European Parliament

Briefing

INDUSTRY, RESEARCH AND ENERGY (ITRE)

Digitising Industry (Industry 4.0) and Cybersecurity

KEY FINDINGS

The implementation of a programme for digitising European industry (Industry 4.0) is an ambitious endeavour, which is linked to a number of new challenges that go beyond the large scale cybersecurity framework tackled until now by the European strategies and legislation.

- Key European strategies and legislation on cybersecurity, including R&D investments are currently focused on:
  - Protection of personal data
  - Security of operation of large scale and publicly accessible information networks
  - Protection of operation of key infrastructures (of public importance)
- The importance of cybersecurity in industrial settings is only marginally recognised in relevant EU policies
- Development of appropriate legislative and support activities particularly adapted to computerized manufacturing has to become a more vigorous feature of the Digital Single Market
- Cybersecurity in the context of digitised industry requires a more holistic approach

1. Background

The widespread adoption by manufacturing industry around the world of information and communication technology is now paving the way for disruptive approaches to development, production and the entire logistics chain. This is increasingly blurring the boundaries between the real world and the virtual world in what are known as cyber-physical production systems (CPPSs). One of the most widely used terms to refer to this development often also considered as a fourth industrial revolution is "**Industry 4.0**" (digitalisation of industrial manufacturing). At the same time a new operational risk for connected, smart manufacturers and digital supply networks appears, and this is cyber. The interconnected nature of Industry 4.0-driven operations and the pace of digital transformation mean that cyberattacks can have far more extensive effects than ever before.

A recent study[1] of the European Parliament and a briefing[2] provided a comprehensive review of certain important aspects of Industry 4.0. This included also reference to cybersecurity features. However, cybersecurity has been developed as a main concern in the operation of information networks. It is also an important aspect within the completion of the Digital Single Market.

Responsible administrators: Miklos GYORFFI
Policy Department A: Economy and Scientific Policy
European Parliament
PE 607.361

The European Commission took initiative in this process through its Communication on Digitising European Industry[3] which takes account of all similar initiatives in the field and provides a review of major issues to be considered. This Communication addresses in fact Industry 4.0.

2. Digitising industry (industry 4.0)

As the EP study highlighted, Industry 4.0 is based on the autonomous communication of technologies and devices implied in the production process all along the value chain. It predicts the model of the 'smart' factory of the future where physical processes are monitored by computer-driven systems, which create a virtual copy of the physical world and make decentralised decisions based on self-organisation mechanisms. The concept takes account of the increased computerisation of the manufacturing industries where physical objects are seamlessly integrated into the information network. As a result, manufacturing systems are vertically networked with business processes within factories and enterprises and horizontally connected to spatially dispersed value networks that can be managed in real time – from the moment an order is placed right through to outbound logistics. These developments make the distinction between industry and services less relevant as digital technologies are connected with industrial products and services into hybrid products which are neither goods nor services exclusively. Indeed, both the terms 'Internet of Things' (IoT) and 'Internet of Services' are considered elements of Industry 4.0.

In another approach[4], Industry 4.0 is based on CPPSs, which are online networks of social machines that are organised in a similar way to social networks. Simply put, they link IT with mechanical and electronic components that then communicate with each other via a network. Radio frequency identification (RFID) technology, which has been in use since 1999, was a very early form of this technology.

Smart machines continually share information about current stock levels, problems or faults, and changes in orders or demand levels. Processes and deadlines are coordinated with the aim of boosting efficiency and optimizing throughput times, capacity utilization and quality development, production, marketing and purchasing.

CPPSs not only network machines with each other, they also create a smart network of machines, properties, ICT systems, smart products and individuals across the entire value chain and the full product life cycle. Sensor and control elements enable machines to be linked to plants, fleets, networks and human beings.

Of central importance for Industry 4.0 is its interface with other smart infrastructures, such as those for smart mobility, the smart grid, smart logistics and smart homes and buildings.

Links to both business and social networks – the business web and the social web – also play an increasingly important role in the digital transformation to industry 4.0. All these new networks and interfaces offered by Industry 4.0 within are an "internet of things, services, data and people".

