EUROPEAN COURT OF AUDITORS

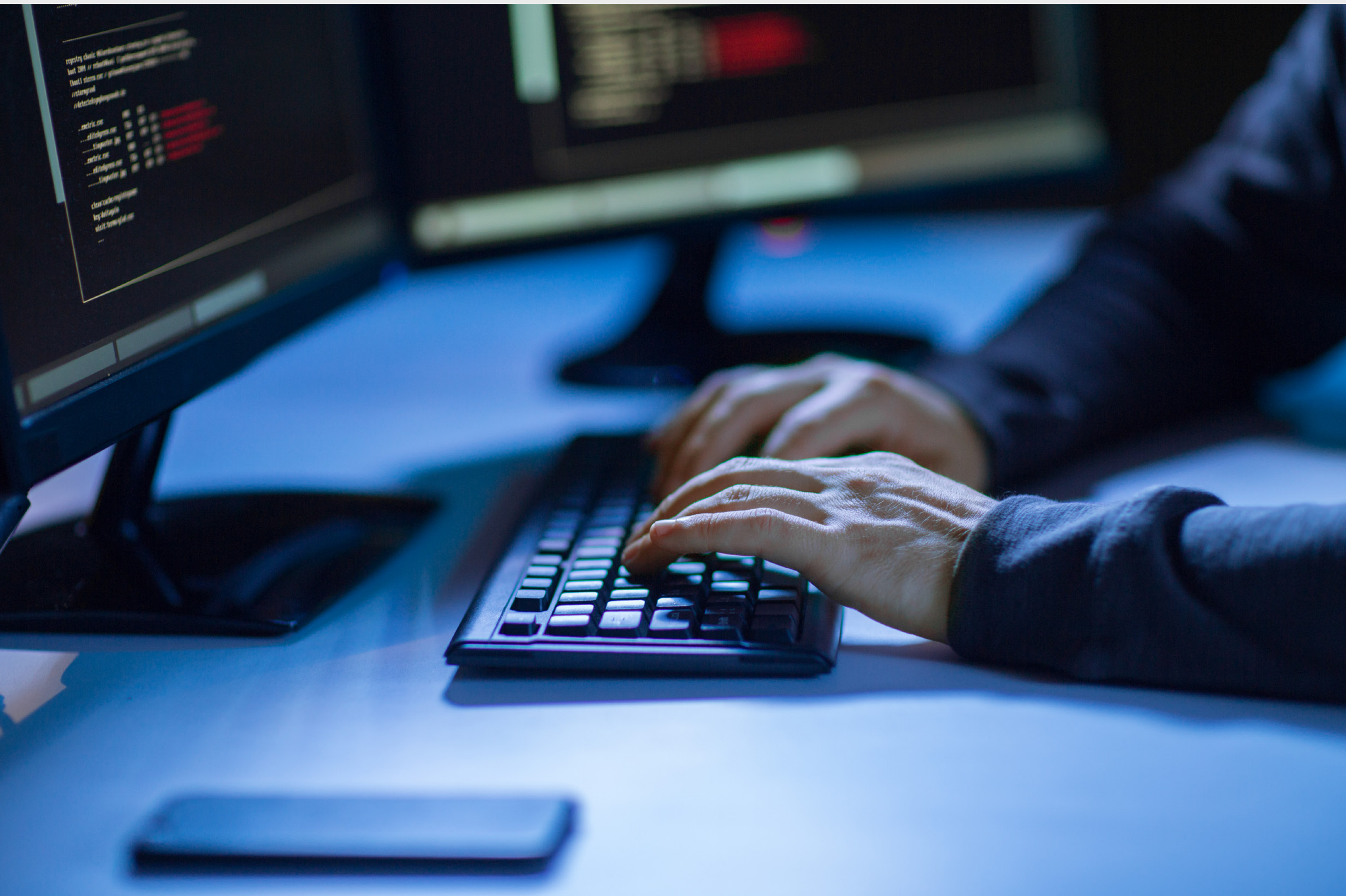
EN

2019

Challenges to effective EU cybersecurity policy

Briefing Paper

March 2019



About the paper:

The objective of this briefing paper, which is not an audit report, is to provide an overview of the EU's complex cybersecurity policy landscape and identify the main challenges to effective policy delivery. It covers network and information security, cybercrime, cyber defence and disinformation. The paper will also inform any future audit work in this area.

