factors that could harm the EU?)

- T1. Rapid rise of non-EU markets and large-scale investments: fast growth of non-EU competitors, penetration in critical components in the supply chain.
- T2. Dependency on microelectronics
- T3. Skills competition
- T4. Legal and market barriers
- T5. Espionage → growing global espionage where often governments are involved

# Action levers

In order to "cluster" recommendations by categories, here is a list of **levers** to strengthen the European cybersecurity value chain and help reach the Vision 2030:

- L1. **Norms**: certification, standardization, regulation
- L2. **Procurement**: public and private procurement rules, guidelines or programs
- L3. **Investments**: coordinated strategic investments for technology deployment, new funding sources or modes
- L4. **Collaboration**: enhanced collaboration between local players
- L5. **Technology** : research, development, innovation, proof of concept and technology deployment
- L6. **Skills**: attract, develop, retain, deploy skills, and promote greater awareness
- L7. **SMEs**: measures to help move research outcomes to start-ups, grow start-ups into scale-ups, and scale-ups into competitive global players

# Detailed recommendation descriptions

### High priority

These actions are clear, detailed, with concrete actions, and have received support from several participants. Some of these actions could be part of an coordinated investment.

| | |
|---|---|
| **R12.** | **Use 5G for cybersecurity innovation and services** |

| | |
|---|---|
| Description | 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 represents 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.This is a potential strategic benefit to Europe value chain for cybersecurity as this rollout will result in new technologies being defined for the network and supporting services. These include the Internet of Things (IoT), Network Function Virtualisation, Mobile Edge Computing, Artificial Intelligence, Augmented Reality and Industrial Automation. All of which will require a new generation of security controls. Each will require research, design, implementation, testing of supporting technology. This value chain doesn't stop when the network is live based on the nature of the telecommunications industry. Value is still being made from securing 2G and 3G networks several generations later.A specific target could be enabling the secure use of 5G services by vertical industries like Health, Transport, Manufacturing, Utilities. Each of these critical services are developing embedded systems to improve their end user services. Pair these embedded services with Europe's strengths in the telecommunications industry and the result is a powerful foundation for tomorrows connected era. Each aspect of the supply chain for these services will require technical and procedural protection throughout the lifecycle of the service. Europe can use its current foundations as a springboard to overcome its cybersecurity weaknesses and create a future competitive position in the era of digital enterprises and society. |
| Objectives | • Take full advantage of the possibilities offered by 5G in terms of security by developing and deploying new cybersecurity applications on 5G. |
| Concrete actions | • Create favourable conditions for 5G networks and for its usage in the end points through various embedded systems like for vehicles, utilities, healthcare, and manufacturing.<br>• Support start-ups and research that has a focus on securing strategic 5G services.<br>• Identify key technologies and service requirements for secure-5G and provide funding to accelerate these deliverables.<br>• 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.<br>• Support hardware development for securing 5G technology, such as embedded systems and new appliances introduced in the standards. |

| | |
|---|---|
| Expected benefits | • Become a leader in technology and services to protect 5G enabled services<br>• Leverage new 5G services faster as they are more secure and therefore available to use by a wider range of services (such as health)<br>• Ensure that all the innovation and services made possible thanks to 5G will be secure (which they will not be without adequate cybersecurity applications),<br>• Become a leader in technology and services to protect 5G enabled services<br>• Leverage new 5G services faster as they are more secure and therefore available to use by a wider range of services (such as health) |
| KPIs | • Target Investment amounts to develop solution : xxx<br>• Number / % of services/application that are adequately secured/not secured<br>• Value of 5G cybersecurity solutions market in Europe, value of exports |
| SWOT Items | S4 , S5, S6, O1, O2, W1, T1 |
| Vision Items | |
| Related items | R18, R36, R41, R34(old action R46 has been merged into this one) |
| Related EU initiatives | • 5G PPP and 5G Industrial Association<br>• EU Council recommendations and process of 26 March : http://europa.eu/rapid/press-release_IP-19-1832_en.htm |

| | |
|---|---|
| **R18.** | **Secure highly critical applications and infrastructure: electricity, gas, water, vehicles…** |

| | |
|---|---|
| Description | Critical infrastructures, such as energy infrastructure (including electricity, oil and gas, water and nuclear) are very complex, as other sector depends on them. We need :<br><br>• to improve the cyber resilience in the highly critical infrastructures to avoid as much as possible the unavailability of the essential services supply system.<br>• To 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.<br>• to build and set-up a European-level cybersecurity regulation for critical infrastructures that allows the provision of essential services for the EU.<br><br>The project will work in three directions:<br><br>• Increasing the protection level of the infrastructure assets against cyberattacks.<br>• Developing advanced mechanism of early cyberattacks detecting and prevention systems.<br>• Restoring the system in fastest way when a cyberattack has successes.<br><br>Example: Car industry<br><br>Among the different verticals, EU car industry is a strong asset which world leaders in the EU. This industry is facing multiple security challenge related to new car functions: connectivity, driverless cars, electrification and connection to smart grids. Cybersecurity could be showstopper. Another challenge is to address the certification of the car and its critical functions and not only the subcomponent (HW/SW).Competition is still open in that field as it is really an emerging domain. The EU has strong research base and cybersecurity ecosystem with world leaders in the EU. Automotive is driving the innovation market for new security technologies (HW/SW) for embedded systems. The proposal is to set up security of clean connected autonomous car as a European priority, and to fund coordinated projects both on security solutions development and security certification in that field.The electric vehicles charging sector also comprises many actors with divergent interests leading to heterogeneous security solutions for charging. Manufacturers, users and charging station operators need a confidence model for interconnection and an agreement for charging on the electric grid. |

| | |
|---|---|
| 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 procedures.<br>• To foster the development of specific cybersecurity solutions that satisfy functional and performance requirements coming from critical sectors.<br>• 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.<br>• To create a specific CERT for high critical infrastructure sector at EU level.<br>• Support hardware development for securing embedded systems and automation architectures.<br>• Support development of Scada systems secured by design.<br>• Support development of detection system adapted to industrial protocols and fieldbus.<br>• Identify key technologies and service requirements for automation and provide funding to accelerate these deliverables<br>• Support the establishment of relevant partnerships between automation actors and cybersecurity firms to enhance protection of installations<br>• Develop new equipment to prepare Industry 4.0 to be resilient on the basis of certification and approval systems.<br>• Launch a European coordinated action to develop security, governance and security certification for sector specific applications. |
| Expected benefits | • Securing the whole energy distribution infrastructure and power distribution in the utility domain as well as in the consumer/prosumer domain.<br>• Enhancement of the security level of highly critical infrastructure, including, energy (electricity, gas, oil), water distribution, telecommunications, etc.<br>• Build European leadership on strong innovative global players to position the European cybersecurity and critical sectors secure equipment providers as an international leader.<br>• To increase confidence in the functioning of a critical sector, based on the development of more robust and secure products.<br>• To ensure that new devices have and will maintain a level of cybersecurity appropriate to highly critical infrastructures, reducing cybersecurity costs based on a common framework that enable the selection of the best provider.<br>• To improve the reaction to cyber incidents, sharing information among the relevant stakeholders involved in critical infrastructure management and operation. |

| | |
|---|---|
| KPI | • 100% availabity of critical infrastructures<br>• Cybersecurity Incidents & Responses, the mean time to detect and mean time to respond are good indicators to check the resilience of an installation.<br>• Propagation effect (number of entities affected).<br>• Number of systems that comply with cybersecurity standards and norms.<br>• Adherence to the Security Policies & Compliance: adherence to the appropriate compliance and regulatory policies prevents legal penalties, public fallouts, and loss of the company's reputation<br>• Cost and availability : the cost of cyber investigation, staff and resources employed in locating the incidents, data restoring, and malware removal are other key performance evaluators. |
| Rationale for coordinated investment | • Critical services and infrastructure can't be exposed to cybercrime or cyber-terrorism, European vital infrastructures and installations need a high level of protection for the competition to become<br>• These infrastructures are more and more the target of leakage attempt or ransomware abuse, intrusion protection system should permit to reduce the risk of a massive attack<br>• European CERT (Computer Emergency Response Team) should contribute to prevent and address cybersecurity problems for critical infrastructure. To do that, Europe need skills in this domain and this should be enhanced through the establishment of relevant partnerships |
| Type of investment envisaged | • Critical Infrastructure awareness and modernization: training and awareness programs oriented to obtain the right skills to manage cybersecurity; update of systems with higher levels of security; improve management of crisis (protection and recovery plans).<br>• Certification and Testing labs: to ensure the compliance to cybersecurity standards and norms.<br>• Manufacturing capacity: critical infrastructure equipment providers to supply more secured products.<br>• Software & HW development: to provide cybersecurity solutions specific for highly critical infrastructure sector.<br>• Common and unified European CERT for critical infrastructures.<br>• Specialized research network: to develop new technologies related to cybersecurity in critical infrastructures. |
| SWOT Items | S1, S2, S3, S4, S5, S7, W1, W2, W4,W5, W12,T1, O17, O22 |
| Vision Items | V2. Protection. V3. Independence |
| Related items | R19. R16 |
| Related EU initiatives | • Under the Cybersecurity Act : ENISA and the Commission will create expert groups to provide input to develop certification for specific sectors<br>• NIS Directive: covers already critical infrastructure, such as operators of critical infrastructure, such as notification of incidents. Some actions are voluntary, but could become mandatory.<br>• JRC Pilot Project on IACS |

| R61. | European Cyber Security Fund & Private Investment Portal |
|---|---|
| Description | Europe is lacking venture capitalist market with similar scale as exists in US or China. EU should be actively creating industry specific investment funds which would be collaborated with private investors. There should be investment funds available for scaling cybersecurity industrial companies for cross boarder expansion inside EU and also for growing globally. Investment funds should have similar "best-practices of success" considered as Israel is using for Cybersecurity or South Korea is using for telecom and consumer electronics + cyber range applications.As an example of Israel cybersecurity-fund collects initial investment back with some pre-agreed returning-rate, allowing governmental fund to increase its' value allowing more fund for investments in the future, once financial liabilities are fulfilled for the government, entrepreneurs have liberty to operate freely. For the start Israeli government, provide some innovative procurement programs to help funded companies to get their first customer references and market testing.The discussion on the design of a dedicated Investment Fund in cybersecurity has been initiated by ECSO in cooperation with international private investors already in 2018. According to the preliminary analysis, the first fund should have the size of minimum 120 M€ with a focus on Series A and Series B investment and targeting 4 transactions per year, with tickets of 4M€ investment per company which have 1M€ of revenue as minimum.In addition, the Fund aims to ease the private investors community: in 2017-2018 ECSO organised 4 events designed to cover the different investment phases, ranging from seeding to strategic investment and M&A, as well as to support companies positioned on the entire cybersecurity value chain. |
| Concrete actions | • Create a dedicated fund and the related managing structure for Cybersecurity within the European Fund for Strategic Investments<br>• Design and implement a specific platform aiming to facilitate the meeting between cybersecurity companies and private investors<br>• Establish a Permanent Selection Committee with the double mission:<br>• 1) To evaluate and select the companies looking for investments according to an agreed selection criteria. Liaise the selected companies with the investor community (IC).<br>• 2) To educate and facilitate the understanding of cybersecurity technologies (technical issues) for generic VCs. In parallel, educate and support start-ups and scale-ups in improve their marketing capabilities (à link to inter-regional accelerator programme).<br>• Finance and organise a European Investor Roadshow like the one organised by ECSO (see the 2017-2018 report) |
| Expected benefits | Support the consolidation of the market and the whole EU catch up gap of global cybersecurity industrial and turn the future development become more competitive instead from the losing global market share to the steady +1% annual growth. |
| KPI | • Fund size : 500 M€ ~ 1 billion €<br>• Number of transactions / deals : 50~100 per year<br>• Average transaction size : > 1M€<br>• Number to stakeholders in the Fund ecosystem (investors, experts, targets, associations) |

| | |
|---|---|
| SWOT Items | S3, S4, S8, W1, W2, O1, O2, O7, T1 |
| Vision Items | V1, V4, |
| Related Items | R22, R39, R35, R31, R50, R53 |
| Related EU initiatives | • EIB, EIC, MFF<br>• Venture EU : http://europa.eu/rapid/press-release_IP-18-2763_en.htm<br>• European Fund for Strategic Investments (EFSI).<br>• DE proposal (Digital Europe Programme) under the next Multiannual Financial Framework (MFF): http://europa.eu/rapid/press-release_IP-18-4043_en.htm |

| | |
|---|---|
| **R50.** | **Create a "Cybersecurity Accelerator" network of industry players and regional ecosystems specialised in cybersecurity** |

| | |
|---|---|
| | A network of regional ecosystems specialised in cybersecurity managed by a central acceleration structure to facilitate the rise of pure players able to compete on the global market. The network is made of regional excellence hubs providing scale-ups (and not limited to early stage start-ups) with key expertise and services on the commercialisation phase of their solutions. The accelerator structure is a network support centres focusing on entrepreneurial initiatives in cybersecurity. They could be located in several EU locations that are ecosystems of emerging cybersecurity industry, academic excellence and a conducive entrepreneurial culture.<br><br>Objective:<br><br>• Identifying, attracting and supporting European entrepreneurship in cybersecurity, focusing on innovation beyond fundamental research<br>• Providing an environment for early-stage high-impact companies in cybersecurity to form and thrive<br>• Becoming the forum and network of choice for all players in the European cybersecurity eco-system<br>• Identifying and promoting best practices in cybersecurity technology entrepreneurship across network locations<br>• Driving co-creation between research, entrepreneurs, industry, SMEs, end-users, investors and regional authorities and governments<br>• Thanks to a network of regional ecosystems, this initiative will stimulate better technologies<br>• Ensuring fast-track market access to SMEs. |
| Description | 4 key European services completing the existing local acceleration layer:<br><br>Potential services:<br><br>• Local immersion & regulatory support: coaching/advisory, support services for growth-stage high-impact companies to better understand the local business environments (e.g. application of the NIS directive, GDPR,)<br>• Shared infrastructure, coaching/advisory, support services for early-stage high-impact companies<br>• Unique commercialization expertise through due diligence, market analysis and seed-stage funding<br>• Network of sales and resellers at regional level (link to the DIHs)<br>• Business- design service driving development of a shared European roadmap and vision with all relevant stake-holders to accelerate progress in order to collectively design the best solution<br>• Driving development of a shared European roadmap and vision with all relevant stake-holders to accelerate progress (similar to the roadmaps in the semiconductor industry)<br>• European Industry Roadshow: a series of competition day at regional level to give best EU scaleups visibility to international investors. Investors deck preparation and readiness coaching is part of this service.<br>• Conferences and workshops as condensation points for a European eco-system in cyber security<br><br>Funding options: |

| | |
|---|---|
| | • Seed-funded by regional authorities and the EC, supported by established industry players (including VC and family offices)<br>• Providing paid-for services to startup investors and industry<br>• In long-term, attracting private-sector funding by running a seed fund for cybersecurity ventures |
| Concrete actions | • Create a "Cybersecurity Accelerator" network of regional ecosystems specialised in cybersecurity ("Cybersecurity Valleys") |
| Expected benefits | • Greater vertical and horizontal collaboration between all players in the value chain<br>• More innovation, best-practice sharing, consolidation around best-in-class<br>• Emergence of European competitive and high level SMEs and companies on cybersecurity |
| KPI | • |
| SWOT Items | S5, S4, S2, W3, W4, W9, W10, W11, O2, O7, O8, O9, T3 |
| Vision Items | V4. Leadership |
| Related items | R61, R69 |
| Related EU initiatives | • Commission initiative on Digital Innovation Hubs in the framework of the Digital Europe Program<br>• Commission proposal for a Cybersecurity Competence Centre.<br>• EIB, EIC |

| **R34.** | **European Data Space: create a framework and infrastructure for secure data communication, storage and handling** |
|---|---|
| Description | We already have a dedicated European-wide communication framework and infrastructure for secure data sharing in some sectors (banking, personal identification, health, social security and pension data → CEF: connected European facilitation network).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 |

