European Cybersecurity Industry Leaders

EU Cybersecurity Package and EU Certification Framework

October 2018

AIRBUS Atos BBVA BMW GROUP

CYBERNETICA ERICSSON F-Secure infineon T

Table of Contents

Introduction – Background and Context

In May 2017 the EU Commission published the comprehensive review of the European Digital Single Market Strategy, with a special focus on the EU's capabilities and instruments for protecting the cyberspace of the European Digital Economy. A permanent, revised mandate for the European Agency for Networks and Information Security (ENISA) and the setting up of an EU certification framework provide the center pieces of the EU Cybersecurity Package, proposed in September 2017. Since the start of 2018, the debate on the respective draft regulation has started amongst the EU institutions as well as with stakeholders from industry. Most recently Angelika Niebler, MEP, from the European Parliamentary Committee on Industry, Research and Energy, has produced a draft report on the proposal, which we find to be on the whole in line with the views expressed in this document and is a substantial improvement on the original proposal, underlining as it does, the need for a more harmonized strategy towards an EU Single Market for cybesecurity.

With DigitalEurope the EC use a new format for strengthening the digital transformation in the EEA. DigitalEurope has a total budget of 9.2 billion € and is based on three of five pillars of interest in the context of cybersecurity: High Performance Computing (HPC), which could also capture Post-Quantum Crypto (PQC), Artificial Intelligence (AI) and Cybersecurity (CS). All three pillars have a possible bridge to each other. HPC can be used for new attack scenarios, as well as AI for example for intelligent side channel attacks.

As "Independent European trusted advisors", the companies of the ECIL Advisory Group have in recent years actively supported the Commission and Member States in the shaping of the European Cybersecurity approach. In the run-up to the Cybersecurity Package, ECIL has proposed substantial input to the Commission. The ECIL members, leading European companies from different sectors, equally dealing with cybersecurity challenges, have analysed the Commission's proposal and are sharing their assessment and recommendations, presented in this non-public document, with the EU's representatives.

The guiding principles and objectives of ECIL's work are the protection of the cyberspace of the digital economy, the strengthening of the competitiveness of

European companies through fostering the further harmonization of the EU's cyber policy and ultimately successfully completing the EU's Digital Single Market. Whilst it is important to note that ECIL is very supportive of the Cybersecurity Act, we underline that this legislation is one step in what we consider to be the need for a more comprehensive and holistic approach towards strengthening the competitiveness of European companies and the completion of the Digital Single Market.

This paper consists of 6 building blocks

A. Certification
B. The Role of ENISA
C. Further Harmonization
D. Incident Sharing and Reporting
E. Encryption – Cooperation with Law Enforcement.
F. Digital Sovereignty

Each section starts with a management summary, highlighting the most crucial remarks for the respective topic.

A. CERTIFICATION

- Due to the increased use of connected devices, in particular IoT devices, additional measures are required in the Digital Single Market to establish an adequate level of cybersecurity, as IoT devices can, in principle, be used as attack vectors.
- All devices, including IoT, have to be developed with a 'Security by Design' approach and have to be compliant with a minimum set of security standards.
- The certification scheme has to take into account the different criticality of each service, product and application, as not every single device has to comply with the highest standards.
- There are already internationally recognized standards, certifications and audit schemes, that an updated certification scheme should build on, rather than taking the approach of reinventing the wheel.
- Users should be able to distinguish secure devices and services from non-secure ones. The well-established CE-Label could serve as a model, but on the path to achieve a harmonized, common security level throughout the EU, a transition to a mandatory scheme needs to be considered.
- The involvement of the private sector in the setting-up of any new scheme is essential.
- We note the positive improvements to the original proposal as detailed in the Niebler report, specifically the proposed phased approach for a certification framework for all ICT services and products, which would not only provide more legal certainty for companies and users but also ensure a higher level of security throughout the European Union. This also includes the demand for a mandatory product declaration, which includes regular updates for certified products and services.
- To achieve efficient functioning of the certification schemes, industry involvement is an essential factor. The Niebler report proposal takes this into account by proposing to set up consultation groups with Industry stakeholders on a case by case basis.

In 1992 the European Council launched the decision (92/242/EEC) proposed by the European Commission to address the issues of information systems in the single market and thereby created the Senior Officials Group on Information Systems (SOGIS). In 1995 the European Council published a recommendation on common information technology security evaluation criteria (95/144/EC9), which set the path in 1997 to create the first member state mutual national certification recognition between France, Germany, The Netherlands and the UK.

Furthermore, this mutual recognition led the way into a bigger mutually recognized computer security certification in Europe, the Common Criteria for Information Security Evaluation, which also became internationally recognized by other non-European countries (the U.S and Canada) in 1998 and ultimately created the ISO/IEC 15408. It´s current version, 3.1 revision 5, is recognized by public authorities in France(ANSSI), Germany(BSI) and Netherlands (NLNCSA) and there are almost 30 private labs accredited by national approval authorities in Canada, France, UK, US, Germany, Spain and The Netherlands. There is also a sub-treaty level Common Criteria MRA (Mutual Recognition Arrangement), whereby each party recognizes evaluations against the Common Criteria standard done by other parties.

As of September 2017, SOGIS has fourteen Member States that coordinate the standardization of the Common Criteria profiles and certification policies between European Certification Bodies, in order to maintain a common position in the fast-growing international Common Criteria Recognition Arrangement (CCRA). With 26 harmonized Protection Profiles[1] spanning SIM-cards, ID and health cards, residence permit cards, ministry employee cards, payment and bank cards, trusted platform module, electronic passport, security boxes such as ATMs and point of sales, tachographs, toll collections and smart meter gateways to name but a few examples, this clearly demonstrates the large range of applications the Common Criteria needs to certify.

