
# *Cybersecurity and Privacy landscape in Europe*

*The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission´s behalf may be held responsible for the use which may be made of the information contained therein.*

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

## TABLE OF CONTENTS

**Page**

## LIST OF ABBREVIATIONS

**AIOTI:** The Alliance for the Internet of Things Innovation
**CDTI:** Centre for the Development of Industrial Technology
**CERT:** Computer Emergency Response Team
**CISA:** Cybersecurity Information Sharing Act
**CLOUD Act**: Clarifying Lawful Overseas Use of Data Act
**CONSENT:** Customer Online Notification for Stopping Edge-provider Network Transgressions Act
**COPPA:** Children´s Online Privacy Protection Act
**cPPP:** Contractual Public-Private-Platform on Cybersecurity
**CSIRT:** Computer Security Incident Response Team
**CSA:** Coordination and Support Action
**CSDP**: Common Security and Defense Policy
**DESI**: Digital Economy and Society Index
**DHS**: Department of Homeland Security
**DSP**: Digital Service Provider
**e-Privacy**: (Proposed) e-Privacy Regulation
**EC3:** European Cybercrime Center
**ECPA:** Electronic Communications Privacy Act
**ECSO:** European Cyber Security Organisation
**EDA:** European Defense Agency
**EIT:** European Institute of Innovation & Technology
**ENISA:** European Agency for Network and Information Security
**EO:** Executive Order
**FRAME:** European ITS Framework Architecture
**FTC**: Federal Trade Commission
**GDPR**: General Data Protection Regulation
**IoT:** Internet of Things
**JCAT:** Joint Cybercrime Action Taskforce
**JRC:** Joint Research Centre
**KIC:** Knowledge and Innovation Community
**MLA**: Mutual Legal Assistance
**MLAT**: Mutual Legal Assistance Treaty
**NIS Directive**: Network and Information Systems Directive
**NIS Platform:** NIS Public-Private-Platform
**NIST**: National Institute of Standards and Technology
**OES**: Operator of Essential Services
**OTRI:** Offices for the Transference of Research Results
**R&I**: Research and Innovation
**SERIT**: Security Research in Italy
**SIEM:** Security Information and Event Management
**UEFI:** Unified Extensible Firmware Interface
**WG:** Working Groups

# 1 INTRODUCTION

This report on Cybersecurity and Privacy Landscape in Europe, Deliverable 2.1, presents a comprehensive snapshot of the current landscape of the cybersecurity and privacy activities in the European Union.

The editorial team took an approach to first define the common terminology and analysis framework that will include technological, policy, economic, legal and regulatory aspects. In so doing, it will consider the specificities of both sides and current as well as proposed legislation.

This approach has resulted in the Cybersecurity and Privacy Landscape in Europe deliverable being divided into four independent sections (not including introduction and conclusions):

Section 2 contains a comprehensive analysis of the cybersecurity and privacy research and innovation topics, taking the taxonomy of the Joint Research Centre (JRC), European Cyber Security Organisation (ECSO), ENISA and other key stakeholders, as its basis for topic selection for analysis;

Section 3 contains an overview of the EU Cybersecurity strategy to the present day;

Section 4 contains an overview of the EU policies and legislation activities to the present day;

Finally, Section 5 presents an analysis of the cybersecurity and privacy market in Europe, and contains a summary of the projects (e.g. H2020 projects), initiatives and platforms that are in place to strengthen the innovation market in the near-, mid- and long-term.

# 2 CYBERSECURITY AND PRIVACY TECHNOLOGICAL ASPECTS (INCLUDING NEW AND EMERGING TRENDS IN TECHNOLOGIES AS WELL AS THOSE FOR CYBER MENACES)

As part of the work in WP2, the AEGIS team analyzed several documents and taxonomies (e.g., the ones proposed by NIS, cPPP/ESCO, NIST, NSF, ISO 27002, etc.) and we studied relations amongst them. After some working meetings, especially with the Project Officers of the European Commission, we have come to the decision to use the taxonomy being developed by Joint Research Centre[1] (JRC). The taxonomy is prepared for the EU Commission and we assume that by selecting this taxonomy, we will ease exploiting our results in the future EU projects. This has been also used as basis of the Atlas survey issued by the EU recently at the beginning of 2018.

The taxonomy has three dimensions / domains: CyberSecurity and Privacy Technology, ICT technology and Application.

The CyberSecurity and Privacy Technical domain provides a comprehensive coverage of the core CyberSecurity and Privacy technologies. The domain is divided into 13 categories, covering low-level aspects of security (e.g., cryptography, operational security, and event handling) as well as high level ones (security management and governance, attacker modelling, education and awareness, etc.).

The ICT technological domains goes into the details of the most significant ICT technologies, which require particular cybersecurity attention. Naturally, the most advanced and quickly developing technologies (e.g., Big Data, Cloud computing, IoT, etc.) require special treatment from security point of view.

The Application domain covers the many applications that require special care and attention from cybersecurity perspective (e.g., Transport, eGovernment, Maritime, etc.). Therefore, in the next sections, we highlight the most important topics within these domains and their peculiarities from the perspective of the EU.

## *2.1 CyberSecurity and Privacy technical domain*

### *2.1.1 Assurance, Audit, and Certification*

For any organization, there is an evaluation process in order to know and ensure the security level of itself. It could comprise following but not limited: auditing, evaluation laboratory accreditation, compliance checking, security certification, and mutual recognition. A security audit, a systematic estimation based on a set of defined criteria, includes penetration and intrusion testing to assess the security of the system. Particularly, it is often used for determining regulatory compliance, and it assesses the environment, configuration, software, information handling processes, and user practices related to the system. The evaluation laboratory accreditation, so-called the Common Criteria Evaluation Methodology, defines the least required work for evaluation and leads to Certification Bodies by providing guidance in order to ensure that ITSEFs are adequate and comparable. When a policy is created, the next step is to compare the current level of the system with

[1] https://ec.europa.eu/jrc/en: European Cyber Security Centres of Expertise Map - Definitions and Taxonomy

the one that was compared to the established policies. To that end, compliance checking is well-suited for various administrative domains as well as operating systems. The Future Internet offers the correctness of the complex ICT services and there is a need for new certification mechanism for these complex systems in order to make it automatic and simple but able to certify in a sophisticated way. Finally, there is a mutual recognition, which is the first certification consensus for the Information Security of the European Commission (from March 1998) that describes the CC certificates up to EAL7.

### 2.1.2 Cryptology

Cryptography is a basic security means to achieve confidentiality and integrity. Nowadays, much progress have been made in this area, but it still full of unsolved challenges. Many (old) cryptographic algorithms have been proved to have serious weaknesses and the work on development of new strong algorithms is going on. This task is especially challenging with approaching of quantum computer development. Also, despite the amount of work on identification of weaknesses in cryptographic algorithms, more work is required to prove some basic assumptions (some of which are already in use, as AES).

The algorithms are to be used in cryptographic protocols, which protect confidentiality and integrity of messages (examples are SSL/TLS, SSH and IPsec). These protocols require secure infrastructure for key distribution, while some incidents (e.g. Diginotar, Turktrust) show that some of these infrastructures are not robust enough. Another challenging area is secure multi-party computation, which guarantees privacy of data processing by multiple agents without involving a trusted third party entity. The progress has been made in this area for threshold decryption, threshold signature, forward auctions and electronic voting schemes, but the computational cost is still too high for complex functions. The operations on encrypted data are especially important today with more and more businesses moving to cloud. The progress on homomorphic encryption provided the schemas for addition or multiplication operations, the ones that allow both of them are computationally impractical.

A lot of attention is currently devoted to quantum cryptography, which utilises quantum information encoded for cryptography. Currently, the most advanced techniques focus on quantum random number generation and quantum key distribution, though other directions also have progressed. Several quantum key distribution protocols have been developed and deployed, but their rate of key generation is low and the distance has been limited to tens of kilometres. Combination of these systems with symmetric cryptographic algorithms, like AES, proved to provide long-term security. Several of such networks have been demonstrated in USA, Australia and Asia.

### 2.1.3 Data Security and Privacy

Modern smart devices and systems aim to store and share a big amount of sensitive data. Moreover, users provide personal data to various online services for different purposes. Thus, the Privacy Enhancing Technologies (PETs) field aims to protect both personal and confidential data from disclosure and illegal usage. There are many techniques for preserving privacy on different levels. Usually, information is encrypted for storing it on external servers. However, cryptography, which is widely in used and low-cost, effects on the time needed to perform requests over data. Moreover, there are many challenges such as incomplete insecure data

access, data integrity, distributed query processing under protection requirements, and privacy of a query.

One of the problems is the protection of attributes, which might disclose sensitive information. For example, the telephone number of a person cannot be reported together with the encrypted name or information of disease. On the other hand, data integrity is necessary for achieving precise analysis result, because it could affect important decision-making. Moreover, it is important to protect data query itself, because it can disclose the interest of the entity. For instance, the user performs the request to the description of the particular disease. Therefore, this person might be suffering from this disease. Thus, the data query must be protected too.

### 2.1.4 Education and Training

Cybersecurity training helps to acquire and improve the knowledge, skills, and aptitude required to carry on professional activities by applying various technologies and pedagogical techniques. Cybersecurity awareness raises consciousness of cybersecurity situation or problem and teaches how to deal with it.

Cybersecurity training is usually performed with simulators (software/hardware tools that model the required properties of system and are able to produce identical observable effects and properties of this system, emulating its behaviour) and emulators (software/hardware tools which mimic the observable properties of the emulated system as close to the reality as possible). Typically, the emulators are used as substitutive elements of the system and simulators are used for analysis, experimentation and training.

Cyber defence exercises are relevant initiatives, during which stakeholders collaborate or compete in a simulated environment to receive and analyse problems and situations in the cyber domain.

### 2.1.5 Operational Incident Handling and Digital Forensics

Many organizations face a huge amount of cyber-attacks every day. There are many techniques to detect attacks. Intrusion Detection Systems are widely used by organizations in detecting anomalies, which potentially could be malicious. However, these systems still have limitations such as detection of algorithmic attacks (e.g., DoS attack), false positives and recognising undetected attacks. There are many IDSs available on the market. While the most widely in use by users are Suricata and Snort, research communities prefer Bro IDS. Moreover, Security Information and Event Management (SIEM) are widely used among organizations for aggregating, normalizing unstructured and unstandardized information in Internet of Things, Cloud Computing and Big Data environments.

Organizations widely use forensic tools, which are classified in proactive and post-incident. While the first class has many similarities with IDS and can only add some features, post-incident tools provide techniques for analysing and understanding past events and to use this knowledge for security propose. Moreover, many organizations produce incidents information and share it with partners in order to perform a collaborative analysis. There are many tools and standards used for representation, analysis and sharing incident data. The most common in use are STIX, TAXII and MAEC. While STIX aims to represent a comprehensive description of Cyber Threat Intelligence (CTI) in a structured way, the MAEC language reports malware analysis results performed by various tools (e.g., Cuckoo Sandbox, ThreatExpert). These two approaches can be used together in order to provide

more detailed information about cyber-attacks. Finally, TAXII is a protocol for information sharing including CTI described through STIX and MAEC. CTI described through STIX includes information related to a Threat Agent, attack pattern and malware used by a Threat Agent, system Vulnerabilities with a reference to Common Vulnerabilities and Exposure (CVE) database, and course of action for attack mitigation.

### 2.1.6 Human Aspects

The human factor represents the most important aspect of any cyber-security/privacy oriented applications. Indeed the protection of safety, in the boarder sense of the terms, of human beings is the final goal of any ICT application, and the human intervention is the most critical part of the implementation of security controls, despite the improvements and the enhancements in the technology.

The most effective cyber attacks as phishing, ransomware, credential/identity stealing, fraud as BEC, etc., essentially exploit the weakest element of the security chain that is represented by the end-user itself.

Moreover, the extent and dimensions of the usage of computing devices (from mobile phone, to wearable devices, domotic appliances, etc.) with ever increasing number of applications has flooded to practically all spheres of human life. They are now widely employed for communications by voice, entertainment, social media, utility, information gathering, news, sports etc., collecting any possible data and information about the users. Most of work activities, as well as economic transactions, are managed by a variety of devices, which security and trustworthiness can only very difficult assessed and evaluated. Indeed many successfully attacks are based on so-called fake apps, that are very effective on mobile/embedded devices. Even worse, such threats are generally neither perceived as such by the majority of public opinion that, instead, continue to trust and rely, also for critical activities, on tools which security properties are long from be reliable.

While companies have invested and are still investing on the development of a cybersecurity and privacy culture, there is no relevant and widespread example of such initiatives toward the citizens.

Despite such efforts, according to a SANS Institute's survey[2], 74% of responders still consider the e-mail attachments/links a serious security concern, while they general deploy end-point protection tools widely (81%), eventually combined with log-based security analytics [1].

The expected diffusion of even more pervasive applications generally under the umbrella of IoT/IoE, will increase the number of non-mediated interactions between the users and the ICT ecosystem, that will be very relevant not only for the security in the cyberspace, but also in the physical space.

### 2.1.7 Identity and Access Management

Authentication is an ISO/ITU standardized term that describes the process of identifying an entity to a system. This process provides confidences that an entity is not attempting a masquerade or unauthorized access attempt. In order for a user to authenticate itself to a system, the information that has to provide includes something that the user knows (PIN), has (TOKEN) or is (BIOMETRICS). Today, the

[2] SANS Institute, 2017 Threat Landscape Survey: Users on the Front Line

dominant form for user-authentication is text-based passwords. Mostly, users are required to create accounts for accessing services which increases scalability problems when they have to select and maintain several passwords. Thus, the need of password replacements is emerging. Many technologies have been proposed such as Password managers, Single sign-in services, Personalized authentication, Two-factor authentication, User-to-Device, vice versa or even Device-to-Device Authentication. A combination of the previous is used by most applications. Each authentication system has to solve crucial challenges in order to be accepted in real world over the areas of Security, Privacy and Usability. Nowadays, there exist several tools for password cracking that have as an input a dictionary of known words and password hash to find a combination to crack the password. The widespread access to information supported by ICT Technologies brings significant benefits allowing users to access electronic services and resources everywhere, anytime. These advantages come at a price of privacy risks as information often is out of control of its owner. A proper *access control framework* should regulate information exchange and access among parties, which is very challenging today. Several access control solution have neem proposed and in the last 10 years particular attention has been given to solutions over user authentication and credential or attribute based specifications. The basic idea behind these solutions is that not all access control decisions are identity-based. The research challenges include the areas of Anonymous credentials, Semantics- and context-based policies, Smooth integration with Web-based technologies, User privacy preferences, Storage at external servers and policy confidentiality and Multi-ownership management. Access control solutions are implemented in different ways within different systems. They may work at application or system level. The eXtensible Access Control Markup Language (XACML) has been receiving considerable attention. Moreover, examples of credential-based solutions are: Identity Mixer (Idemix) which is a cryptographic library of such kind algorithms and U-Prove which is a cryptographic solution that allows users to minimally disclose certified information about themselves when interacting with servers.

### *2.1.8 Security Management and Governance*

The policy enforcement applications comprise four main functions, namely, (1) policy definition, (2) compliance checking, (3) reporting, and (4) remediation. In order to regulate these functions, there are different applications including antivirus solutions, host-based application firewalls, network access controls, and others. Due to the complexity and scale of networks, the network management is becoming complex as well. In this regard, the Internet of Things (IoT), Cloud, virtualization centres are the main influencer for this issue. In particular, assessing and managing the endpoints are the most challenging part. In order to deal with this, there are available management tools provided CISCO, IBM, or HP.

It is obvious that the complexity of system challenges the cyber security experts and risk management. Although there is a number of approaches and frameworks for managing risks, none of them fits into the current situation due to the paucity of awareness of decision makers, lack of interoperability and standardized metrics, the cost-benefit ratio, static assessment model, and lack of statistical data. In addition to these issues, fast evolving threats, sophisticated attacking techniques, and motivated attackers are making the traditional way of risk management unreliable. In order to overcome these problems, we need to devise dynamic, novel, disruptive, interoperable, standardized, reactive and holistic approaches for estimating and reducing the risk in real-time, and the risk assessment and remediation activities that incorporate the threat intelligence frameworks.