| | |
|---|---|
| Concrete actions | • Develop cloud framework with high level of authentication and secure data lake.<br>• Enable secure and privacy enhancing End-to-End communication between devices, individuals and legal entities for pan-national and pan-sector specific use<br>• Create a dedicated European-wide harmonised communication framework and infrastructure for secure data sharing<br>• Support the cybersecurity analysis of emerging technologies (Artificial intelligence , quantum, cognitive technologies…) and their use in innovative protection products, services and processes |
| Expected benefits | • Support European autonomy and sovereignty for industry and citizens privacy |
| KPI | • Information confidentiality for citizens and companies should be enforced with those type of framework, ensuring a privacy high level.<br>• All data vulnerabilities, including internal and external, along with their aging, can help the security professionals validate the effectiveness of the imposed security structure |
| Expected investment amount | • ~100 M€ |
| Type of investment envisaged | • Creation of the European Data Space Platform for connecting Data Providers and Data Users.<br>• Definition of the Gobernance rules of the Platform<br>• Standardisation and certification frameworks for a secure data exchange with the possibility of certifiable software, systems and services part of the European Data Space Platform (EDSP) or users of the EDSP.<br>• R&D for new components of the EDSP using AI, cognitive technologies, …<br>• Deployment of the European Data Space Platform in specific verticals (banking, automotive, energy, cybersecurity, …) as well as cross-sectorial domains.<br>• Deployment of the European Data Space Platform at national and regional levels. |
| Rationale for coordinated investment: | • Depending on the US cloud infrastructure, such as Amazon, Azure, or other Google platforms is a weakness for information and data security in Europe, affecting confidentiality and privacy of European citizens and firms. Moreover, industrial systems are increasingly dependent on cloud services. Having a European sovereign solution is a key point to protect this critical infrastructure and for intellectual protection in all the domains. |
| SWOT Items | |
| Vision Items | V2. Protection, V3. Independence |
| Related items | R21, R6 |
| Related EU initiatives | • German “Industrial Data Space”<br>• Industrial Data Organisation (IDS) |

| R66. | **Create the next generation EU framework for PKI infrastructure and European DNS management for critical infrastructure** |
|---|---|
| Description | Public Key Infrastructures (PKI) and the Domain Name System are two extremely relevant enabling element to create and maintain a trusthworty and reliable European Digital Society.PKIs play a key role in establishing trust over the Internet as allow on a side to mutually authenticate parties (human or machines) an on the other, if used correctly, to secure communication channels and data. Today however, many PKI (Public Key Infrastructure) applications are not accepted on the long end, due to the lack of access to open, trustworthy, affordable and well-recognized PKI infrastructure, (i.e. cross-border applications for eHealth, eID, intelligent transport systems, e-government services etc). This is a clear obstacle to the development of a more interoperable and secure digital space.The DNS is instead part of the backbone on which every digital service is built on today. Even if the Internet has no central coordination point, its addressing structure is centrally coordinated through its DNS, roughly speaking a set of hierarchical phonebooks, where names of "online services" are associated with IP numbers. For example, the DNS ensures the mapping between www.nature.com and its IP address, 151.101.240.95. Without DNS, the majority of the Internet Services would not be accessible, including those services which are typically considered "critical". In other words, its operation is today essential for the European Digital Society.This consideration let emerge two major issues:1) DNS was believed to be extremely roboust, however, cyberattacks happened in the recent years (e.g. Mirai attack), demonstrated how its infrastructure is today potentially vulnerable.2) The governance of DNS, since its creation, has been in the hands of ICANN, a private organisation under the US law.The fact that ICANN in practice "sets the rules for the Internet addressing systems making Internet based services available" implies that its decisions have a global impact on online services and on citizensThese two points highlight how is in the interest of Europe to ensure (1) that DNS is adequately protected and fit to answer to the challenge of the full digitalisation of the European Society, and (2) the alignement of its governance with the European interests. |

| | |
|---|---|
| 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 an European Standardisation Organization (ESO) to create a harmonised PKI standard. It would aim at the definition of a common trustworthy Authentication Framework.<br>• 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.<br>• Establishment of 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<br>• 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).<br>• 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…) |
| Expected Benefits | Support European digital space security, autonomy and sovereignty: A framework providing in one hand PKI infrastructure, and on the other hand trustworthy European DNS, would contribute to several market segments using critical technologies (Digital identities – biometrics, IoT security). A European DNS would make internet exchanges more reliable: ICT-internet and Private Network should be understood as solutions within the presented value-chain. These two approaches will impact many sectors and more precisely the critical ones as defined by NIS directive (Energy, Transport, Financial Services, Health, Water, Digital Infrastructure) |
| KPI | • Successful harmonisation of European PKI infrastructures<br>• Definition of an European PKI standard<br>• Successful EU engagement in the international debate on DNS governance<br>• Establishment of a European Secure DNS infrastructure |
| Expected investment amount | • 100 M€ - 500M€ |
| Type of investment envisaged | • Standardisation, manufacturing capacity, software development and infrastructure. |
| SWOT Items referred to | S3, S4, S5, S6; W1, W5; O1, O2, O4, O5; T1 |

| | |
|---|---|
| Vision Items referred to | V2. Protection, V3. Independence, V4. Leadership |
| Related items | R9. |
| Related EU initiatives | |

| **R29.** | **Leverage public procurement in order to increase the overall levels of cybersecurity** |
|---|---|
| Description | Public procurement guidelines designed for contracting authorities/entities or targeted private entities would include minimal security requirements in terms of cybersecurity. This guidelines could be recommended for any public procurement project and/or be mandatory for EU financed projects.When procurement is done or co-funded by EC, guidelines including requirements for a European reference in procurement should exist.Referring to EU certification scheme in public procurement would trigger companies to comply with EU standards.The EU should focus those procurement frameworks on the most vital parts of the value chain first and build upon existing frameworks whenever EU ones are missing.It should be avoided that certain procurement criteria can only be met by non-EU companies. It is important to highlight that the best cybersecurity solutions should be a priority and mechanisms are needed to ensure that European players can reach in time appropriate levels of security.Such a procurement framework could potentially also be applied in the private sector. The extent to which this is possible should be explored.There could be a specific consideration given to EU start-ups and SMEs.Example: most health players are public, and most develop their own systems, and most systems are not secure. Public procurement can be a tool to push for development of state-of-the art, competitive, providers of secure IT services in Europe, by providing them with clear market opportunities. Guidance may be introduced to encourage (or force) minimal security requirements (which will require specialised external providers, and which may exclude low-cost low-quality providers). |
| Concrete actions | • Promote the uptake of the cybersecurity certification framework (a standard) criteria into public sector procurement. |
| Expected benefits | • Higher level of protection for all public institutions and infrastructure in the EU.<br>• More advanced and higher quality produced developed thanks to a “market-pull” effect.<br>• A more dynamic, innovative and expanding European cybersecurity industry serving a growing local market. |
| KPI | • Public expenditure on Cybersecurity at EU, national, regional and local levels<br>• Level of protection at public institutions/infrastructure (firewalls, antivirus, incident detection…)<br>• % of such expenditure awarded to EU players<br>• % of innovative solutions (ie: that did not exist 3, 5, 10 years before) |

| | |
|---|---|
| SWOT Items | S1, O2, T4 |
| Vision Items | V1. Market share, V2. Protection, V3. Independence |
| Related items | R51, R52, R17, R54 |
| Related EU initiatives | The Defense and Security Procurement Directive (2009/81) |

| | |
|---|---|
| **R6.** | **Promote greater sharing of cyber threats, vulnerability and incident information** |

| | |
|---|---|
| Description | 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 expertise 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 counter- measures.This body will act as 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.This points to two main issues when it comes to cybersecurity information sharing in Europe:<br><br>• Lack of harmonisation or automatized mechanisms as regards data breach notification and / or incident reporting requirements. NIS and GDPR are only two of the current reporting requirements (applied across sectors) but when looking at specific sectors, there are several other regulations to consider. I.e. in finance, in addition to NIS and GDPR, one must also consider eIDAS, Target2, PSD2, and ECB reporting requirements, each of which have different taxonomies and ontologies, timeframes and templates for reporting. There is a huge fragmentation of approaches here which leads to lost time that should be used for response.<br>• Information sharing on cybersecurity as it currently stands, whether through entities such as ISACs or open source platforms, is usually performed ex-post which means its purpose serves mainly for statistics or adapting behaviour for future mitigation. Moreover, information sharing for a tend to include users/operators, solution providers, and consultancies alike, meaning that intelligence sharing on trends and threats and trust-building is impeded. The introduction of tools and solutions that facilitate trust, a simple and anonymous exchange of information and a simple and understandable re-use of information exchanged would be beneficial for all stakeholders, but this should be considered in a tiered approach to allow for users/operators to gather in a trusted environment for sharing of information and intelligence.<br><br>The EU should embrace a similar system to Coordinated Vulnerability Disclosure (CVD) that will allow European digital entities to share potential threats, backdoors, and overall weaknesses in systems and designs before any data breach of incident may occur. In addition, an EU-wide approach is essential to prevent a scattering of national approaches to vulnerability disclosure. An EU coordination body or steering group that defines a standard for intelligence and information sharing and helps to keep things federated and synchronised could be envisaged, fitting in more easily with existing domestic sharing structures, and with ENISA, Europol/EC3 and the NISD CSIRT Network.Make sure that more organisations introduce policies in the field of coordinated vulnerability disclosure (so that hackers that find vulnerabilities report this to a designated organisation so that they can be solved). More insight into vulnerabilities means that the products and services will get better. Once a climate starts to exist in Europe where reporting these vulnerabilities becomes the norm quality security automatically improves. This will also safeguard a better quality of the information being shared, meaning that preventive and responsive measures will improve Governments can play an important stimulating role.So Cyber Security information harmonization means the development of dedicated Ontology and Taxonomy on a specific language or also cross |

| | |
|---|---|
| | languages. The derived semantic interoperability is the fact of sharing standard terminologies between stakeholders/end-users on their communications, chats or exchanged reports. If they communicate using a common semantics, it means the understanding of a message is easier and smarter. This can lead, after a common reasoning about a specific theme, the decision makers to operate quickly, so saving time on reaction and moving immediately to operational activities.Setup a policy ensuring access to detected vulnerabilities to stakeholders. Provide security researchers clear guidelines to coordinate disclosure of vulnerabilities. |
| Objectives | • Improve the collection, structuring (through standardisation), sharing and usage of threats, vulnerability and incident information including<br>• Improve cyber threat detection and hunting, coordination of vulnerability disclosure, including using with AI<br>• Improve EX-ANTE analysis by means of advanced behavioural algorithms such us Emotions and Computational Stylometric analysis; so understanding the Human Factor side inside natural language contents<br>• Improve EX-POST analysis by using AI/Cognitive algorithms on occurred events and case histories |
| Concrete actions | • Implement and optimize existing rules, guidelines and framework for disclosure and information sharing on incidents/breach reporting and for vulnerabilities detection.<br>• 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.<br>• Create a Cyber Security Ontology and Taxonomy on a specific language and cross languages. So, putting human/domain expert know-how into a cognitive computing engine (based on either Semantics or Machine learning)<br>• Create (manually or automatically) the semantic rules in order to apply categorization, entities/relations extraction and consequent terms normalization automatic activities<br>• 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.<br>• Strengthen the role of trusted intermediary parties (as in the case of the MISP).<br>• Promote a culture of (inhouse) ethical hacking.<br>• Define an ISAC standard (guidelines, requirements) paper in cooperation with CEN CENELEC JTC13 (cybersecurity TC) covering the ISAC information management, processes etc. 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 EU |

| | |
|---|---|
| Expected benefits | • Sharing relevant data is vital for the single market to function.<br>• Reduced fragmentation of approaches<br>• Coordinated measures and platforms for information sharing, intelligence sharing and crisis management (note : the Blueprint for sectoral cooperation on skills (Skills Agenda for Europe) foresees more than that).<br>• Improved 24/7 automatic analysis with no human subjectivity<br>• Reduced time from the Request for Information to the specific concrete action on the field<br>• Interoperability and exchange of data<br>• Improved understanding and response to threats and incidents, so reducing time to operational tasks<br>• Improved understanding of behaviour of (potential) cyber attackers<br>• Improved understanding of citizen perception about digital innovation (web campaign) |
| KPI | • Number of incidents/threats/vulnerabilities reported, intercepted<br>• Number of categories and hierarchy levels in the taxonomy<br>• Number of concepts included in the ontology<br>• Number of European languages considered<br>• Number of semantic behavioural attributes extract from analysed contents (Human factor attributes) |
| SWOT Items | S2, S5, S8 |
| Vision Items | V2. Protection, V4. Leadership |
| Related items | R7, R10, R4, R21 |
| Related EU initiatives | • ECCC, ENISA, NIS directive, Cybersecurity Act<br>• Must take account of the status quo – provisions of the NIS Directive and in particular the cooperation in the CSIRT Network, Cybersecurity Act. Make recommendations on that basis.<br>• YesWeHack present ZeroDisclo.com. This non-profit platform provides the technical means and the required environment for all to adopt the coordinated reporting of vulnerabilities commonly known as "Coordinated Vulnerability Disclosure". https://zerodisclo.com/header/01_how_it_works/ |

| **R54.** | **Increase innovative public procurement** |
|---|---|

| | |
|---|---|
| Description | European cybersecurity products and solutions that manage to cross the "Valley of Death", *i.e.* from research to market, are not widely deployed across European and global markets. European cybersecurity industry has developed largely on the basis of national governmental demand, including the defense sector. In parallel a multitude of innovative SMEs has also emerged both in specialty and niche markets (e.g. crypto systems) and in well-established markets with new business models (e.g. antivirus software). Despite this evolving market structure companies still have difficulties growing outside their national market. While European companies tend to be strong and innovative, their size and capacity (mostly SMEs) are smaller in comparison to their global competitors.European Union should develop a new program from innovative cybersecurity procurement scheme. Program should start from EU own procurement and to scale all the member states.Innovative procurement should be based on describing the problem or challenge, not solely strictly defined technical specifications. Public procurement plays also a crucial role in providing public references to European companies and especially SMEs and start-ups entering the market.Whether offering consists SME based products or services, it should be more favoured. EU should sponsor Member State with providing for example 10-20% support for MS (out of purchase value) if they follow EU recommendation.There should be also encouragement for find European cybersecurity solutions from other Member State. If offering consists cybersecurity products or solutions from other Member State, there should be some additional funding provided by EU. |
| Concrete actions | • Develop a new decisive program for innovative cybersecurity procurement scheme.<br>• Create incentives to find European cybersecurity solutions from other Member States for national procurements. |
| Expected benefits | More EU cybersecurity SME based innovations finds a way to market, with real customer reference, and practical feedback from the market. Cross boarder, collaboration encouragement dismounts practical trade barriers inside European Digital Single market. |
| KPI | |
| SWOT Items | S1, S3, S5, W1, W2, O4, O5, T3 |
| Vision Items | V1, V3, V4 |
| Related items | R29 |
| Related EU initiatives | |

| | |
|---|---|
| **R39.** | **Clarify and raise awareness of the role of the various European bodies involved Cybersecurity: ENISA, ECSO, ECCC, regions…** |