Challenged by the increasing cyber-attacks, as well as coping with the expansion of new technologies and systems such as the IoT,[2] along with the need to avoid further fragmentation on ICT Certification, the European Commission introduced a new cybersecurity legislative package COM(2017) 477 that included within the Cybersecurity Act a proposal to elaborate and adopt a pan-European system for the cybersecurity certification scheme for ICT Products and services (art. 44) with very specific security objectives (art. 45) as well as with an assurance level (art. 46). The next articles in the COM (2017) 477 detail the cybersecurity certification and address national certification schemes and certificates, identification of the national competent supervisory authorities and

[1] https://www.sogis.org/uk/pp_en.html

[2] IoT (Internet of Things) devices adds security concerns beyond human controlled devices. The human controlling the device actually manage the device and can from that act to mitigate security risks by e.g. turning off or disconnecting the device from the network. The human can initiate software upgrades and also handle secret information for identity and key management e.g. by remembering a PIN code. With human control disappearing for an IoT device this means that other means needs to be in place like trusted computing and Hardware root of trust in the device and the usage of network controls like proxies, device/security management and patching in order to provide proper level of security and preventing IoT devices from being used as attack vectors.

conformity evaluation institutions and concludes by specifying the different notifications needed in the process as well as the penalty regime.

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators and connectivity which enables these objects to connect and exchange data.[3] By 2025 IoT will be a $6.2 trillion industry[4] and by 2020 it is estimated that there will be seven smart devices per person. Considering some of the typical security vulnerabilities of the IoT[5], it may be concluded that there is a need to mitigate against them. The creation of certification schemes may help in certain scenarios but products and services might be used in different ways and for each risk scenario there might be multiple mitigation paths which are also dependent on the acceptable risk level for each company or sector. In other words, each connected device has some risks, and so the approach to mitigate them should be risk-based and developed using Security by Design or Security by Default principles, based on internationally recognized security standards. The following are a few examples of the possible certification challenges.

Common Criteria is appropriate for less complicated products, including some Internet of Things devices and some of their intrinsic security capabilities, but the Common Criteria certification system is not a silver bullet and there are some scenarios that are not applicable or it is not used for IoT products with a very short life cycle, very low price level due to the business case and competition, complex devices and systems that mutate or that have extremely frequent updates. Common Criteria is also unsuitable for Commercial Off The Shelf (COTS) software including Software as a Service (SaaS) or Open Source. Moreover, there are usually additional IoT functions that may need to be considered for certification outside of the Common Criteria framework, for example, security aspects of communication protocols, APIs, IDAM and Device Management, including patching, where real-time active network controls sustain the lifecycle security management.

---

[3] IoT has quickly become a popular enabler for massive Distributed Denial of Service (DDoS) attacks. Mitigating DDoS is problematic as neither the owners nor the sellers of the devices bear the costs of the attacks. Minimum security requirements for IoT devices should include mitigations against being used in DDoS attacks (botnets, amplification attacks, etc.)

[4] https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity

[5] http://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+infosecResources+%28InfoSec+Resources%29

Furthermore, it is important to note that the ecosystem of certification expands to other areas and industry sectors where Common Criteria does not apply or has not been used. An overview of some scenarios is described below.

In the telecommunication sector, there is the 3GPP/GSMA SECAG/NESAS standard that defines the security validation of mobile network equipment on a complex system level and forms the basis of inspections of design processes to be in line with "Security by Design" principles. In addition there is the Global Certification Forum (GCF) that develops self-certification tools for mobile devices according in line with the 3GPP standards for functionality, including security. GCF validation is commonly demanded by network operators and commonly (not universally) used by device vendors. It has proved to be a very effective tool in avoiding recalls of devices and unnecessary customer care costs due to malfunctioning devices. GCF certification is one of the tools that has contributed to the growth penetration of the 7 billion mobile devices worldwide.

The financial sector is subject to supervisory scrutiny in operational- and cyber risk, obligatory independent third-party audits, as well as periodic audits done by the European Central Bank. In additional, they need to comply with multiple specific regulations such as the ICT risk assessment guidelines and outsourcing requirements. This requires the application of due care regarding third parties being used, assuring that they are in compliance with security requirements and controls which are sometimes certified using attestations such as SSAE 18, a SOC 2 Type II based on an ISO 27001. Internally, banks and payment providers need to comply with vendor-specific standards such as the Payment Card Industry Data Security Standard (PCI DSS) or the S.W.I.F.T program.

Additionally, there are Member States' national security interests that require specific cybersecurity certification schemes. Some examples are the federal ministries in France who use electronic employee cards for physical access in public buildings and logical access to ICT networks, to the server- and databank systems (Card Argent Public) which are certified by ANSSI. Germany certifies, via BSI, the Toll Collect systems on the free flow registration, counting and automating the billing of trucks and buses along 12,000 kilometres of highways. Since 2014, the private taxi drivers in The Netherlands require a taxi driver license, these driver cards and the onboard units (OBU) are security certified from the NCSA.

There are many other examples of the successful schemas of existing specifications and certification approaches, such as Safe Code or Trusted Computing, in the market. They are designed for a specific purpose or scenario and have proven to be valuable. These working schemas should be recognized in the new European cybersecurity certification schema.

The responsibility of having to comply with different standards and the corresponding certification is highly costly, especially if it is necessary to comply with multiple ones that have different rules, as is the case with some sectors, such

Health, Telecommunications and the Financial sector. In recognizing this, weighing up the balance between the complexity and cost, a number of public authorities from The Netherlands, France and Germany now work on a joint Lightweight Certification Framework, also called baseline certification, which can address certification using black-box test methods. Baseline certification captures the so-called minimum security aspects and functionalities and is much easier and shorter than the process used in the Common Criteria high-level security domain. It has proven to be effective in electronic jetons, used for example in Casinos in France, connected devices used in smart homes in Germany following the principle of Consumer Electronics (CE) on broadband WIFI routers. In 2017 the NCSA in The Netherlands also created a new baseline certification framework for IoT components with a focus on public procurement. Companies which offer IoT-devices, systems and services must declare to the public authorities that their products, systems or services are protected against published successful cyber-attacks.