Industry 4.0 depends on a number of new and innovative technological developments[5]:

- The application of information and communication technology (ICT) to digitise information and integrate systems at all stages of product creation and use (including logistics and supply), both inside companies and across company boundaries;
- Cyber-physical systems that use ICTs to monitor and control physical processes and systems. These may involve embedded sensors, intelligent robots that can configure themselves to suit the immediate product to be created, or additive manufacturing (3D printing) devices;

- Network communications including wireless and internet technologies that serve to link machines, work products, systems and people, both within the manufacturing plant, and with suppliers and distributors;
- Simulation, modelling and virtualisation in the design of products and the establishment of manufacturing processes;
- Collection of vast quantities of data, and their analysis and exploitation, either immediately on the factory floor, or through big data analysis and cloud computing;
- Greater ICT-based support for human workers, including robots, augmented reality and intelligent tools.

3. Cybersecurity risks in industry 4.0

The technological developments which are at the base of Industry 4.0 do raise at the same time a vast number of associated of security concerns. Industry 4.0 means opportunities and challenges[6]. Integrating the concept within an organisation means opening up the company's IT infrastructure, making it more susceptible to errors and more vulnerable to attacks. Unfortunately, intruders will not stop trying to find new ways of breaking into business networks. Attacks specifically designed to penetrate industrial control systems present a threat to production facilities. Infected computers can be controlled remotely and their data stolen. Other linked or built-in devices such as microphones, keyboards and monitors can also be spied on. As the malware exploits unknown security holes, firewalls and network monitoring software are unable to detect it.

Risk scenarios

Scenario 1

Attackers install malicious programs and block all production and logistics operations. Production and capacity utilisation data are inspected, and application and system data manipulated. In a worst-case scenario, a misdirected machine could cause physical damage in its vicinity.

Scenario 2

Commands to industrial robots are sent via embedded systems, which are usually connected to a programmable logic controller. The control components are linked to the Internet. An attacker can therefore read application and system data, install data packets designed to sabotage the production lines, related systems or even the entire corporate IT infrastructure.

Scenario 3

Social engineering: attackers exploit human characteristics, such as helpfulness, trust, curiosity or fear, to manipulate employees and gain access to data, to circumvent security precautions or to install malicious code on their computers. Their objective is to spend time undisturbed inside the company's network.

Thus *cyber risks in an industrial setting*, although still associated with the classic computer and network security perspective, develop a number of specific features[7]. They might affect sharing data across the Digital Supply Networks (DSN) which does imply increased access to data for more stakeholders and vendor acceptance and payment in a broader market. New cyber challenges are created also by connected production. Misused or manipulated requests for ad-hoc production lines can result in financial loss, low product quality, and even safety concerns for workers. The targets in the smart factory primarily focus on the availability and integrity of the physical process rather than confidentiality of information, as with traditional cyber risks.

Cyber risks in the age of Industry 4.0 extend beyond the supply network and manufacturing, however, to the product itself. As products are increasingly connected – both to each other and, at times, even back to the manufacturer and supply network – cyber risk no longer ends once a product has been sold.

Connected objects also have a risk level, because IoT devices often present significant cyber risks. Security implications of compromised IoT devices include production downtime, damage to equipment or facilities that could include catastrophic equipment failure, and, in extreme case loss of life. In addition, potential monetary losses are not limited to production downtime and incident remediation but can extend to fines, litigation expenses, and loss of revenue from brand damage. IoT devices that perform some of the most critical and sensitive tasks in industry are often the most vulnerable devices found on a network. Therefore, an integrated approach to protecting devices must be taken.

The nature of cyber risks in Industry 4.0 thus is largely dependent on the particular industrial portfolio and therefore requires adequate action from the concerned industrial decision making factors. However, *given the fact that industrial production is governed by a number of regulations industrial cyber risks should also be a concern for regulators.*

4. Cybersecurity in the eu policy context

The key objectives of the EU Commission in the field of cybersecurity[8] are:

1. Increasing cybersecurity capabilities and cooperation

The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.

2. Making the EU a strong player in cybersecurity

Europe needs to be more ambitious in nurturing its competitive advantage in the field of cybersecurity to ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology, which is interoperable, competitive, trustworthy and respects fundamental rights including the right to privacy. This should also help take advantage of the booming global cybersecurity market. To achieve this Europe needs to overcome the current cybersecurity market fragmentation and foster European cybersecurity industry.