| | |
|---|---|
| Description | Fragmentation is a key weakness of the EU, notably in Cybersecurity. This fragmentation is seen at all levels, not just between countries but also between various EU institutions. This results in an inefficient environment for regulation, funding R&D, strategic infrastructure, public procurement, standardisation, and certification. Europe must have **coordinated actions for Cybersecurity** (along the same model as the US Federal Aviation Administration, or the European Space Agency) and seek strategic autonomy.Responsibilities need to take account of the European political landscape and are include ENISA, FCC, ECSO and the various DGs of the EU Commissions, the national agencies (ANSSI in France, BSI in Germany…) and regional authorities.The scope of ENISA has recently been reinforced with the "Cybersecurity Certification Framework", and its role could be further expanded in the future, excluding the creation of standards (which should come from standardisation bodies and driven by market demand).The following responsibilities need to be allocated to one or several agencies, as appropriate:<br><br>• act as the **European Authority** on all matters related Cybersecurity (such as to produce certification schemes, standards, propose draft regulation),<br>• set **procurement guidelines** or rules, for public / private organizations, and sharing among Member States.<br>• establish innovate **procurement** program for cybersecurity to speed up global regaining market share,<br>• disseminate knowledge, share good experiences,<br>• provide/channel **funding** for hardware, software, services, infrastructure, industrial deployment,<br>• launch calls for projects,<br>• build partnerships between industrials and research stakeholders from different countries, and work closely with already structured **regional cybersecurity ecosystems,** in order to develop European Cybersecurity value chain,<br>• manage European funds to finance Cybersecurity research,<br>• **Monitoring market data** for agile decision making (see V1)<br><br>Ideally, we should have a "**one-stop-shop**" European body would be the main partner of companies and research organizations working in the field of Cybersecurity. It could have branches in several member states / region, based on the presence of local industrial and technological players. |
| Concrete actions | • Create a European optimised NIST-like framework |
| Expected benefits | • Vital to preserve sustainability of digital society and economy.<br>• Hard to do by Member States themselves. |
| KPI | |
| SWOT Items | • S1, S5, S7, W2, W3, W4, O7, T4 |
| Vision Items | V1. Market share, V2. Protection, V3. Independence, V4. Leadership |
| Related items | R35 |

| | |
|---|---|
| Related EU initiatives | • The Commission proposed for a Cybersecurity Competence Centre (CCC) and network.<br>• Cybersecurity Act |

| **R35.** | **Develop a comprehensive EU strategy to support EU players in critical cybersecurity areas** |
|---|---|
| Description | To focus investment on competitive advantages for the market uptake of European demand-oriented solutions. It is essential to involve European operators and final users for the identification of needs and requirements. European Cybersecurity suppliers (especially SW companies) need to gain more support to accelerate in scale, and grow faster.Therefore the EC should promote the inception of a Master Plan to deploy an EU Cybersecurity Investment program funded by all EU financial instruments available (Horizon Europe, Digital Europe, InvestEU, European Investment Bank, etc...).Indeed, public funding is essential to stimulate and catalyse public & private operators (financial services, transport, energy, utilities, etc...) long-term investments through European collaborative projects in specific verticals within an Investment program... This is in the essence of the EC as regards SVCs and IPCEIs.One of the problems of the European Union is that there is little or no public procurement at the EU level (there are many national initiatives, but often with insufficient scale to compete with similar Chinese or US initiatives).The future EU centre of competence shall be key for its conception and implementation. |
| Expected benefits | |
| KPI | |
| Concrete actions | • Create a large funding platform and program to support high-potential cybersecurity players, or to invest in critical/sensitive areas (energy, transport, health). |
| SWOT Items | |
| Vision Items | V4. Global Leader |
| Related items | R39, R61 |
| Related EU initiatives | Horizon Europe, Digital Europe, InvestEU, European Investment Bank, European Strategic Fund, national Public Investment Banks, Sovereign Investment Funds, |

| **R58.** | **Fast-track Research to the access on the markets** |
|---|---|

| | |
|---|---|
| Description | Often cybersecurity solutions and products are aging fast and market access for SMEs is particularly difficult and market access for SMEs is particularly difficult. Industry is dynamic, and often baseline research takes a long time.One challenge is to getting industry involved or collaborating with research, and then commercialise the developed solutions. Majority of cybersecurity industry is relatively small incapable to sacrifice key resources for time consuming collaboration with slow progressing research, not paying off in the next months.Cybersecurity research and cybersecurity ecosystems need a new type of market test-bed-model, and fast track market access to commercialise these solutions. That would allow researchers to test market innovation already in the early stage with the market, is there some critical, revolutionary ideas or finding which have real interest of market and if those are really having some opportunities to survive in the future. It could allow "research team" to cope also with some SMEs more closely.In case there is no SMEs, researchers could be creating "test-bed company" for measuring market reaction for the idea. If "test-bed" is passed with base evaluation requirements, it could be introduced to private investors already in the early stage, and parallel research team may still continue research work with higher motivation in order to expecting to meet better real-market demand. |
| Concrete actions | • Dynamic cybersecurity research model<br>• Designing an interregional acceleration program to create a market place with reduced costs for local SMEs to commercialize their solutions. |
| Expected benefit | European cybersecurity research would become more agile. It could be more collaborating with the industry which contain mainly in cybersecurity SMEs. Research investments and focus would be better coordinated, with less failures expected. |
| KPI | |
| SWOT Items | S3, S5, W3, W4, W6, O4, O6, O7, T3 |
| Vision Items | V1, V3, V4, |
| Related items | |
| Related EU initiatives | • FP9 |

| | |
|---|---|
| **R21.** | **Shared Database for AI development in cyber security** |

| | |
|---|---|
| Description | The adoption of AI and machine learning for security uses are slowed down because it is difficult to access real data and attack data for sensibility reasons. It would be helpful to have a shared database at the European level of attacks and legitimate data (facts, events, network flows, etc.).The shared database could also be composed by different remote databases as in a network of federated databases. The important fact is to have a normalized terminology stored into databases so to improve, to maximize the comprehension and inter communications between final users. Terminologies in multiple languages can be managed by means of a specific semantic layer for normalization and correlation tasks either in the storing phase or in the retrieval one.And more, having a powerful and federated cognitive search engine, based on deep semantic analysis, is a must so that end-users and stakeholders can access remotely and in an easy way also using natural language questions, so not only Boolean operators as in the standard search engines. The same end-users can browse the databases using the extracted semantic attributes, so allowing them to be guided and transforming a normal search activity into a discover one. |
| Concrete actions | Definition a Cyber Security data model based on a dedicated taxonomy and ontology also in a multi-language modeDeveloping an avant-garde cognitive engine capable to accept natural language questions also by different languages (f.e European official languages)Developing an avant-garde discovering engine |
| Expected benefits | Smarter and easier access to stored informationEnhanced capabilities to discover (not only searching) targeted contents by using extracted semantic attributes/tags other than metadata |
| KPI | |
| SWOT Items | S2, W12, W14, W15, O17, O22, T23, T25 |
| Vision Items | V3. Independence |
| Related items | R20, R6, R7 |
| Related EU initiatives | • UE strategy on AI.<br>• Project AI4EU<br>• Research programs : FP9, DEP |

| | |
|---|---|
| **R36.** | **Assess the necessity for mandatory cybersecurity certification or general cybersecurity legislation for all IoT products** |

| | |
|---|---|
| Description | Anything ‘smart’ can also be vulnerable. Even if devices are smart and connected, they are not always upgradeable, and eventually they will become vulnerable for attacks. The EU should promote the security of B2C IoT devices and consumer products.The Cybersecurity Act establishes a framework for the establishment of European cybersecurity certification schemes for ICT products and services and defining these along the lines of ICT products and services which require high, substantial and basic assurance levels.As a function of their criticality, mandatory certification for certain industrial IoT devices (consumer, industrial, medical…) could be introduced through a specific sectorial legislation. Alternatively, horizontal legislation could include cyber security as part of product safety requirements and CE-marking. |
| Concrete actions | • Explore the necessity and feasibility of horizontal legislation such as the Review of the Radio Equipment Directive to include cyber security as part of product safety requirements and CE-marking.<br>• Develop basic level cyber security standards (e.g. with ETSI, CEN CENELEC). |
| Expected Benefits | Increase cyber security awareness of consumers and wider public. Protect European consumers of B2C IoT and smart devices. Possibility of leading in developing global standards. |
| KPI | |
| SWOT Items referred to | S1, S4, S7, O1, O2. |
| Vision Items | V2. Protection |
| Related items | R4 |
| Related EU initiatives | • Cybersecurity Act |

| **R22.** | **Support emergence of a European cloud service that can provide the highest levels of security and functionalities, and can compete internationally** |
|---|---|
| Description | Depending on the US cloud infrastructure, such as Amazon, Azure, or other Google platforms is a weakness for information and data security in Europe, affecting confidentiality and privacy of European citizens and firms. Moreover, industrial systems are increasingly dependent on cloud services. Having a European sovereign solution is a key point to protect this critical infrastructure and for intellectual protection in all the domains.Several European start-ups have tried to create a local solution, sometimes with the support of local governments, and sometimes with much better security and functionalities that the solutions of global leaders (Dropbox, Google Drive, One Drive, Amazon AWS…) but most have failed to reach sufficient to become viable.The automotive industry has its own cloud service called “BNX”, where all the OEMs (Renault, BMW…) and Tier1 suppliers share data on a very high security platform. All the big European players (Siemens, Schneider…) have their own in-house system. In Germany, there is even a dedicated secure cloud service for SME.In all these examples, successful could service benefit for the support of strong backers (either public authorities, or key users). |

| | |
|---|---|
| Concrete actions | • Public investment funds (EFSI, national sovereign funds) to invest in the development of a promising existing European cloud service and boost it to global scale<br>• Public administrations to use European cloud services for data storage (ie: procurement legislation)<br>• This cloud service should incorporate some new value-added technology, to justify dedicated funding and procurement requirements.<br>• Develop and use a competitive European cloud based on open solution such as *OpenCloud* will allow development of autonomous and protected services (see *Orange* or *Numergy* in France).<br>• |
| Expected benefits | • Independent, secure, competitive and high-performance could storage and other cloud services for all EU players<br>• Sovereignty, user data confidentiality and privacy, hardware and software security. |
| KPI | • |
| SWOT Items | S3, S4, S5, W10, W11, W15O18, O19, T25 |
| Vision Items | V3. Independence |
| Related items | R61, R29, R54 |
| Related EU initiatives | |

| | |
|---|---|
| **R16.** | **Develop and strengthen a highly skilled workforce in all parts of the cybersecurity value chain** |

| | |
|---|---|
| Description | Foster a greater education and awareness system for cybersecurity solutions within Europe – focusing on all parts cybersecurity value chain (from research to service)In an ever-increasing digitalisation world, developing digital skillsets is now more important than ever. There are not enough professionals with the knowledge and skills to protect, data systems and networks from cyberattacks.A true cybersecurity skill shortage persists in Europe. Moreover, general understanding of cybersecurity knowledge and certifications is missing.In addition, it is critical to note that many cyber-attacks/ incidents occur through human error that is entirely preventable. As many studies have shown, even just considering that regardless of educational efforts 4% of people will click on any given phishing campaign means that 100% security in hardware will not prevent cyber-attacks.Therefore, a skilled workforce is missing in EU and competition is strong. EU should map out the skills needed along the value chain, identifying also means to fill the gap and relevant timeframe for implementation alongside looking to retain cybersecurity specialists. EU could help universities and other education/ training institutions to build new degree courses in cooperation with industry and built on excellence of European academic research, operation education and training for cybersecurity specialists, both in the research, development of products and solutions and in operating cyber secure systems, with a strong knowledge of EU products. This action would also benefit from a larger availability of test facilities for cyberattack simulations, subsidized penetration tests of business systems and Training Facilities like Cyber Ranges.The creation and coordination of a network of interoperable federation of cyber ranges to train in cybersecurity, staff coming from start-ups, SMEs and large companies, critical infrastructures, as well as students at different educational levels (primary and secondary school, university, professional training) would be of interest. Special attention could be devoted to sectorial cyber ranges for industries like energy, automotive, transport, finance, health…<br><br>It is a methodology, proposed in the Skills Agenda for Europe, for strategic sectoral cooperation for skills. What you probably propose is to launch a sector skills alliance that will implement the Blueprint in Cybersecurity. And by the way Cybersecurity is one of the eligible sectors for Erasmus+ Sector Skills Alliances implementing the Blueprint. Erasmus+ call for proposals expected in October 2019. |
| Objectives | • Europe needs to look at public procurement from a new perspective and through security lenses. A certain level of European independence, with competitive and state-of-the-art European solutions in key areas, is crucial.<br>• 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 layers from European providers where possible.<br>• The objective of this action is to use public procurement as a level to:<br>  o increase the level of cybersecurity in Europe,<br>  o boost the market for advanced and high quality cybersecurity solution,<br>  o promote European solutions in public procurement,<br>  o support the European cybersecurity ecosystem. |

| | |
|---|---|
| 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.<br>• 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.<br>• Launch a sector skills alliance that will implement the Blueprint in Cybersecurity.<br>• Map skills demand and launch a sector skills alliance that will implement the Blueprint in Cybersecurit<br>• 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. |
| Expected Benefits | • With a substantial increase in European expertise, who are at the forefront of cybersecurity solutions, this will not only ensure that Europe has the global experts, researchers into cybersecurity solutions, but also that the likely outcome of cybersecurity innovative solutions well derive and flourish in Europe.<br>• Training people from a young age, allows for retaining cybersecurity talent in Europe.<br>• EU certification for instance young college students, explaining common risks and solutions would promote the cybersecurity profession, which ensures cybersecurity hygiene and improves solutions quality in the long-term.<br>• Improve awareness of citizens and companies on cybersecurity matters.<br>• Creation of a new generation of cybersecurity professionals taught in learning by doing.<br>• Possibility of executing cyber exercises at different scales depending on specific needs.<br>• Higher competitiveness of European cybersecurity industry.<br>• Improve the core cybersecurity digital skills and understanding in Europe. |
| KPI | • Increase the number of European citizens receive (some form) cybersecurity education certification.<br>• Raise the overall understanding and knowledge of EU citizens in relation to cybersecurity.<br>• Successfully (re) train 30% of workforce on cybersecurity skills by 2025.<br>• Increase the number of cybersecurity professionals by 2022 (currently 350,000 in Europe) |

| | |
|---|---|
| SWOT Items | S2, S3, S5, S9, O3, O6, T3 |
| Vision Items | V1, V2. Protection, V3, V5 |
| Related items | R28 |
| Related EU initiatives | • There is a methodology, proposed in the Skills Agenda for Europe, for strategic sectoral cooperation for skills.<br>• Cybersecurity is one of the eligible sectors for Erasmus+ Sector Skills Alliances implementing the Blueprint. Erasmus+ call for proposals expected in October 2019. |

| | |
|---|---|
| **R7.** | **Develop and maintain European excellence in cyber threat understanding and hunting** |

| | |
|---|---|
| Description | European policymakers have acknowledged the value of voluntary cyber threat information sharing to understanding the threats, protection, information and networks, and how to preventing cyber threats 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. This points to two main issues when it comes to cybersecurity information sharing in Europe:1. Lack of harmonisation or automatized mechanisms as regards data breach notification and / or incident reporting requirements. NIS and GDPR are only two of the current reporting requirements (applied across sectors) but when looking at specific sectors, there are several other regulations to consider. I.e. in finance, in addition to NIS and GDPR, one must also consider eIDAS, Target2, PSD2, and ECB reporting requirements, each of which have different taxonomies and ontologies, timeframes and templates for reporting. There is a huge fragmentation of approaches here which leads to lost time that should be used for response.2. Information sharing on cybersecurity as it currently stands, whether through entities such as ISACs or open source platforms, is usually performed ex-post which means its purpose serves mainly for statistics or adapting behaviour for future mitigation. Moreover, information sharing for a tend to include users/operators, solution providers, and consultancies alike, meaning that intelligence sharing on trends and threats and trust-building is impeded. The introduction of tools and solutions that facilitate trust, a simple and anonymous exchange of information and a simple and understandable re-use of information exchanged would be beneficial for all stakeholders, but this should be considered in a tiered approach to allow for users/operators to gather in a trusted environment for sharing of information and intelligence.EU has strong research base and cybersecurity ecosystem. Maintain its excellence in threat mastering through R&D in attacks, ethical hacking, bug bounty, market survey, and vulnerabilities sharing. Security analysis of emerging technologies (AI) is also a key subject that the Commission will tackle with increased international collaboration between national cybersecurity competence centres. The future European Cybersecurity Competence Centre (ECCC) and stakeholder community should help in this process. The EU could encourage alliances between companies involved in cyber threat detection / hunting to get a volume effect in analysis and machine learning to be and develop an EU threat intelligence capacity. Putting together different European technologies so to improve EU Cyber Threats intelligence capability, such as understanding events in advance (EX-ANTE) and studying them after they've occurred (EX-POST). A particular focus is to invest on biometrics technologies as for example the following ones applied on content coming from the web or any other source:<br><br>• **Emotions analysis** that is able to extract anxiety, stress, fear, .. so not only the capacity to extract sentiment (positive, negative or neutral) but going in depth analysing the specific mood referred to a specific people, organization, infrastructures, ..This enables end-user to understand future potential actions on dedicated targets<br>• **Styometric analysis (Writeprint)** that is able to extract conjunctions, verbs, adjectives, vocabulary richness and complexity, lexical differentiation and usage of specific jargon, slangs, etc. strictly related to specific human factors and behaviour. The target is, f.e, to understand if a writer has a style of writing which can be related to criminal groups or if published content on the web using different accounts/nicknames are actually related to the same person. This can contribute to report malicious profiles on social network that may be involved, at various level, in "cyber security threats" |