Taking into the consideration the current panorama of existing certifications and the diversity of scenarios, ECIL proposes several recommendations which are outlined here.

Regarding migration and timeline, we believe that the security industry in Europe needs a smooth transition phase to the new cybersecurity framework, as published on 13th of Sep. 2017, which could be obtained with the creation of a new central function for ENISA who would lead the creation of the necessary processes. As of today, ENISA has no resources or experience in this matter. This limitation should be addressed by creating the necessary budget and resources but more importantly acquiring the skills and knowledge. We foresee the necessary step to include member states, industry and certification organizations as key players to collaborate in the initial steps of this journey where ENISA will need to understand the ecosystem and its concerns. For example, ENISA will need to take into consideration the certifications such as the Common Criteria Scheme which deals today with some hundred new certificates over 12 months and so any new certification scheme should be able to manage at the same time thousands of certificates, including the issues of maintenance and support.

In addition, the European Commission should also attempt to define the scope of these certifications. A more clear and transparent definition of products, systems and services is recommended to differentiate between the coverage of each of them, for example, what must be security certifiable, what can be certified and what cannot. Caution should be exercised here in order to avoid creating a definition that "softens" the certification resulting for example in the exclusion of vital IoT devices or critical infrastructure products and services, which should be within the scope of a must-be certified category. Furthermore, during this analysis, it should consider those sectors or industries that have mandatory

certifications and standards in place already to avoid the burden of having to comply twice with the same security control measures.

Another important step would be to harmonize, or bridge the gap, between the new European Cybersecurity Act and existing European regulations that require the compliance of security measures. For example, the NIS Directive, PSD2, GDPR or eIDAS, as well as specific sector-based regulations. These require necessary measures to be in place or to be based on "Security by Design" principles, thus minimizing security incidents and proving the due care security of your business. This is especially crucial for the IoT industry and critical infrastructure operators where devices are not often created with the necessary functionality to provide security updates. [Thus, a clear definition of which products and services are needed along with their criticality level, setting their security targets, the protection profiles, and the certification targets is needed].

One approach could be to create a security rating with the ability to assure compliance with different regulations and/or standards, as well as to rate different levels of maturity, robustness and/or compliance. This would enable compatibility between different existing certifications, industry levels of maturity and create a link between the rating system and certifications, standards and /or regulations based on different levels of maturity and robustness (for example based on the granularity of compliance of a control such as the strength of the password). Other factors such as the criticality of the product and / service could help shape a minimum baseline requirement for each industry, bearing in mind that the risk appetite, the scenarios, and the risk management policy of each certifying organization will also have to be applied. The certification will help to obtain a minimum baseline but cannot replace the risk management process needed to evaluate the risk scenario of each organization. Using the security rating will allow the owner of the system to choose the suitable level of protection (i.e., the level of security required) by selecting an appropriate rating level according to the risk appetite or potential impact in the organization.

Also, due to the international dimension, the scope of the industry and a pan European market for security evaluation with over 30 existing private certification labs, the introduction of the new responsibilities, new governance structures and decision-making processes require a multi-step approach to enhance the collaboration between European industry and European & national authorities. The new certification scheme should address the overall pan European necessities, harmonizing and enabling compatibility between Member States while allowing room for each Member State and it´s industry to capture specific requirements which could potentially be reused by other Member States. This approach will strengthen the competitiveness and security of the Digital Single Market.

Equally important is the interregional scope of ICT products and services, such as the "as a Service" (aaS) ICT products and services being offered globally, as well

as the COTS and Open Source industries which could benefit from a voluntary, easy, effective, reasonable and interregional certification process. It should be borne in mind that there are already internationally recognized standards, certifications and attestations from organizations such as NIST, ISO, COBIT, CSA, C5 and others. The creation of a mutual recognition or homologation process in Europe and internationally is an aspect that is missing from the draft Cybersecurity Act. The creation of a rating system mapping to certifications, standards, and regulations based on different levels of maturity, criticality and robustness could help bridge this gap.

Regarding the voluntary regime of the Certification, it is worth mentioning some key aspects. With voluntary schemes, it is probable that not all manufacturers of ICT products and services will meet required security standards. However, the quality of an EU-wide certification and labelling scheme must not be undermined by this, and hence the Commission's voluntary regulatory scheme should be flanked by more ambitious actions. A good initiative would be to create awareness campaigns and economic incentives for the promotion of the voluntary labelling. It should target the industry as well as the consumers, explaining the benefits of using these types of certifications. In this respect, the well-established CE-Label or the Energy Label could serve as a model to assure basic, up to high-level, security. In very specific cases, a mandatory certification regime might also be required, to guarantee a harmonized, common level of enforcement and legal certainty across the European Union. These specific cases would depend on the criticality of the service, product, application or process and care would be needed, to avoid creating barriers to SMEs or new innovations entering the Digital Single Market.

Finally, the involvement of the different private sectors in the setting-up of the new scheme is absolutely essential, especially those who are sustaining the critical infrastructure of the digital economy. The Commission proposal remains unclear on the cooperation mechanism between national or European authorities with the involvement of the industry. Currently, we observe a lack of dialogue between Member States and key national experts or their industry. Continuing on this path will most likely create a top-down approach that would foster a non-transparent process which could affect many industries, as well as Member States maturity levels. The principle of a public-private partnership, which is driven by the European Commission, could be one of the instruments for the active participation of all stakeholders, including the European security industry that clearly needs the mandate to participate actively in the European Cybersecurity Certification Group.

Recital (53) of the "Cybesecurity Act" specifies that "The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products and services. These schemes should be implemented and supervised by national certification supervisory authorities and certificates issued within these schemes should be valid and recognised

throughout the Union. ***Certification schemes operated by the industry or other private organisations should fall outside the scope of the Regulation****. However, the bodies operating such schemes may propose to the Commission to consider such schemes as a basis for approving them as a European scheme*."