### 2.1.9 Network and distributed Systems

Network security was traditionally concerned about the perimeter protection (e.g., firewalls, IDS, etc.). Currently, such an approach suffers from many drawbacks, such as BYOD practices, outsourcing of business functionalities to cloud, usage of mobile devises, etc. On the other side, the attacker put more and more effort to augment their capabilities and make their penetrations more effective. This brings new challenges for the traditional protection techniques. Nowadays, next to the traditional network packet filtering firewall, there are statefull and deep-packet inspection firewall, which allow detecting complex and more sophisticated attack, as well as host-based firewall, which protect an endpoint. IDSes, both signature and behaviour-based also need to adapt to the networks with blurred perimeter and, at the same time, look for efficient means of analysis to ensure timely response. Botnets, often used for DDoS/DoS attacks, become more robust, resilient and stealthy. The means for detection and protection against such attacks are very demanding.

Not only technical means require improvement, but the approach to network usage and management need to be updated. Virtualization, ubiquity through heterogeneous connectivity and the tendency toward Ethernet/IP as a transport over physical media demand changes in the view of networks as a closed environment with some points for communication.

### 2.1.10 Software and Hardware Security engineering

Nowadays, ICT systems usually are not designed with cybersecurity in mind. This leads to a number of problems and high costs which could have been avoided if security had been taken into consideration from the start. Security- and Privacy-by-design principles must be embedded into the software/hardware engineering practices to reduce the number of grave and costly incidents. Today there are solutions for securing the application under development at all stages of the software development life-cycle (SDLC). Some of these solutions target early stages of development, providing verification of security properties (such as secrecy and authentication) or formally analysing the design (e.g., SecureUML) or requirements (e.g., KAOS or Tropos); others target implementation level ensuring secure coding and testing the code. Moreover, new approaches to secure design are demanded by flexible and modular nature of the future applications. Trusted relations should be established on the fly, rather than build-in, as it is done today.

In the realm of tech-related society, the cyber security, where the offensive methods are countless, is becoming one of the challenging tasks we have to cope with. Attackers are no longer motivated only by fame or skill demonstration, but also are encouraged by the financial and political reward. The well-known offensive methods are namely infiltrating a malware or virus, creating botnets, executing buffer overflows attack, penetrating a system based on known vulnerabilities, and sending spam emails. Currently, there are other challenges in terms of research in this field: Polymorphic/Metamorphic Attacks, Undetected Threats, and Advanced Persistent Threats.

### 2.1.11 Security Measurements

In cyber security, there is a lack of well-defined standards, sophisticated models, and the prediction model of any system's behaviour. The reasons are divided into 4 major parts: (a) *rapid technology progress*, which makes old systems and standards obsolete; (b) additional dependencies and expansion of the attack surface cause by *networking*; (c) *complexity* which rises as systems become more

potent, (d) *the malicious nature of the threat* with intent that makes the traditional ways of measuring cyber security futile. The integrity, confidentiality and availability are the aspects that any security metrics should take into account.

In order to efficiently measure the security of any system, both researchers and practitioners have been introducing methods and models. For instance, the International Systems Security Engineering Association's "*SSE-CMM Project*" the National Institute of Standards and Technology's "*IT Security Assessment Framework*" the National Institute of Standards and Technology's "*Security Metrics Guide for Information Technology Systems*" the US Department of Defense's "*Information Assurance Readiness Project*" the ISO standard for "*Common Criteria*" and the "*Security Metrics*" guide introduced by the Center for Internet Security (CIS), which is in the right direction comparing to others. However, some researchers such as M. Satyanarayanan from Carnegie Mellon University, propose the idea to establish fair and consistent system of public challenges, rather than metrics. Despite the effort, there is still a need for measurable, attainable, repeatable, and time-dependent standards to establish (George Jelen, in "SSE-CMM security metrics"). In particular, such metrics must be meaningful and consider which metrics are leading/lagging in a real system so that it will be synchronized into risk assessment.

### *2.1.12 Legal Aspects*

In the recent years, the most relevant event related to the regulation and legal aspects of the cyber security and privacy can be considered the adoption and application by the EU of the new General Data Protection Regulation.

That is because its scope of applicability (essentially the management of any data that can be related to EU citizen) has important economic implications for the most of enterprises that have interest in the EU market (so far, the largest and richest single market in the world).

The new regulation is attempting to harmonize the approaches developed by Member States in the application of former EU's directives, building a common foundation for citizen's digital privacy rights.

It puts an end to the enterprise self-regulation approaches as binding corporate rules and various forms of privacy shields. Moreover it is considered by many non-EU countries and companies as a form of protectionism, since it limits the provisioning of services. Some non-EU service providers have retired their offerings from the EU market, since they are still evaluating/implementing the burden of the new regulations.

While GDPR is seen as being a positive step to enforce the use of appropriate processes and technologies in order to keep personal data handled with diligence, there are some concerns being raised about its impact especially on the smaller SMEs and start-ups, which wouldn't have the resources and/or legal expertise or funds for the administrative and legal costs. In addition, the GDPR impact on technologies such as blockchain technologies raises a certain paradox, being coined as the "Blockchain-GDPR Paradox" [2] as some of the protection mechanisms and encryption techniques being used by blockchain doesn't exactly match the requirements of GDPR, as even though they are quite secure and robust, it doesn't technically speaking match the definition of data "should be erasable" even if it is encapsulated quite securely. Therefore, in its current form, blockchain technologies cannot be considered as fully complying with GDPR requirements and there is a need for research and innovation in order to find a satisfactory solution for this. Some potential work-around solutions are outlined in [2].

Despite the important result, it can be considered a downside compromise, since in many aspects it is somehow more permissive that some local regulations (for instance, it does not provide any data protection rights to organization, but only to individual). Moreover, it is established that the legal competence for multinational/transnational companies operating in the EU is based on the country that such companies have selected for their local representative, instead of the country of the resident EU citizen. That means that large enterprises can virtually select the actual legal framework and the national authority to deal with that is a clear market distortion, in particular with respect to the SMEs. The same approach has been adopted in the past for fiscal aspects and it has been resulted in tax heavens within the EU, so it is wondering if it could result into a sort of "privacy heaven".

In any case, it is still unclear about the effectiveness of GDPR in preventing large scale data abuse scandals, such as "Facebook and Cambridge Analytica".

### *2.1.13 Theoretical Foundations*

During the last two decades, there has been increasing interest in foundations for various methods in computer security, including the formal specification, analysis and design of cryptographic protocols and their applications, the formal definition of various properties of security (such as confidentiality and integrity) and well as access control mechanisms. A relevant strand of research is language-based security that includes the modelling of information flow and its application to confidentiality policies, system composition and covert channel analysis. This large research area covers new programming platforms that deliver development and runtime environments for trustworthy application code to be executed in the complex application scenarios. Research is also on language design and implementations, including middleware and run-time environment. Several types of systems, verifying compilers, support for run-time property verification and enforcement have been addressed here as well. Programming principles and constructs have been investigated in order to ease secure service development and composition for the new application scenarios. Code signatures and well as code instrumentations, aspect oriented and other composition techniques for security and secure execution environments are also in the scope of this area. Specifically in the context of service creation, we will address security issues in Business Process Modeling and Execution languages.

The research area encompassing the formal analysis of security protocols/architectures is central in the development of protocols and software-based services to ensure confidence (assurance) about the security level. This research theme will thus cover testing methodologies such as black- and white-box testing, model based testing, static code analysis as well as dynamic code analysis. Moreover, verification approaches such as model checking and theorem proving techniques have been adopted at several levels from requirements analysis down to source code. Also correctness-by-construction methods, in particular, step-wise refinement have been developed. This approach uniformly covers all essential phases of the software development life cycle (SDLC). Recently, run-time verification methodologies and distributed monitoring and compliance frameworks have been established as a formal tool for dynamic monitoring of system execution. Covert channels and information flow properties have been also widely studied using formal models.

### 2.1.14 Trust Management, Assurance, and Accountability

Individuals need to be empowered to develop trust into digital services and/or apps for them to make informed decision. Thus, methodologies to focus also on Trustworthiness need to be designed. Trust management has also been advocated in many places while recognized as key to fully embrace the Digital Society. Among others, it is expected to enable Trusted (Cloud) Services to be developed in any layer (IaaS, PaaS, SaaS) in order to reduce the consequences of the vulnerabilities at each layer.

Trusted hardware addresses a broad range of devices, could be stationary and could be mobile. All these trusted hardware are connected to a network like the web or mobile network (GSM, UMTS, LTE, 5G). There are some pre-requisites to trust a connected IoT device in the field. Trusted hardware could be having different form factors such as vehicle, machine, mobile device, others stationary device, energy network train transportation, finance. Trust into IoT devices and nodes like Gateways, Routers, Connectors, Actuators, Sensors and End Nodes require trust into the components used and the related implementation of those into the device. Starting with the trust into the hardware, meaning the semiconductor components need to fulfil basic security requirements and minimum standards which might defer on sectors. The root of trust and the secure boot loaded from end nodes to the back end system is based on components with secure key storage to offer security for deviceID and encryption. All interconnected devices could be defined as cyber physical systems (CPS). It should be taken into account that the definition of security for a complete system cannot be higher than the definition of security for the storage of keys for cryptographic operations on IC level. Interoperability with other IoT devices within the infrastructure is a desirable objective. IoT devices should be marked with security labels to generate trust into connected IoT devices towards citizens, end users and businesses. One of the main strategically axis for Mobile security is to protect the access of the future 5G European network. It is strategic cybersecurity issue and a strong authentication protocol should be invented in Europe.

## 2.2 ICT technology domain

### 2.2.1 Information Systems

The impact of cyber-attacks in general, and of cybercrime, on businesses is rising almost everywhere around the world, it looks like to be very hard to stop and even to contain. Moreover, among the digital transformation trends, the responses to these menaces are one of the most relevant driver in the evolution of Enterprise Information Systems.

Indeed, in many enterprises, the awareness of the cyber-menace is very low at board/strategic level, while the information security officers, given also the contribution of regulatory pressure, will become more and more important, in terms of roles and contribution to the overall business.

Indeed, the very last successful of an organization (or its own persistence) can be deeply related to the capability to face with such threats, providing its own users/customers with an adequate assurance.

Despite that, many executives do not get it as a priority, while not enough resources are available for the protection of the organization. Such aspect is very relevant in SMEs, where the security posture is not generally adequate, and there is a lack of specialized profiles.

In general, the evolution of the Information System as whole, from the cyber security perspective, is driven by a number of factors as: the availability of skilled cyber security professionals, the continuous assessment and audit of the environment, the increase of role and responsibilities of the CISO, the sharing of intelligence data as well as the ability to effective employ them.

For instance, the raising trend of the Cyber-Threat Intelligence (CTI) has pointed out that despite the availability of adequate information about menaces and indicators of compromise (IOC), the organizations experience serious troubles in the effectively rely on them for improving the security posture. Sometime too much information is available and it is very difficult to map to the Information System landscape in order to evaluate the relevance or the actual exploitability (e.g., exposure) for a given single organization, considering also the speed of changes also from the architectural perspective (e.g., the migration to the cloud or the adoption of other hybrid computing models).

Indeed, according to some surveys[3], while the perception of the risk is high and increasing, most of security professionals are sceptical about the actual capability of the organization in defending its own Information System [3]. Therefore, there is a general agreement (71%) about the fact that a data breach involving high value information with a negative impact on the organization (e.g., brand/reputational damage) is highly probable in next years.

### 2.2.2 Mobile Devices

The Internet services are heavily used by mobile devices, such as smartphones and tablets. Such reliance on mobile devises also requires good security. There are several approaches to prevent malware attacks. The prevention-based approach applies cryptographic algorithms, digital signatures, hash functions, and has to be running at real time. Detection-based approach is, similar to other IDSes, is divided to anomaly- and signature-based. Several mechanisms are able to control applications running on a mobile devise. Some of them are based on static code inspection at load time, while others impose policies on application execution and enforce them at run-time. Some hybrid mechanisms exist as well. Also, mobile devises may benefit from the trusted computing technologies, which provide a root-of-trust for the smartphone and then apply a number of cryptographic technics to establish trust in the executed applications.

### 2.2.3 Operating Systems

Operation systems today are huge and have million lines of code. On the other hand, the size and complexity of the code provokes system bugs, which can be exploited by attackers. In order to address the problem several techniques were proposed. System hardening requires minimising of the number of trusted system components and improving security by fin-grained permission checks in order to reduce possible impact a component may cause if compromised. Detection and prevention techniques try to detect and mitigate intrusions when they happen. Updates are able to patch discovered vulnerabilities, but so some operating systems (e.g., for mobile or IoT devices) such approach is not as quick as required. Virtualization helps to keep applications isolated, but also runs on current operating systems and add even more complexity.

[3] Ponemon Institute, 2018 Study on Global Megatrends in Cybersecurity, Feb. 2018

### 2.2.4 Big Data

Big Data refers to very large, dynamic, multi-sourced data sets. Analysis of Big Data could reveal relationships and insights that would be very valuable. Therefore, collecting, storing and analyzing Big Data is essential to develop strategies, policies and solutions to pressing problems. Given that data has become a new factor of economic competitiveness and production, it is essential to have the right technological basis and organizational structure to acquire and exploit data. Big Data is directly generated by users or indirectly derived from their activities or automatically by the systems that make up our digital environment. Classical approaches are not suitable enough for Big Data analysis due to the scale of the data and its dynamic sources and varying structure. This instead became possible by a variety of novel and original enablers, such as data mining techniques, which are collectively referred as Big Data Analytics techniques. Security mechanisms in the Big Data domain need to address speed and scalability as major concerns, so data at rest, data in transit and data in use need to be secured under these constraints. In addition, malicious nodes and sources could destabilize the Big Data environment and therefore they need to be secured focusing more in problems arisen in the implementation rather than design. Big Data technologies can be divided into two groups: batch and stream processing, which are analytics on data at rest and in motion respectively. An example of batch processing is the MapReduce programming framework. The most common example of this approach is Hadoop. The stream processing technologies include Storm, which is an open source distributed and fault-tolerant real-time computation system designed for supporting real-time processing of large scale streaming data on clusters of horizontally scalable commodity machines. Other examples include Spark and Dremel. In the Big Data for security intelligence, domain large companies like IBM and RSA provide emerging security analytics tools that are envisioned to multiply with SME's in the coming 3 to 5 years. With the democratization of cloud infrastructures and the availability of open source solutions, the tools SME's need to innovate in Big Data are coming together.

### 2.2.5 Vehicular Systems

Information systems, networks, electronic devices, and sensors are playing an increasingly important role in the evolution of transport systems, as instruments used for different purposes under different conditions.

In particular, the evolution of Intelligent Transportation Systems (ITS), that apply information and communication technologies to every transport mode and provide services which can be used by both passenger and freight transport, is aiming of integrating the capabilities that can be deployed on vehicles, in order to improve the general safety of the transportation infrastructure as well as its performance (e.g., form self-driven/assisted-driven vehicle, to traffic management and power management).

Indeed, one of main challenge lies in the integration of existing technologies with the aim of making transport more sustainable, which involves a compromise between efficiency, eco-friendship and safety.

Several approaches and technologies (e.g., VANET, V2I and V2V) to the communication have been devised and investigated so far, but without a general coordination among different vendors and authorities/countries, leading to a proliferation of standards and technical solutions, with a variety of heterogeneous visions and approaches. A suitable implementation of such technologies will, hence, require a huge integration and harmonization effort.

The European ITS Framework Architecture (FRAME)[4] has been developed in Europe in order to support the development of ITS and to foster their roll-out by the Member States.

Moreover, as well as other embedded technologies, the ones currently considered for vehicular applications have not been designed considering the security aspects from the very begin, and generally speaking security controls have been implemented by retrofitting.

### 2.2.6 Critical Infrastructures

In the EU, as "Critical Infrastructure", we generally identify the assets and the related processes that need to operate at a level such that the users, or anyone that benefit from the outputs of such systems, have a seamless experience.

Among these are generally enlisted power grid, water supply, telecommunication, transportation, law enforcement, payment transaction processing, and many such systems that need to work seamlessly at any time, or, in other words, that are always available, unless to pose a serious threat to the safety and health of the served community.

Most, if not every, of such infrastructure has been deeply re-architected and integrated with the surrounding digital (e.g., ICT) environment as many of Industrial Control Systems (ICSs), in order to improve the automation level, resulting in a reduced level human intervention and subsequent error proneness.

Among various benefit coming from the digitalization of the critical infrastructure, there is the possibility to generate and collected more and more data from various sources. Such data result to be very useful for descriptive and predictive analytics in order to schedule preventive maintenance and prevent failures.

Therefore, data-driven approaches to critical infrastructure have been perceived as an important driver to improvements in efficiency and overall reliability.