3. Mainstreaming cybersecurity in EU policies

The objective is to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the loT.

Currently cybersecurity policy framework within the EU is defined by the ***EU Cybersecurity strategy***[9]. *The aim was to better protect Europeans online*. As the Strategy states, information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

The strategy articulates the EU's vision of cyber-security in terms of five priorities:

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Developing the industrial and technological resources for cyber-security
- Establishing a coherent international cyberspace policy for the European Union and promoting core EU values

The cybersecurity strategy is complemented by European Agenda on Security 2015-2020, which aims, among others, to provide the framework for fighting cybercrime more effectively.

The ***Directive on security of network and information systems (NIS Directive)***[10] aims to ensure a high common level of cybersecurity in the EU. The Directive builds on three main pillars:

- ensuring ***Member States preparedness*** by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
- ensuring ***cooperation*** among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
- ensuring a ***culture of security*** across sectors which are vital for our economy and society and moreover rely heavily on information and communications technologies (ICT). Businesses with an important role for society and economy that are identified by the Member States as operators of essential services under the NIS Directive will have to take appropriate security measures and to notify serious incidents to the relevant national authority. These sectors include ***energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.*** Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

The Digital Single Market Strategy[11] includes a ***public-private partnership (PPP) on cybersecurity***. The goal of this partnership is 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 partnership would be instrumental in structuring and coordinating digital security industrial resources in Europe. It includes a wide range of actors, from innovative SMEs to producers of components and equipment, critical infrastructure operators and research institutes. The initiative would leverage EU, national, regional and private efforts and resources - including research and innovation funds - to increase investments in cybersecurity.

Ultimately, the partnership would help to:

- gather industrial and public resources to deliver innovation against a jointly-agreed strategic research and
- innovation roadmap;
- focus on targeted technical priorities defined jointly with industry;

- maximize the impact of available funds;
- provide visibility to European research and innovation excellence in cybersecurity.

Delivering on the above EU strategies the Commission also made steps in order to increase cyber resilience within the EU and develop cybersecurity Industry[12]. It includes a set of measures aiming at:

- stepping up cooperation across Europe: the Commission encourages Member States to make the most of the cooperation mechanisms under the NIS Directive and to improve the way in which they work together to prepare for a large-scale cyber incident. This includes more work on education, training and cybersecurity exercises.
- supporting the emerging single market for cybersecurity products and services in the EU: for example, the Commission will explore the possibility of creating a framework for certification of relevant ICT products and services, complemented by a voluntary and light weight labelling scheme for the security of ICT products; the Commission suggests also possible measures to scale up cybersecurity investment in Europe and to support SMEs active in the market.
- establishing a contractual public-private partnership (PPP) with industry, to nurture cybersecurity industrial capabilities and innovation in the EU (cf. above).

Another legislative action to fight cybercrime that might be considered as applicable to industrial settings is the 2013 Directive on attacks against information systems, which aims to tackle large-scale cyber- attacks by requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions.

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data deals with issues of data protection relevant for the national security, public security, personal data security, network and information security, public health and social security.

Cybersecurity is also among the main tasks of EU level networks / organisations. The European Union Agency for Network and Information Security (ENISA) was set up in 2004 to contribute to the overall goal of ensuring a high level of network and information security within the EU. ***ENISA helps the Commission, the Member States and the business community to address, respond and especially to prevent NIS problems***.

The EU Computer Emergency Response Team (CERT-EU) was set up in 2012 with the ***aim to provide effective and efficient response to information security incidents and cyber threats for the EU institutions, agencies and bodies***.

The Europol's Cybercrime Centre (EC3) was set up in 2013 as integral part of Europol and has become a focal point in ***combatting and preventing cross-border cybercrime***.

EU funding for Research and Innovation also invested in cybersecurity and online privacy projects. Topics such as trustworthy network and service infrastructures, cryptology and advanced biometrics were addressed under the 7th Framework Programme (FP7) and the Competitiveness and Innovation Programme (CIP). During the same period, the Security Research theme of FP7 invested €50 million in cybercrime projects addressing topics like the economy of cybercrime, risk analysis for infrastructure protection, money laundering and dedicated road mapping actions.