| | |
|---|---|
| | It might also help the EU larger emerging ethical hacking platforms (comparable to US Hackethone 150K members). The establishment of an EU community of ethical hackers and cybersecurity professionals would not only create a culture of trust and provide a mechanism for stakeholders to obtain advice on threats & trends, but it could also facilitate the emergence of EU players in cybersecurity. Foster intelligence sharing as regards threats, trends and lessons learned among different verticals, governments and other key actors such as national CERTs and law enforcement. Develop links with the users and operators. Raising the discussion around CvD amongst cybersecurity stakeholders and vendors. |
| Concrete actions | • Develop rules, guidelines and framework for disclosure and information sharing on incidents/breach reporting and for vulnerabilities detection.<br>• Create a Cyber Security Ontology and Taxonomy on a specific language and cross 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<br>• Create a “Cybersecurity Information Sharing Network” where parties can join on a voluntary basis, and adhere to specific information sharing rules (L4)<br>• Support research in attacks and vulnerability analysis<br>• Support cyber threat intelligence sharing and analysis platforms for different verticals, governments, and national CERTs and law enforcement<br>• Concerning worldwide private actors, support the idea to split Worldwide Cyberthreats Intelligence platforms (receiving all cyberthreats data from customers) by creating European CyberThreat Intelligence platform restricted to data coming from European customers |
| Expected benefits | • Enhance EX-ANTE analysis capabilities<br>• Enhance EX-POST analysis capabilities, so improving understanding and reasoning about lesson learned |
| KPI | • Number of semantic behavioural attributes extract from analysed contents (Human factor attributes) |
| SWOT Items | S2, S5, W2, W4,W5,T1 |
| Vision Items | V4. Leadership, V2. Protection |
| Related items | R6, R10, R4 |
| Related EU initiatives | - Must take account of the status quo – provisions of the NIS Directive and in particular the cooperation in the CSIRT Network, Cybersecurity Act. Make recommendations on that basis.- YesWeHack present ZeroDisclo.com. This non-profit platform provides the technical means and the required environment for all to adopt the coordinated reporting of vulnerabilities commonly known as "Coordinated Vulnerability Disclosure". https://zerodisclo.com/header/01_how_it_works/- YesWeHack (since 2013) #1 european bug bounty platforme with 10k members |

| **R8.** | **Develop and deploy end-to-end data protection solutions using advanced cryptography** |
|---|---|
| Description | Launch a European coordinated action to develop advanced cryptographic functions and protocols (fundamental research, and operational Proof-of-concept)EU has strong research base and cybersecurity ecosystem, but cybersecurity solutions must often rely and work with out-of-EU enablers (such as cloud) or components (antivirus). Technical challenge is to build global secure solutions with untrusted/unsecured components.Cryptography is the key technology to secure digital applications. Europe has a strong background in theoretical and mathematics basis of cryptography, and innovative schemes development should be encouraged, supported and pushed to proof of concept and standardization.Homomorphic encryption 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.European commission could, in collaboration with Member States, make available, research and innovation funds (H2020) for breakthrough and patenting on advanced cryptography. This should comprise also innovative cybersecurity deployment projects, including pilot lines launch calls for proposals for an amount to be defined.DARPA is currently financing procurement projects to develop general |
| 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 unsecure environments<br>• Develop algorithms in following domains : ABE attribute-based encryption, IBE identification-based encryption, homomorphic encryption, anonymization, zero knowledge, block chain, quantum safe cryptography<br>• Develop adequate architecture to support this.<br>• Support technology from fundamental research to operational proof of concept in advanced cryptographic.<br>• Define EU policy and guidelines on cryptography (there is no such thing for the moment)<br>• Provide funding to encourage the 6~7 EU start-up companies that have development specified niche solutions to team up to develop a more comprehensive solutions for cryptography |
| Expected benefits | • support European autonomy and sovereignty |
| KPI | • number of international or European standards published |
| Type of investments | • Hardware, embedded software, application, HSM (hardware security modules) |
| SWOT Items | S2, S5, W2, W4,W5,T1 |
| Vision Items | V4. Leadership |
| Related items | R64. |
| Related EU initiatives | • European Cybersecurity Comptence Center : should select this issue as priority<br>• Horizon Europe, Blockchain Observatory, Quantum Flagship Initiative |

| **R64.** | **Develop homomorphic encryption** |
|---|---|
| Description | Cryptography is the key technology to secure digital applications. Europe has a strong background in theoretical and mathematics 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 ouf reach of laws like American Cloud Act of March 2018.Need for standardised use within Europe regarding cloud applications to protect sensitive data - work with ESOs is essential, such a proposal could be introducing in the annual rolling plan for ICT Standardisation.Efficient algorithms are needed. At present time, performances provided by R&D labs are too weak to meet operational requirements. More investment are needed to improve these performances, and also to look for specific hardware accelerations. Specific research funding could be allocated through Horizon Europe Program in parallel with ESOs activities. |
| Concrete actions | • Support R&D in homomorphic encryption to allow data privacy in hostile environments by introducing dedicated R&D budget in the new "Horizon Europe" research budget (continuation of "Horizon 2020")<br>• Make proof of concept for homomorphic encryption:<br>• Server development<br>• Client encryption/decryption<br>• Real-life use cases<br>• Support implementation of the newly designed algorithms on hardware acceleration platforms (FPGA, etc.) |
| Expected Benefits | Data is an additional layer of solutions to be considered in the presented value chain. Homographic encryption is one of the critical technologies and processes that Europe should mastered as a forefront protection of data privacy.This technology will have a strong impact on many verticals and especially for the most critical ones. |
| KPI | |
| SWOT Items referred to | S2, S5, S6, S7, W2, W5, O2, O4, O5, T3 |
| Vision Items referred to | V2. Protection |
| Related items | R8. |
| Related EU initiatives | H2020-ICT32-2014-RIA: HEAT (Homomorphic Encryption Applications and Technology, https://heat-project.eu/): KU Leuven, UBristol, UL, UPMC, CRX, NXP and Thales UK |

| | |
|---|---|
| **R31.** | **Cyber security SME Hub: an unique platform supporting the “Cyber security Made in Europe”** |

| | |
|---|---|
| Description | Cybersecurity technology is changing rapidly and only the SMEs, due to their agility, can provide the cutting-edge solutions needed to remain competitive. While the US has the largest market, specific regulatory framework (e.g. the Small Business Act) and Silicon Valley ecosystem, Israel has a strong military-academic-industry partnership and China has a protectionism strategy, EU is still looking for an appropriate business models on SMEs.SME are generally more reactive and able of fast innovation. They are therefore critical in EU to prove the viability and the efficiency of new cybersecurity tools. However, with a domestic market valued at EUR 25 billion and a very diverse industry landscape, made of 12 000 companies of which 74 % are micro companies and SMEs (source: 2018 ECSO Estimation), the European offering is not yet consolidated partly due to a difficult access to the market for young companies specialised in cyber security.<br><br>The SME Hub is intended as a market support and networking tool for European Cyber SMEs. It shall help SMEs to create **more market transparency and to reach out far beyond their traditional home markets**, which are usually nationally or regionally limited.<br><br>The Hub consists of three main functionalities aiming to give more visibility to European SMEs:<br><br>• **The Registry.** The SME hub shall be a publicly accessible platform where SMEs can register their company and define the services or products they offer in a predefined market segmentation structure which is based on the ECSO Taxonomy. Accordingly, this platform can be searched by interested companies who require services or products, based on type, quality and delivery capability of the registered SMEs. The provided market segmentation and categorisation can also be used to build consortia of different SMEs over larger parts of the value chain, e.g. when required for a project or large RfP.<br>• T**he "Cybersecurity Made in EU" label**. The label is a **private marketing tool** fostering the claim of quality and security of European companies and NOT a certification. The label would target companies and NOT Products / Services, is based on self declaration and NOT technical audit, is aimed mainly at SMEs but NOT excluding large companies. The operational model is based on a multiscale approach NOT competing with existing (similar) national label but rather aiming for synergetic co-existence with existing national/regional initiatives. The criteria are:<br>o 1)The company is a registered entity located in Europe with headquarters are in Europe (if part of a group, then group headquarters in Europe)<br>o 2) European ownership: company provides reasonable assurance that there is no majority ownership/control from outside Europe (declaring ownership structure / majority stakes)<br>o 3) The company's has cybersecurity >50% of cybersecurity R&D activities located in EU and >50% of staff (FTE)<br>o 4) The company offers trustworthy cybersecurity (ICT) products / solutions: The company declares to comply with the basic requirements defined by the ENISA Essential Security requirements for ICT including No-spy declaration: No offered product or solution contains backdoors (non-declared functionality)<br>• **The Quadrant.** The Hub shall give the possibility to serve as a market differentiator between SMEs based on their broadness of service, quality and capability to deliver. This shall be achieved by deriving various "European Cyber Quadrants" for the different market sectors, where cyber SMEs will be ranked according to clear and unambiguous criteria regarding quality and capabilities.The platform shall be open to |

| | |
|---|---|
| | all European Cyber SMEs, neutral and unbiased. It shall be provided via a web platform which is easily accessible by potential customers. The governance of structure, contents and criteria shall be done by a neutral governance body consisting of industry participantsECSO, and in particular its Working Group focusing on SMEs, is currently finalising the business and operating model. A test is expected to be launched in Q4. |
| Concrete actions | • Create a pan-European incubator for SMES to ensure short time market access.<br>• Provide funding to help cybersecurity SMEs to obtain certification<br>• Support SMEs and start-ups with getting certification and EU funding<br>• Reinforce and promote the use of the European "Small Business Act"<br>• Support the ECSO initiative to design and implement a SME Hub and the related functionalities: Directory, Label, Quadrant |
| Expected benefits | • bring products sooner to the market<br>• avoiding SME leaving the EU |
| KPI | |
| SWOT Items | S1, S3, S5, W1, W2, O4, O5, T3 |
| Vision Items | V1. Market share, V2. Protection |
| Related items | R50 (European accelerator network), R61 (to facilitate SME to access to finance). The conjunction of R31, R50, R61, will foster the consolidation of the EU market. R42 |
| Related EU initiatives | To some extent, the European Enterprise Network carries out some of these activities. |

| | |
|---|---|
| **R42.** | **Speed up the use of the EU Cybersecurity Certification Framework and support the SMEs to receive certification** |

| | |
|---|---|
| Description | The cybersecurity act has been recently adopted. It creates a cybersecurity certification framework to certify products services and processes.Certification is based on schemes specifying the type of product, service or product that can be certified, the security requirements for certified items and how to certify them.Schemes are proposed by the European Commission in the Union Rolling Work program for Cybersecurity Certification.The recommendation is to speed up and enforce the use of the European security certification by initiating the definition of schemes in critical areas (IoT, medical devices, automotive, industrial systems), helping companies (specifically SMEs) to certify their products and promoting the use of certified products (requirements in call for tenders), on the basis of international IEC/ISO and market-adopted standards.Ensure that the certifications is cross sectorial, to avoid creating silos or internal barriers between different cybersecurity sectors.<br><br>• Certification is complex and expensive creating delays in their uptake.<br>• Support SMEs and start-ups with getting certification and EU funding.<br>• This will help to bring products sooner to the market (and avoiding SME leaving the EU).<br>• SME support solutions could be linked to national and regional competence centres, brokers, clusters, and coordination centre that are aware of new EU programmes and funding opportunities.<br><br>In particular with regards to the role of regions, Wallonia(BE) launched in 2018 “KIS: Keep It Secure”, a recent mechanism to raise awareness and enhance maturity about cybersecurity among SMEs in Wallonia (BE). The regional authority acts as the facilitator to raise the level of maturity of SME end-users willing to implement audit and IT security analysis. In particular, Wallonia regional authorities aim to liaise end users with a list of validated and authorised security audit providers through a dedicated funding support “cheque entreprise”. The end-users using the regional mechanism will get funded 75% of the costs of IT security solutions. |
| Concrete actions | • Fill in Union Rolling Work program for Cybersecurity Certification with critical products, services and processes (IoT, medical devices, automotive, process/secure development life-cycle, industrial systems) → Norms<br>• Help industry in using European certification (information, training, dedicated funding) → SMEs<br>• Promote and/or incentivise the use of certified products (in call for tenders, in future sectorial regulations) → Procurement<br>• Have mandatory certification in energy<br>• Initiate the process with some critical verticals where Europe has a leadership position (autonomous electric vehicle for example). |
| Expected Benefits | • To enhance the security level of systems by using secure components<br>• To maintain a control on non-European and untrusted components (evaluated and certified in Europe)<br>• To give a label to quality secured European components. |
| KPI | • |
| SWOT Items | S1, S4, S7, O2,W3, T1, T4 |

| | |
|---|---|
| Vision Items | V2. Protection |
| Related items | |
| Related EU initiatives | |

| **R24.** | **Support European cybersecurity hardware suppliers** |
|---|---|
| Description | Recent attacks show that hardware is a new entry points for attackers. The vulnerabilities exploiting hardware are hard to detect since it relies on proprietary specifications. The hardware founders could even add back doors (exp. Hardware Trojan) without being detected by final users. Having an industry of electronic components in Europe would help to maintain sovereignty on these technologies.Examples: to build a washing machine, you have 270 suppliers (both hardware, software, etc…). Today, there is no guidelines on the sourcing requirement regarding cybersecurity. The washing machines could be hacked to have 1 million washing machines starting at once. It is a real cybersecurity threat and there are no security measures or framework in place for the moment.Rationale:<br>• Current dependency of non-EU suppliers<br>• Hardware is a hard segment to invest in<br>• IPCEI already exists in microelectronics<br>• We can develop specialized EU chips for cybersecurity applications |
| Concrete actions | • Coordinated investments between cybersecurity hardware manufacturers to compete with non-EU actors |
| Expected benefits | |
| KPI | |
| SWOT Items | S4, S5, W10, W11, W15O18, O19, T24, T25 |
| Vision Items | V2. Protection, V3. Independence, V4. Leadership |
| Related items | R31, R61, R38, R65 |
| Related EU initiatives | |

| | |
|---|---|
| **R53.** | **Review and adjust EU innovation funding instruments to make them competitive and relevant for the fast evolving cyber security industry.** |
| Description | European funding mechanisms are not competitive enough compared to the way some of EU's biggest competitors support cyber security industry and innovations (peer review). In the EU instruments application, implementation and reporting processes and time frames are long and cumbersome to be relevant for companies competing in the fast evolving global cyber security market. Assess the feasibility to use cascade funding as part of larger research projects. Increase understanding what kind of innovations and solutions are needed in the market. Support the SMEs and start-ups in participating in the EU funded projects.Make a study on different public funding models on cyber security industry and innovation (EU vs main competitors). Assess the requirements in the EU financial instruments and interview CTOs of European cyber security companies to identify the main bottlenecks hindering participation in the EU projects. Make recommendations to address identified shortcomings and problems. |
| Concrete actions | • Introduce specific rules/tools to support to simplify the participation of SMEs in EU-funded projects |
| Expected Benefits | Increased investments in the innovation and growth in the European cyber security industry. Stronger and bigger European cyber security ecosystem and solutions. Increased global market share in cyber security supply. |
| KPI | |
| SWOT Items | W2, W3, T1 |
| Vision Items | V4. Leadership |
| Related items | R61 |
| Related EU initiatives | |