On the other side, most of such infrastructures have become more and more exposed to incidents and attacks related to the digital components as networking and computing for several reasons. The first one is related to the actual reliability of complex ICT systems that is of some order of magnitude lower that "legacy" control automation technologies: e.g., the agility and flexibility provided by a software-defined environment comes at a price. While some digital control technologies can be even formally validated during the design, there is no feasible approach to obtain a similar assurance for general purpose computer software, when even an entry-level operating system kernel can be composed by millions of line of code.

Moreover, as other ICSs, most of such infrastructures have been designed and implemented assuming they will be insulated from mainstream communication network (the so-called "air gap"). It is worth mentioning that critical infrastructures are very valuable targets from the attacker perspective because their own importance and visibility.

As matter of example, we can consider the reliability and resilience of the old landline telephone networks (e.g., PSTN) compared to VoIP solutions.

However, the effort in improving the overall resilience of digitalized and network-connected critical infrastructure is a very relevant topic. In particular, the availability of near real-time data about such infrastructure is considered a critical asset for effective strategies against cyber-attacks, given the possibility to implement reliable monitoring and alerting systems. Therefore, there is the need

[4] http://frame-online.eu/

for an actual sharing of such data among the various authorities that are involved in the protection of these infrastructures. In these respects, the new EU NIS Directive plays an important role in order to establish an effective coordination and sharing environment amongst EU Member States.

### 2.2.7 Industrial Control Systems

ICSs are mainly focused on controlling physical processes in critical infrastructures starting from food production up to electricity production and distribution. With the new era of the Internet of Everything, where all systems are interconnected through the Internet, ICSs become vulnerable to cyber threats. According to security reports provided by different sources (e.g., US ICS-CERT, Kaspersky-Lab), the number and complexity of cyber-attacks on ICSs are still increasing in dangerous ways. The report by ICS-CERT defines 322 new vulnerabilities to industrial control systems discovered in 2017. The most common types of vulnerabilities include buffer overflow and improper authentication.

Currently, there are many issues for achieving security in ICSs. It is required to ensure that the input data is not used by an attacker in gaining access privileges. Access to ICS is provided with a combination of password/username or even without any authorisation. The access is not controlled continuously, allowing performing any uncontrolled operation after the access is granted. The majority of software for ICS was designed and integrated without following secure concepts. The communication protocols contain unprotected sensitive data. Many ICS networks contain firewalls with weak rules and ICS LAN might be not routed through firewalls at all.

### 2.2.8 Supply Chain

The evolution of business models induced by the Globalization and other related trends, has requested to the enterprises, in order to remain competitive in the market to adopt agile approaches to their own organization and in the management of the supply chain, regardless the kind of goods or services involved.

On the other hand, the regulatory pressure in most market sectors has driven the demand of appropriate tools to preserve the trustiness and assurance levels, even in such competitive environment. Any suitable approach, despite it is related to a technologic-driven market as the ICT, has important implications on the organizational side.

Indeed, many security frameworks that could adopted by an organization, as the ISO/IEC 2700x standard body, put a special attention to the management of business relations in the supply chain for the aspects related to the information security.

Generally, security and privacy requirements are pushed down through the supply chain, but the enforcement of security controls are rarely monitored or audited. Even worse, in many cases such requirements are not actually enforceable at all.

For instance, the lack of an effective IP protection regulation in countries like China, where most of hardware devices are produced or assembled, has driven not only to a rich market for counterfeit goods (that is an issue by itself), but also to a proliferation of fake devices and components (e.g., CPU, chipset, FPGA, controllers), that once included into other products (or used by themselves), can be an effective way to introduce vulnerabilities or, even worse, to deploy backdoors (a sort of trojan horses).

### 2.2.9 Internet of Things

The Internet of Things could be seen as a worldwide network of interconnected entities. The application of IoT are numerous, but mostly related to environment monitoring and information collection. It is heavily used in various industry sectors, transportation, retail, healthcare, etc. Smart home is another well-known area of IoT application.

The IoT has a number of distinct features which make it unique. IoT consists of multiple devices of various kinds and created by various producers, performing different actions and heaving different capabilities (heterogeneity). In theory, the elements of the IoT could be in any place of the world using the Internet as a means of communication (distribution). The number of the network participants is expected to be huge, i.e., much higher that the Internet experiences today (large scale). The dynamicity of the network, both in terms of space and re-organisation and evolution is high (dynamicity). From the security point of view, IoT has a particular interest also because the devices often not produced with cyber security in mind and have limited capabilities for demanding security features (e.g., cryptography). Because of that and the vast amount of data IoT collects, IoT becomes an attractive target for attackers who may get much information through compromised devices.

The IoT community in the EU is quite vibrant with a number of groups and initiatives taking centre stage in recent activities. These include:

1. AIOT[5]I (Alliance for Internet of Things Innovation), whose members include key IoT industrial players – large companies, successful SMEs and dynamic start-ups – as well as well-known European research centres, universities, associations and public bodies
2. The IoT FORUM[6] – THE INTERNET OF THINGS INTERNATIONAL FORUM, which is a member based organization which aims to promote international dialogue and cooperation on the Internet of Things; organize events and conferences, such as the IoT Week, and develop activities and synergies with and among its members. It supports the development of a worldwide interoperable Internet of Things, addressing technology barriers, business and societal challenges to create the conditions for a truly worldwide Internet of Things ecosystem and market. It does this through promoting international dialogue and cooperation on the Internet of Things between diverse actors from industry, research and government and across sectors.
3. IoT Council[7], which is an members based IoT ecosystem advising on the ecosystem management, building of quality relationships with all stakeholders and curating a conversation for an EU – led approach to IoT systems.
4. NGI[8] (Next Generation Internet), which is a nascent EU programme that started in 2016, which aims to shape the future internet as an interoperable platform ecosystem that embodies the values that Europe holds dear: openness, inclusivity, transparency, privacy, cooperation, and protection of data.

In addition, there are some Member States initiatives in relation to IoT; for example, IoTItaly[9], which takes a strong national approach to working with the IoT stakeholders in the country to develop systems that are interoperable.

[5] https://aioti.eu/
[6] https://iotforum.org/
[7] https://www.theinternetofthings.eu/
[8] http://www.ngi.eu/
[9] http://www.iotitaly.net/

### 2.2.10 Hardware

Generally speaking, in the cyber security community, one of the most vulnerable technology layers is considered the software layer; in particular, the application/custom software applications, because of poor design and even poorer test. On the contrary, hardware devices (from CPU, to memory, to chipset/BIOS to motherboard, etc.) are considered reliable, sound and vulnerability free. Indeed, at the end any information system security feature in some form relies on the security capabilities provided by the underlying hardware infrastructure (e.g., consider the privileged and user execution modes of the modern CPUs).

However, a number of hardware-oriented threats have emerged in these years. For instance, attacks toward firmware have been discovered (e.g., Equation Group, Row Hammer), and these kinds of attacks tend to be very sophisticated and difficult to detected and eventually eradicated.

The industry has replied to this threat by introducing some forms of hardware based protection, such as the UEFI (that protect the system against compromised OS images during the boot) and firmware protection using digital signature-based sanity check, update, and recovery approaches.

Nevertheless, the disclosure of CPU-rooted vulnerabilities as SPECTRE and Meltdown, that exploit architecture and design flaws of mainstream CPUs (e.g., Intel, AMD, ARM, and, to a lesser extent, SPARC) to steal information, bypassing any protection and process insulation mechanism that can be enforced at software level (i.e., meaning at the OS kernel level), has raised many concerns. In particular they are focused on an element of the computing infrastructure (the CPU) so far considered the most reliable one.

These vulnerabilities, instead, are not only not detectable using available tools, but they could be exploited by zero-day attacks and they can be used in multi-tenant/cloud environment to virtually evading any segregation mechanism provided by the hypervisor.

Some technologies, as the Moving Target Defence (MVT), can provide some help in intercepting the attack at some stage of the kill chain, but they cannot completely compensate the design flaw of the underlying hardware components.

Moreover, such kinds of vulnerabilities have made clear to the user, that while the software can be patched, the same is not always true for the hardware. So far the available patches, despite not completely effective, involves sensitive performance degradation on affected systems. A valid solution will require a deep revision of CPU architecture, in particular for the speculative execution part, and it will require a substitution of the affected devices, with a relevant foreseen expenditure.

Moreover, these vulnerabilities have pointed out that the lack of appropriate tools and processes to deal with them.

The hardware-related threat landscape, in particular for the implications on embedded/pervasive devices, has been also addressed by ENISA [4].

### 2.2.11 Cloud and Virtualization

Cloud computing could be seen as a business model that by means of various technologies provides remote dynamic and flexible IT services. The model has a number of challenges related to securing the technologies in use, but it also have some unique problems caused by Cloud Computing as a holistic paradigm. Many of these problems have a root in the lost control over the system. Once the business is shifted to a cloud, the internal IT team has much less capabilities to ensure its secure execution. Moreover, there is an additional risk of the potential abuse (of

security or privacy) of the outsourced assets by the cloud provider. From the attacker perspective, clouds, which now run businesses of many clients, become much more attractive targets. These challenges and attractiveness of the new business model make security in Cloud a very important topic.

### 2.2.12 Pervasive Systems

The evolution in the field of the so-called edge-computing has leaded to the concrete possibility to deploy large and complex systems that are able to collect data (and, eventually, to perform actions) pervasively in the physical world. The availability of network communication stacks (possibly radio-based) optimized w.r.t. the power consumption, of compact and affordable system-on-chip devices (even for consumer/SOHO market), and of distributed algorithms for data collecting and processing are the main enabling factors that drive such market sector, whose range of application is still in evolution, as well as the technology foundations.

Such kind of system generally requires a reduced human interaction, but, on the other side, there is a lot of machine-to-machine (M2M) interactions, because the physical distribution of the system itself, and the fact that each networked "smart" devices has limited computing power (in terms of CPU, memory, storage, bandwidth, and even battery capacity), so the communication architecture has to be accordingly designed, including also resilience, availability, and security features.

In other words, such pervasive and ubiquitous systems and support networks, despite they facilitate the processing and collection of data generated by field sensors, need to be adequately protected, in order to ensure data privacy and integrity, since they represent a significant increase of the attack surface.

Given the application of such technologies in many critical contexts (ICS, banking, transportations, and healthcare), involving high sensitive data, the necessity to reduce the attack surface acquires a paramount importance.

Even more, pursuing such goal is very complex because the technology landscape is very heterogeneous both from the technology vendor perspective, both from the architectural reference models. Most of these applications have been designed with their own network and computing model that are generally denoted as "ad hoc". So the reuse of solutions and security controls between different system is a very hard task. A suitable strategy to improve the security posture in this field must operate at different levels, which means considering the security requirements in policy, business, and technological domains in a coherent way. Moreover, a standardization of protocols and approaches is expected by the main market vendors and associations.

An analysis of threat landscape for pervasive systems, focused on networking communication aspects, is available from ENISA[10] [5].

### 2.2.13 Embedded Systems

The embedded systems/devices are one of the main enabling factors of the development of many segments of the ICT industries.

Some technologies (e.g., Raspberry Pi, Arduino) are generally available in the mainstream consumer market rendering the "smart-thing" concept a common place. Many of such systems are embedded in day-by-day device, has home appliances, TV sets, surveillance camera, domotic controllers, etc., and there are

[10] ENISA, Ad-hoc & sensor networking for M2M Communications - Threat Landscape and Good Practice Guide, Jan 2017

several examples of so-called "smart-building" that are able to autonomous control the environment based on the external (e.g., weather) and internal (e.g., the number of guest) factors, even considering trends and occupation forecast.

Such devices are essentially a specialized and rugged computer (optimized for the field deployment) but that share with traditional computing devices many features, and from the security standpoint, vulnerabilities. That means that they need to be adequately protected, despite they are not generally perceived as a potential threat source.

A lot of exploits of such kind of devices have been reported so far. For instance, the SHODAN website[11] maintain an inventory of Internet-facing compromised devices that count several thousands of elements, many of them have been simply deployed without changing the default administrative password.

Specific malwares (as Mirai) have been developed and deployed in order to build large botnets of such devices (thousands or event hundreds of thousands). This approach has demonstrated to be very effective, since relying on such botnets, some record-breaking DDOS attacks[12] have been successfully deployed.

A very important issue in such context is that many vendors do not provide adequate security information about their products neither support/post-sale updates even in case of security vulnerabilities. Even more, there is also a lack of transparency in the communications with end-users/customers. For instance, most of so-called P2P IP cameras available on the market, used for video surveillance in SOHO/SME context rely on the processing/distribution of the video streams captured by the device to the user for remote viewing through server systems located anywhere, without clear statement about the protection of data and user privacy, excluding some weak corporate self-regulation. Despite the strong regulation of the data privacy topic in the EU, there are no evidences of any action addressing such kind of issues.

### *2.2.14 Quantum Technologies*

The quantum technologies have two major implications in the field of cyber-security and related applications.

The first one is the exploitation of quantum entanglement of elementary particles (as photons) to securely transmit information, or, even better, to securely distribute the keys to be used to actual exchange the data. Such quantum based communication channels are expected to be immune (by physical properties rather by mathematical ones) to tampering and eavesdropping.

From the architectural standpoint, the quantum network is a layer on which the key distribution system operates providing the foundation on which the conventional communication network can be established. Moreover, quantum properties can be exploited to improve the bandwidth (i.e., the noise tolerance) of a channel w.r.t. to the classical approaches.

The second application of quantum technologies is related to the implementation of a so-called quantum computing device that is expected to be able to solve some problems that are actually infeasible using standard computing devices that actually mimic a deterministic computing machine. Some of the problems that are expected to be solvable using a quantum computing device are related to some of most relevant cryptographic standards used nowadays as number factorization, discrete

[11] https://www.shodan.io/

[12] It was the first DDOS attack that has surpassed the 1 Tbps volume threshold: https://www.deepdotweb.com/2016/11/06/analysis-record-ddos-attacks-mirai-iot-botnet/

logarithm, etc. Despite the fact that the actual computing limits of quantum computer devices is not completely understood (and the maturity of the corresponding implementations is quite low, at least according to the results published), it is expected that many of cryptographic tools currently in use will be considered weak in some near future and will need to be replaced.

The availability of such kinds of technology will also imply a serious concern about the legal validity of digital signatures applied to contacts and documents that are expected to last for several decades.

### *2.2.15 Artificial Intelligence*

The adoption of so-called Narrow AI technologies, in particular Machine Learning or Deep Learning approaches, in many general available applications is gaining speed and acceptance by the users and the ICT market in general.

Moreover the availability of computing power (eventually relying the elasticity provided by cloud computation model and big data tools) and of many extensive data sets about the behaviour of the users and of real-world "thinks" (e.g., data collected by IoT), have enabled the possibility to semi-automatically or automatically train some very accurate statistical models that can be deployed to semi or fully automate a wide range of tasks.

In particular, such model can be used to implement smart-controllers that could be used to monitor a process and to perform corrective actions of component interactions, in order to improve security and resilience.

There are also many use cases based on such technologies that are relevant for the cyber-security field. In particular, unsupervised learning approaches can be exploited in order to detect attacks by identifying anomalies in operational or communication, to discover patterns and relationships to support cyber-threat intelligence and analytics capabilities. There are several case of advanced attack techniques detected by applying big data learning tools to mine the data generated by protocol heavily exploited by attackers as DNS query logs.

Inferred models can be exploited to evaluate incoming data against policies and known behaviours, to detect anomalies or to adjust the behaviour considering the new information. Technique like graph analytics can be exploited to show relationships among disparate data points, pointing out unusual elements, in order to evaluate the risk level of an event. So it can be greatly alleviate the burden for human analysts that can focus their efforts in the analysis of most relevant events, resulting a productivity and accuracy boost.

Generally speaking, the cyber security community is expecting a foundational contribution by these technologies in increasing the reliability and the security posture of ICT environment.

On the other side, there are already several examples of AI-based security attacks that leverage on the same technologies to threat the users and systems, resulting also in serious data-breaches. For instance, the large bot-nets, mimic the end-user behaviour, have been deployed to manipulate product/service rankings on the Internet. As well as, new sophisticated phishing attacks rely on advanced algorithm for automatic text synthesis, easily fouling the users (even the most experienced ones).

In other words, the army race between the defender and the attacker communities is expected to include AI-based tools in both sides.

### 2.2.16 Robotics

The developments in the field of robotics are considered strategic by most of countries, as well as by the EU, that has launched a Strategy Research Agenda on Robotics since 2014.

Despite the huge impact on society and economics, the development of robotics technologies, supported by the evolution of AI technology, poses a number of ethical questions, in particular when such tools are employed to perform actions without the human intervention or supervision.