Cybersecurity and privacy are part of two streams of the Horizon 2020 programme, too:

- Under the Societal Challenge "Secure societies – Protecting freedom and security of Europe and its citizens". The Digital Security strand focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets and market incentives in Europe. Security is also a so-called “digital focus area” under other challenges (privacy and security in eHealth; energy; transport; innovative security solutions for public administrations). The aim is to ensure digital security integration in the application domains.

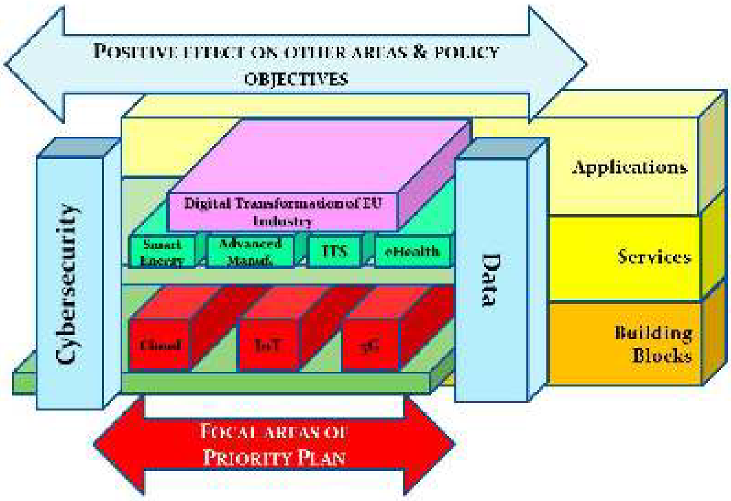
The Fighting Crime and Terrorism strand focuses on increasing the knowledge of the cybercrime phenomenon

- its specificities, its economy (including its unlawful markets and its use of virtual currencies) and the means for law enforcement authorities to fight it more efficiently and to prosecute offenders with more solid evidence from specialised forensic activities.

- Under Leadership in enabling and industrial technologies Projects on dedicated technology-driven digital security building blocks are funded (such as the 2014 calls on Cryptography and Security- by-Design). Security is also integrated as a functional requirement in specific technologies, such as the IoT, 5G, Cloud, etc.

An important milestone in the development of EU policies in respect to cybersecurity in industrial settings is the policy on standardization[13]. Among the priority domains one can find the building blocks of ICT standard setting for the IoT, (big) data technologies and cybersecurity. Areas such as eHealth, smart energy, intelligent transport systems and connected and automated vehicles, including trains, ***advanced manufacturing***, smart homes and cities and smart farming will significantly benefit from the proposed prioritisation of standards, as they rely on the essential building blocks identified. The figure below shows this context, including the different layers of technology areas, enablers, services and applications (Figure 1).

Figure 1


POSITIVE EFFECT ON OTHER AREAS & POLICY OBJECTIVES
Cybersecurity
Digital Transformation of EU Industry
Smart Energy
Advanced Manuf.
ITS
eHealth
Cloud
IoT
5G
Data
Applications
Services
Building Blocks
FOCAL AREAS OF PRIORITY PLAN

Source: COM(2016) 176 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ICT Standardisation Priorities for the Digital Single Market

5. The mid-term review of the DSM strategy[14] and cybersecurity in industry 4.0

This review continues to give high priority to cybersecurity, particularly in making protection of privacy and personal data a reality in the internet. In this respect the priority is put on the ***General Data Protection Regulation*** (GDPR) which is an essential tool to safeguard individuals’ fundamental right to the protection of personal data in the digital age. Similarly the proposal for a revised ***ePrivacy Regulation*** would complement the GDPR while also ensuring alignment with the relevant rules of the GDPR. It will further increase legal certainty and the protection of users' privacy online, while also increasing business use of communications data, based on users' consent.

The mid-term review also tackles the development of the ***European Data Economy***. In this respect the rollout of the IoT is considered to bring significant new challenges in terms of the safety of connected systems, products and services, as well as for businesses' liability. Faulty sensors, vulnerable software or unstable connectivity may make it difficult to determine who is technically and legally responsible for any ensuing damage. The Commission will consider the possible need to adapt the current legal framework to take account of new technological developments (including robotics, Artificial Intelligence and 3D printing), especially from the angle of civil law liability and taking into account the results of the ongoing evaluation of the Directive on liability for defective products and the Machinery Directive. Predictability on the access to patent protected technology endorsed in standards (standard essential patents) is key for the rollout of IoT where a broad range of sectors will implement standards on mobile connectivity. The Commission is assessing effective means to ensure a balanced framework for the licensing of this intellectual property respecting the interests of both developers and users of technology.