Consequently, only schemas, like SOG-IS with government supervision fall with certainty within the scope of the Cybersecurity Act. With the limited bandwidth of such government supervised schemas, for example SOG-IS can handle some 300 products per year, it is essential to consider both the scope and role of such government supervised schemas against what would be the scope and role of Industry driven schemas and how such industry driven schemas may be used, as stated in the recital above, "as a basis for approving them as a European scheme."

Different methods for security standardization and certification exist. Some examples are:

- "Security by Design" through recommendations on software product level and generally, for example by SafeCode or on system level through 3GPP/GSMA SECAM/NESAS
- Security at an operational level through standards like the ISO 27000 family.
- Standards and certifications for trust modules, TPMs and others as per TCG and Global Platform.

In some cases, such standards can be transferred into the equivalent of Protection Profiles in the Common Criteria and SOG-IS methodology, but third-party inspection based on such high assurance, is often too costly and only works for a specific product release and configuration, thus it is not a tool that can be used universally.

"Security by design" is normally a more efficient way to achieve security in products than "Security by Inspection". Therefore, some form of recommended compliance to such methodologies and either an associated compliance declaration or third-party process audit as part of such a European scheme could add substantial value.

Sector-specific security standards e.g. Financial – PCI-DSS, Healthcare, Automotive and other sectors may be developed through industry organisations as well as international standardisation organisations.

It would be beneficial to define a process for such an industry-specific approval as a European scheme. Once proven, this could be recommended to other regions in the spirit of global harmonization. Existing approaches, such as the development of European Norms based on accredited SDOs ETSI, CENELEC etc. could be considered, though such processes and organisations may not have the necessary security certification competence. A collaboration between

ENISA, the European Commission, the European Cyber Security Certification Group and Industry could define criteria for such schemas and assign a right to such schemas to provide an EU kitemark, based on defined criteria. During the development process the interests of the Industry, the economy, efficient functioning of the Digital Single Market and the protection of consumers, SMEs and society should be considered in a balanced way. In this regard the first attempt promoted by the European Commission to create a private and public stakeholder group[6] that will work to define the first European Cybersecurity Certification scheme for Cloud Service Providers is a good step forward. This stakeholder group is taking into account current European Certifications, both public and private, such as ANSSI SECNUMCLOUD[7], BSI C5[8] or the private Leet Security certification scheme, along with international standards such as the ISO family and the ENISA Cloud Certification scheme[9] . The group will then, include new user and Cloud Service Requirements such as controls. Examples of such controls are those from the Cloud Security Alliance and NIST, specific sector controls such as EBA outsourcing guidelines, PCI-DSS or regulations that may help on the readiness and compliance issues such as the GDPR, eIDAS, PSD2 or the NIS Directive.

Overall the limited bandwidth of government supervised schemas such as SOG-IS suggest these should be used only for such functionality that is considered critical for the society. The vast majority of cybersecurity certification would have to rest on market-driven approaches, using international standards to the extent that is possible. Consequently, to be meaningful, such schemas need to have a market leverage that incentivises good security, without stifling innovation. In some cases for example with consumer devices connected to critical infrastructure, the market is likely to fail because the producer and buyer of such products would not be harmed by the lack of security, if their consumer devices could be hijacked into botnets and causing harm to others.

[6] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security

[7] https://www.ssi.gouv.fr/actualite/secnumcloud-la-nouvelle-reference-pour-les-prestataires-dinformatique-en-nuage-de-confiance/

[8]https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html

[9] https://resilience.enisa.europa.eu/cloud-computing-certification

B. THE ROLE OF ENISA

- One of the Agency's priorities should be the support for the implementation of the NIS-directive across the Union.
- Another key task of ENISA will be the implementation of the Certification Framework. The agency should assume the task of an independent audit and certification authority, which monitors and audits the standardization and certification processes in the EU.
- The principle of subsidiarity must be respected. The competences and sovereign rights of the Member States in controlling their critical infrastructures and service, in enforcing the respective legislative and regulatory framework, must remain with the national authorities.
- ENISA should not only put its resources at the disposal of the Member States, but also help companies in uncovering and removing security breaches in outdated hard and/or software, including backdoors in products and IT components.

Currently, the Agency does not have the resources and expertise to meet the requirements of the new task, Hence, ENISA will only be capable of fulfilling its mission under the new mandate after a transition period which has not been defined to date.

With the initiative to allocate more resources to ENISA, the Commission is responding to the urgent need to progress more swiftly on the path of harmonization towards a Single Market for cybersecurity across the EU. Currently, the Agency does not have the manpower, operational capabilities and know-how to meet the requirements of the proposed EU-certification framework. Hence, ENISA will only be capable of fulfilling its tasks under the new mandate after a transition period which has not been defined to date.

One of the Agency's priorities should be the support for the implementation of the NIS-directive across the European Union. So far, this process is another example of the lack of a harmonized approach between Member States. Equipped with more staff, ENISA should serve as a hub for the exchange of information between Member States for the prevention of incidents or, in the case of attacks, with cross-border impact. ENISA could support a consistent interpretation of vague legal terms within EU member states regarding European specifications such as the NIS Directive. ENISA should not, however, have power of authority towards national supervisory authorities, who should continue to be solely responsible for applying and enforcing national legislation. Implementing the specifications and recommendations of ENISA should assist EU member states

and obligated businesses in developing effective fulfilment methods, thereby promoting a harmonized approach towards implementing EU legislation.

With regard to support capacities, ENISA should not put its resources solely at the disposal of the Member States, but also help companies in uncovering and removing security breaches in outdated hard and/or software, or backdoors in products and IT components, as well as providing support with existing, and the development of new, technical standards. Here, ENISA could serve as an information exchange hub for all EU Member States.