Indeed, many of such technologies are very opaque to use, that means that sometime is very difficult to explain how an algorithm, eventually based on some kind of machine learning, is producing an output, that means is selecting an option or a behaviour. In other words, their actions are often no longer intelligible, and no longer open to scrutiny by humans. Considering the expected impact of these technologies, this is a not very reassuring conclusion.

Indeed, applications as the advanced mechatronic, that combines AI/ML, WSN, IoT, mechanical and electrical engineering, are expected to enable the development of wide range of increasingly sophisticated robotic and high-tech systems for practical applications in service and production industries (from the domotic to the health care, retail, and logistics) and security and safety, as well as other critical domains, as the autonomous vehicles and weapon systems.

Moreover, many AI models are based on large dataset which sources are not always clearly established (the countries as the US and China that lead the AI research, in particular for military application, generally do not put the privacy of the user/citizen at very first place) and they are private and for large part based on proprietary technologies.

On such respects, the European Group on Ethics in Science and New Technologies of the European Commission has developed a statement on "Artificial Intelligence, Robotics and 'Autonomous' Systems" in order to investigate these issues and concerns. In particular, they have established some foundational principles and requisites in order: to preserve the human dignity and the autonomy of human being, to enforce the responsibility of the AI research and the accountability, to support the democratic values and rights, etc. It is expected that such technologies will be sustainable and be provide a contribution to justice, equity, and solidarity, as well to safety and security.

### 2.2.17 Blockchain and distribution Ledger Technology

Blockchains (or distributed ledger technology) evolution has been considered as very disruptive technology (like the early Internet) in terms of potential impacts industries including Healthcare, Public Sector, Energy, Manufacturing and particularly Financial Services. It has also been predicted[13] that it could represent the foundation of the new finance global ecosystem.

Waiting for the realization of such predictions, so far, these technologies have introduced some not very pleasant implications from the cyber security perspective.

First of all, Bitcoin and other cryptocurrencies are nowadays the most preferred payment method for cyber-extortion (e.g., ransom-ware), not mentioning the usage as generally accepted currencies in the Dark Web for any sort of "business" transaction, as well as a very effective trans-border money transfer/laundry tool

[13] Deloitte EMEA Grid Blockchain Lab, Blockchain & Cyber Security, 2017

(on the contrary, the killer application for such technologies has been clearly identified).

Even worse, the trends in the quotation of many of these currencies are such that one of most prominent menaces is the so-called Bitcoin Mining Attacks, which are cyber-attacks aimed at stealing computing power from the victims for mining cryptocurrencies that can be instantly monetized. Some of these attacks are implemented using HTML5/JavaScript technologies, so they could easily deployed from a defaced website or, even easier, from a webpage that is vulnerable to XSS/CSRF to a wide audience with a minimal investment from the attacker point-of-view. These kind of attacks are generally very difficult to detect (e.g., they can be implemented file-less, so current anti-malware tools are not very effective against them), and sometimes they are neither perceived by end-users, who could simply experience a slow-down of her/his computer, that could be ascribed to many other causes. Many attacks can be also persistent, which means that the mining process remains active even after the exit of the web browser process.

Concurrently, there is also a proliferation of malware that explicitly targets the user cryptocurrency wallets in order to steal a credit amount; in particular, many of them spreading, in the form of fake applications (apps) for mobile devices. In that case, the lack of any authorization/secondary control, as well as a central authority or third part verification, results in an unavailability of any effective protection (excluding conventional end-point protection tools).

The distributed ledger technology, moreover, poses some security challenges by itself as: the lack of confidentiality about exchanged information and transaction history (besides the anonymity of account owner), the lack of standard network access controls (many blockchain implementations have been devised as public services), the need for an always available network connectivity among the peers, and the difficult to provide "the right to be forgotten" and as well as the non-repudiation. Indeed, despite the blocks of the chain are actually digitally signed, the identification and authentication of the signer is far from being reliable. On the other hand, these technologies can provide a good resilience assurance given the almost absence of single-point-of-failure.

Some of these issues can be actually addressed in not-public (e.g., private and/or controlled) GL implementations, but the high computational impact due to the proof-of-work/proof-of-stake approach, render such technology viable only in such cases where no central authority can be established and only a peer-to-peer approach is accepted by the network members.

As already addressed in section 2.1.12, the" Blockchain-GDPR Paradox" [2] must also be addressed by the research and innovation communities to ensure that Blockchain technologies indeed comply with the EU's GDPR guidelines.

### *2.2.18 High-performance computing*

HPC systems are for some aspects very similar to conventional IT/enterprise computing, since they share most of technological foundations, but for some other aspects, there are very relevant differences.

In particular, they have very distinctive modes of operation focused on mathematical computations or other CPU-intensive tasks and they can run highly exotic hardware and software stacks (e.g., GPU or FPGA) that are not compatible with mainstream tools and approaches.

Nevertheless, from the cyber security standpoint, the main feature they exhibit is the extreme openness to users, also in order to enable broad scientific collaboration, often involving contribution from several countries.

It means that security controls are not the top-most priority in the design and implementation of high-performance computing platform, and many commonplace solutions and approaches do not fit with constraints of HPC.

On the other side, such platforms can deal with very sensitive data (e.g., medical science applications).

Hence, there is the need for additional/complementary security tools that could help to enhance the security posture for these applications, leading to the implementation of suitable compensative controls (e.g., segregation, boundary access controls, centralized management, etc.).

### 2.2.19 Satellite systems and applications

Many economic activities are dependent on secure telecommunication services, including those implemented using satellite telecommunication systems.

For example, a large part of satellite systems infrastructure is integrated into the backbone of the Internet and its communication protocols. Many services as television broadcast, phone, GPS and network connectivity are provided via satellite links.

To provide a secure, robust communications, monitoring, positioning capabilities to the users, these systems are designed to implement defence in depth from targeted attacks and component failure as well as operate effectively in very adverse environmental conditions. Indeed, due to the prohibitive cost of replacement, communication satellite spacecraft need to be designed with lifespans of over decades, providing a continual service, considering unacceptable any downtime.

That means that it is required the continuation of operational capabilities even in case of cyber-attack, and the traditional incident management approaches based on isolation and quarantine are not applicable. It implies, hence, multiple levels of redundancy in terms of information and service paths, protocols and implementations.

Nevertheless, satellite ground systems represent an often neglected aspect of cyber security, but if compromised could be exploited by attacker to gain the control of the overall satellite-based communication infrastructure. Some examples of satellite seizing by hackers are reported by the press, but generally they are focused on using such devices as broadcast medium to reach a larger audience.

Even more, despite satellite systems can be an important enabling factor in the implementation and deployment of new services and applications, the impact of new regulation frameworks (e.g., about telecommunications, lawful interception, encryption, privacy and data protection) should be adequately assessed. It is expected it could drive an evolution of future satellite systems, since non-compliance with such regulations could prevent the operator to provide services in a given market/area[14].

### 2.2.20 Human Machine Interface

The Human Machine Interfaces are gaining more and more interest because they are considered a valuable target in many scenarios.

For instance, in many SCADA/ICS systems, attackers tend to target the HMI since it represents the main hub for managing the infrastructure. If it can be compromised,

[14] ESA, Cyber Threats on Satcom Networks and Impacts on the Global Society, 2017

just about anything can be done to the infrastructure itself, including physical damage.

Since the HMI acts as the main hub for managing the infrastructure, controlling it allows an attacker to harvest information about it. An attacker could also disable alarms and notifications, which means suppressing alerts operators in case of dangers to equipment.

Indeed, many HMI solutions result to be based on poorly designed and coded application software, that presents many vulnerabilities (from memory corruption issues, to code injection, lack of authentication/authorization, usage of deprecated/unsupported libraries, etc.), that could easily exploited to gain the control of the system itself. Even more, there are also several cases, in particular, from niche/small vendor, of HMI applications that mandate for obsolete or unsupported client operating systems (e.g., Windows XP).

Generally, the vendors do not implement an adequate secure software lifecycle management process that could help in capturing many of such vulnerabilities before the release, and there is also a significant delay in the availability of security patches if compared with other ICT market segments (in average, the wait time between the disclosure of the vulnerability and the availability of the patch is 140 days[15]).

Similar considerations are valid also to other contexts as medical devices[16].

## 2.3 Application Domains

### 2.3.1 Defence

Since most of crises and conflicts in the world have a cyber dimension, almost all country defence organizations consider the Internet (i.e., the cyber space) as a possible war zone.

Moreover, also many private organizations are now facing attacks that for the extent and complexity are likely to be backed by nation-level agencies[17].

Despite the identification of attackers in the general case is neither easy neither reliable, in many policy frameworks it is allowed to consider cyber-attacks from hostile actors as an act of war that justifies, under the most serious of circumstances, a response with conventional weapons.

Generally speaking the adequate development of cyber defence capabilities and supporting resources is considered a strategy priority from Member States as well as by the EU (that includes the Cyber Security into its own Common Security and Defence Policy) and by the NATO.

### 2.3.2 Digital Infrastructure

Under the umbrella of the Single Digital Market, the EU has adopted a strategy oriented toward the implementation of Gigabit Society by 2025.

In particular, such strategies is articulated on the following main actions:

1. To provide Gigabit connectivity to main socio-economic actors;

[15] Trend Micro, Hacker Machine Interface, 2017
[16] BSI Group, Cybersecurity of medical devices, 2017
[17] Ponemon Institute, The Rise in Nation State Attacks, 2015

2. To deploy uninterrupted 5G coverage on all urban areas and major terrestrial transport ways;
3. To provide connectivity offering at least 100 Mbps for all households.

The implementation of these actions is charged to each Member State, which is monitored by the Commission that evaluates a Digital Economy and Society Index (DESI), summarizing relevant indicators on digital performance and tracking the progress Member States in digital competitiveness. This index does not consider only the connectivity and the infrastructure aspects, but also the human capital development, the integration of business processes, etc..

According to last available data, while the standard network connectivity is generally available across the EU, the distribution of the access to ultra-broadband or next-generation technologies (as defined by the strategy) is quite heterogeneous (in particular in rural regions). The declining of the telco market is not helping the investment required to build such digital infrastructure[18].

### 2.3.3 Energy

Electric utility networks nowadays tend to move towards "smart grids". Such grids are able to communicate via the high-voltage lines, using the powerline-carrier system and have been designed to dynamically integrate decentralized grid components. A big problem in the securing of grids is grounded in the fact that protocols, meters and other utilities are not designed with security in mind and have little capability to support security features. This weakness, together with high decentralization.

### 2.3.4 Financial Services

The financial services suffer from threats to on-line banking, payment processors, financial markets and securities. Attackers may achieve their goals through installing a malware, social engineering, targeted attacks, Advanced Persistent Threat (APT), Denial of Service Attack (DoS) and Distributed-denial-of-service Attack (DDoS).

### 2.3.5 Government and public authorities

The digital transformation is generally considered a very important opportunity for government and public authorities to improve their own processes (and hence improve the efficiency and reduce the waste of resources) as well as to improve the quality of the relationship with the citizens.

Moreover, one of most important enabling factor is represented by the digital identity management, since it is a foundational element required to deliver any kind of service to the user. So far, various Member States have been established their own framework for provide a form digital identity management (and strong authentication tools) to their citizens since late '90 with the first smart-card applications, and there are also some attempts to integrate them in a coherent way at EU level with the eIDAS regulation, since it is considered also a cornerstone element of the Single Digital Market. It is expected to provide a common legal basis to Member States enabling the recognition of e-IDs issue by others MS to effectively implement a cross-border interoperability. Considering the diffusion in the target population of mobile devices, most of technical approaches leverage on

[18] European Commission, Europe's Digital Progress Report, 2017

the capabilities of such products to operate as security token/authentication device. Moreover, many vendors have already released biometric authentication features (e.g., fingerprint, face-recognition, etc.) that can be employed to further improve the identity assurance level.

### 2.3.6 Health

Nowadays, many health services require electronic devices and/or the access to the network to share data and receive further guidance and usual mobile devises, like mobile phones and laptops, are increasingly used in the area. Moreover, the traditional model of a stand-alone Health Information Systems (HIS) transforms into networked HIS, where sensitive health data are exchanged with other HISes and third parties. Despite the amount of research in the area of eHealth security, acquired knowledge and a spectrum of pertinent standards, cyber security remains an issue for eHealth.

### 2.3.7 Maritime

Given the trends of in the global trade as well as the development of both cargo and cruising industries, also the maritime transportation sector is experiencing a very important transformation in the adoption of ICT both for ashore and on-board applications.

Nevertheless, some of most relevant victims of last large scale ransom-ware attacks ware some maritime cargo market leaders.

Indeed, when we keep into account the evolution of the so-called Smart Cruise Ship, it looks like that they have to provide to the served community (can that be estimated in terms of some thousands of individuals) a whole portfolio of digital services, from the rough network connectivity to telephone services, from TV/VOD and entertainment media distribution to environment controls, from location-based services (e.g., internal positioning and routing and kid finding) to social networking/messaging, from intelligent room assistant to payment and billing, that can easily match in variety and complexity a smart-city environment.

Conversely, such services must be operated in safe and secure way in an environment that must be considered insulated, because the reliability of communication means in open seas, and with a very short team. Remote management cannot be considered as a suitable option. That implies the need for adequate tools, which have to be able to provide a strong level in terms of automation, requiring a low management effort.

### 2.3.8 Audiovisual and media

The Media and Entertainment business is a typical target of cyber menaces because the market value of the copyrighted material that they produce and distribute.

Historically, the piracy of audio/visual content can be considered the first form of mass data breaches. The wide adoption of IP-based TV broadcasting, VOD and other streaming technologies have greatly extended the attack surface. Moreover, most of copy protection technologies deployed so far on the market (e.g., DVD CSS, Blueray Disk AACS, DRMs, watermarking) have demonstrate to be ineffective. Even more, the adoption of encryption technologies, in particular to preserve the user privacy and the copyrighted content from the disclosure, has relevant implication in the architecture of streaming farms, due to the burden of cryptographic algorithms.

Many content providers/distributors have developed their custom players, in order to incorporate additional security controls (e.g., encrypted network streams, back-end authentication, dynamically generated end-points), but they are reliable until the client platform (i.e., the end-user device) is able to prevent the user from executing privileged operation (e.g., using a debugger or other low level diagnostic tools). Such assumption does not hold in the case of general purpose PCs, but it has regained importance with the wide spreading of new kind of devices as gaming consoles, smart-phones and tablets that, by design, grant to the owner only very limited privileges (unless they have been rooted or jail-braked by the user in order to circumvent such restrictions).

In any case, with the affirmation of mobile broadband networks (e.g., 4G/LTE), also the consumption of entertainment media is expected to evolve with the growth of the consumer that will be access to these contents in mobility.

The **New European Media (NEM) Technology Platform** [19] of Europe is a European Technology Platform (ETP), fostering the convergence among Media, Content, Creative industries, Social Media, Broadcasting and Telecom sectors, as well as Consumer electronics to develop a common innovation environment for the new European media landscape. NEM Platform is a very active community, working closely with the European Commission in developing the strategic research and innovation agenda of the network and electronic media sectors.

### *2.3.9 Industry 4.0*

The Industry 4.0, also known as 4th Industrial Revolution, aims at implementing a connected (or even smart) factory, in order to improve the manufacturing processes rely on the innovation provided by evolution of the ICT and represent a cornerstone point of the digital transformation of the global society.

Nevertheless, it represents also a very valuable target for the cyber menace because also of its intrinsic nature of Cyber-Physical System. As many other examples of CPS, it also suffers from a general immaturity of available technology, as well as of the organizations that are willing to adopt such new manufacturing paradigms, but that have not adequate skills and expertise for ICT and Cyber Security. Among the challenges that must be faced in this domain, we have, hence: an increased general system complexity, an increase of number of cyber menaces and attack paths, and an increase in terms of sensitiveness of processed/exchanged data.

### *2.3.10 Nuclear*

Nuclear-based power generation plants (and other supporting facilities, as for fuel and waste management) are one of the most critical infrastructure to be protected against the cyber menaces.

Indeed, as any other critical infrastructure, they are required to always operate in order to provide the expected outputs to the users, that relies on the power supply for a number of applications, so they need to be protected against any threat that could disrupt the operational status (many countries rely on nuclear power plants to sustain a relevant part of their energy needs).

But, they are also a valuable target for cyber terrorist due the huge expected extent (and visibility) of an incident resulting from a sabotage.

[19] https://nem-initiative.org/

In recent years, several incidents/cyber-attacks involving this kind of facilities have been tracked, despite the actual identity of the attackers has not be clearly established (as the most part of more important/sophisticated cyber-attacks).