| | |
|---|---|
| **R55.** | **Enable and encourage cross boarder collaboration on cybersecurity products and services** |

| | |
|---|---|
| Description | Mainly Member States have local cybersecurity service and product suppliers. Those may be well-established in one MS market, but growth cross boarder inside EU, is not happening. Often trade-barriers are invisible: business-culture, language, mis-trust and etc. SMEs has often easier way to grow to non-EU markets than inside EU. EU should build program where existing SME has opportunities to find new partners, distributors and solution integrators from the other MS. EU should finance business-workshops for Cybersecurity companies where companies are driven "even forced" to work together inside workshop for building joint-offering together. The program could be financed by EU and it should include travelling costs for those company participants.Example: If three companies are able to make pilot-proposal to EU for build joint-offering, EU would provide financing for that to test it. Financing would be conditional until, offering could be proven in the practice. |
| Concrete actions | • Create dedicated strategic funding programs in support of SME collaboration |
| Expected benefits | More local or regional European cybersecurity companies are able to find partners inside EU to build joint-offering. If offering is match, it increases odds to have more industry related consolidation inside EU instead to have non-European cybersecurity giants conducting acquisition from EU, buying out promising SMEs in the early stages. This lowers practical at same time trade barriers inside European Digital Single market. |
| KPI | |
| SWOT Items | S5, S8, W1, W2, W4, O1, O2, O10, T1 |
| Vision Items | V1, V3, V4, |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| **R56.** | **Support industrial buyout and investments inside EU** |

| | |
|---|---|
| Description | Europe is lacking of venture capitalist for scaling up investment rounds. Cybersecurity markets are globally ruled by large cybersecurity industrial giants, where exists non-European based companies. Often global markets are having unfair competitive activities provided by some countries allowing some business advantages companies originating, competition is not always played by “fair-play” market-economy, with international trading rules.Europe must have scheme providing more visibility of cybersecurity industry existence inside EU with providing more opportunities for venture capitalist and industrial investments to find potential companies inside EU. There should be new encouragement for buyout happening within EU origin cybersecurity companies. Enablers could be as an example:<br><br>• tax deduction,<br>• easy loans from public institutions (national of EU banks),<br><br>industry specific investment funds, with dedicated facilities to help mergers and growth. |
| Concrete actions | • Create dedicated strategic funding programs in support of market consolidation |
| Expected benefits | • more globally compelling European based cybersecurity companies borne and industry origins remains more often inside EU. |
| KPI | • |
| SWOT Items | S4, S5, W1, W2, W3, O7, O10, T1, T2 |
| Vision Items | V1, V3, V4, |
| Related items | |
| Related EU initiatives | |

| **R57.** | **Accessing Global market** |
|---|---|
| Description | There should be support industrial access to the global markets. EU has extensive network of EU embassies all around world. Those organizations should have a special scheme to support European based SMEs to find market information of partners, re-sellers and customers. US, China and many other countries have trade counsellors located in their embassies to enabling industry to access new markets (EU do not allow it).EU could also establish industry related scheme to have trade counsellors focused in the industry specific sectors. Those trade counsellors could be co-financed with industry itself, coordinated with some industry clusters or association to maintain “fair-equal treatment” for all companies interested penetrate those markets. |

| | |
|---|---|
| Concrete actions | • Introduce advisory services for European Business within the EU delegations network |
| Expected benefits | increasing new business growth opportunities for cybersecurity industry and research to getting access in to the new markets and lowering business risks for early stage failures. This is equalizing global trade opportunities between EU and competing countries. |
| KPI | |
| SWOT Items | S5, W1, W2, W3, W9, O4, O7, T1, T3 |
| Vision Items | V1, V3, V4, |
| Related items | |
| Related EU initiatives | |

| **R60.** | **Integrate existing expertise into to the EU decision making processes** |
|---|---|
| Description | One of the biggest weakness in EU is lacking industrial voice from decision-making. Dynamic and critical business sectors, such as cybersecurity requires continuous visibility to real economy and business. Today's framework of EU conducts surveys and studies, and decision bases on those outputs. In the practice non-European ICT sector is well-equipped in Brussels with their armies of lobbies. In the mean while EU own industry has no change to contribute or to be heard. EU needs a new industrial advisory framework, which has well-build structure throughout the whole EU. There should be reasonable number of European Cybersecurity companies present covering different size and types of companies with balance of geography. Beside of the industry, there should be also similar network researcher cross EU. Framework should call advisory board to meet quarterly to provide advice, generate some new ideas, consultancy and help adequately to build real-time SWOT, updated KPIs etc. for EU. Industrial specific clusters should be used more efficient manner for selecting Advisors. |
| Concrete actions | • EU Advisory board for supporting continuous decision making helping Cybersecurity related DGs<br>• We need to have a clear voice from the EU cybersecurity industry. ECSO could enlarge its membership and play that role. |
| Expected benefits | helps the whole EU base decisions making process to interact between industry and research cross-EU more efficiently, not only being depending closely available lobbies. |
| KPI | |
| SWOT Items | S1, S4, W7, W8, W11, O1, O2, O7,T1, T4 |

| | |
|---|---|
| Vision Items | V4, |
| Related items | |
| Related EU initiatives | • Contractual public-private Partnership with ECSO and the Commission proposal for a Competence Centre and network. |

| **R65.** | **Certifiable secure firmware on open hardware for Europe** |
|---|---|
| Description | Secure hardware components, i.e. secure chips or secure hardware building blocks are more and more being incorporated into larger system on chips (SoC). Main SoC players and developers are residing outside of the EU. They are therefore in a good position to also provide secure software on top their proprietary hardware. Therefore it is important to promote the development of open source security hardware that can be used to both create stand-alone security chips and that can be integrated into larger systems on chip. In addition a framework is required to allow for development of a secure and security certifiable firmware / software on top of such open source hardware. Open Hardware can also provide protection from in–built trojan horses. Yet a successful certification is difficult to achieve because developers as well as hackers have the same information level. |
| Concrete actions | • Need of certifiable hardware-based firmware and applications which can be trusted by users. - This work could be conducted under the responsibility of the future European Cybersecurity Competence Centre<br>• Need of scalable solutions according to the environment and the level of potential attack. - This topic could be tackled by the European Commission's annual workplan for certification with proposals to work on a EU candidate scheme in parallel to the need of EU standards addressed by the MSP for standardisation.<br>• Provide funding for and set up an EU driven community for open source security hardware. |
| Expected Benefits | Facilitate access to (EU) certification and increase the consumer's confidence level by placing on the market secure and reliable ICT solution.Increase the robustness of European ICT solution, taking advantage of the European Certification Framework and enabling European manufacturers and solution providers to compete on the world stage.Security certification (dynamic) besides Safety requirements for placing a product on the European market, is also a stage that should be integrated in the presented value chain.Create an open platform for security software and applications on top of openly defined hardware and enable EU based companies to provide security solutions independently. |
| KPI | |
| SWOT Items referred to | S5, S7, W1, W4, W5, W6, O2, O4, O9, T1, T2, T4 |
| Vision Items referred to | V1. Market Share, V2. Protection |

| | |
|---|---|
| Related items | R4. R66 |
| Related EU initiatives | |

| **R59.** | **Market data availability and awareness** |
|---|---|
| Description | Cybersecurity related market data, “the correct data” is not easily available. Detail market studies are continuously updated and especially for small companies, it is almost impossible to have access for relevant cybersecurity market data. European Union should have continuous production of relevant indicators of cybersecurity market data. There should be 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 inside EU in the field of Cybersecurity.This mapping also needs to include competences. The Pilot Action is using the CRAFT tool, developed by Bureau Développement Innovation of the Brittany region.The S3 Pilot Action on Cybersecurity led by Brittany Region has started the process, as explained in ECSO’s position paper, using the ECSO taxonomy on the cybersecurity market. The Pilot Action is fully willing to share its experience if considered useful. |
| Concrete actions | • 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**.<br>• EU provides itself or throughout other third parties real-time cybersecurity statistics to be available for public sector, industry (including end-users, providers and SMEs) and research (for bench marking and support for decision making) |
| Expected benefits | helps the whole EU base decisions to more relevant data. It applies to EU itself, Member States, private industry and research. Updated correct data is one of the most important way build Situational Awareness of Cybersecurity, all over EU. At same time all stakeholder in EU has the similar starting-point to build their baseline for their decision-making processes.This mapping exercise is the first step to create a comprehensive European value chain that include all actors. It will be a useful tool to further identify strengths and weakness of the European cybersecurity industrial base, to connect actors together across Europe, to create synergies and complementarities, based a common “language” and understanding of the moving landscape. |
| KPI | |
| SWOT Items | S3, W7, W8, W9, W11, O4, O7, T3, T4 |
| Vision Items | V1, V3, V4, |
| Related items | |

| | |
|---|---|
| Related EU initiatives | |

| **R71.** | **Risk Information Sharing Platform: Collaboration in risk management towards informed governance** |
|---|---|
| Description | Many regulations and laws ask stakeholders to take a risk-based approach; risk management is finally becoming a board topic. This evolution has been sped up by GDPR and the NIS directive. However, there is only a framework available for risk management, namely the ISO/IEC 27005. What scope stakeholders should analyse in their risk management approach is completely unclear. There is no guidance on what scenarios to include, what probabilities of threats to apply and what ease of exploitation of vulnerabilities or what efficiency of risk mitigation measures.This situation is most unsatisfactory, as it is sheer impossible to compare risk assessments done buy different stakeholders. This makes cross-stakeholder risk management impossible. The risk lying in long interdependency schemes cannot be qualified or analysed, which makes regulation as well as governance impossible.By taking this approach, stakeholders will work on a comparable model and produce comparable results. This would lead to more objectivity and to more board level involvement. Risk assessments can be linked and combined to create larger overview of a corporate or even a sector. |
| Concrete actions | For this reason, it is proposed to start a 2 phased informed governance project, which brings together actors with the aim to define a common taxonomy for **risk management**:The first phase will focus on **basic risk management scenarios**:<br><br>• Definition of minimum set of risk scenarios (asset – vulnerability – threat). The CERT community as well as the Security Operations Centres have extensive knowledge what are the most common scenarios leading to incidents; these should be identified and qualified.<br>• Definition of metrics for threat probabilities, ease of exploitation of vulnerabilities and efficiency of risk mitigation measures by the same community (related to R21, R6, R7)<br><br>In a **second phase regulators should step** in and help to address the remaining governance aspects like minimum scope, minimum impact qualification (in case of NIS and GDPR), and of course an acceptable risk acceptance matrix.This approach will lead to a better risk management, a better governance and an increased level of security in Europe.The same approach would be chosen **for advanced, more sector specific risk management**. For each NIS sector, stakeholders meet in ISAC setups and discuss sector specific risk scenarios as well as threat probabilities, ease of exploitation of vulnerabilities and efficiency of risk mitigation.Upon these risk scenario models, standard as well as advanced **certification schemes will be created.** |

| | |
|---|---|
| Expected benefits | • The project will lead to an information sharing platform for risk management.<br>• Individual time spent in risk management would be reduced due to the availability of scenarios and metrics.<br>• Stakeholders will work on a comparable model and produce comparable results. This would lead to more objectivity and to more board level involvement. Risk assessments can be linked and combined to create larger overview of a corporate or even a sector.<br>• This approach will be supported by the private sector as it will lead to harmonisation of regulatory requirements in cybersecurity and **thus reduce the regulatory burden and increase the attractiveness of the European Union**.<br>• This approach would lead to more security, as risk management gets much more objective and comparable. Regulators as well as corporates can implement better governance models. |
| KPI | |
| SWOT Items | S1, S3, S5, S6, S7, O2, O5, W3, W5 |
| Vision Items | V2. Protection, V4. Leadership |
| Related items | R21, R6, R7 |
| Related EU initiatives | • Risk management approach of the legal frameworks<br>• Certification frameworks |

| **R69.** | **Create a network of experts to provide assistance and training to public procurement agencies for their cybersecurity procurement needs** |
|---|---|
| Description | Contracting authorities need access to cybersecurity expertise when planning their IT infrastructure and procuring IT equipment. As building in-house cybersecurity capacity is not feasible in the majority of cases, on-demand access to expertise should be available in competence centres. Already existing networks of competence centres may develop this additional expertise, .e.g. Digital Innovation Hubs, national/regional innovation agencies, or newly established structures may be envisaged. |
| Concrete actions | Define cybersecurity expertise in public procurement competency;Identify suitable existing competence centres to develop cybersecurity consultancy capacity;Envisage funding programme; |
| Expected benefits | Increase of cybersecurity awareness of contracting authorities;Increase of cybersecurity level of public IT systems;Increase of chances for innovative and possibly EU made solutions to be purchased in public procurement. |
| KPI | Cybersecurity competence centre network creation; |
| SWOT Items | S1, S3, S4, S5, S6, S7, S9, W1, W2, W5, W8, W9, W10, O1, O2, O6, O7,O9, O10, T3,T5 |

| | |
|---|---|
| Vision Items | V2 Protection, V3 Independence |
| Related items | R50 |
| Related EU initiatives | Digital Innovation Hubs (CNECT), Procure2Innovate (CNECT) |

| | |
|---|---|
| **R25.** | **Coordinated EU cybersecurity strategy and governance for the smart grid** |

| | |
|---|---|
| Description | From electrical distribution to power, to advanced distribution management systems, EV charging infrastructure and up to electrical panels guarantee interoperability and seamless security along the propagation of energy and metering. This can be applied to smart grids, micro grids, smart cities, distributed energy resources integration (PV, storage, genset, …) where orchestration will happen. It will require local intelligence (edge), rule based engines as well as orchestration from the cloud (weather prediction data plus tariff management plus power availability, demand response state, …).Challenges of the Smart Grid sector in the field of cybersecurity<br><br>• Lack of a common European regulation and certification framework in cybersecurity<br>• Lack of governance for Authentication of third parties during the all vehicle lifecycle<br>• Product life cycle management<br>• Resilience of the ecosystem<br>• Integration of multi-energy and connection to a grid (electric, gas, etc.)<br><br>Among the different verticals, EU car industry is a strong asset which world leaders in EU. This industry is facing multiple security challenge related to new car functions: connectivity, driverless, electrification and connection to smart grids or different gas providers. Cybersecurity could be showstopper.Competition is still open in that field as it is really an emerging domain. EU has strong research base and cybersecurity ecosystem with world leading companies. Automotive is driving the innovation market for new security technologies (HW/SW) for embedded systems. The proposal is to set up security of clean connected car as a European priority, and to fund coordinated projects both on security solutions development and security certification in that field. Charging vehicles sector (electric, hydrogen, LNG, natural gas for vehicles) comprises many actors with divergent interests leading to heterogeneous security solutions for charging. Manufacturers, users and charging station operators need a confidence model for interconnection and an agreement for charging on the electric grid or other fuel.Regulation & Certification Framework:<br><br>• Although some specific standards have been defined regarding cybersecurity issues for industrial and automotive systems, there still a lack of a unified regulation and certification framework at European level for energy providers and technology suppliers. (*Utilities don't know what to require; manufacturers don't know what to develop).*<br>• ENISA is working at the definition of a unified regulation for the electric sector and this should concern smart charging.<br>• Definition of the cybersecurity ecosystem should facilitate in order to speed up the harmonisation at EU level (need of trust).<br><br>Smart charging for electrical vehicle :<br><br>• Smart Grid provides electrical supply to many other critical infrastructures (hospitals, defence, transport, telecommunications, public institutions, …).<br>• Smart Grids and Telecommunication Networks should be strongly integrated. Cybersecurity of networks, authentication and authorisation for charging on the grid at the good/authorized moment will be mandatory. |