Another key task of ENISA will be the implementation of the Certification Framework. The agency should assume the task of an independent audit and certification authority, which monitors and audits the standardization and certification processes in the EU, when new schemes are rolled out, or national schemes are migrated under the European framework. The agency should provide the technical support for management of the framework at EU level, as this would facilitate, for example, the launch of new cross-border services in the Single Market. In all cases though, the principle of subsidiarity must be respected. The competencies and sovereign rights of the Member States in controlling their critical infrastructures and services as well as in enforcing the respective legislative and regulatory framework, must remain with the national authorities.

C. FURTHER HARMONIZATION

- Following the current review of the ENISA-mandate the Commission should launch an "NIS 2.0" process to tackle the shortcomings of the legislation, as the NIS-Directive in its current version only has a "minimum harmonization" approach.
- The capabilities of the operators of networks and information systems to detect and counter incidents are limited and therefore all market participants who are exposed to risks need to be covered by the review of the NIS-Directive. This would include providers of essential services and would cover relevant requirements, such as providing patches for known vulnerabilities for hard- and software components,
- Additionally, all operators in the digital value chain, especially over-the-top-players (OTT's) as well as hard- and software manufacturers should be integrated into the obligations of the directive.
- Consequently, the directive should apply to all providers of services and components which are connected with networks, or Information services which are used by the – already regulated – operators of networks and information services.

As stated above, support for the Member States during the implementation process of the NIS-directive will be an important task for the future ENISA on the path to achieving a common, higher level of security throughout the European Union. As part of this, the Agency should help to repair the shortcomings of this directive which, as it has to be acknowledged, has been a first, and to a large extent, successful test for EU-wide legislation in the ICT-security domain.

Nevertheless, the full vision of a secure digital market needs to be materialized, especially as the directive in its current version only addresses the "minimum harmonization" approach. The directive does not cover all operators of the digital value chain, leaving important over-the-top-players (OTT's) as well as hard- and software manufacturers out of the scope of the obligations. This leads to the situation where a full and fair competition with non-European market participants cannot be achieved.

However, the extension of the scope of the NIS-Directive is not only a step towards a level playing field for all, but goes beyond the principle of fair competition, and has concrete implications for the security of networks and

services. Premeditated cyber-attacks target all market participants along the digital value chain, for example security gaps and vulnerabilities of essential services and hard- and software components. The capabilities of the operators of networks and information systems to detect and counter these incidents are limited and therefore all market participants who are exposed to risks need to be covered by the review of the NIS-Directive. This would include providers of essential services and would cover relevant requirements such as providing patches for known vulnerabilities for hard- and software components. In the case of the impossibility of tracing the source of the incident, a notification to the responsible authorities would be sufficient, as these could issue a general report or warning.

Therefore, following the current review of the ENISA-mandate the Commission should launch an "NIS 2.0"-process to tackle the shortcomings of the legislation.

1. Recommendations

- Following the review of the ENISA-mandate, the Commission should launch an "NIS 2.0" – initiative in order to address the shortcomings of the NIS-directive in the areas of a) a level-playing field for all the OTT's, b) efficient and valuable incident sharing (see below) and c) the scope of the current legislation.
- An "NIS 2.0" should cover all relevant security incidents and risks. Consequently, the directive should apply to all providers of services and components which are connected with networks or Information services, or which are used to operate networks and information services. The definitions of market participants in the directive should be amended accordingly.

D. INCIDENT SHARING AND REPORTING

- Incident reporting to regulators and supervisors produces important value. To increase effectiveness this must not be a one-way-street – it needs to be a bi-directional exchange.
- Between industries and private players, information exchange has to be enabled.
- In certain boundaries the use and sharing of Personally Identifiable Information (PII) has to be enabled if it is needed for effective protection of IT-systems.
- Reporting obligations are important, but it has to be ensured that there isn't a multitude of bodies to report to. A One-Stop-Shop is urgently needed, as well as a unified taxonomy for this reporting.
- Awareness measures and training campaigns are not solely a duty of private companies, but also for governmental bodies.

1. Current situation

Over the past decade the number of information security breaches has been growing exponentially. This rise affects consumer trust and increases the pressure on companies who are not only affected economically but also suffer damage to their trust image or reputation. The many incidents and their related costs have shown that cybersecurity has become a financially material issue which has to be managed diligently to protect corporate value. The costs of cybercrime are manifold and can impact the company in different ways. Internal costs are operational costs and relate to dealing with the cyber-crime and incidence prevention. External costs include the consequences of the cyber-attack, such as the loss or theft of sensitive information, operations' disruption, fines and penalties, infrastructure damage and revenue losses due to loss of customers.

The current focus is on how well companies are prepared to prevent major cybersecurity incidents and if they can react appropriately in case of an attack. Companies are also evaluated on past information-cybersecurity incidents they may have experienced and the financial consequences of these. Perimeter security cannot mitigate cyber-attacks even from attackers with modest resources. European enterprises, network operators, and government agencies need to assume that their networks will be breached and take the required actions to mitigate the impact of such breaches.

Regulators and supervisors have to be aware of the fact that not all companies have equal resources and expertise. They behave with different maturity levels and have applied security and privacy regulations with the hope of defending consumers. Therefore, a minimum, uncomplicated baseline of measures to mitigate future intentional or non-intentional incidents is required.