Hence, most of countries, including the EU and its Member States, have recognized that this is a critical sector that need appropriate security measures in order to face the challenges it poses. Given the nature of the menace and its implication, a viable strategy must include also near/connected non-EU countries.

According to the recommendations[20] of the Energy Expert Cyber Security Platform to the European Commission, in particular the nuclear sector (and its related fuel/water management cycles) must be explicitly included into the scope of the NIS Directive in order to promote a consistent development of defences against cyber-attacks. Leaving such critical area to the initiative to each Member State may negative impact the effectiveness of defence strategy starting from the information exchange and the cooperation in the incident management.

### *2.3.11 Tourism*

As businesses within the travel and hospitality sector grow, so too does their global footprint of sensitive data.

Two main trends are driving the evolution of the cyber security this domain: the first is impact of regulations that most of countries are adopting and that affect travel operators since their intrinsic trans-national nature; the second is the primary role that ICT technologies has assumed in the implementation of business transactions with the raise of Internet-based booking/virtual travel agencies (while conventional travel agencies are disappearing, many travellers can book even a very long/articulated journey without any human interaction).

Indeed the tourism industry (and in a wider sense the travel and hospitality) is beginning to acknowledge the importance of cyber security in its day-to-day operations.

Each operator need to manage all kinds of sensitive data on their customers (e.g., personal information, payment data), as well as their own staff and suppliers. The consequences of organisations experiencing cyber-attacks, eventually resulting in data breaches, are now higher than ever before. The consequences of these incidents can be very relevant in terms of financial, legal, and reputational effects.

Moreover, the maturity and the readiness of the organizations operating in this domain w.r.t. the ICT in general and Cyber Security is not generally very high, because so far these components haven't played a so primary role in their business.

Indeed, they are one of most valuable target for cyber extortion[21], despite the amounts involved in the average incident, the affected target base is very large and there is a high likelihood that most of such incidents are never declared because of the negative reputational impacts.

The guest privacy is also threated by the fact that most of WiFi services provided them by the hotel are generally unsecured, to their communications are exposed to eavesdropping and their devices could be exposed to hacking attempts.

Even more, many hotel-chains are continually adopting any sort of advanced domotic and environment control technologies to improve their customer experience, aiming at implement a sort of smart-hotel. As consequence they are,

[20] EECSP, Cyber Security in the Energy Sector - Recommendations for the European Commission, 2017

[21] https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html

hence, facing the all kinds of reliability and security problems that such technologies carry with them[22].

### 2.3.12 Smart Ecosystems

The objective of smart eco-systems as smart-cities, smart-homes, etc. is to dynamically optimize the environment in order to offer a better quality of life to the citizens and to drive economic growth, through the application of ICT tools and applications.

The increase of data exchange controls multiple services and assets leads to a higher degree of automation of the environment. As several critical services become interconnected, the need for cyber security oriented approach is vital to protect data exchanges, privacy as well as the health and safety of users.

However, there is currently the lack of harmonised guidelines or standards to address the challenges posed by the rise of smart environments. Indeed each authority, vendor, service provider, operator, is acting independently, and many implementations result to be inadequate in terms of resilience, performance, and scalability.

There are several sectors that are affected by this revolution, from transportation/mobility to energy distribution, from water supply to waste collecting and disposal, from environment control to health-care, from government to public safety and security. In other words, almost every aspect of the citizen personal and professional life are touched and, hence, are potentially exposed in case of a cyber security attack or incident targeting the smart ecosystem platforms.

For instance, one of most successfully applications in this respect, is the video-surveillance, with many public/mass CCTV systems around the world, that, despite they could in some way contribute to the street crime fighting, are, without adequate controls in place, clearly prone to be abused, representing a serious threat to citizen privacy. So far, large scale smart surveillance systems have been implemented by Countries where privacy is not really a concern[23].

Generally speaking, effective cyber security is increasingly complex to deliver, and in this scenario is even very hard to clearly define the perimeter to protect, given the high number and variety of involved actors. Indeed, the kind of threats to face spread from hardware faults to common usage software bugs, from human error to cyber extortion and terrorism.

Many technical and organizational tools can be considered in order to improve the security posture of such applications. However, generally speaking, in order to ensure an adequate resilience, it is highly advisable to include a complete secure test bench of such systems[24] and to address the operational continuity of the most critical services and processes even in case of serious attack/disaster, developing back-up and DR plans[25].

### 2.3.13 Space

Space is considered a key strategic asset for its navigation, observation and data transmission capabilities.

[22] https://www.bbc.com/news/technology-43896360
[23] https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/
[24] CSA, Cyber Security Guidelines for Smart City Technology Adoption, 2015
[25] EY, Cyber Security - A necessary pillar of Smart Cities, 2016

Most of the global critical infrastructure (e.g., communications, air transport, maritime trade, financial and other business services, weather and environmental monitoring and defence systems) heavily relies on the space infrastructure, including satellites, ground stations and data links at national, regional and international levels.

Moreover, as many other domain, also this industrial sector are facing the disruption of the global digital transformation of the social and economic environment. Indeed, there are several small-satellite initiatives that are demonstrating the viability of employment of many spacecrafts far smaller than traditional satellites. Such approach could easily revolutionize many applications, since networks of linked small-sats can easily and efficiently provide network access, communications, data storage and transmission, imaging, and remote sensing, enabling many commercial and scientific applications. Many of such new technologies share their ICT foundation with common IoT devices, and, hence their intrinsic vulnerabilities and weakness.

So, since space activities can provide valuable services and data, they are an interesting target for cyber espionage, including economic cyber espionage, and cybercrime. In other words, the cyber security must become a priority also in space sector, both for public and private operators that, in the meanwhile, are greatly extending their capabilities (including also unmanned launching, while manned private space flight are expected to occur in very next years).

Initiatives as the Galileo System, Space Surveillance Awareness (SSA), Copernicus System, and several other earth/environment monitoring missions, have demonstrated that when Member States cannot autonomously achieve their goals and fulfil their needs, because of gaps in technological and/or investment capabilities, the EU can play a very prominent role in developing and supply common services and technologies. Therefore, it is important to extend such cooperation also to include cyber security aspects, aligned with other EU initiatives in such domain (e.g., relying on NIS Directive).

### *2.3.14 Public Safety*

Public Safety agencies must face the cyber threat menaces not only because there are by themselves a very important target for attackers, but also because among their duties there is the defence of the citizen and of the digital society against cybercrime and connected illegal activities (e.g., money laundry, digital piracy, dark market, cyber terrorism, online fraud, etc.), even pursued by the organized crime at international level.

In order to establish a common ground for cooperation among different countries and their law enforcement agencies and strengthen the response to cybercrime, for instance, Europol has set up European Cybercrime Centre (EC3). It provides strategic guidance, training, capability building, operational support for cyber intelligence, joint task forces, and digital forensics expertise to other agencies.

According to their analyses[26], while some kind of menaces (as exploit kit market) are declining, the threats posed to digital infrastructures are increasing because the evolution of attacks leveraging on even more advanced techniques as botnets and social engineering, while the shortage in terms of capabilities and skills by the targeted organization continue to be an issue, despite the large number of initiatives. Menaces as ransomware are expected to persist in the near future, unless a valid countermeasure will be generally available. Moreover, the cybercrime community is adopting even more secure and advanced techniques to prevent

[26] Europol, Internet Organised Crime Threat Assessment, 2017

interception and tripwire of their communications. Darkweb forums and communities continue to be a valuable source of intelligence, but their relevance is declining. Even more, there is a convergence between cybercrime and terrorism, having terrorists leveraging on cybercrime tools for their activities (e.g., coordination, fundraising, illicit market), despite their capabilities to launch important cyber-attacks are estimated to be quite limited.

The cooperation among law enforcement agencies and private organizations is a key success factor in contrasting the cybercrime, in particular working together on threat analysis and prevention initiatives.

### 2.3.15 Supply Chain

The supply chain is fundamental aspects to any manufacturing organization. It is also deeply connected to consumer demand, since most of organizations use demand forecasts to determine the quantity of materials necessary, manufacturing line requirements, and distribution channel loads.

It is, hence, possible to obtain great benefit from the adoption of analytics models to can be used to understand and predict customer buying patterns and, hence, the resulting demand.

In general evolution trend, driven by the Industry 4.0 technologies, it is expected that also the supply-chain structure will be deeply impacted by introducing intelligent, connected platforms and devices across the ecosystem, resulting in the construction of a Digital Supply Network (DSN) as ultimate evolution of the so-called Business Partner Integration (BPI). It would improve the overall the management and flow of materials and goods, the resources usage efficiency, the customer satisfaction.

Indeed, as the supply chain will evolve toward a near real-time dynamic environment (where demand and offer will have to match), the need to open data to all participants will increase, posing a question about the trade-off between the transparency required by the process and the need to preserve the confidentiality of business critical information.

Organizations may thus want to consider ways to secure that information to prevent unauthorized users from accessing it across the network.

Not only manufacturing supply chain is affected by cyber threats, but also the software industry has been victim of this kind of attack, resulting in the compromising of a software product with millions of impacted users[27]. Indeed this approach is very attractive because several factors: it allows to infiltrate also in well-protected organizations by leveraging a trusted channel, it can spread across a vast user base very quickly because of automatic updates, it can exploit elevated privileges required by the installation process itself, and it is very difficult to detect.

This will place even more constraints on 3P risk management.

### 2.3.16 Transportation

Increasing interconnectivity and interdependence of transportation increases their vulnerability to cyber-attacks. Moreover, it is enhanced by increased connectivity and reliance to the Internet and embedded devices. Thus, system access due to interoperability of transport systems becomes critical in assets like static field devices, dynamic transport management systems, connected vehicles and freight transport management systems.

[27] https://blog.avast.com/progress-on-ccleaner-investigation

Two general methods used by attackers. First is altering data storage by sabotaging the system through physical alternation or destruction of system components or jamming/denial of service attack. Of course, it could also happen via malware infection to make data unusable. The second one is the alternation of information exchange. This method includes message falsification, selective message dissimulation or delay and malware infection or framing attacks. Moreover, this method could also include software and sensor manipulation, denial of service attacks and message linking.

There are several measures, although not uniformly applied, with vast variance between each other. These measures are Authentication and digital signature, Messaging protocol and encryption, Information privacy, non-repudiation and secure routing.

Nevertheless, ENISA has developed some guidance for the protection of public transportation system from cyber menaces[28], supporting an integrated and uniform approach that is expected to promote the collaboration among involved public and private actors and to enhance the overall status of cyber security.

[28] ENISA, Cyber Security and Resilience of Intelligent Public Transport, 2015

# 3 EU CYBERSECURITY STRATEGY

The EU outlined its cybersecurity strategy in 2013, titling it "An Open, Safe and Secure Cyberspace [6]". The document summarized the EU´s five strategic priorities and actions in the short and long term and how it would achieve these goals. The following are the priorities established in the EU cybersecurity strategy:

- Achieving cyber resilience;
- Drastically reducing cybercrime;
- Developing a cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP);
- Developing the industrial and technological resources for cybersecurity;
- Establishing a coherent international cyberspace policy for the European Union that promoted core EU values.

The AEGIS White Paper on Cybersecurity Policies[29] breaks down the European cybersecurity strategy as well as EU policies and legislations in detail. In addition, the White Paper also outlines US strategies and policies in this area.

The next sections will outline a number of additional tactical directives and activities carried out in Europe as part of its cybersecurity strategy in the last 4+ years.

## *3.1 NIS Directive*

The Directive on security of network and information systems (the NIS Directive) is the first set of rules on European security approved by the European Union. The directive was adopted on July, 6 2016 and took effect in August 2016 [7]. The NIS directive includes three essential points:

- Strengthening cyber security management capabilities in every state of the European Union.
- Increasing the level of collaboration between the States of the European Union;
- Strengthening risk management strategies and reporting cyber security incidents.

Its main objective is, therefore, to achieve a high common level of network and information security in all Member States of the European Union and to achieve greater cooperation between all Member States in order to facilitate information sharing on risks and cooperation with particular reference to the management of IT security incidents and related risks.

More specifically, the NIS Directive establishes a set of network and information security requirements that apply to operators of essential services and digital service providers (DSPs)[30]. Under the new directive, in order to achieve a culture of safety in those sectors, which is vital to the EU economy, operators of essential services and digital service providers will have to adopt appropriate security measures and report serious incidents to the competent national authority. Operators of essential services include the following sectors: energy, transport, banking, financial market infrastructures, health, drinking water supply, distribution, and digital infrastructure sectors. Digital service providers, on the other hand, include "online marketplaces, online search engines, cloud computing services"[31].

[29] D1.3White Paper on Cybersecurity Policies: Common Ground for EU-US Collaboration
[30] https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts
[31] http://europa.eu/rapid/press-release_IP-15-6270_it.htm

One of the essential characteristics of the NIS directive is to build a solid foundation for forming a European network and information security framework. Thus, it arises from the need of each Member State to secure its infrastructures and guarantee their functioning according to common rules and requirements. To achieve this consistency, each country must therefore align its methods, approaches, and security practices. This strategy will prevent European companies from operating in a fragmented environment and will facilitate and improve their compliance efforts. European Union countries will have time until May 9, 2018 to implement the directive at the national level.

The NIS directive requires that each Member State of the European Union complies with a series of obligations. In particular, the NIS Directive defines specific obligations and rules for operators of essential services and digital service providers. These entities will need to take appropriate organizational measures to manage security risks related to network and information systems and minimize the impact of incidents affecting the level of network security and information systems used for the provision and continuity of these services. Furthermore, the Directive requires a national IT security authority and a national CSIRT to manage IT risks and notifications in case of major incidents involving critical infrastructures in each Member State[32]. Essential and digital service providers will be obliged to notify this type of event to the competent authorities without undue delay and this notification should include information to enable the authorities to determine the severity of the incident and the possible impact[33].

## 3.2 NIS Public Private Platform (NIS Platform)

The establishment of the NIS Public-Private Platform (NIS Platform [8]) was announced in the Cybersecurity Strategy of the European Union. It shared the same objective as the Cybersecurity Strategy [6] and the NIS Directive [7], i.e. to foster the resilience of the networks and information systems which underpin the services provided by market operators and public administrations in Europe. At the initial scoping meeting in June, 2013, the NIS Platform was designed into three distinct working groups in order to implement the measures set out in the NIS Directive and to ensure its convergent and harmonised application across the EU. The main goals of the NIS Platform were to help public and private organisations improve cybersecurity risk management and information sharing, and to prepare a Strategic Research Agenda for secure ICT. A key focus was on turning research results into commercial products, to serve Europe's growth and jobs objectives.

Operationally, an initial meeting was held in June, 2013 to discuss and scope the working groups' formation and the first official kick off meeting of the three NIS Platform working groups was held in September, 2013. The working groups were the following:

- WG1: Risk management, including information assurance, risks metrics and awareness raising;
- WG2 on Information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
- WG3 on Secure ICT research and innovation.

[32] https://clusit.it/wp-content/uploads/2017/02/direttiva_nis.pdf
[33] http://community.forumpa.it/system/files/file_upload/Direttiva%20NIS%20-%20allegato%201.pdf

The working groups were cross-cutting, with all relevant sectors represented and worked together to identify cross cutting / horizontal best practices.

A complete set of deliverables for each of the Working groups were delivered over a period of 2+ years and a comprehensive set of all the documents can be downloaded from https://resilience.enisa.europa.eu/nis-platform/shared-documents.

## 3.3 CPPP

Within the Digital Single Market Strategy, the European Commission has established a contractual Public-Private Partnership (cPPP) on cyber security, with the aim of strengthening the EU's cyber security industry. The purpose of the cPPP, which is mainly to stimulate the European cyber security sector, is considered strategic within the EU, and therefore needs to be pursued through several actions:

- Bringing together industrial and public resources to improve the European industrial policy on cyber security, focusing on innovation, and following a jointly agreed strategic research and an innovative path;
- Promoting trust between Member States and industrial actors by fostering bottom-up cooperation for research and innovation;
- Helping to stimulate the cyber security industry by aligning the demand and supply of cyber security products and services and allowing the sector to efficiently address the future needs of end users;
- Using funding from Horizon 2020 (H2020) and maximizing the impact of available sector funds through better coordination and a better focus on certain technical priorities;
- Improving the visibility of European excellence in R & I in cyber security and digital privacy.

The public part of the cPPP is provided by the European Commission, while the private part is provided by a fully self-financed non-for-profit organization under the Belgian law, called The European Cyber Security Organization (ECSO) [9]. Currently, ECSO[34] (https://ecs-org.eu/) has around 220 members.