We based our analysis on a documentary review of publicly available information in official documents, position papers and third party studies. Our field work was carried out between April and September 2018, and developments up to December 2018 are taken into account. We complemented our work by a survey of the Member States' national audit offices, and through interviews with key stakeholders from EU institutions and representatives from the private sector.

The challenges we identified are grouped into four broad clusters: i) the policy framework; ii) funding and spending; iii) building cyber-resilience; iv) responding effectively to cyber incidents. Achieving a greater level of cybersecurity in the EU remains an imperative test. We therefore end each chapter with a series of ideas for further reflection by policy-makers, legislators and practitioners.

We would like to acknowledge the constructive feedback received from the services of the Commission, the European External Action Service, the Council of the European Union, ENISA, Europol, the European Cybersecurity Organisation, and national audit offices of the Member States.

Contents

Executive summary

I Technology is opening up a whole new world of opportunities, with new products and services becoming integral parts of our daily lives. In turn, the risk of falling victim to cybercrime or a cyberattack is increasing, the societal and economic impact of which continues to mount. The EU's recent drive since 2017 to accelerate efforts to strengthen cybersecurity and its digital autonomy come therefore at a critical time.

II This briefing paper, which is not an audit report and is based on publicly available information, aims to provide an overview of a complex and uneven policy landscape, and to identify the main challenges to effective policy delivery. The scope of our paper covers EU cybersecurity policy, as well as cybercrime and cyber defence, and also encompasses efforts to combat disinformation. The challenges we identified are grouped into four broad clusters: (i) the policy and legislative framework; (ii) funding and spending; (iii) building cyber-resilience; and (iv) responding effectively to cyber incidents. Each chapter includes some reflection points on the challenges presented.

The policy and legislative framework

III Developing action aligned to the EU's cybersecurity strategy's broad aims of becoming the world's safest digital environment is a challenge in the absence of measurable objectives and scarce, reliable data. Outcomes are rarely measured and few policy areas have been evaluated. A key challenge is therefore **ensuring meaningful accountability and evaluation** by shifting towards a performance culture with embedded evaluation practices.

IV The legislative framework remains incomplete. **Gaps in, and the inconsistent transposition of, EU law** can make it difficult for legislation to reach its full potential.

Funding and spending

V **Aligning investment levels with goals** is challenging: this requires scaling up not just overall investment in cybersecurity – which in the EU has been low and fragmented– but also scaling up impact, especially in better harnessing the results of research spending and ensuring the effective targeting and funding of start-ups.

VI **Having a clear overview of EU spending** is essential for the EU and its Member States to know which gaps to close to meet their stated goals. As there is no dedicated EU budget to fund the cybersecurity strategy, there is not a clear picture of what money goes where.

VII At a time of heightened security-driven political priorities, **constraints in the adequate resourcing of the EU's cyber-relevant agencies** may prevent the EU's ambitions from being matched. Addressing this challenge includes finding ways of attracting and retaining talent.

Building cyber-resilience

VIII Weaknesses in cybersecurity governance abound in the public and private sectors across the EU as well as at the international level. This impairs the global community's ability to respond to and limit cyberattacks and undermines a coherent EU-wide approach. The challenge is thus to **strengthen cybersecurity governance**.

IX **Raising skills and awareness** across all sectors and levels of society is essential, given the growing global cybersecurity skills shortfall. There are currently limited EU-wide standards for training, certification or cyber risk assessments.

X A foundation of trust is essential for strengthening overall cyber resilience. The Commission itself has assessed that coordination in general is still insufficient. **Improving information exchange and coordination** between the public and private sectors remains a challenge.

Responding effectively to cyber incidents

XI Digital systems have become so complex that preventing all attacks is impossible. Responding to this challenge is **rapid detection and response**. However, cybersecurity is not yet fully integrated into existing EU-level crisis response coordination mechanisms, potentially limiting the EU's capacity to respond to large-scale, cross-border cyber incidents.

XII The **protection of critical infrastructure and societal functions** is key. The potential interference in electoral processes and disinformation campaigns are a critical challenge.

XIII The current challenges posed by cyber threats facing the EU and the broader global environment require continued commitment and an ongoing steadfast adherence to the EU's core values.