The current landscape in Europe is that there are a disparate number of data protection laws that function differently. Additionally, there are different regulatory flavors, some regulations target privacy, others cybersecurity or operational/IT risk. The GDPR is the opportunity to harmonize them all. Some examples are:

- There are national laws that enforce the reporting of data breach incidents not taking into consideration other aspects.
- Other national regulations such as the critical infrastructure incidents do take these other types of incidents into account.
- Some Data Protection laws do allow restricted intelligence sharing of Personally Identifiable Information (PII) between banks, or with law enforcement agencies under certain conditions. An example can be seen in the case of Italy where banks can share data directly to the Italian Polizia Postale. However, the Italian Police cannot share PII with any other bank, limiting the return value that other banks may receive. Similarly, companies in Estonia have been affected by attacks against digital infrastructure in other EU member states.
- However, other member states such as Spain or Belgium prohibit the sharing of PII between banks or other public institutions.
- Effective intelligence sharing collects information from multiple sources and provides insights to several organizations and states so that all may benefit. We note that such systems also incentivize data owners to participate as they receive something for what they provide. Furthermore, we must not forget that IP address analytics is a critical part of network anomaly detection that may help in finding the Command and Control nodes of botnets and other cyberattacks.
- Incident reporting to regulators and supervisors is a related topic that serves as another example of the fragmentation seen in some member state countries when multiple regulators request simultaneous reporting of the same cybersecurity incident. This overlap is observed in some national laws where there is a data protection law (GDPR), a critical infrastructure law(NIS), eIDAS, and a Central Bank requirement to report a cyber security incident as well as for PSD2 and TARGET2 incidents.
- Each of these regulations is adding complexity and cost due to the disparity of taxonomies, thresholds or templates being requested, leaving the decision to harmonize them on member states. It is important to note also that due to the transposition of some of the previously mentioned

Directives, companies are detecting different sanction and security measure regimes, leading to further regulatory fragmentation. This might lead to incentivizing companies to operate in those countries with less restrictions and sanctions, generating a competition issue.

As an example, to demonstrate the complexity and cost of a significant incident scenario, we can imagine a financial institution that has had a significant data breach to report. This institution would need to report the incident to different regulators and supervisors (GDPR, NIS, ECB and PSD2) using different templates, taxonomies and under different timeframes. In most cases, this information would potentially be shared between other national regulators and supervisors, even to other law enforcement entities and governments, but not to the rest of the financial industry which could be potentially affected in the short run. In other words, this reporting would flow one way to authorities and no feedback would be returned.

Surely other financial institutions would benefit from this reported information, such as attack vectors, to avoid being the next in line to be attacked, or to deploy resilience measures. The case of the financial industry could be highlighted as one with some type of intelligence information already in place via platforms such as FS-ISAC. However, not all types of incident information can be legally shared using this type of private ISAC.

In most Member States' regulations personal information such as an IP address of the attackers cannot be shared, and probably, under the GDPR, this will be prohibited extensively to all member states. This restriction means that crucial information which could alert and allow prevention measures will not be shared in real time between private institutions, who could benefit and possibly avoid being the next victim of, for example, a DDOS campaign. Additionally, regulators and supervisors will not alert banks because incident reporting is presently a one-way reporting mechanism where regulators and supervisors do not provide any feedback or intelligence information of systemic cyber-attacks. In this regard, there is a need to enhance the public-private partnership with regulators, supervisors and Member States that can facilitate the simplification of regulations, and more importantly the joint collaboration, trust and coordination of crisis management when under attack.

2. Challenges

There is a need to create a one-stop-shop mechanism as well as a bi-directional reporting between private institutions, regulators, supervisors, and governments.

There is also a need to standardize the reporting taxonomies, thresholds, and templates as well as a need to do so with the security measures and sanctions. The heterogeneous transposition of the NIS directive is creating divergence in the economic penalties as well as with the security measures requested by different Member States. This is certainly because the detailed implementation of directives are subject to the interpretation of Member States, and therefore this might lead to a situation where some Member States will have a more rigid regime than others, creating an ecosystem where some companies may prefer to operate in particular countries and not in others.

3. Opportunities and next steps

It is necessary to improve the dialogue between Member States and the industry in the regulatory process. This dialogue should cover the improvement of intelligence information sharing within the boundaries of data protection laws but permitting the sharing of some PII (for example IP addresses or mule accounts) where necessary.

It is also necessary to formalize the way in which different regulators, supervisors, law enforcement and industry experts can be reached in an efficient, harmonized (One-stop-shop mechanism). This would avoid bureaucracy in the templates, thresholds and taxonomies. A one-stop-shop could would also enable a two-way reporting system where regulators and supervisors can alert the industry of possible cyber-attacks in real time. The Blueprint and the Rapid Reaction Force initiative being discussed, as well as the ENISA mandate, are great opportunities for this. There is however a need to involve key players from the industry. Especially critical infrastructure players who are constantly at the forefront and are therefore in a position to bring a lot of experience into the dialogue for a more efficient and effective solution.

Cybersecurity Innovation that engages in finding a solution to the previously discussed challenges should be promoted. There are proof of concepts available exploring new ways to secure transactions online. Distributed Ledgers technology is still in the early phases of exploration but looks promising in this area as identities and transactions could be shielded as another extra layer of the internet. Similarly, Secure Computing technology could build threat data analysis systems that do not need unrestricted access to the personal records of individuals. Instead, confidential inputs from all relevant sources are collected under strong encryption and converted into insights without removing the protective mechanisms.

There is a need to allow this type of experimentation and areas set aside where regulators and supervisors should incentivize them to build upon this work.

Regulatory sandboxing in certain countries such as the UK, under the financial sector, looks promising, and many other countries in the European Union should take learnings from it.

A strong dialogue should also be undertaken with the European Institutions who, as our main supervisors, should take the lead in the search for new opportunities and help the industry to become stronger, stay trustful and innovative. The digital transformation of the different industrial sectors has already begun, and it is vital that those sectors stay competitive and healthy.

There is a clear value to the citizen or individual end-user in having access to secure and reliable services. The regulator should take this into account and look

to explore ways to allow for a balanced approach to implementing the GDPR by allowing the sharing of some PII in the context of incident sharing and reporting. The GDPR is designed to protect the individual, but so is the provision of secure services and this would be greatly facilitated with a regulatory framework that allows such special cases of PII sharing. In other words, protection of privacy of individuals could be better served if service providers can share some PII data, ensuring that individuals would see their data better protected, and with a far lower risk of being stolen by attackers.