The constitution of the cPPP allowed a budget growth, which is available in the remaining part of H2020 from 200ME to 450M Euros. This increase seems to be possible for FP9 (post H2020) as well.

The vastness and complexity of the issues related to cybersecurity require forms of cooperation between entities that, although with different roles, operate in this sector, which is essential for the security and the economy of the European Union and of our country. In order to achieve a more effective management, it is necessary to develop every possible synergy that facilitates these integrations and, in this context, ECSO represents a strategic element of great importance.

## 3.4 EU Global Strategy for Foreign and Security Policy

The EU Global Strategy adopted in June 2016[35] increases its focus on cybersecurity, and supports multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of information. It will enhance its cybersecurity cooperation with core partners such as the US and NATO. The EU's

[34] https://ecs-org.eu/

[35] Shared Vision, Common Action: A Stronger Europe. Global Strategy for the EU's Foreign and Security Policy, June 2016

response will also be embedded in strong public-private partnerships. Cooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cyber security culture, and raise preparedness for possible cyber disruptions and attacks.

## 3.5 European Agenda on Security

The new European Agenda on Security 2015-2020[36] gives renewed emphasis to implementation of existing policies on cybersecurity and addresses new threats and threats that are more international, cross border and cross sectorial, with cybercrime as one of the three top priorities (alongside terrorism and organised crime).

## 3.6 Digital Single Market Strategy

The Digital Single Market Strategy (2015) [37] includes a contractual public-private partnership (PPP) on cybersecurity to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions. This will be described in more detail in section 5.

[36] The European Agenda on Security. Strasbourg, 28.4.2015. COM (2015) 185 final
[37] Digital Single Market Strategy https://ec.europa.eu/digital-single-market/en/digital-single-market

# 4 POLICIES AND LEGISLATIONS

## 4.1 CyberSecurity Package

In light of the significant cybersecurity changes that have occurred in the European in the last years and the increasing risks due to the increasing interconnectivity, the Commission decided to reinforce the EU's capabilities to react to cyber-attacks.

For this reason, on 13 September 2017, on the occasion of the State of the Union speech, the European Commission (also known as "Commission" or "EC") presented a comprehensive package of measures to strengthen cybersecurity within the EU.

In particular, it builds upon existing procedures and introduces new initiatives to further enhance EU cyber resilience, deterrence, and defence. The goal of this package is to promote cybersecurity preparedness, flexibility, and harmonization, but, at the same time, it is aimed at avoiding implementation challenges and regulatory fragmentation across the EU. The package includes a recommendation[38], two communications[39] [40], a proposal for a regulation[41], and a proposal for a directive[42]. Some of these documents became immediately operative, others will be adopted as soon as the legislative procedure ends.

The initiative, announced by President Juncker in his speech on the "State of the Union" has a clear objective:

- Increasing the resilience of the EU against cyber attacks;
- Creating effective deterrence to protect the emerging single market of cyber security through concrete actions;
- Contributing to the construction of a solid and coordinated institutional structure at the European and national level.

These strategies are based on the following elements:

- An existing European agency, ENISA, whose mandate is made permanent. ENISA has currently new tasks and resources in order to take on a more operational role and support the Commission and Member States;
- A set of rules for an EU security certification of ICT products, systems and services, based on international standards and a voluntary basis;
- The Blueprint, i.e. a set of principles and mechanisms that involve objectives and methods of cooperation to respond in a coordinated way to incidents and cyber security crises on a large scale;
- The proposal to create a European network and a cyber security research and expertise center.

To this it is necessary to add a proposal for a directive to counter fraud and counterfeiting of non-cash payment instruments (credit and debit cards) and provide a more effective response. This proposal focuses on the detection, traceability and repression of cyber criminals involved in transnational activities. These involve terrorism, drug trafficking and human trafficking, as well as a framework for a joint EU diplomatic response to harmful cyber activities and measures to strengthen international cooperation on cyber security.

[38] http://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF
[39] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN
[40] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
[41] https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en
[42] https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-489_en

It is possible to grasp the wide scope of the intervention by looking at the contents of the communication related to the NIS directive and its transposition, which include a document containing operational indications. In this context, the Commission's concern becomes clear (it already expressed it in its 2016 Communication): because the NIS Directive is the cornerstone of the European cyber security strategy, its implementation by the Member States must take place on the basis of a harmonized approach, and it is necessary to avoid misalignments and fragments that could jeopardize the existing efforts.

Hence a series of concrete indications, which constitute an operational manual for the Member States that need to meet the deadlines of May 9 and November, 9 2018 for the transposition of the Directive and the designation of operators of essential services respectively.

First of all, it is necessary that Member States have a national cyber security strategy, which defines objectives and actions that are appropriate from a political and regulatory point of view on the basis of a holistic and coordinated approach.

The Commission document dedicated particular attention to another relevant aspect, which is the identification of the entities to which the rules of the directive apply. While Member States do not have to indicate digital service providers, the designation of operators of essential services is a complex and sensitive issue. To this extent, the directive defines the criteria to apply at the national level. The main goal is that these criteria will be applied through the Union in a coherent manner and that, in case an operator delivers services in different Member States, an agreement between them will regulate their definition, according to the Directive. It is therefore necessary to avoid a different regulatory approach depending on the country.

Furthermore, the Member States have the possibility of extending the scope of the Directive and therefore applying its rules (in terms of safety and notification requirements) to areas, which are not directly covered by the Directive, such as public administration, postal service, the food sector, the chemical and nuclear industry, the environmental sector and civil protection.

## 4.2 CyberSecurity Act

### 4.2.1 Background

Following the introduction of NIS Directive in 2016, ENISA is supposed to play a more significant role in the European cybersecurity landscape. Therefore, in addition to providing expert advice, ENISA will also a more operational and central role in achieving cybersecurity resilience. To this extent, ENISA will potentially be reformed and improved with the aim to strengthen its capabilities and capacities to support Member States in an appropriate manner.

Additionally, the proposal also foresees the creation of the first voluntary European cybersecurity certification framework for ICT products, which will contribute to promoting a culture of cybersecurity across Europe.

Through this set of initiatives, the European Commission aims to mark a big step in its strategy that initially included other provisions in the technological and cybersecurity policy area. This alert will focus on the proposed new Cybersecurity Act Regulation (the "Regulation").

### 4.2.2 The reorganization and strengthening of ENISA

In 2004, ENISA was established by Regulation (EC) No 460/2004, and in 2013, Regulation (EU) No 526/2013[43] established the new mandate of the Agency for a period of seven years, until 2020. ENISA is based in Greece; its administrative offices are located in Heraklion (Crete) and the core operations in Athens. The Agency acts as a centre of expertise dedicated to enhancing network and information security in Europe and supporting capacity building of Members States.

The agency was initially established with the aim to contribute to the overall goal of ensuring a high level of network and information security within the EU. It also assisted European institutions, entities, offices in developing and implementing policies necessary to meet the legal and regulatory requirements and enhanced their capability to prevent, detect and respond to security incidents.

ENISA supports the following categories in addressing, responding, and especially in preventing network and information security problems:

- European institutions;
- Member States;
- Business community.

It carries out the previously-mentioned activities through a series of steps across five areas identified in its strategy

- Expertise: provision of information and expertise on key network and information security issues;
- Policy: support to policy making and implementation in the Union;
- Capacity: support for capacity building across the Union (e.g. through trainings, recommendations, awareness raising activities);
- Community: foster the network and information security community (e.g. support to the Computer Emergency Response Teams (CERTs), coordination of pan-European cyber exercises);
- Enabling (e.g. engagement with the stakeholders and international relations).

The introduction of the Cybersecurity Act Regulation grants a clearer and more permanent mandate to ENISA and reinforces its role, turning it into the "EU Cybersecurity Agency". It also delineates a new scope of its mandate adding new areas:

- Those regarding the consistency in the implementation of the NIS Directive;
- The upcoming Cybersecurity Blueprint for cyber crisis cooperation;
- Functions related to security certification in Information and Communications Technology ("ICT").

From the operational point of view, the new European Agency will have collaboration with the public and the private sector. As for the public sector, it will contribute to making improvements:

- It will enhance public authorities' capabilities;
- It will facilitate cooperation among Member States in dealing with cybersecurity emergencies;
- It will reinforce the existing preventive operational capabilities.

As for the private sector, ENISA will provide best practices on cybersecurity and will play the main role in the EU policy regulatory developments regarding the ICT cybersecurity certification area.

[43] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

### 4.2.3 The establishment of a Cybersecurity Certification Framework for ICT products and services

The European Commission describes the European cybersecurity landscape as a fragmented reality ("patchy"). Thus, having identified its consequent costs and impacts, it decided to establish a new European scheme. The Cybersecurity Certification will be based on European Cybersecurity Certification Schemes and will enrich the scope of cybersecurity certifications through specific features. For example, one of these features will involve the identification of categories of products and services, the specification of cybersecurity requirements and the level of assurance they are supposed to guarantee (basic, substantial or high).

The proposal also introduces a new concept of trust and security called "security by design." This new principle assumes that ICT products and services need to directly incorporate security features in the early stages of their technical design with the aim to establish and preserve trust throughout the project process. Therefore, customers and users need to be able to determine the level of security assurance of the products and services they procure or purchase. The Cybersecurity Certification plays an important role in increasing trust and security during this procedure.

In particular, the Certification consists of the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance in products and services[44]. The most significant characteristics of the Cybersecurity Certification is that it serves as the purpose to inform and reassure purchasers and users about the security properties of the ICT products and services that they buy or use.

With the introduction of the proposal, Member States established several mutual recognition agreements and other initiatives regarding the cybersecurity certification of ICT products and services. ENISA will be involved in the preparation of these schemes and will rely on the advice of the European Cybersecurity Certification Group, consisting of national certification supervisory authorities of all Member States.

Once adopted, manufacturers and providers will be able to submit an application regarding their ICT products and services to a conformity assessment body of their choice. These entities will be third-party independent bodies established under national law and accredited by an accreditation body after assessment of compliance of certain requirements.

Through the creation of this framework, companies will be equipped with a proper procedure for cybersecurity certification. The adoption of the cybersecurity certification will potentially lead to the following benefits:

- Reducing costs;
- Facilitating cross-border operations;
- Avoiding fragmentation.

Additionally, the framework is intended to increase cybersecurity assurance for ICT products and services of pivotal sectors (such as transport, energy, health, automotive, finance) and raise consumers' trust.

Activities such as monitoring, supervisory and enforcement tasks will not be centralized at the European level. Each Member State will have to create a certification supervisory authority and manage all compliance obligations.

[44] http://community.forumpa.it/system/files/file_upload/PART-2017-404392V1.pdf

### 4.2.4 Next steps

In the current European context, individual actions by EU Member States and a fragmented approach to cybersecurity of the Union will not be sufficient to increase collective cybersecurity efforts. Consequently, it is necessary to establish a global consensus behind the new proposal, so that the Cybersecurity Act Regulation can easily follow the ordinary legislative procedure.

However, it is too early to anticipate if there will be challenges imposed by the Cybersecurity Act; and whether all Member States will easily accept what the Regulation prevents them to do and the creation of new assessment and certification bodies and authorities.

On the one hand, the interdependencies across Member States, including those related to the operation of critical infrastructures, make public intervention at the European level very challenging, but also necessary. On the other hand, EU intervention can bring a positive effect because sharing good practices across Member States can result in an enhanced cybersecurity framework within the Union.

## 4.3 GDPR and ePrivacy

The General Data Protection Regulation (GDPR), which has already entered into force, is applicable from May 25, 2018 and will replace the 1995 Data Protection Directive. The main purpose of this regulation is to reform, update and modernize European data protection legislation, to make it more robust and coherent. The GDPR will have a direct impact on each Member State, which in turn will be required to comply with uniformly applied rules within the European Union. In particular, personal data refer to all information relating to an individual and his professional and public figure[45]. Privacy and data protection are already a priority for many organizations, but the transition period that preceded the date of application of this regulation is crucial for many individuals, organizations, businesses and services operating in the European Union. . In fact, these categories will have to re-evaluate their current approach to data protection in order to identify possible gaps between the methods applied and the requirements imposed by the GDPR. It will therefore be important to make all the improvements necessary to achieve data management that meets the requirements. To this end, companies must place user privacy at the center of their internal processes and enhance corporate communication through specific training programs that guarantee adequate preparation for those who have access to personal data of users[46].

The GDPR requires companies to review their data management systems within their organizational structures and prevent the loss or incorrect sharing of the same. Firstly, the new regulation requires companies to review the concept of accountability, i.e. "accountability"[47]. In fact, those who are responsible for data processing must be able to use and implement a set of technical, organizational and legal measures relating to the protection of personal data. In this regard, the GDPR requires individual companies to envisage the figure of the Data Protection Officer (DPO) who has the task of overseeing internal organizational processes and is an

[45] http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT
[46] http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili
[47]http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati

expert in the field of data protection law and techniques. The GDPR, moreover, requires the application of the principle of privacy by design that involves those involved in the development and design of services, products, applications that make use of personal data; the data controller must therefore perform an evaluation of the management of personal data from the design phase in order to operate in line with the regulation[48]. The GDPR, therefore, provides a set of basic rules for companies that manage the data of citizens of the European Union. Companies that do not comply with the provisions of the GDPR by the deadline are subject to penalties of up to 20 million euros, or up to 4% of the total turnover recorded in the previous year. However, the new regulation will provide companies with an opportunity to redefine company policies and staff training.

[48] http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento

# 5 STRENGTHS AND WEAKNESSES OF THE EUROPEAN CYBERSECURITY AND PRIVACY MARKET.

Over the last number of years, cybersecurity and privacy concerns have risen to become among the most important dimensions of the Digital Single Market (DSM). For instance, survey results suggest that at least 80% of EU companies have experienced at least one cybersecurity incident over the last year. For example, the ransomware attacks in February 2016 demonstrated that attackers can cripple the operation of major hospitals by depriving them of access to their data. Such attacks have proven that the threat to the Digital Single Market is so important that Andrus Ansip, Vice-President for the Digital Single Market, said at the launch of the contractual Public-Private Partnership on cybersecurity (cPPP): "Without trust and security, there can be no Digital Single Market. Today, we are proposing concrete measures to strengthen Europe's resilience against such attacks and secure the capacity needed for building and expanding our digital economy."

Having realized the importance of cybersecurity and privacy, as described above in section 3, the European Commission, the Member States and the major European stakeholders have implemented the European Cyber Security Strategy, as described in the 7/02/2013 communication on "Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace" published jointly by the European External Action Service (EEAS) and the European Commission.

To increase the impact of this European Strategy, the European Commission and industry launched the NIS Platform [3] and signed a contractual Private Public Partnership on cyber-security (cPPP): a revolutionary approach to "foster cooperation at early stages of the research and innovation process and to build cybersecurity solutions". Cybersecurity market players, represented by the European Cyber Security Organisation (ECSO) [4], a legal association, are coordinating the efforts and to date, there are currently over 220 members in ECSO.

From its outset in 2013, the NIS Platform carried out activities that have significantly contributed to the examination of the weaknesses and steps forwards towards the strengthening of the EU Cybersecurity and privacy market and this section will highlight these important activities. Operationally, this important topic was addressed primarily in WG3, Secure ICT research and innovation, in order to align the activities with those of the research and innovation agenda being developed by WG3.

To examine the marketplace of cybersecurity and privacy markets in the EU at that time, a dedicated team or research and innovation and industry experts came together to examine the availability of new and improved cybersecurity and privacy products and services that would benefit the European economy by reducing the cost to European organisations and individuals arising from security breaches and related incidents, addressing the risks (real and perceived) associated with new technologies and practices, and to introduce potentially valuable innovations because of concerns over security, and enable increased revenue generated for European companies from new products and services, and the employment generated from growth in established businesses and creation of new companies.

This work resulted in a report entitled Business Cases and Innovation Paths, published in May, 2015 [10]. This report complements the other WG3 deliverables by looking at the Strategic Research Agenda from a market-oriented perspective in order to gain insight into the key aspects of demand for NIS innovation so as to ensure cybersecurity and privacy research is focused on challenges achievement of

which would have the greatest impact and research & innovation (R&I) models and processes that are most efficient and effective in bringing usable, affordable and timely solutions to market.

The key recommendations of this report were the following:

1. **For the NIS Strategic Research Agenda:** The report recommends the commissioning of a study that:
   - Traces the research origins of concepts underpinning successful NIS products and services;
   - Tracks whether and how past NIS research results have been exploited, especially those perceived as significant at the time the research was performed;
   - Devises success indicators for applicable NIS research results and sets up a system for monitoring the future exploitation of results.