However, the *Commission does not present yet any immediate actions in respect to particularities of cybersecurity in Industry 4.0 context.*

The Commission also considers to foster a trustworthy cyber ecosystem and to tackle cybersecurity challenges together. In this respect the review of the Cybersecurity strategy is foreseen. It also considers the need for a review of the mandate and tasks of the European Union Agency for Network and Information Security (ENISA), taking in particular into consideration its new role under the NIS Directive. The Commission also wishes to develop measures on cyber security standards, certification and labelling, to make ICT-based systems, including connected objects, more cyber-secure.

Special emphasis is given to **digitisation of industry.** As already mentioned, the landmark initiative in this respect is the communication on **Digitising European Industry**[15]**.** In this the Commission establishes that "Digitisation of the industrial fabric brings also ***new regulatory challenges***. This includes issues relating to data generated by the multitude of new smart products, liability of more autonomous systems and safety with the increasing need for interaction between humans and smart devices. It requires striking the right balance between legitimate business interests and the fundamental rights ensuring protection of personal data and privacy, as set out in the General Data Protection Regulation. The further development of the IoT and big data pose also important ***trust and security*** challenges for any company and for public acceptance."

However, the communication for the time being only establishes that digital technologies are developing so fast that the legal framework needs to be monitored constantly to make sure it remains in line with the technological development. It also pointed out that stakeholders expressed a need to examine the regulatory framework for digital innovations with a view to provide further clarity on the following:

- Ownership and use of data generated in an industrial context are major areas of concern. When it is personal data, protection is dealt with in the General Data Protection Regulation, together with the ePrivacy Directive. The already foreseen initiative on "free flow of data" under the DSM will examine issues of ownership, interoperability, exploitation and access to data, including industrial data.
- Autonomously acting systems pose a challenge to current safety and liability rules where a legal person is ultimately responsible. Legal implications of the roll-out of IoT

are wider than the allocation of liability as recognised in the DSM strategy and also need to be addressed.

- Apps and other non-embedded software (not contained in a tangible medium) might also raise potential safety risks and are currently not fully addressed by the EU legal framework.

6. The new cyber security package and its possible links to industry 4.0

The new cybersecurity regulatory package of the European Commission launched on 13 September 2017 encompasses a holistic review of all EU level initiatives concerning cybersecurity. The Communication16 concerned presents the general framework of the package, which primarily addresses the new mandate for the European Union Agency for Network and Information Security (ENISA). This would be entrusted to provide support also for businesses in key areas including the implementation of the NIS Directive as well as in the cybersecurity certification framework. It would conduct yearly pan-European cybersecurity exercise and serve as a focal point for information and knowledge in the cybersecurity community, potentially manufacturing industry, too.

The package also proposes the setting up of an EU cybersecurity framework, aims to create a single cybersecurity market. In which stakeholders would be invited to focus on security in critical or high-risk applications, among which it identifies also machineries in factories. It acknowledges that the cybersecurity threat landscape is evolving, however only mentioning in this respect essential services (and specific sectors) such as transport, energy, health care banking, financial market infrastructure, drinking water or digital infrastructure.

Liability raised by new digital technologies17 were also recently tackled, nevertheless the next steps in this respect are expected to be concluded in 2018.

The implementation of the NIS Directive18 is also revised, although the main scope continues to be large-scale cybersecurity incidents affecting not only one Member State and key strategic sectors like banking, energy or transport. The objectives of the directive are limited to improve national cybersecurity capabilities, build cooperation at EU level and promote a culture of risk management and incident reporting among key economic actors, notably operators providing essential services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSPs). Still, the Commission proposes to provide freedom to Member States should they wish to include19 some of additional sectors like: a) public administration, b) postal sector, c) food sector, d) chemical and nuclear industry, e) environmental sector, g) civil protection. This constitutes a broadening of target sectors, still ***digitised manufacturing industry is not included***.