| | |
|---|---|
| | • Cryptography, Public Key Infrastructure and secure database are tools of success and are also issues<br><br>Product Life Cycle Management:<br><br>• Cybersecurity innovative solutions created in R&D projects should be deployed in an old and geographically disperse infrastructure with thousands of legacy devices.<br>• We have to think in life cycle products of 20-30 years with continuous vulnerability revision (*defence that works now may not work tomorrow*) that will affect the manufacturing, upgrading and certification process.<br><br>Resilience:<br><br>• Disaster response should be improved.<br>• Greater coordination with other stakeholders and with other cybersecurity organisations<br>• The volume of electronic (IoT) devices to be integrated or connected to the smart grid will grow exponentially in the coming years with extremely actualisation costs:<br>• Electric vehicles will require specific equipment to be integrated in the infrastructure (recharging posts and stations).<br>• Distributed Generation (domestic PV panels, wind generation, …)<br>• Future threats will come from IoT devices connected to the Smart Grid (How can security be assured?).<br>• How to detect massive attacks from IoT devices (for example, HVAC systems, domestic appliances, …).<br>• People awareness:<br>• As in many other sector, infrastructure is only a part of the whole system. People continue to be one of the main sources of vulnerabilities.<br>• There are more and more external personnel in the Smart Grid facilities. It is necessary to raise awareness of the staff.<br>• Greater participation of the final user, for example in energy demand-response scenarios.<br><br>Integration of smart devices and IoT: |

| | |
|---|---|
| Concrete actions | • Fund coordinated projects to reach a secure, clean, and connected car both on security solutions development and security certification. Develop an ecosystem based on trust model for interconnection and agreement for charging, for instance on the electric grid, but also for gas solutions.<br>• Smart Grid is considered one critical sector and could be one of the first verticals for R42. (R42, “Speed up and enforce the use of the EU Cybersecurity Certification Framework”, proposes to “initiate this process with some critical verticals where Europe has a leadership position (autonomous electric vehicle for example)”.)<br>• To set up an alliance integrating stakeholders of the smart charging (network operators, technology suppliers, cybersecurity solution providers, standard and certification bodies, etc.) for defining cybersecurity standards and test procedures.<br>• To foster the development of specific cybersecurity solutions that satisfy functional and performance requirements.<br>• Investment in R&D: new technology could be needed, R&D projects to validate the solutions<br>• Telecommunication and energy sector coordination to jointly define security aspects.<br>• Creation of a specific CERT for the sector at EU level.<br>• From 61850 as a communication protocol to last mile technology (Power Line Carrier, 5G, LoRA, Zigbee, …) for the sake of securing Distributed Energy resources, demand response, advanced metering, sharing energy (maybe enabled by blockchain), this in accordance with country regulation and orchestration of utilities and keeping the consumer becoming a prosumer in the loop. This can be derived to home automation starting from industrial use cases from power critical and power intensive customers (Oil & Gas, Healthcare, Data centers, …). Enabling 62443 certifications or other standards, guarantying as well GDPR rules conformity. |
| Expected benefits | • Build European players in vehicle charging, whether it's gas or electricity, with secure networks and cybersecurity for charging solutions<br>• Enhancement of the security level of the Smart Charging<br>• To position the European cybersecurity and smart charging sectors as an international leader.<br>• To share a common framework will make easy interoperability, select the trust provider, and globally reducing cybersecurity costs.<br>• Development of more robust and secure products, increasing trust in the new technology and charging systems.<br>• Increase the sharing of information among the relevant stakeholders: for instance, provide a better and faster response to cyber incidents.<br>• Ensure that new devices, including IoT devices, have and will maintain a level of cybersecurity appropriate to the Smart Grid. |
| KPI | • |
| SWOT Items | S1, S3, S4, S7, W12, O17, O22 |
| Vision Items | V1 Market share, V2 Protection, V4 Leadership |

| | |
|---|---|
| Other potential interested parties | • EC: promotion of a common regulation for the whole EU regarding cybersecurity requirements for design, implementation, operation and maintenance of smart charging platform.<br>• Standardisation and certification bodies: definition of and compliance with specific cybersecurity standards for the smart charging. This should include standards and certification process for the different actors involved in the implementation, operation and maintenance of equipment and infrastructure (see IEC, ETSI, ENISA, etc.).<br>• Utilities: deployment of standards (operation, management, maintenance); employees training and awareness on cybersecurity issues; cyber incident response;<br>• Vehicle equipment providers: provision of certifiable secure systems; new procedures for up-to-date secure systems (lifecycle management of secure equipment).<br>• Equipment providers: such as electric vehicles and charging stations, IoT plug & play devices … to provide compatible cybersecure systems.<br>• Engineering & Integration companies:<br>• Cybersecurity solution providers: development of technologies and solutions for cyber-attack and anomalies detection, security level monitoring and control in the smart ecosystem.<br>• Hardware providers: development of certifiable cybersecure HW components that meet the high-performance requirements of the smart grid.<br>• Cybersecurity services/consultancy companies (CERT, SOCs, …): support and development in the application and deployment of policies, standards, etc.<br>• R&D technology entities: research on new technologies - such as AI - to support the development of new solutions for cyber incident prevention, detection, identification and/or response. |
| Related items | R42, R18 |
| Related EU initiatives | • JRC Pilot Project on IACS |

| | |
|---|---|
| **R10.** | **Support to the development of European breakthrough technologies applied to cybersecurity** |

| | |
|---|---|
| Description | The exploitation of emerging technologies (Artificial intelligence, quantum, cognitive technologies, DLTs…) in the cybersecurity field can help to develop a new range of product and services.Cognitive/AI technologies can support also the analysis of citizen perception about Security from social networks as it's diffused an erosion of citizens' trust and confidence in digital trustExamples:<br>• new detect function, preventive analysis of potential cyber threats on social networks (either Surface or Deep/Dark web), analysis of the behaviour of "potential hackers" (Emotions and Style of Writing) on nodes exposed to simulate a critical infrastructure, the creation of a "cyber" taxonomy for categorisation,<br>• the creation of a "cyber" ontology for the normalization of terms exchanged by stakeholders at European level and the extraction of personal information as related to the GDPR issue.<br>• the understanding of the Human Factor side of social network contents; so extracting behavioural attributes expressed by writes and giving the possibility by end-users/practitioners/phycologists to understand how messages are spread into the web, if they are pro or counter messages, the methods of approaching people, who is the boss of a group in a forum, ….<br>• the understanding of specific slangs, dialects and misspellings typical of social networks languages such as talkative languages |
| Concrete actions | • Support of emerging technologies (Artificial intelligence , quantum, cognitive technologies…) and their use in innovative protection products, services and processes<br>• Developing of advanced behavioural AI algorithms in order to understand the "Human Factor" from unstructured contents and into multiple languages. |
| Expected benefits | • Enhanced comprehension of the style of approaching of cyber attackers<br>• Advanced prevention capabilities<br>• Understanding the human factor side into web contents<br>• Improving finalization of targeted web campaign<br>• Understanding social network targeted slangs<br>• Understanding fake vs real news |
| KPI | • Number of semantic behavioural attributes extract from analysed contents (Human factor attributes) |
| SWOT Items | S2, W4, W5, O5, O7 |
| Vision Items | V4. Leadership |
| Related items | R7 |
| Related EU initiatives | |

| R32. | Development of Industrial cybersecurity building on Europe's strong industrial base |
|---|---|
| Description | Europe has core competences in the development of industrial security and embedded security and is able to compete globally. Robust cybersecurity for the whole range of IoT and IIoT products, services and processes is a longer-term and strategic perspective to cybersecurity.Consequently, to spur industry-wide uptake of integrating cybersecurity solutions into products, including the development of products, and after-sales, establishing cybersecurity development processes (e.g. IEC 62443-1-4) factually increases cybersecurity in the long-term, in particular stimulating innovation and investments into cybersecurity solutions.<br><br>• Industrial cybersecurity leaves room for further improvements.<br>• Certification and standards covering the entire life cycle would be valuable.<br>• This would establish a cybersecurity by design approach.<br>• A focus on full life cycle development may also enfold opportunities for new service offerings: companies or shared service centres focusing on delivering industrial cybersecurity solutions. |
| Concrete actions | • Build policies on existing industry security measures, including investments towards industrial cybersecurity solutions.<br>• Draft a cybersecurity life cycle management methodology to train software, hardware and infrastructure developers. |
| Expected benefits | • Boost Europe's cybersecurity capacities, in particular for its industrial infrastructure<br>• Setting the global standard on cybersecurity<br>• Building trust in the Single Market |
| KPI | |
| SWOT Items | S7, S4, S11 |
| Vision Items | V4 |
| Related items | |
| Related EU initiatives | |

| R23. | Implementing a secure European Operating System for critical applications |
|---|---|

| | |
|---|---|
| Description | There is no Operating System being developed and maintained in Europe.In addition, development of an Operating System secured and maintained in Europe is fundamental for all the services that rely on it.Academic research with a strong implication of European industry and European Union Agency for Network and Information Security (ENISA) should help such an implementation.Within many architectures hardware is a new entry points for attackers. Vulnerabilities inside hardware are hard to detect since the latter relies on proprietary specifications. Hardware founders could even add back doors (exp. Hardware Trojan) without being detected by final users.Having an industry of electronic components in Europe would help to obtain strong sovereignty on these technologies. |
| Concrete actions | • Created a public/private consortium to develop an EU OS<br>• Investing in research to secure hardware and OS is one of the necessary means to defend European industry and sovereignty |
| Expected benefits | • Sovereignty, user data confidentiality and privacy, hardware and software security. |
| KPI | |
| SWOT Items | S4, S5, W10, W11, W15, O18, O19, T25 |
| Vision Items | V3. Independence, V4. Leadership |
| Related items | R21 |
| Related EU initiatives | |

| **R41.** | **Set up a special training program and professional certification in the cybersecurity** |
|---|---|
| Description | We can use the private background skill and academic to create a centre of excellence in cybersecurity IoT devices and driverless car to complete the state of the art gaps.Expected Benefits: export the human value for the entire cybersecurity lifecycle. Export the value of "The EU cybersecurity IoT Certification". Growth employment and business. Starting from the European e-Competence Framework (e-CF) - part of ISO 11506 and receive the EN 16234 from European Committee for Standardization – we can set up a special training program and professional certification in the cybersecurity IoT lifecycle to improve the skills, knowledge and proficiency levels. We can sign a MoU with ENISA and NIST (National Institute of Standards and Technology) to export and trust the framework around the world (i.e.: accreditation or certification accredited by ...). First training:<br><br>• IoT awareness and knowledge base;<br>• IoT cyber security issues;<br>• IoT security lifecycle. |

| | |
|---|---|
| Concrete actions | |
| Expected benefits | |
| KPI | |
| SWOT Items | S7, W3, O3, T3 |
| Vision Items | V1, V3, V5 |
| Related items | R16, R28 |
| Related EU initiatives | |

## Medium Priority

These actions are clear with concrete actions, but have received only limited or mixed support from participants (apart from the party submitting the proposal).

| **R43.** | **Fund European research, development, demonstration and deployment in Cybersecurity** |
|---|---|
| Description | Dedicate significant part of European R&D funding (H2020, …) to the R&D covering all the chain of security technologies and their integration in critical systems:<br><br>• Cryptography<br>• Threat intelligence and vulnerability detection on hardware, software and systems<br>• Security of emerging technologies (AI)<br>• Developments, analysis and validation tools<br>• Large scale demonstrators and proofs of concepts<br>• Create a DARPA-style process to fund R&D with clear applications and a clear client already in mind. The projects are proposed with a short 4-page document.<br>• Key areas :<br>  ◦ cyber range applications and services,<br>  ◦ cybersecurity assessment tools for digital systems,<br>  ◦ physical & cybersecurity supervision systems,<br>  ◦ secure AI components. |
| Concrete actions | • Boost European research funding for cybersecurity<br>• Create dedicated strategic funding programs to fund large scale demonstrators and proofs of concepts |

| | |
|---|---|
| Expected benefits | • Maintain and enforce the European expertise in security technologies<br>• Help in generating "Made in EU" cybersecurity solutions<br>• Help in developing technological bricks for industry (start-ups, SMEs, large groups) to build offer on. |
| KPI | • |
| SWOT Items | S2, S5, O5, O6, O7, W2, W4, T3 |
| Vision Items | |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| **R38.** | **Create European world-class player for Firewall and Antivirus** |
| Description | Bringing together important knowledge and innovation subjects could help: next generation firewalls (how to prevent from becoming dependent on solutions from the US, Russia and Israel). |
| Concrete actions | |
| Expected benefits | |
| KPI | |
| SWOT Items | |
| Vision Items | V4. Leadership, V2. Protection |
| Related items | R24 |
| Related EU initiatives | |
| **R44.** | **EU strategy for research focusing on excellence** |

| | |
|---|---|
| Description | Review and selection process needs to be substantially improved: more emphasis on excellence in record of accomplishment (both for reviewers and for participants) – too much average and "me too" research is funded and some of the top teams do not even participate. Strategic choices on what to research (which topics and in which phase) needs to be improved substantially.For most projects, there is a misalignment between goals (market impact) and timescales (80-90% of EU projects in cybersecurity has zero market impact). Funding should go to strategic basic research with a time horizon of 4-5 years that has the potential to make an impact rather than "applied" research that should be done over 2 years but takes 5 years from conception to result and subsequently has 0 impactSolution: develop strategy on which areas and research to fund and focus on excellence<br>• strategic basic research with horizon of 5 years<br>• fund DARPA-style research (clear goals)<br>• close follow-up by experts on a quarterly basis and demand prototype that satisfy customer after 2-4 years (rather than reviewers and the commission). This requires overhead and top technical/business expertise at the side of the funding agency.<br>• Fund R&D of innovative SMEs<br><br>Some areas research is not strong enough: e.g., system and network security, malware. For example, a platform to foster and harness CvD amongst cybersecurity stakeholders and vendors. |
| Concrete actions | |
| Expected benefits | |
| KPI | |
| SWOT Items | W2 |
| Vision Items | V4. Leadership |
| Related items | R3 |
| Related EU initiatives | |

| **R28.** | **Skills insights** |
|---|---|
| Description | • It is unclear what specific skills and professionals are needed.<br>• It should be easier to find people with specific skill sets (at universities, employers).<br>• A tool could help to understand what skills are currently present in the workforce and what capacity is needed in the future.<br>• This would help for instance universities to train certain professionals and close the skills gap more accurately. |

| | |
|---|---|
| Concrete actions | • Develop a platform that provide insights into the current and needed skills capacity, per Member State.<br>• Develop a cognitive algorithm in order to extract attributes linked to a specific skill from natural language contents either online (web, social network, email) or offline (such as surveys) |
| Expected benefits | |
| KPI | |
| SWOT Items | O3, T3 |
| Vision Items | |
| Related items | R16 |
| Related EU initiatives | • ECSO is already working on getting such an overview (comparable with Cyberseek).<br>• European e-Competence Framework |

| | |
|---|---|
| **R27.** | **Ensure that European security interests, high cyber security requirements and diversity of providers are part of the public procurement.** |
| Description | Establish a single market for public procurement and EU-wide publication of tenders. Ensure quality and security at all stages of the process. Security aspects should be an integral part of public procurement in cyber security. Price should not be the main consideration but priority should be given to the high level of cyber security. Build public procurement around finding a solution to a problem or challenge and not only on pre-determined specifications. It is important to ensure diversity of solution and service providers, as cyber security is provided in layers of products and solutions. Not all those layers should come from one provider or even one country.To support the emergence of global innovative players in Europe at critical levels of the cybersecurity and ITC value chain, regulation should be introduce to incentivise and/or oblige EU players, especially public players, to use European solutions whenever a credible offer exists. |
| Concrete actions | Review EU public procurement regulation (do we need a change) and prepare guidelines on public procurement in cyber security. Train and educate public procurement officials in procuring cyber security solutions. Require and advice EU institutions to ensure diversity of cyber security products and solutions. |
| Expected Benefits | Growth in European cyber security industry. European cyber security product and solution providers will get an important access point to the market and relevant references. |
| KPI | |
| SWOT Items | S3,S4,S5, O1, O2, O5, W1, W3, T1 |
| Vision Items | V1. Market share, V2. Protection, V4. Leadership |
| Related items | |