To establish a stable and consistent research agenda, they suggested that need to get ahead of the game and focus on principles required to underpin the vision of a secure society. The most fundamental requirement is the creation of an engineering science of secure/trustworthy software and human-technical systems, including reference architectures and design patterns, so that security can be built into systems from the beginning.

The research agenda must be owned by a coalition representing all stakeholders, including end-user organisations and NIS vendors and service providers as well as public authorities and citizen rights organisations. It must be managed actively, and revised whenever necessary. Furthermore, there must be means of tracking progress towards its goals.

The NIS research and innovation portfolio should include projects that are aimed at defining and maintaining reference architectures, frameworks and interface standards, and encourage and co-ordinate the creation of ecosystems of compatible and interoperable products and services across a cluster of research and innovation projects. It is important that these architectures, frameworks and standards are defined in such a way as to promote competitive innovation, and are designed for evolution.

The NIS research and innovation portfolio should include projects that are aimed at providing innovation-friendly NIS platforms, i.e. technological environments in which a range of novel NIS products and services can be brought to market or deployed in combination to protection applications and processes.

They reiterated the importance of the requirement - driven road-mapping approach; however, emphasised that the required depth needed was beyond the scope of the current NIS Platform's WG3 activities and the roadmap would have to be revisited regularly and maintained actively.

The carrying out of these recommendations should encourage the establishment of a competitive European NIS market place, by lowering the barriers to entry to new players. There will be opportunities for providers of best of breed platforms and individual services as well for providers of complete solutions. In the report (in chapter 4, entitled *An approach to prioritising research topics*), the authors provide a requirement-driven methodology is designed to contribute to an NIS research roadmap that will prioritise the research topics with the highest potential for market impact.

2. **Stimulating and promoting innovation:** The next set of recommendations relate to the stimulating and promoting of innovation in Europe.

One of the challenges in Europe is to transform research results into tangible business opportunities. Evidence suggests that European research results do not

reach the market in the majority of cases [11, 12] with technology transfer being one of the main challenges.

However, it is not all bad news and the report recommends that experiences from successful EU innovation centres should be leveraged. One of the most representative European examples of this type of centre is the KIC "EIT ICT Labs" [13] with its network of nodes spread across a growing number of EU Member States.

It references several other EU based organisation that aim to bring innovation to the market already exist. These examples adopt a minimal set of high level general requirements, identified and summarized as:

- Multi-stakeholder approach: This aspect is the fostering of fruitful collaborations between large industries and academia, involving SMEs;
- R&D organizations and policy makers. This is also the approach recommended by the EU Cybersecurity Strategy [6].
- Targeted focus: Every innovation centre should concentrate their effort and energy in specified areas of interest, knowing that societal needs are an essential element to improve the quality of life.
- Metrics: you cannot manage what you do not measure. With this in mind it is clear that innovation companies need to implement a KPIs policy which measures the number of innovations incubated, the number of start-ups launched and the number of knowledge transfers.

The document also highlights a number of successful organisations and initiatives across Europe, who have successfully utilised these requirements. These include the following:

**Italy** – Technological districts, Technology Platforms, such as **SERIT (Security Research in Italy**[49]), which is a joint initiative launched by CNR and Finmeccanica, brings together Italian industries (both large industries and SMEs);

**Spain** - **CDTI (Centre for the Development of Industrial Technology)**[50]**:** it is a national Public Business Entity, answering to the Ministry of Economy and Competitiveness, which fosters the technological development and innovation of Spanish companies. Also **OTRI (Offices for the Transference of Research Results**[51]): Offices for Transference of Research Results were created at the end of 1988 as structures for promoting and facilitating cooperation in the area of R&D activities between researchers and businesses, both in Spain and across Europe. **ERAC Peer Review of the Spanish Research and Innovation System**[52]**, a** report69 commissioned by the European Commission delivered by an Independent Expert Group for the Spanish Ministry of Economy and Competitiveness, the Spanish Secretary of State for Research, Development and Innovation and for the European Research Area and Innovation Committee.
United Kingdom - **Technology Strategy Board**[53]: it is a non-departmental public body sponsored by the UK Government Department for Business, Innovation and Skills. Its aim is "to accelerate economic growth by stimulating and supporting business-led innovation". **Catapult centres / Technology & Innovation Centres:** Catapult centres[54] are initiatives led by TSB that aim to catalyse and

[49] http://www.piattaformaserit.it/?lang=en
[50] http://www.cdti.es/index.asp?idioma=1
[51] http://www.universidad.es/en/spain/research-spain/research/research-resultstransfer-offices-otris
[52] http://www.mineco.gob.es/stfls/MICINN/Prensa/FICHEROS/2014/140801_final_report_public_version.pdf
[53] https://www.gov.uk/government/organisations/technology-strategy-board
[54] https://www.catapult.org.uk

support research and development, foster links between business and academia and promote economic growth. The UK has 7 catapult centres, each centred around a specific location and each focusing on a specific field of innovation. These currently in 2018 include: Cell and Gene Therapy Catapult, Compound Semiconductor Applications Catapult, Digital, Energy Systems, Future Cities, High-value manufacturing, Medicines Discovery, Off-shore renewable energy, Satellite applications and Transport systems. **Centre for Process Innovation (CPI)**: it is a UK-based technology innovation centre [CPI] and part of the High Value Manufacturing Catapult. They use applied knowledge in science and engineering combined with state of the art facilities to enable their clients to develop, prove, prototype and scale up the next generation of products and processes. **BAE Systems I3 Programme[55]:** Investment In Innovation (I3) is a multi-million pound investment programme run by BAE Systems, which supports SMEs and academia in accelerating the development of research and innovation. The focus of the programme is on technologies of relevance to the defence and security sector, with current areas of interest including cybersecurity, surveillance and biometrics. Available support includes funding, knowledge and skills sharing, provision of facilities and examples of governance and best practice. **Malvern Cybersecurity Cluste[56]:** Malvern Cluster is a group of 50 SMEs located in Malvern, Worcestershire, who collaborate on a range of initiatives to build their businesses and help local organisations to improve their cybersecurity. The Cluster provides a variety of services to its members and the local community including: Regular meetings for members, including core SME members and broader engagement with larger organisations; Skills and training initiatives including visiting local secondary schools and supporting development of apprentice programmes; and events for the general public to increase awareness of cybersecurity risks and mitigations.
**The UK Innovation Forum (UKIF[57]):** The UK Innovation Forum was established with the support of the Science and Technology Facilities Council, a non-departmental public body within the UK, and aims to support collaboration between businesses, investors, research and academia.

3. **Total Network and Information Security (NIS) and Research and Innovation (R&I):** The final sets of recommendations relate to the necessarily combined approaches of NIS and R&I actors.

To encourage efficient technology transfer, and prepare the way for innovation, research projects should:

- Include application case studies, demonstrators and pilots to guide projects, validate results, and establish an effective two-way dialogue with 'innovators' and demand-side stakeholders;
- Consider how the threat environment will respond to widespread knowledge of the new NIS technologies;
- Consider compatibility of the NIS technologies being developed with current tools and practices. Will market disruption be required for the technology to be exploited to its full potential?
- Include business-oriented activities such as exploitation road-mapping and preparation of outline business models and investment cases.

NIS researchers should be provided with opportunities to train and gain practical experience in innovation and entrepreneurship. They should be encouraged to take their research results through to innovation by forming start-up companies and/or transferring to/within industry. Both academic and industrial carrier paths and

[55] http://www.baesystems.com
[56] http://www.malvern-cybersecurity.com/
[57] http://uk-if.org/

qualifications should recognise the value of mixing research, innovation and operational experience.

A searchable repository of historic results, combined with an innovation broker services could help release the latent value of NIS research. Royalties or licensing fees could be paid to the owners of the results in return for making their results available to innovators.

Finally, it was recommended that the NIS research and innovation projects should be structured and organised in such a way that the direction of research may be adapted during the life of projects as the market evolves.

An agile approach to combined R&I and operations for NIS would be of great value. Such a 'Total NIS R&I' methodology could, for example, be based on the DevOps approach to integrated software development and operation, but specialised to NIS and extended 'upstream' to embrace aspects of R&I. It is interesting to note that the WP2018 programme in relation to the Next Generation Internet initiative [14] (NGI) is taking this approach whereas the funding model is based on cascading funded projects, that are paid for and carried out over three research cycles, taking into account the ongoing developments in the research and innovation, coupled with commercial activities within industry, in smaller yet more agile projects in duration and scope, especially with participants from smaller companies, including start-ups and entrepreneurs.

## 5.1 Projects and Initiatives addressing these recommendations

A number of relevant activities have been carried out by a variety of projects and initiatives towards addressing the strengthening of bringing cybersecurity and privacy research and innovation to the markets. The table in is section will highlight those activities.

Please note that this is not an exhaustive table of all EU funded projects and initiatives related to cybersecurity and privacy. It is only highlighting the projects and initiatives that are dealing with addressing the topics of moving easier from research to innovation and strengthening the market value of cybersecurity and privacy research and innovation. A full catalogue of EU funded projects' research and innovation service offers in cybersecurity and privacy is available from the cyberwatching.eu project [15], which is involved in the clustering and coordination of projects in this research and innovation area.

**Table 1 – Projects and initiatives addressing cybersecurity and privacy (CSP) innovation**

| *Project - Initiative / web link* | **Short description / key results** | **Impact on / benefit for / innovation in CSP** |
|---|---|---|
| **Projects directly related to CSP and innovation / markets improvements** | | |
| **SecCord (CSA) and CSP-Forum**<br>2012 - 2015<br>http://www.cspforum.eu/ | • Organisation of annual event CSP forum (Cybersecurity & Privacy Innovation Forum)<br>• Maintenance of CSP-Forum web portal with content syndication and latest news from EU projects<br>• Analysis of research project results and promotion of success stories<br>• Mapping of research to demand side needs and supply side trends<br>• Clustering of EU projects. | • Networks included key industry actors/ networks<br>• Included innovation as a core element of the annual CSP Forum events with strong CSP industry participations in a dedicated day on innovation topics. |
| **CYSPA (CSA)**<br>2012 - 2015<br>http://www.cyspa.eu/ | • FP7 support action focusing on cyber-security risks and users in critical infrastructures;<br>• Creation of *sectoral* based sub-communities (transport, finance) to elaborate risk profiles<br>• Initial model for the creation of the cPPP. | • Cooperation mechanisms focused on specific industrial sectors;<br>• Creation of a visual, navigable and dynamic 'who's who' in cyber-security, including industry key actors. |
| **BIC, INCO-Trust (CSAs) 2008 -2013**<br>http://www.bic-trust.eu/ | • Organization of international events (USA, Korea etc.) to promote EU research projects visibility and to identify common topics at research, but also key innovation levels. | • network of contacts in working groups included key industry players in CSP;<br>• Know-how of research and innovation programmes inside and outside EU. |
| **PRIPARE (CSA)**<br>2013 - 2015<br>http://priparepr oject.eu/ | • Coordination and support for research and innovation related to privacy by design. | • Link with privacy industry communities;<br>• Adoption of security and privacy by design principles in CSP technologies. |
| **IPACSO (CSA)**<br>2013 - 2015<br>https://ipacso.eu/ | • Supporting Privacy and Cyber Security innovations in Europe with State of the Art innovation methodologies and best practices in their innovation process;<br>• Developed a structured knowledge and decision-support innovation framework for identifying, assessing and exploiting market opportunities in the privacy and cyber security technology space. | • By utilising the IPACSO framework, innovators are able to find their road to market faster, more effective and more efficient;<br>• Innovation contests were carried out as part of the CSP Innovation FORUMs. |

| *Project - Initiative / web link* | **Short description / key results** | **Impact on / benefit for / innovation in CSP** |
|---|---|---|
| **CAPITAL (CSA)** 2013 - 2015<br>http://www.capital-agenda.eu/ | • Delivered an integrated research and innovation agenda (RIA) for cybersecurity and privacy; this was used for the preparation of the cPPP SRIA. | • Methodology and results included how to further the innovation cycle from research;<br>• Examined IT trends with implications for security and privacy (Future Clouds, Internet of Things, Mobile Computing, Big Data and Critical Industrial Systems). |
| **ACDC** 2013 - 2015<br>https://www.acdc-project.eu/ | • CIP Pilot action focusing on fighting botnets;<br>• Creation of a community of solution providers and ISPs effectively sharing sensitive data;<br>• Use of collaborative mechanisms to create new joint solutions from different pre-existing market or research solutions. | • Cooperation mechanisms to elaborate joint solutions;<br>• Operational experience of sharing of sensitive data across borders, including legal analysis;<br>• Creation of sub-community of expertise esp. with industry;<br>• Collaboration with Europol EC3. |
| **CIRRUS (CSA)** 2012 - 2014<br>https://cordis.europa.eu/project/rcn/105735_en.html | • International collaboration, standardization and certification for cloud security. | • Some common issues and certification approaches have been proposed for cloud security, in order to increase uptake of cloud solutions. |
| **SysSec (NoE)** 2010 - 2014<br>http://www.syssec-project.eu/ | • FP7 Network of Excellence in cybersecurity;<br>• Creation of a Think-Tank in the area of Systems Security to engage in discovering the threats and vulnerabilities of the Current and Future Internet. | • A Community of researchers (both in Academia and Industry) in the area of Systems Security;<br>• Collaboration experience for research and innovation road mapping. |
| **NESSOS (NoE)** 2010 - 2014<br>http://www.nessos-project.eu/index.php | • Research agenda for secure software engineering;<br>• NESSoS had an industry advisory Board where several CSP-PACT members served;<br>• NESSoS created an active research and innovation community of near 300 people in the field and several successful events. | • Link software engineering community to cybersecurity topics and challenges;<br>• Strong activity of the industry advisory board. |
| **NeCS - European Training Network on Cyber Security** 2015 - 2019<br>http://www.necs-project.eu/ | • EU H2020 MSCA project devoted to the consolidation of a research and training community. The project is coordinated by Fabio Martinelli (CNR) of AEGIS. | • NeCS research and innovation networks to identify research strands and activities in the short/mid-term. |
| **CIRAS** 2014 - 2016<br>http://www.cess-net.eu/de/projekte/ciras.html | • Funded by European Union DG HOME;<br>• Critical infrastructure risk and cost/benefit assessments. | • Adoption of economic models and link to risk management and critical infrastructure community. |
| **CAMINO (CSA)** 2014 - 2016<br>http://www.fp7-camino.eu/ | • Cybercrime and cyber terrorism roadmap;<br>• CSP Road-mapping experience also with inclusion of SMEs. | • Usage of experience, SMEs contacts and road-mapping experiences.<br>• Consortium came together from the Integrated Mission Group for Security (IMG-S), a wide European Network |

| *Project - Initiative / web link* | **Short description / key results** | **Impact on / benefit for / innovation in CSP** |
|---|---|---|
| | | bringing together technology experts from Industry, SMEs, Research and Technology Organisations (RTOs) and Academia.<br>• Wide understanding of the cyber technologies and their application in several fields. |
| **CyberWISER (IA)**<br>2018 - 2021<br>https://www.cyberwiser.eu/ | • Full name: Cybersecurity risk assessment for SMEs.<br>• Answered the call DS-07-2017 - Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors | • Links to SME cybersecurity in various domains. |
| **SMESEC (IA)**<br>2017 - 2020<br>https://smesec.eu/ | • Full name: Cybersecurity for SMEs;<br>• Answered the call DS-02-2016; Cyber Security for SMEs, local public administration and Individuals. | • Developing a cost-effective framework composed of specific cyber-security tool-kit to support SMEs in managing network information security risks and threats, as well as in identifying opportunities for implementing secure innovative technology in the digital market. |
| **FORTIKA (IA)**<br>2017 - 2020<br>http://www.fortika-project.eu/ | • Full name: FORTIKA - Cyber Security Accelerator for trusted SMEs IT Ecosystems<br>• Answered the call DS-02-2016; Cyber Security for SMEs, local public administration and Individuals. | • Aims to (1) minimise the exposure of small and medium sized businesses to cyber security risks and threats, and (2) help them successfully respond to cyber security incidents, while relieving them from all unnecessary and costly efforts of identifying, acquiring and using the appropriate cyber security solutions. |
| **AEGIS (CSA)**<br>2017 - 2019<br>http://aegis-project.org/ | • Full name: Accelerating EU-US DialoGue for Research and Innovation in CyberSecurity and Privacy<br>• Answered the call DS-05-2016; EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation. | • Organises Open Cyber Camps and Round Tables to facilitate the creation of ideas for effective development of security solutions, creating synergies and stakeholders' engagement from EU and US;<br>• Promotes policy debate and empower stakeholders throughout Europe and the US to work together to effectively address cybersecurity challenges, adopting common approaches and bridging fragmentation between multiple communities of researchers, innovators, technologists, policy makers and influential government stakeholders;<br>• Provides guidelines for innovation partnership in cybersecurity and privacy EU-US collaboration. |
| **cyberwatching.eu**<br>**2017 - 2021**<br>http://www.cyberwatching.eu | • Full name: The European watch on cybersecurity privacy;<br>• Answered the call DS-05-2016; EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation. | • Addressing needs from the perspectives of R&I teams and projects (clustering), promotion of mature results (based on market and technology readiness to find potential customers for their new products and services; SMEs and large companies as potential users of services, including the dedicated cyberwatching.eu end-user club; Financial services and insurance |