4. Recommendations

- Incident reporting to regulators and supervisors produces value for them. However, since the information is not shared back into the rest of the industry, it only goes one way. Allowing incident sharing within the industry could improve effectiveness and value as it can help to predict future attacks to other industry players and/or increase the cyber-resilience. However, care must be taken to share information whilst maintaining its confidentiality, especially regarding personal data (consistent international privacy laws) and intellectual property.
- Due diligence is needed to avoid cyber criminals snooping into this data (trusted channels needed).
- Cyber threat intelligence needs to be easy to interpret and evaluate (need for a common taxonomy and thresholds to share data).
- Consumers are largely the ones that enable the running of the economy, and they too need to stay secure as they tend to be the weakest in the security chain. It is up to companies servicing them as well as the law enforcement agencies, governments and regulators to help them (awareness and free training campaigns) to benefit the greater majority. There are excellent opportunities to discuss these issues in G7 or G20 events as this is a global issue. However, it is necessary to start small and engage those bodies and entities that are decision makers, largely the DPA, ECB, European institutions, national governments and expert industrial institutions.
- We recommend that possible solutions such as regulatory sandboxing and balanced approaches to the implementation of GDPR, as well as other Cyber security regulations, should be brought to the attention of such bodies. These bodies should be encouraged and supported to initiate activities that find solutions to the challenges laid out in this paper. If all players can clearly understand the problem(s) in a first stage there should be a better opportunity to find solutions; however all need to be seated together first, and we believe this dialogue needs to be promoted by the Presidency of the European Union.

- An EU-wide, harmonized, implementation of the proposed legal e-evidence act will be a complex endeavour. Hence, its impact on the judicial cooperation between Member States and between companies and authorities should be assessed carefully before considering further steps. The option of direct access and real-time interception throughout the Union should also be addressed with great caution once the e-evidence regulation is adopted. The granting of civil rights must be an absolute priority here.
- Encryption is one of the most important protection measures against the misuse of personal data. Weakened encryption measures put security and privacy of the users at risk and have to be avoided.
- Standard mechanisms where the encryption is opened at the appropriate point and through an appropriate and highly secured procedure that cannot be subject to unauthorized use, and only when following a well-defined legal and audited process by the proper controls of elected officials, are being used in some domains like telecommunications.
- Acknowledging the general need to access data by law enforcement agencies, a weakening of those encryption measures (for example via Backdoors) must not be allowed as evidence shows it could not be limited to legitimate purposes of legitimate actors.
- Every existing and future access for law enforcement agencies to encrypted data has to be limited to certain judicially defined cases where a misuse can definitely be prevented (no Backdoors).
- An additional prerequisite for every enabling of access is transparency for the users and legal certainty for the involved companies

1. **Access to data**

European companies appreciate the EU' s intention to reform investigation and prosecution procedures and enhance cross-border law enforcement, by facilitating law enforcement and judicial authorities' access to electronic evidence to fight crime and terrorism more efficiently in the digital age. Pan-European network operators and provider of services, especially in the Cloud area, have been and will continue to be a key contacts for judicial authorities and law enforcement throughout the EU.

Hence, the potential of increasing legal certainty and of standardizing procedures for the cooperation of service providers with judicial authorities is

considerable. But several crucial issues must be addressed before adopting new legislation.

Regarding the proposed European Production Order providers need the possibility to legally challenge a request at national level if they consider the order to be conflicting with national legislation or data protection requirements. Furthermore, clarification is necessary with respect to the scope of the criminal offences and threshold of a three-year-conviction.

A centralized European authority as the issuing authority for orders would be a competent platform to ensure the safety and legal conformity of data provisioning according to the e-Evidence Framework. Such a centralized authority should also ensure that EU data only leaves the EU if this is based on a legal framework which has been accepted by all EU Member States.

The European Preservation Order must not implicitly impose new obligations for storing data or lead to real time interception of communication. Currently telecommunication operators store costumer data only for a very limited period of time, i.e. for billing purposes.

Clarification is also needed regarding the international judicial cooperation. Data gathered under the e-evidence framework must not leave the European Union under a mutual legal assistance agreement concluded between one EU Member States and a third country.

On the other hand, due to the nature of the global cyber-crime, European companies are struggling to prosecute criminals who are acting from outside the EU. Thus the European Union should use its diplomatic and judicial toolbox to promote multilateral cooperation and reach agreements with those countries which are not transparent about all the information required to stop cyber-crime in their territory. Many companies do not consider engaging in criminal prosecution with certain countries as the costs of judicial procedures and legal protection are immense. The lack of capabilities for prosecuting and detaining criminals in certain "offshore" countries has to be addressed.

One option of fostering efficiency in international cooperation could be the strengthening of institutions like Europol or ENISA. Another is enhancing multilateral cooperation by establishing a level playing field in cybersecurity regulation and in fighting cybercrime in the global outreach of G20 or the WTO. Rules for cybersecurity could be included into Free Trade Agreements (FTA's).

2. **Encryption**

European companies must be in control in the selection of algorithms for encryption/decryption through the standards process, as well as the security assurance of the implementation of such algorithms. Open algorithms or other

means that only rely on proven mathematics are to be selected. The algorithms to be selected shall balance implementation complexity/cost with the needed level of protection. In principle, data shall always be protected against any technically foreseeable means to break the security algorithms (as much as possible including quantum computing). International standards that fulfill these criteria are preferred. Standards such as CCRA and SOGIS with mutual recognition across all EU member states, also for more demanding Assurance levels like EAL 2-5, will lead to a large and coherent pan-European market therefore giving economies of scale beyond any other region. The EU can thus create a reagional market advantage. Furthermore, it is important to note that the Internet is a global vehicle and any regional fragmentation would be undesirable. The European Union and individual Member States should not regulate the choices of algorithms or any other technical details at all. This decision is best left for the market to decide.