| | |
|---|---|
| Related EU initiatives | |
| **R9.** | **Define an EU Digital Trusted Attestation model** |
| Description | The question in Cyber security protection level is about Digital Trust. The EU could create its own certificate signature under a relevant certificate Authority name. Any validated contributor will have the possibility to link its Digital PKI to this trustworthy EU certificate authority as a delegated trustworthy authority.With an appropriate delegation model to setup, “actors/contributors/members” in the EU would have the possibility to offer, in their respective products and services, a trusted digital certificate to build a strong Digital Trust for their own customer. This concept will the opposite of the current many self-generated certificates present in products on the EU market.The delivery of the service should be free. |
| Expected benefits | |
| KPI | |
| Concrete actions | Create an EU certificate signature under a relevant certificate Authority name |
| SWOT Items | S7,S3,W1,T1 |
| Vision Items | V2. Protection |
| Related items | R66 |
| Related EU initiatives | |
| **R13.** | **Promote Secure Systems Life Cycle through the whole Supply Chain (Cybersecurity by Design)** |
| Description | Current cyberattacks are exploiting existing vulnerabilities in operating systems, products and communications that were designed and developed without cybersecurity requirements. If cybersecurity by design does not start to be used the same problem is going to be faced in the future. Developing vulnerabilities free software for complex systems is still a challenge.Promote the knowledge and use of secure systems (software, hardware and communications) development methodologies, tools, standards, … through the Life Cycle and Supply Chain. Help developers build systems with the appropriate level of cybersecurity and ready for assessment and certification when needed. On the other hand, recent DARPA project demonstrated conclusively that certain pathways for attackers have all been shut down in a way that is mathematically proven unhackable for those pathways. The EU has strong research base and cybersecurity ecosystem in secure software and formal methods. European commission could, in collaboration with Member States, make available, research and innovation funds (H2020) for the availability of new tools for SW development and security analysis. |

| | |
|---|---|
| Concrete actions | • Create an agency, i.e. Cybersecure Systems Engineering Organisation in charge of creating, testing and applying tools, technologies and practices to acquire, develop, operate and maintain innovative and trustworthy systems.<br>• Create awareness around secure systems life cycle among companies.<br>• Research & Innovation funds for the availability of new methodologies and tools for secure systems LifeCycle through the Supply Chain. |
| Expected benefits | • Facilitating cybersecurity by design.<br>• More secure systems.<br>• Developers and integrators with cybersecurity knowledge.<br>• More cybersecure European Industry.<br>• Easily certificable systems.<br>• Public and private procurement asking for “Made in Europe” secure systems Life Cycle use. |
| KPI | |
| SWOT Items | S2, S3, S4, S5, S6, S7, W1, W2, W5, O4, O5 |
| Vision Items | V2, V2, V3, V5 and V6 |
| Related items | R7, R11 |
| Related EU initiatives | • SDLC : software development lifecycle – a framework and methodology to ensure safety of software<br>• OWASP : “Organization for Web Applications Security Project” international framework to test application. |

| **R17.** | **Setup a pan-European campaign to educate and raise awareness about cybercrime** |
|---|---|
| Description | EU awareness is rather strong, but there a still room for better awareness for citizens who are in general not too aware about the threat scenario, ongoing cybercrime or that the police do not have resources/capacity to prioritize the crimes. EU should be at the forefront to develop a toolkit that gives companies the opportunity to secure their systems and encrypt data to secure valuable information, including trade secrets (technical/commercial) and confidential business information which could be key to maintain competitiveness. A pan-European campaign to educate and raise security awareness could also be valuable. |
| Concrete actions | • |
| Expected benefits | |
| KPI | |
| SWOT Items | |
| Vision Items | V2. Protection |
| Related items | R29, R15 |

| | |
|---|---|
| Related EU initiatives | |

| | |
|---|---|
| **R19.** | **Improve the level of security of the enterprises and strengthen industrial leadership in secure infrastructure through certification, ecosystem creation and stepped-up EU research and innovation** |
| Description | The increasing use of industrial automation systems in Europe entails risks linked not only to information security, but also to the physical security of citizens. Consider the potential impact of cyberattacks on critical infrastructures and automated industrial plants.World leaders in secure infrastructure are in the EU.Identify and promote good practices for the adoption of cost-effective models aimed at the development of high-level skills and advanced technological solutions for the security of critical infrastructures and Cyber Physical Systems at both national and European level. Leverage the development of 5G by exploiting the inherent security capabilities of 5G to provide such secure infrastructures.It could be worth creating a full European cybersecurity ecosystem from training, to products and services to address the protection of the European infrastructure. This ecosystem should encompass the adoption of **unified Cyber Security standards** (like ISO 27001 and IEC 62443) across Europe but also a European **certification scheme for products, systems and service providers** |
| Concrete actions | Identify and promote good practices for the adoption of cost-effective models aimed at the development of high-level skills and advanced technological solutions for the security of critical infrastructures and by assuring the full life cycle of Cyber Physical Systems |
| Expected benefits | |
| KPI | |
| SWOT Items | S1, S2, S6, S7, W1, T1 , S4,W2,W5,O1,O4 |
| Vision Items | V2. Protection |
| Related items | R1 |
| Related EU initiatives | |

| | |
|---|---|
| **R20.** | **Enhance the use of AI (Artificial Intelligence) for cybersecurity** |

| | |
|---|---|
| Description | AI is a promising technique that could be used to enhance attack detection and implement new counter measures. Several initiatives exist but a European approach of the topic would increase the impact of the underlying technology. This could power resilient and self-healing systems. |
| Concrete actions | • Create specific open sources libraries with AI algorithms addressing different cybersecurity needs |
| Expected benefits | |
| KPI | |
| SWOT Items | S2, W12, W14, W15, O17, O22, T23, T25 |
| Vision | V4. Leadership |
| Related items | R21 |
| Related EU initiatives | |

| **R52.** | **Align cybersecurity strategies of public institutions within EU** |
|---|---|
| Description | In order to allow for good procurement of cybersecurity solutions, public institutions should have a clear view of their needs, level of protection, interoperability of their equipment etc. The aim of this action is to make sure that national and regional strategies exist and that these strategies are well coordinated at the EU level to optimise their performance.Having said that, any industrial EU strategy should not seek to simply replicate existing mature ecosystems (e.g. Silicon Valley in the US or Beersheva in Israel). It should instead recognise and take advantage of our own European distinctive strengths and values, which are the basis to help cybersecurity ecosystems to emerge. The EU should play as a geographic constellation of "Cyber valleys". In this scenario, each regional ecosystem contributes to a common programme and facilitate a quick access of local cyber security SMEs to the European market.In this framework, Smart Specialisation in cyber security and inter-regional cooperation should become a permanent feature of the post-2020 European cyber security ecosystem.Expected Benefits<br><br>• Coherent approach to cybersecurity issues, based on national, regional specificities, among public institutions;<br>• Setting good strategic goals may drive the market to bring more advanced solutions;<br>• Ranking of public institutions will help them in defining their procurement needs;<br>• Ranking of public institutions will help the markets to adapt/standardise their product. |

| | |
|---|---|
| Concrete actions | • Open dialogue with the national cybersecurity authorities to:<br>  ○ Review the existing strategies<br>  ○ Prepare new coordinated strategies<br>• Rank public institutions into categories according to sensitivity and provide them with adequate assistance (competence centres)<br>• Develop a common methodology to measure the cybersecurity readiness for public institutions, unified and applicable across sectors.<br>• Define the activities of competence centres, their funding, status, etc.<br>• Reinforce the need to come up with a strategies, while keeping national sovereignty. |
| Expected benefits | • Aligned strategies could strengthen the economic impact of actions.<br>• Full coverage of highest standards across the EU could avoid the weakest link to be attacked.<br>• A common methodology for measuring cybersecurity readiness allows for transparent comparison. |
| KPI | • |
| SWOT Items | S1, S5, S7, S8, S9, W3, O1, O2, O6, O7 |
| Vision Items | V2. Protection |
| Related items | R29, R22, R39, R27, R51 |
| Related EU initiatives | • NIS Directive obliges national authorities to have a national strategy. |

| **R11.** | **Setup a R&D and methodology to certify complex systems, complex solutions and services** |
|---|---|
| Description | The EU has strong research base and cybersecurity ecosystem. The EU has also strong competences in certification and standardization. Cybersecurity solution are generally composed of various subcomponents. Certifying them is necessary. Certifying the overall solutions is more challenging with no method and approach yet available. EU could ease and encourage alliances between European companies involved in the field to work on process and tools for certification of complex systems or cybersecurity solutions. |
| Concrete actions | • Make available, research and innovation funds (H2020) for the availability of new methodology to certify complex systems, complex solutions and services.<br>• Integrate the UNI 11506 and (ISC)2 framework, furthermore encourage the alliance with product vendor certification (i.e. Cisco, CheckPoint, etc) |
| Expected benefits | The benefit is to reduce the cost of certification process |
| KPI | |

| | |
|---|---|
| SWOT Items | S9 |
| Vision Items | V2. Protection |
| Related items | R7, R13 |
| Related EU initiatives | |

| **R4.** | **Labelling of cybersecurity solutions in sensitive digital domains** |
|---|---|
| Description | Over the years, there has been an erosion of citizens trust and confidence in digital trust. EU could promote the use of cybersecurity certification in critical product and services for the safety and the privacy of European citizens. EU could support and encourage the development of **sectorial certification schemes** in the European cybersecurity certification framework (**IoT, consumer electronics, medical devices, wearable,** etc.). Alternatively, for less sensitive areas EU could also promote labels.Use this new cybersecurity certification framework to promote schemes for products, services and services. Voluntary approach that should come from the industry.By default, developing the certification scheme should be a voluntary approach by industry players with compulsory implementation once the scheme has been developed and approved by the commission, and the relevant standardisation organisations. If needed, such scheme development could be made compulsory by regulation. |
| Concrete actions | • Support and encourage the development of sectorial certification schemes in the European cybersecurity certification framework (IoT, consumer electronics, medical devices, wearable, etc.)<br>• Create associate labels<br>• Launch communication/awareness campaign on such labels<br>• Encourage the alliance with ITU, ISO, NIST organization to evolve the schema in emerging technology (i.e. IoT) |
| KPI | • |
| Expected benefits | |
| SWOT Items | S1, S2, S7,S9, O1, 05 |
| Vision Items | V2. Protection |
| Related items | R36 |

| | |
|---|---|
| Related EU initiatives | • In the Cybersecurity Security Act there is already the possibility to have a label for each certificate<br>• There is already an international rating system for each specific application. “Magic Quadrant of Gartner”, but this really targets experts |

| **R68.** | **Develop cyber-insurance in Europe** |
|---|---|
| Description | Introduce incentives for cyber insurance, to force institutions to implement certain cybersecurity measures. Let the market drive it for the insurance companies to shape the insurances.Cybersecurity insurance exists in the US. |
| Concrete action | • Create a European insurance |
| Expected benefits | This approach could significantly stimulate the compliance with EU standards and principles.The development of a cybers-insurance market is expected to be economically viable and to make a substantial economic impact.Insurance companies can take up the role of informal regulators to strengthen cybersecurity levels. |
| SWOT Items | |
| Vision Items | |
| Related items | |
| Related EU initiatives | |

| **R3.** | **Standardization of cybersecurity protocols and languages for better interoperability, ergonomics and secure cybersecurity solutions** |
|---|---|
| Description | Usability and ergonomics of secure product can be complex for non-cybersecurity expert. Lack of interoperability is also an issue. The EU should enable and promote interoperability and increased ergonomics of cybersecurity products and services.This innovation will conduct to a set of new security functions (like discovery and automated association), standardized commands and instructions to offer structured and secure communication streams between trusted IP connected products and services. |
| Concrete actions | |
| Expected benefits | |

| | |
|---|---|
| KPI | |
| SWOT Items | S7, W6 |
| Vision Items | V2. Protection |
| Related items | |
| Related EU initiatives | |

| **R5.** | **Maintain high security and privacy standards for better user protection and support for EU players** |
|---|---|
| Description | As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based. Stronger rules on data protection mean that people have more control over their personal data and that businesses benefit from a level playing field. This privacy regulation is challenged by foreign rules (like the US Cloud Act for example) but the EU should continue integrating high privacy and IP requirements in certification schemes in the European cybersecurity certification framework.We should continue integration of high privacy requirements in certification schemes in the European cybersecurity certification framework. |
| Concrete actions | |
| Expected benefits | |
| KPI | |
| SWOT Items | S1, S2, S4,S5, W1 |
| Vision Items | V2. Protection |
| Related items | |
| Related EU initiatives | |

| **R73.** | **Develop cybersecurity solutions for connected and autonomous vehicles (V2X) and related infrastructure** |
|---|---|
| Description | EU automotive industry is a strong one with world leaders and the autonomous connected vehicles is a worldwide race that the EU must not lost. But cybersecurity can be a handicap and at the same time a promoter of this kind of vehicles. For this reason cybersecurity of the vehicle as well as of the communications V2X must be assured not forgetting the charging of the vehicles either electric or by other means.In this direction, the EU is already working on elaborating the regulatory and enabling a framework where cybersecurity will be essential to guarantee vehicle safety. In the same way that in 2011 the ISO 26262 functional safety standard established a clear engineering process, cybersecurity needs to be designed and built into automotive systems throughout the development lifecycle to provide defence in depth by providing an engineering process as specified in the [J3061] recommended practice. Both standards aim at minimising risks coming from unwanted electronic/electrical malfunctions and cybersecurity attacks respectively. It is worth noting how the aforementioned J3061 guidelines are already on its way to turn into a standard under the *ISO/SAE CD 21424 Road Vehicles -- Cybersecurity engineering* name. ISO 21424 is supposed to be released in the latest 2019 or beginning of 2020.Among others, one of the key steps during that process is the security testing, which is particularly important to ensure that no vulnerabilities can lead to safety hazards or privacy issues. |
| Concrete actions | • Build an automotive cybersecurity testing laboratory, where full vehicle cybersecurity assessments can be performed in an independent manner<br>• Make cars safety and security transparent and comparable for customers, so that they can include this information in their purchase decision<br>• Provide consumer information on vehicle´s cybersecurity robustness<br>• Delivery of security and safety information to the automotive sector<br>• Establish a rating in terms of cybersecurity<br>• Define a coherent governance for secure electric vehicle charging. |
| Expected benefits | • More secure vehicles and transport infrastructures.<br>• Better knowledge of the level of cybersecurity of autonomous and connected vehicles.<br>• Improve the competitive position of the European automotive industry as well as the creation of specialised cybersecurity automotive industry |
| SWOT Items | S2, S3, S4, S5, S7, W1, W2, W4, W5, T1, T2 |
| Vision Items | V2, V3, V4 and V6 |
| Related items | R18, R25 |

| **R51.** | **Build cybersecurity functionalities within existing Public Procurement Competence Centres** |
|---|---|

| | |
|---|---|
| Description | As public buyers cannot be specialists in all areas, competence centres need to be established to build-up expert knowledge that is available on demand to them.Various types of competence centres already exist, the objective of this action would be to identify the existing ones and to develop their cybersecurity function.Public buyers drive 14% of GDP and administer many sensitive IT systems. Their competence in cybersecurity needs to be strengthened. |
| Concrete actions | • Identify existing structures, competence centres or similar organisations that could develop a new cybersecurity public procurement consultancy-like activity, e.g.<br>  ○ Digital Innovation Hubs (some 270 organisations, managed by CNECT, GROW is in contact for this idea already);<br>  ○ Big Buyers Initiative (a starting GROW project among big institutions to cooperate on selected themes);<br>  ○ InnoBroker type institutions – ensure that the top-edge innovative technologies are known public buyers;<br>  ○ Other similar type of organisations networks (innovation agencies).<br>• Develop a set of minimum actions, common methodology, etc.<br>  ○ Needs identification;<br>  ○ Preliminary market consultation;<br>• Technical specifications and tenders certification, etc.<br>• Ensure cooperation within the competence centres and focus on sharing best practices. |
| Expected Benefits | • Increase cybersecurity competence within the public buyers community<br>• Increase the dialogue with the cybersecurity industry to match the best solutions with the identified needs. |
| SWOT Items | S5, O1, O6, O7 |
| Vision Items | |
| Related items | R29 |
| Related EU initiatives | |