The proposed establishement of the network of cybersecurity competence centres and of the European Cybersecurity Research and Competence Centre would address a number of cybersecurity items with significance for manufacturing industry, too (blockchain and secure digital identities, access to mass data for EU based companies, encryption). The design of ICT products and system which incorporate security principles from the very beginning (security by desgin) is identified as a goal for development of cybersecurity skills base, under guidance from the European Cybersecurtiy Research and Competence Centre and ENISA. ***Such products could also contribute to a much higher resilience of a digitised industry.***

The Commission also endeavours to promote cyber hygiene and awareness as businesses must adopt appropriate cybersecurity programmes and update them regularly to reflect the evolving risk landscape. Still, the target seems to continue to be the general security of network and information systems, rather the specific needs of a digitised manufacturing industry. It identifies the strong role of industry in general, however, with particular attention to digital service providers and manufacturers.

Another positive approach is the introduction of cyber deterrence, concerning a more effective law enforcement response focusing on detection, traceability and prosecution of cybercriminals. This concerns first the identification of malicious actors (and improving technologies for doing so), setting up the law enforcement response (putting forward a proposal in 2018 to facilitate cross-border access to electronic evidence) nevertheless focusing on fraud[20], defence related issues and political/diplomatic framework. Still, the EC concludes that the orientation of the package is to enhance European cybersecurity and to address threats to both civilian and military targets, in which ***digitised manufacturing industry is not excluded, but it does not constitute a focal area.*** Objectives and scope of the European Parliament and the Council Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.212 August 2013, are to approximate the criminal law of the Member States in the area of attacks against information systems and to improve cooperation between competent authorities. Specific criminal offences are defined, namely:

- Illegal access to information systems as such;
- Illegal system interference which includes any illegal access to an information system causing its functioning to be seriously hindered or interrupted;
- Illegal data interference which refers to any unlawful interference with computer data as such impairing its integrity or availability;
- Illegal interception of non-public transmissions of computer data and electromagnetic emissions from an information system carrying such data;
- Illegal provision of tools used for committing the mentioned offences. In this context, such tools could be a computer programme as well as a computer password or any other data allowing access to an information system.

In addition, the Directive extends criminal liability to incitement, aiding and abetting by natural and/or legal persons to commit and their attempt to commit the offences mentioned above. Thus the Directive provides an excellent base of legal pursuit of cybercrime action within digitised manufacturing industry, too. The Comission now provided report on the implementation of the Directive[21]

The Commission Recommendation on Coordinated Response to Large Scale Cybersecurtiy Incidents and Crises[22] clearly ***does not address digitised manufaturing industry*** (as it considers a cybersecurity incident as a crisis at Union level when the disruption cause dby the incident is too extensive for a concerned Member State to handle on its own or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level. Nevertheless it identifies pan-European cyber incident exercises (‘Cyber Europe’) regularly organised by ENISA as essential to stimulate and improve cooperation among Member States and the private sector. Still the lates one[23], had as goals:

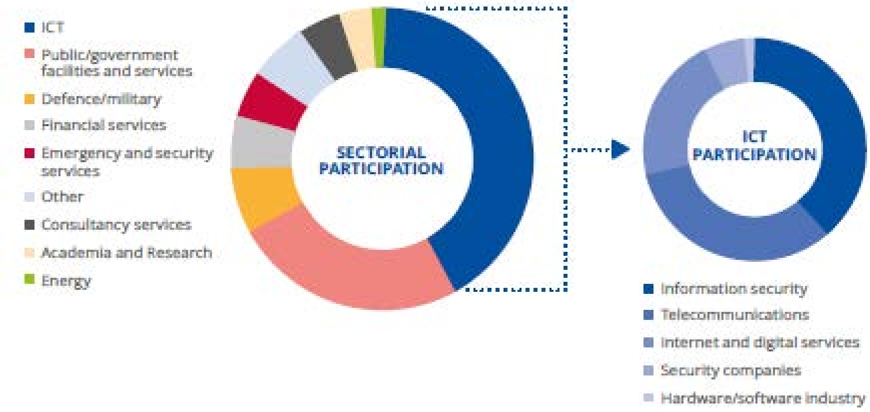
G1. Test EU-level cooperation processes.