Any form of "security by obscurity," intentional weaknesses, or backdoors shall not be used or promoted as this will only create a false and dangerous sense of security. Any weakness known by the "good guys" will at some point in time or at some cost, also reach "the bad guys" thereby creating a situation of constantly broken trust. Only mathematics is to be the trust base. No other means through people access, physical locks, etc. can provide the required level of trust needed for the Digital Society of today and of the future. The European Union should not suggest nor incentivize another Clipper chip. Any backdoor requirements on European companies are a huge market disadvantage for the whole European industry. It also opens a major information security risk for European companies forced to use these backdoors.

Where interception is needed for legitimate reasons such as crime prevention, law enforcement and anti-terrorism, the transparent regulation defines the types of services that are affected, and the circumstances under which an interception is required.

The "Lawful Intercept" (LI) model currently used in telecom and other industries is a method that is working to date, assuring both legal and privacy certainty. By this model, the LI is audited and set under the controls of the democratic constitution of the state including the legislation that protects privacy and fundamental human rights. Such a standard mechanism might work as follows:

a: the encryption is opened at some appropriate point and through an appropriate and highly secure procedure that cannot be subject to unauthorized use, and

b: the opening of the encryption can only be possible following a well-defined legal and audited process by the proper controls of elected officials, or by procedure, for example through an order of a prosecutor or a court of law

It remains to be proven if such a mechanism would work for End-to-End encrypted services by an uncountable number of digital service providers. Such a model would have to give a clear, transparent, and proper model for the various service providers and equipment vendors that would be covered by such LI principles. Furthermore, this would have to address the need for clarity of transparency that for example the operator Yahoo has demanded from the US government.

In any regard, a possible intercept model – if at all possible taking into account what has already been stated – would apply to the service provider of the specific end-to-end service. This also means that interception requirements on (mobile) operators should be limited to the connectivity service provided by the (mobile) operator, not the application layer service delivered OTT over the connection. Such obligations shall treat all entities equally, meaning that no one category of providers (e.g. regulated telco operators) can be forced into being "a proxy" for other service providers and act as the "appointed extended arm" of the government. In addition to being unfair and inefficient, such a "proxy for the government" regulation would create severe commercial and brand imbalance. The European Union has all the possibilities to force any provider of services (or devices) in the Eurozone, irrespectively of whether the provider is an EU or non-EU company, to comply with such principles.

3. Recommendations

- An enhanced cooperation mechanism between European companies and law enforcement authorities across the European Union needs to be created by harmonization efforts at European level. A centralized European authority should be established as a trusted and competent body which ensures the safety and legal conformity of e-evidence requests across the Union.
- Any Lawful Interception model must have a clear, transparent and proper approach for various service providers and equipment vendors in the cyberspace. However, the service providers should not take on the role of a "proxy" for the government.
- The use of open security algorithms based on guidelines from the EU must replace "Security by Obscurity" and must avoid backdoor functions.
- Well defined staged security levels as used in the eIDAS regulation 910/2014 should strike a balance between the implementation complexity and cost on one hand and the needed level of protection of data on the other.
- International security certification standards, such as CCRA and SOGIS-MRA should be capable of being used through mutual acceptance of the certificates in the Member States. Common Criteria Certification and Baseline Certification address different security levels and can capture a broad range of IoT components, which deal with confidential data.
- The selected encryption technologies must protect confidential data against foreseeable cyberattacks, including quantum computing to strengthen the Single Digital European Market
- Backdoors for illegal use must be prevented; access should be permitted for legitimate use only if a) strong legal procedures are in place and b) there is a technical guarantee that it cannot be misused.
- So far a proven model where legitimate access for legitimate actors can technically be limited to legitimate purposes does not exist.

F. Digital Sovereignty and the need for a holistic platform approach

DigitalEurope could be seen as a response to the recent actions of the two important economic regions, the US and China. In the last two years both countries have shown clear protectionism with the China Security Law and the US National Security Directive.

Digital sovereignty, digital autonomy and the secure value chain for ICT products would be key elements to strengthening the EEA with the citizens, the enterprises and the public area. One lighthouse example for digital autonomy would be the satellite navigation system GALILEO, which is totally independent to GPS in the US and GLONASS in Russia.

Elements from the DigitalEurope program should not only be seen as efforts to increase knowledge and capabilities in specific areas such as cybersecurity, AI, and high-performance computing (HPC), but rather they should be seen as elements of a growth and competitiveness driven European industrial policy. Europe needs a platform to secure sovereignty and efficient single market oriented digital capabilities. Technology elements like 5G, Cloud, IoT together with the defined priorities within cybersecurity, AI and HPC should then be part of such a holistic platform where policy and business incentives should work together to enhance prospects for Europe in the global landscape. Unlike the US and China, the EU still suffers from its natural fragmentations, but to ensure a sovereign and competitive digitalization platform the Single Market and competitiveness efforts needs to have a proper holistic industry policy focus.

The introduction of GSM now almost 30 years ago unleased enormous value for Europe through combined policy, technology, and market elements. The introduction of a new digitalization platform, involving such technologies as 5G, Cloud, cybersecurity, AI and HPC could create a similar effect. If successful, the history of GSM could repeat for today's emerging smart connected devices and applications such as smart vehicles, healthcare, cities, utilities, manufacturing, automation and other IoT and cyberphysical applications.

These sectors are all areas where Europe enjoys a strong position in terms of industries, jobs, GDP and general prosperity. There is a clear need for a digital transformation platform enabling Europe's fundamentals and strong legacy activities to succeed in the global digital transformation as well as laying foundations for new innovations and businesses. The EU is in competition with increasingly protectionist regions and needs to overcome the internal inefficiencies of fragmentation thereby driving competitiveness through the creation of sustainable, trustworthy and dynamic domestic market conditions.