| | |
|---|---|
| **R2.** | **Proactively identify and respond to violation of trade rules by foreign countries** |

| | |
|---|---|
| Description | The EU cybersecurity industry has the level to become a good player on the world market. Some countries are trying to set legal and trade barriers to protect their internal ecosystem. The EU should monitor and tackle unfair practices in third countries, such as the through the application of The EU Trade Defence Instruments measures. If the legal conditions are fulfilled, the Commission may launch investigations with a view to determining whether the adoption of trade defence measures would be warranted.The European "International Procurement Instrument" (IPI) process, when adopted, would allow to apply measures restricting the access to the European procurement market for companies, goods and services from the third country that do not allow equal access and reciprocity in public procurement to their own markets. Potentially powerful, it is important that this process delivers effective leverage to negotiate the opening of third country procurement markets. Sufficient resources need to be allocated to ensure proper identification, investigation and response.Apply the rules of the Internal Market to cybersecurity products and applications |
| Concrete actions | • Accelerate the adoption of the "International Procurement Instrument".<br>• Envisage IPI also for Cybersecurity, to ensure identification and response to non-reciprocity in public procurement by foreign countries.<br>• Dedicate sufficient resources and ensure an agile organization setup. |
| Expected benefits | |
| KPI | |
| SWOT Items | W6,O5 |
| Vision Items | V1. Market share |
| Related items | |
| Related EU initiatives | |

| **R30.** | **Create an EU training facility centre** |
|---|---|
| Description | • Create an EU network of associate experts that train professionals and students<br>• This training facility could link to national training facilities.<br>• Next to trainings, this centre could be responsible for testing, piloting, and realising commercial deployment.<br>• Such a facility could be a potential coordinated investment and is distinct from the EU competence centre. |
| Concrete actions | Create an EU training facility centre. |

| | |
|---|---|
| Expected benefits | |
| SWOT Items | O3, T3 |
| Vision Items | |
| Related items | R18 |
| Related EU initiatives | Builds upon EU Cybersecurity Competence Centre. |

| **R45.** | **Law Regulation and Compliance for the IoT devices and Driverless Car** |
|---|---|
| Description | Using the support of academic, institutions and private contribution we can create *the EU research academy* focus on law regulation and compliance for IoT devices and driverless car. GDPR is good starting point to produce a practical documents and case studies. Expected benefits: Better EU reputation in the world. EU driving the compliance and law in the world. Business growth: consulting and technology...We can use the SAE publications and/or California Consumer Privacy Act connected devices document to start our program, in this way we can create a law base knowledge to introduce the practical documents to explain what are the steps in case of start a civil or penal action and export the framework.First guide/document:<br>• IoT devices in Civil and penal action;<br>• Driverless car in EU;<br>• US law and compliance vs EU |
| Concrete actions | • |
| Expected benefits | • Better EU reputation in the world. EU driving the compliance and law regulation in the world. Business growth: consulting and technology. |
| SWOT Items referred to | S1, S2, S6, S7, W4, O1 |
| Vision Items | V1, V3, V4, V5 |
| Related items | |
| Related EU initiatives | |

| **R40.** | **Cyber Security and Forensics in IoT devices and connected mobility** |
|---|---|
| Description | Using both experience of the academic research specialized in the cybersecurity IoT and driverless car and the private Companies specialized in big projects in military area we can create a consortium, and/or research valley, and/or innovation environments/platforms, specialized in cybersecurity or in connected mobility to write scientific papers,set up innovative case studies and patents, as well as to provide with support for the actors of the connected mobility sector to ensure cybersecurity safety of mobility solutions to customers and users.Expected Benefits EU attractive for the venture capital, export the patents and the business growth |
| Concrete actions | Export our knowledge outside EU and become attractive for the worldwide venture capital, in this way we can cover the unexplored and innovative areas. First research projects:<br>• vulnerability assessment and penetration test on the IoT devices and driverless car<br>• prevention and prediction cyber-attacks on the IoT devices and driverless car;<br>Forensics acquisition for the IoT devices.Creation of innovation platforms in partnerships with territories recognised for their expertise on connected mobility or digital in general, that could :<br>• support mobility actors with methodological and operational guidance/expertise to allow them to ensure maximum cybersecurity of their products and services to their customers/users<br>• to provide with cybersecurity analyses of connected mobility solutions<br>• to offer proof-of-concept testings for their products, services, applications etc/ |
| Expected benefits | |
| SWOT Items | S2, S6, W4, O1 |
| Vision Items | V1, V2, V3, V4, V5, V6 |
| Related items | |
| Related EU initiatives | |

| **R26.** | **Develop and promote appropriate tools for funding industrial deployment of new technologies** |
|---|---|

| | |
|---|---|
| Description | Europe has adequate tools for financing research, primarily through the Commission and Member States, in the form of subsidies, for which there is no expectation of return on investment (ROI). However, it lacks adequate tools for financing the subsequent phases of industrial deployment (prototypes, demonstrators, and large-scale rollout). These investments are often not eligible for subsidies, and struggle to raise capital due to uncertainty on ROI. This threshold effect (no ROI expectation for research, high ROI expectation for industrialisation) is one of the reason that some good technologies fail to be deployedIn some cases, the stakes involved go well beyond pure ROI considerations: environmental or societal benefits, sovereignty, security… Failing to deploy the technology simply because and ROI cannot be demonstrated for an early stage deployment is a key weakness for Europe compared to China (where state funding is massively available with no ROI considerations) and the USA (where private investors are willing to take large bets).This is problem is especially acute for Cybersecurity, where the benefits for society will be significant, but will require massive investments in the coming decades to renew infrastructure, and for which the business models are not easy to see today (ex: competitivity will depend on scale, so small scale deployment will not be competitive).<br>The European Investment Bank (EIB) is seen as a natural provider of funds for industrial deployment (Investor Portal), but its solutions may not be sufficiently well know or may not be suitable (i.e.: strict ROI requirements for equity, strict Debt Service Coverage Ratio (DSCR) for debt). |
| Concrete actions | A collaboration should be initiated between the Commission, Member States, public financial institutions (BEI, EBRC, Sovereign investment funds, national development banks) and private investors (banks, private equity, corporate) to develop and promote appropriate European financing tools, with appropriate levels of funding (hundreds of billion € overall), dedicated to financing large scale technology deployments. These tools should promote appropriate risk sharing and alignment of interest between all participants involved in a project. |
| Expected benefits | |
| SWOT Items | W2, W3, T1 |
| Vision Items | V4. Leadership |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| **R72** | **Enhance cybersecurity for the industrial domain and for the automation and communication systems that ensure safety, availability and process integrity.** |

| | |
|---|---|
| Description | Protection of critical and essential infrastructure is essential for the sovereignty and security of European nations. In accordance with Network and Information Security Directive, development of new secure technologies in detection, protection and reaction systems is a major opportunity for defence and cybersecurity of European industry. Collaboration within this domain between suppliers and operators for new and legacy systems should strengthen system security. European companies are not sufficiently present on this market to compete in a rapid rise of non-EU markets and large-scale investments. Identification of Advance Persistence Threats with monitoring and detection solutions is a response to massive and distributed attacks on industrial sector and IOT architecture. New technologies have to be promoted and developed. |
| Concrete actions | Develop complete intrusion detection systems for “essential” industry in Europe. Connection with SOC and development of AI to identify complex incident and advance attack is becoming a necessity. |
| Expected benefits | Invest in a market where non-EU are present, develop solution for Europe in a NIS domain. Make Europe independent |
| KPI | |
| SWOT Items | S4, S5, S6, S7, W4, W5, O5, O6, O7, T1 |
| Vision Items | V2, V3, V5 |
| Related items | |
| Related EU initiatives | |

## Low Priority

The recommendations below were not included in the Action Plan, because they were either not clear or did not get sufficient support from the reviewers and other participants, or may be redundant with other recommendations.

The participants who initiated or who support these recommendations are invited :

- to review them to clarify and complete,
- mere or integrate some of the key ideas in other existing recommendation (to avoid redundancy)
- solicit support of other participants if they wish to introduced the recommendations below into the Action Plan

| | |
|---|---|
| R14. | Generalizing the cybersecurity risk management in safety analysis frameworks. |
| Description | Most of the safety critical applications use safety analysis and certification through dedicated standards and norms. Merging safety and cybersecurity analysis in the same framework is a way to improve efficiency both in terms of security of the citizen and cost and time to market. |

| | |
|---|---|
| Concrete actions | Support and encourage merging safety and cybersecurity analysis in the same framework through R&D and standardization |
| Expected benefits | |
| SWOT Items | S1,S7, O1,O4,O5,T3 |
| Vision Items | V2. Protection |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| R15. | To promote a top-down culture of safety and risk-management through the conscious adoption of policies and procedures appropriate to each industrial reality |
| Description | To support the internal skills or to develop services devoted to help the enterprises to tackle the goal of developing new solutions including security and privacy by design models.To support the internal capabilities or to develop services devoted to help the enterprises to tackle the goal of developing new solutions including security and privacy by design models.To promote a top-down culture of safety and risk-management through the conscious adoption of policies and procedures appropriate to each industrial reality |
| Concrete actions | Support the internal skills or to develop services devoted to help the enterprises to tackle the goal of developing new solutions including security and privacy by design models. |
| Expected benefits | |
| SWOT Items | S1, S7, O1,O4,O5,T3 |
| Vision Items | V2. Protection |
| Related items | R17 |
| Related EU initiatives | |

| | |
|---|---|
| R67. | Set test labs using critical infrastructure as a platform for testing innovative solutions |
| Description | |
| Concrete actions | Create thematic cyber labs, give examples of existing platforms. |

| | |
|---|---|
| Expected benefits | |
| SWOT Items | |
| Vision Items | |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| R33. | Create a code of ethics/conduct to guide the use of cybersecurity |
| Description | Cybersecurity solutions can be used for both good and bad purposes. In the light of cybercrime, it is important to look at the avoidance of message by highlighting the ethical dimension of cybersecurity.There is large debate recently about the report of the Commission's group of High Level experts on AI. This report discusses the ethical dimension and red lines for the development of AI solutions. Ethics is a wide term although it often mistaken as purely moral principles. But ethics is about values and the axioliogy base of societies. We are talking about concepts that have to do with right or wrong and ultimately justice. At the very end ethics have always been the determining factor of social rules :namely lawBoth the Cybesecurity Act , GDPR regulation, promote ethics and norms on information security. The Cybersecurity Act introduced the Cybersecurity Certification Framework which promotes the principles of "security by design" and "privacy by design" whereas the GDPR promotes "privacy by design". Both, are expected to become global standards (GDPR already is). The goal of these legislations is to promote trust and confidence to the digital environment and facilitate the success of the Digital Single Market. On the other hand the security and privacy features that developers must embed to their products by design, are helping businesses and citizens to get better protection from Cybecrime, which is hitting hard the European economy. |
| Concrete actions | • Create a code of ethics to guide the use of cybersecurity |
| Expected benefits | • |
| SWOT Items | S7, O6 |
| Vision Items | |
| Related items | |
| Related EU initiatives | • Cybersecurity Act, GDPR, Cybersecurity Certification Framework, Digital Single Market |

| | |
|---|---|
| R37. | Internet access should be encrypted all the way, from sender to receiver |
| Description | Some private homes or organisations connect to the internet without any form of encryption. Routers gateways / connectors should always use encryption. We should create router platforms for encrypted communication protocols. |
| SWOT Items | |
| Concrete actions | |
| Expected benefits | |
| Vision Items | |
| Related items | 6 |
| Related EU initiatives | |

| | |
|---|---|
| R47. | Educate start-ups on their values |
| Description | Educate start-ups on their values: aim is to avoid start-ups being sold at a price far below their current but also expected value in 2-5 years, to promote EU players and to restrict the loss of knowledge to foreign countries.Note: suggestion is to look at model in Israel where start-ups need to pay back a certain amount of what the government has invested in them. |
| Concrete action | |
| Expected benefits | |
| SWOT Items | |
| Vision Items | |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| R48. | Make lifecycle support mandatory for manufactures |
| Description | |
| Concrete action | |
| Expected benefits | |
| SWOT Items | |
| Vision Items | |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| R49. | Liability |
| Description | To be implemented as a mandatory requirement, sector-based and carefully implemented. Aim is to incentivise actors to increase security (e.g. of connected devices). |
| Concrete action | |
| Expected benefits | |
| SWOT Items | |
| Vision Items | |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| R62. | Focus funding on areas of specific EU excellence or critical needs |
| Description | Areas must be selected from security and business points of view. Policy should not be based on usual suspect-philosophy, by selected the most popular sectors. It should be based on the real European skills analysis, where EU could and should having strengths, where exists widows of opportunities or/and where EU have to have some critical capabilities its own for security reasons. |
| Concrete actions | |

| | |
|---|---|
| Expected benefits | better coordination of resources and ability to focus selected must-win battles instead trying to be good in everything – but being below average in everywhere |
| KPI | |
| SWOT Items | S1, S5, S7, W1, W2, W3, W11, O1, O2, O3, O4, O5, O6, O7, O8, O9, O10, T1, T2, T3, T4, T5 |
| Vision Items | V1, V2, V3, V4, |
| Related items | |
| Related EU initiatives | |

| | |
|---|---|
| R63. | European must get maximum out its geography on the cybersecurity research |
| Description | Europe has research and education scattered around EU widely. In EU exists huge numbers of research institutes and universities, but the most of cybersecurity research is focused on the same research areas with each other organization, with the very limited resources. Instead to scatter every research resource around, there should be more encouragement for selections of key success research areas for each organization. There should be foundation what each research institutes should “and choose” to focus.There should be some evaluation of track-record, skills & resources what specific fields of cybersecurity organization could be qualifying for EU funding. When focused is selected, the organi9zation may qualify for those chosen areas only EU funding – not other areas. With better focus, more coordinated resources there will be significantly improved outcomes and EU based innovations are gaining back some key areas of cybersecurity. Note! EU need only for sector of cybersecurity 350 000 new professionals. |
| Concrete actions | |
| Expected benefits | Limited research and training resources should better coordinate inside Single European Digital Market in order catch up the global market gap. |
| KPI | |
| SWOT Items | S2, S7, W4, W6, O3, O6, T1, T3 |
| Vision Items | V1, V2, V3, V4, |
| Related items | R62, R60 |
| Related EU initiatives | |

| | |
|---|---|
| R1. | Speed up the implementation of the European cybersecurity certification framework |
| Description | The growth of the cybersecurity market in the EU – in terms of products, services and processes – is held back in a number of ways (lack of standard, reduced interoperability). It is also due to lack of a cybersecurity certification scheme recognised across the EU that ease in return market access to poor security content product from non EU industry companies. The Commission is already putting forward a proposal to set up an EU **certification framework** with ENISA at its heart. This framework should become a marker of EU cybersecurity excellence helping EU industry for market dominance with world-recognized schemes and reduced administrative complexity.Related issues:<br>• Reduce fragmentation between countries and within sectors<br>• The regulation to create this Certification Framework has been voted in March 2019 by the EU, and needs to be implemented<br>• Created guidelines for the implementation<br>• Incentives for the industry to apply the existing framework instead of introducing a new one |
| Concrete actions | Speed up the implementation of the European cybersecurity certification framework, enforce its use and help industry (including SMEs) to use it to certify their products and explore to make it compulsory in some activity sectors such as energy. |
| Expected benefits | |
| KPI | |
| SWOT Items | S4, S8, W1, W3, 04 |
| Vision Items | V4. Leadership |
| Related items | R19 |
| Related EU initiatives | |

| | |
|---|---|
| R70. | Develop secure solutions for continuous improvement of security systems |
| Description | • |
| Concrete actions | |

| | |
|---|---|
| Expected benefits | |
| KPI | |
| SWOT Items | |
| Vision Items | |
| Related items | |
| Related<br>EU initiatives | |

Development of a Hydrogen based propulsion system for regional/local trains operating on non-electrified routes or segments

**Deploy vehicle-to-grid on a large-scale in Europe**

in term of volumes and market adoption. In order for the EU to regain leadership in innovation, a