G2. Provide opportunities for Member States to test their national-level cooperation processes.

G3. Train EU- and national-level capabilities.

The main target audience of the exercise was individuals and organisations involved in information security activities in the information and telecommunications technology (ICT) sector (Figure 2). ***Digitised manufacturing industry was not involved***.

Figure 2



Source: Cyber Europe 2016: After Action Report (June 2017) Findings from a cyber crisis exercise in Europe

Similarly ENISA is still not involved in cybersecurity problems of digitised manufacturing industry. According to its lates annual incidents report[24] the services and network assets most affected were:

- Mobile internet most affected service (44% of all reported incidents).
- Emergency services (20 %).
- Interconnections between providers (4 %).
- Switches and routers: Overall, switches and routers were the network components most affected by incidents (13%), followed by mobile base stations (10%).
- New services affected: TV broadcasting/Cable TV Networks (13,7%) and SMS/MMS (13%), public email (5,8%), IPTV (5,1%), VOIP services (4,3%) were the most affected services among the new ones included from this year.

However, Commission identified[25] that the cybersecurity landscape is evolving fast with new threats. The Internt of Things creates new possibilities and the current mandate does not equip ENISA with the necessary tools to face the current and future cybersecurity challenges. Therefore, ***the EU needs a focal point to address new threats which are horizontal in nature and impacting on multiple industrial sectors.***

Within this logic the Commission proposes a renewed mandate for ENISA[26]. Beyond the different elements aimed to reshape and strengthen the role of ENISA as THE EU cybersecurity agency, the Commission wishes to entrust ENISA also with ***capacity building*** (to contribute to the establishement of iInformation Sharing and Analysis Centres (ISACS) in various sectors) and ***market related*** (ICT standardization and ICT cybersecurity certification) tasks***.*** Particulary ***cybersecurity certification of ICT products and services*** (which encompasses the direct incorporation of security features in the early stages of their technical design and development (security by design) might be extremely relevant to industrial automation control system, thus for digitised manufacturing, too. Nevertheless, both the voluntary nature of envisaged certification, as well as the quite widespread current opinion that existing certification schemes do not support the needs of Europe's industry, put a question mark on when and how certification will become an reliable tool to cyber protect digitised manufacturing.

[1] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf

[2] Ron Davies, EPRS, Industry 4.0: Digitalisation for productivity and growth (2015, 10 p)

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0180&from=EN

[4] https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/manufacturing/ch-en-manufacturing-industry-4-0-24102014.pdf

[5] Ron Davies, EPRS, Industry 4.0: Digitalisation for productivity and growth (2015, 10 p)

[6] https://www.infosecurityeurope.com/__novadocuments/304922?v=636135137079870000

[7] https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html

[8] http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_ 41543.pdf

[9] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[11] COM(2015) 192 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe

[12] COM(2016) 410 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

[13] COM(2016) 176 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ICT Standardisation Priorities for the Digital Single Market

[14] COM(2017) 228 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All

[15] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0180&from=EN

[16] JOIN(2017)450 final Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

[17] COM(2017)228

[18] COM(2017) 476 final Communication from the Commission to the European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

[19] COM(2017)476 final/2 Annex I

[20] COM(2017) 489 Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

[21] COM(2017)474 final Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[22] C(2017)6100 final

[23] Cyber Europe 2016: After Action Report (June 2017) Findings from a cyber crisis exercise in Europe

[24] Annual Incident Reports 2015, Analysis of Article 13a annual incident reports in the telecom sector, September 2016

[25] COM(2017) 478 final Report from the Commission to the European Parliament and the Council on the evaluation of the European Agency for Network and Information Security (ENISA)

[26] COM(2017)477 final Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU)526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

DISCLAIMER

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

This document is available at: www.europarl.europa.eu/studies
Contact: Poldep-Economy-Science@ep.europa.eu
Manuscript completed in November 2017
© European Union
ITRE-2017-10
PE 607.361

CATALOGUE: QA-06-17-174-EN-C (paper)
CATALOGUE: QA-06-17-174-EN-N (pdf)
ISBN: 978-92-846-2168-2 (paper)
ISBN: 978-92-846-2167-5 (pdf)
doi:10.2861/268729 (paper)
doi:10.2861/564550 (pdf)