| *Project - Initiative / web link* | **Short description / key results** | **Impact on / benefit for / innovation in CSP** |
|---|---|---|
| | | industry: foster the implementation of best practices through the cyberwatching.eu cyber insurance pilot service as the cyber insurance market evolves in response to new risks and requirements for compliance filter through the market.<br>• Offers catalogue of services from cybersecurity and privacy projects available at https://www.cyberwatching.eu/services/catalogue-of-services/ |
| **Platforms / Initiatives / Agencies directly related to CSP** | | |
| **ENISA**<br>2004 – present<br>https://www.enisa.europa.eu/ | • Organization of a set of events to increase awareness on cyber security as part of their cybersecurity month;<br>• Involvement in development of National Cyber Security Strategies. | • Cooperation in establishing expert groups, working groups, involvement with NIS Platform, ECSO, and EU Commission activities and event organization. |
| **EOS** Cyber security working group<br>2007–present<br>http://www.eos-eu.com/ | • Running as an industry led activity within EOS, the cyber-security working group produced joint position papers on the need for a cyber-security strategy with agreement across major cyber-security market players;<br>• Annual publications from 2009 to 2012, followed by focused contributions including to ECSO and cPPP. | • Effective collaboration experience across market players, learning how to collaborate beyond potential conflicts of interests with respect to market positions.<br>• Large experience of EU policies and link with EU Institutions. |
| **TDL (Trust in Digital Life)**<br>2009 - present<br>https://trustindigitallife.eu/ | • Industry led, guided by SRA with active community (also WGs);<br>• Stimulate development and user acceptance of innovative but practical trustworthy ICT;<br>• Cross-sector collaboration and aggregation of the results into industry recommendations for policy makers (e.g. TDL recommendations to NIS platform);<br>• Annual conference (Trust in Digital World). | • Complementary focus on trustworthy ICT and innovation;<br>• Experience in new tools and techniques that deliver (e.g. sprint R&I project incubator concepts, …);<br>• Experience in gathering of different communities and delivering focused recommendations. |
| **DigEnlight (Digital Enlightenment Forum)**<br>2011 - present<br>https://digitalenlightenmentforum.com | • Member based non-profit association that aims to stimulate multi-stakeholder discussions and collaborations towards finding and proposing game-changing strategies concerning digitisation in society. | • Focuses on innovation and sustainable evolution of a society respecting human values.<br>• The Forum brings representatives of science, technology, policy, law and society together for outcome-focused debate, we propose principles, policy recommendations and activities at technical, legal, societal and market levels. |
| **NIS Platform**<br>2013 - 2016<br>https://resilience.enisa.europa.eu/nis-platform | • EU platform on Network and Information Security (NIS) set up to support the EU Cyber Security Directive[58] ;<br>• Multi-stakeholder Platform with strong emphasis on public/private | • Experience in the gathering from the large sized cross cutting CSP community and aggregation and compilation of writing a large scale Strategic Research and Innovation Agenda (SRIA). |

[58] http://ec.europa.eu/digital-agenda/en/cybersecurity

| *Project - Initiative / web link* | **Short description / key results** | **Impact on / benefit for / innovation in CSP** |
|---|---|---|
| | cooperation;<br>• WG3 with a focus on secure ICT research and innovation provided a unique opportunity to better understand NIS Challenges, Threats and Risks and for influencing future Research & Innovation (R&I) in NIS issues. | • Experience in gathering of different communities and disciplines across results oriented Working Groups, including strong emphasis on business and innovation activities. |
| **DPSP Cluster (Data Protection, Security and Privacy in the Cloud)**<br>2015 - present<br>https://eucloudclusters.wordpress.com/2015/05/11/eu-projects-clusters/ | • Cluster environment where projects funded by the European Community (in particular, the recipients of ICT7 and H2020 grants) can interact and find synergies among them. | • Each cluster has set specific goals but all of them focus on collaboration among members on technical aspects as well as on the identification of trends in the relevant markets and on engaging in innovative ways to address such trends;<br>• Working to maximize the impact of EU-funded research and innovation project results in the areas of Data Protection, Security and Privacy in the Cloud. |
| **ECSO** (European Cyber Security Organization)<br>2016 - present -<br>https://www.ecs-org.eu/ | • ECSO the industry-led support organisation of the contractual Public Private Partnership in cybersecurity (cPPP); has 6 WGs:<br>○ WG1: Standardisation, certification, labelling and supply chain management;<br>○ WG2: Market deployment, investments and international collaboration;<br>○ WG3: Sectoral demand;<br>○ WG4: Support to SMEs, coordination with countries (in particular East and Central EU) and regions;<br>○ WG5: Education, awareness, training, cyber ranges;<br>○ WG6: Strategic Research and Innovation Agenda (SRIA). | • As ECSO is industry and R&I driven, most of the WGs are contributing to strengthening the cybersecurity market activities in the EU;<br>• WG2 is addressing many of the recommendations made in the previous section and has the following strategic working groups (SWGs):<br>○ SWG 2.1 Market development market, products and stakeholders update;<br>○ SWG 2.2 Investments, innovative business models;<br>○ SWG 2.3 International cooperation, global competitiveness and support to export;<br>○ SWG 2.4 Dissemination & awareness, events etc. |
| **Projects / Platforms / Initiatives / Agencies indirectly related to CSP** | | |
| **ERCIM** (EU Research Consortium for Informatics and Mathematics)<br>1989 - present<br>https://www.ercim.eu/ | • | • ERCIM set up a successful WG on security and trust (WG on STM) embodying several researchers and industry experts in Europe;<br>• They also organise events and newsletters that frequently address cybersecurity security and privacy and trust challenges;<br>• Promotes cooperation in research, technology transfer, innovation and training. |
| **EARTO** (EU Associations of Research and Technology Associations)<br>2012 - present | • Network of major RTOs in Europe;<br>• RTOs perform research and work with industry and agencies from Member States. | • Gathers a better knowledge on RTOs strategies and policies with regard to cybersecurity;<br>• Direct connection with RTOs for contacts, roadmap exchange and workshop participation. |

| *Project - Initiative / web link* | **Short description / key results** | **Impact on / benefit for / innovation in CSP** |
|---|---|---|
| http://www.eartO.eu/ | | |
| **ECP EU Cloud Partnership** 2012 – 2014 (with some follow up DSM activities after their report)<br>https://ec.europa.eu/digital-single-market/en/european-cloud-partnership | •The European Cloud Partnership (ECP) was established under the 2012 European Cloud Strategy. | • ECP emphasized the need for Europe to develop its own cloud infrastructure, rather than depend on that of the United States[59].<br>• Completed a report titled "Trusted Cloud Europe" in February 2014 defining its policy, and outlining a process for effective public and private sector participation in cloud computing development in Europe.<br>• The report recommended that the commission identify technical, legal and operational best practices, and promote these through certifications and guidelines, and facilitate recognition across national boundaries[60].<br>• The report also recommended that the commission identify cloud computing stakeholders and help them work together through consultations and workshops[61]. |
| **5G-PPP** 2013 - present<br>https://5g-ppp.eu/ | • Joint initiative between the European Commission (EC) and the European ICT industry and aims to deliver 5G solutions, architectures, technologies and standards. | • 5G-PPP Security WG is looking at R&I challenges and solutions;<br>• 5G-PPP security projects (starting first with 5G-ENSURE and COGNET 5G-PPP project on network management including security. |
| **AIOTI (Alliance for Internet of Things Innovation)** 2014 – present<br>https://aioti.eu/ | • Members of the Alliance include key IoT industrial players – large companies, successful SMEs and dynamic start-ups – as well as well-known European research centres, universities, associations and public bodies. | • Mapping and evaluating global IoT innovation. We make actionable business insight and market data available to all our members;<br>• lead on convergence and interoperability of IoT standards, including those related to cybersecurity and privacy. |
| **BDVA-PPP (Big Data Value Public-Private Partnership)** 2014 - present<br>http://www.bdva.eu/PPP | • Self-financed and not-for-private counterpart to the EU Commission to implement the BDV PPP programme (Big Data Value PPP). | • Greater than 150 members all over Europe with a well-balanced composition of large and small and medium-sized industries as well as research organizations;<br>• Coordination in cybersecurity activities and R&I for Big Data Value;<br>• Number of projects related to Bid Data Value Security projects. |
| **Cloud28+** 2015 - present | • Cloud28+ is the world's largest independent community, promoting | • Focused on delivering a seamless on and off premises experience to |

[59] https://www.zdnet.com/article/after-prism-europe-has-to-move-to-its-own-clouds-says-estonias-president/
[60] https://www.bankingtech.com/2014/07/six-reasons-why-cloud-computing-will-transform-the-way-banks-serve-clients-and-the-five-hurdles-to-overcome/
[61] https://books.google.se/books?id=2fWYBAAAQBAJ&pg=PA22&redir_esc=y#v=onepage&q&f=false

| *Project - Initiative / web link* | **Short description / key results** | **Impact on / benefit for / innovation in CSP** |
|---|---|---|
| https://www.cloud28plus.com/ | cloud services and knowledge sharing. It serves end customers, cloud service providers, solution providers, ISVs, systems integrators, distributors, and government entities dedicated to accelerating enterprise Cloud adoption. | customers in each region around the globe; approach is by pooling resources to share and promote a common platform to accelerate the acquisition of Cloud knowledge and tailored solutions, matching each customer's unique digital transformation;<br>• The Cloud28+ community and hybrid IT business platform foster collaboration to increase knowledge sharing, create new business alliances, and accelerate business outcomes. |
| **DISCOVERY** 2016 - 2017<br>http://discoveryproject.eu/ | • Full name: Dialogues on ICT to Support COoperation Ventures and Europe-North AmeRica (Canada and USA) sYnergies;<br>• Answered the call ICT-38-2015 - International partnership building and support to dialogues with high income countries. | • Stimulated industry engagement and innovation partnerships between the industry, research and academia, using a unique set of participatory and co-creative methods and people-centric facilitation techniques to stimulate interaction among the groups of participants in project events, such as the ICT Discovery Lab and well-targeted capacity-building workshops;<br>• Working group on cybersecurity as part of their Transatlantic ICT Forum (TIF). |

# 6 CONCLUSIONS AND RECOMMENDATIONS

One of the objectives of the AEGIS project is to identify and analyse the current technological, market, policy and regulatory landscape for cybersecurity and privacy in Europe and the United States. The mapping of the cyber security landscapes is based on a common approach, which allows us to examine the similarities and differences between the cybersecurity landscape in each jurisdiction in relation to their technology, strategy, policy and innovation driven approaches in the fields of cybersecurity and privacy.

This report, "Cybersecurity and Privacy Landscape in Europe," presents the results of the analysis in 5 sections:

1. Introduction. Overall introduction to the document.
2. Cybersecurity and Privacy Technologies. This section used the taxonomy as defined by Joint Research Centre, ECSO, ENISA and other key stakeholders, and describes the current state of the art in the basic technologies and/or emerging threats related to cybersecurity and privacy from the European perspective. In particular, we have addressed the implication of most recent and disruptive changes induced by the digital transformation of the society, as well as keeping into account the evolution of the threats that it is facing. These were broken down over the following areas:
   a. Cybersecurity and Privacy technical domains;
   b. ICT technology domains;
   c. Application domains.
3. EU Cybersecurity Strategy, describing the current overarching strategies being undertaken in the EU in relation to Cybersecurity and Privacy.
4. Policy and Legislation activities in the European perspective.
5. Strengths and Weaknesses of the European Cybersecurity and Privacy Market.

Generally speaking, while the cyber security and data privacy issues have been acknowledged as top priorities by the EU, the Member States, citizens and enterprises, resulting in a relevant effort in terms of initiatives on various aspects, the pace of the technological and market evolutions (and, hence, of related cyber menaces) is such that the containment actions are responsive rather than preventative. Most of such changes can be very disruptive, and the impacted scope is not completely understood.

Indeed, while some threat actors still remain active and dangerous since many years and they are far from being eradicated (e.g., phishing, ransomware, etc.), new menaces appear in the landscape even from unexpected directions (e.g., blockchain).

Moreover, the European context suffers also for a high degree of fragmentation both at policy and regulatory levels, rather than economical, because most of its productive lifeblood environment is represented by SMEs that are generally not very mature nor ready in contrasting the cyber menaces.

Therefore, in order to deal with such fragmentation and speed of change, most of actions are focused on collaboration and knowledge sharing, aiming at generating the adequate milieu and supporting links from both organizational and cultural standpoints.

Even more, in many relevant segments of the ICT market (with also notable exceptions), the technological and industrial leadership is not recognized to EU-based enterprises. In other words, there are neither tech giants that could drive in some way the trend of the ICT market, and neither innovation hubs that are able to deliver to the mass market such killer apps and services that nowadays are shaping the Digital Global Society (e.g., the social network paradigm and its implication on almost every interpersonal relationship). Even worse, there many examples (e.g. Skype) of successful European start-ups that have been acquired by non-EU enterprises.

In other words, while the actual capability of monitoring and controlling on many of such external actors by the regulatory bodies of EU and Member States is quite limited, the capability of the EU and each Member States (even acting individually) to improve the overall resilience against cyber menaces could be seriously threatened by the fact that they are not very involved in the decision making process; instead we undergo a hegemony of others. A stronger coordination among European actors and even a common industry development policy (with related investments) in such a context is highly advisable.

The next steps for this deliverable will be to share it with the members of the Cybersecurity Reflection Group EU-US established in WP1 to gather their feedback to see if this portrays an accurate picture of the cybersecurity and privacy landscape in Europe.

In addition, the work will be analysed further in WP3, in terms of priority setting for defining opportunities for EU-US cooperation in Cybersecurity and Privacy R&I.

# REFERENCES

[1] SANS Institute, Threat Landscape Survey: Users on the Front Line (2017).

[2] The Blockchain-GDPR Paradox, available at https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047.

[3] Ponemon Institute, Study on Global Megatrends in Cybersecurity, (February, 2018).

[4] ENISA, Hardware Threat Landscape and Good Practice Guide, Version 1.0, (2017).

[5] ENISA, Ad-hoc & sensor networking for M2M Communications - Threat Landscape and Good Practice Guide, (Jan. 2017).

[6] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. (2013). Retrieved from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf & https://ec.europa.eu/digital-single-market/en/cyber-security

[7] NIS Directive. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive & https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts

[8] NIS Platform - https://resilience.enisa.europa.eu/nis-platform

[9] European Cyber Security Organisation (ECSO) - https://ecs-org.eu/

[10] Kearney, P., Dooly, Z. et al. Business Cases and Innovation Paths, NIS PLATFORM, WORKING GROUP 3 (WG3) FINAL, Version 1.1, (May, 2015)

[11] Cleary, F., et al., SecCord Deliverable pg 91 Success Stories http://www.cspforum.eu/Yearbook2013-V1.42.pdf.

[12] Figel, Ján, European Commissioner for Education, Training, Culture, and Multilingualism, http://europa.eu/rapid/press-release_IP-06-201_en.htm.

[13] EIT ICT Labs https://www.eitdigital.eu/

[14] Next Generation Internet Initiative: http://www.ngi.eu/

[15] cyberwatching.eu_R&I-Service-Offers_April2018_web.pdf, available from cyberwatching.eu project at https://www.cyberwatching.eu/services/catalogue-of-services/

aegis accelerating EU–US Dialogue in Cybersecurity and Privacy

**Quotation:**

When quoting information from this report, please use the following phrase: "Cybersecurity and Privacy Landscape in Europe. AEGIS project."

## Consortium:

inmark europa

Consiglio Nazionale delle Ricerche

Waterford Institute of Technology

Hewlett Packard Enterprise

european american chamber of commerce new jersey

THE PROVIDENCE GROUP

RUTGERS

aegis-project.org linkedin.com/company/aegis-project @aegis_cyber