Introduction

01 Technology is opening up a whole new world of opportunities. As new products and services take off, they become integral parts of our daily lives. However, with each new development our technological dependence rises, and so too does the importance of cybersecurity. The more personal data we put online and the more connected we become, the more likely we are to fall victim to a form of cybercrime or cyberattack.

What is cybersecurity?

02 There is no standard, universally accepted definition of cybersecurity[1]. Broadly, it is all the safeguards and measures adopted to defend information systems and their users against unauthorised access, attack and damage to ensure the confidentiality, integrity and availability of data.

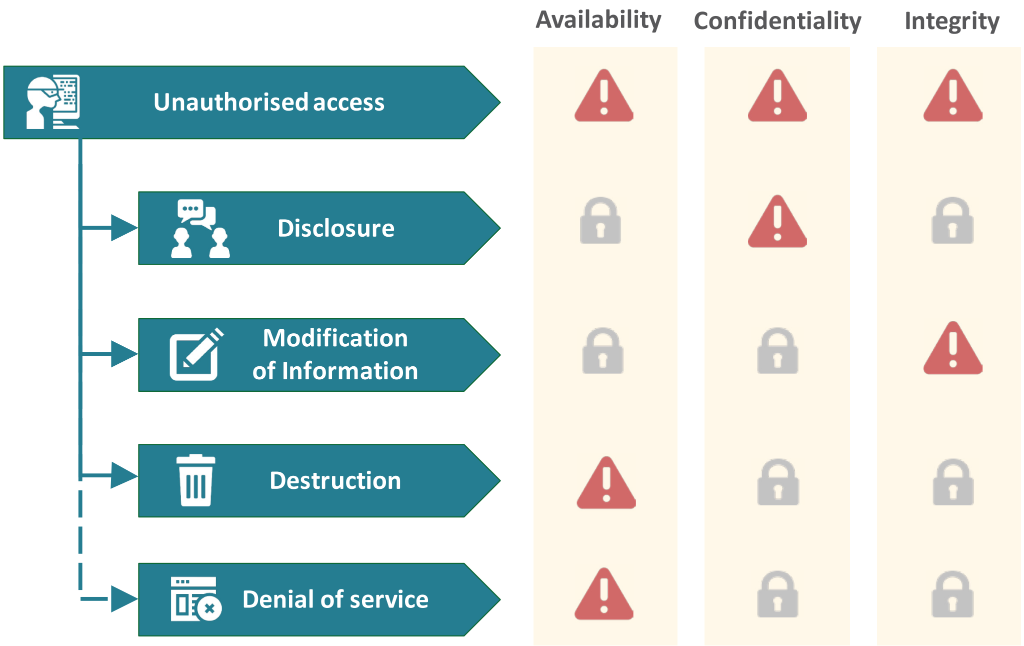
03 Cybersecurity involves preventing, detecting, responding to and recovering from cyber incidents. Incidents may be intended or not and range, for example, from accidental disclosures of information, to attacks on businesses and critical infrastructure, to the theft of personal data, and even interference in democratic processes. These can all have wide-ranging harmful effects on individuals, organisations and communities.

04 As a term used in EU policy circles, cybersecurity is not limited to network and information security. It covers any unlawful activity involving the use of digital technologies in cyberspace. This can therefore include cybercrimes like launching computer virus attacks and non-cash payment fraud, and it can straddle the divide between systems and content, as with the dissemination of online child sexual abuse material. It can also cover disinformation campaigns to influence online debate and suspected electoral interference. In addition, Europol sees a convergence between cybercrime and terrorism[2].

05 Different actors – including states, criminal groups and hacktivists – instigate cyber incidents, moved by different motives. The fallout from these incidents is felt at the national, European and even global level. However, the intangible and largely borderless nature of the internet, and the tools and tactics used, often make it difficult to identify an attack's perpetrator (the so-called "attribution problem").

06 The numerous types of cybersecurity threats can be classified according to what they do to data – disclosure, modification, destruction or denied access – or the core information security principles they violate, as shown in ***Figure 1*** below. Some examples of attacks are described in ***Box 1***. As the attacks to information systems increase in sophistication, our defence mechanisms become less effective[3].

Figure 1 – Threat types and the security principles they put at risk



	Availability	Confidentiality	Integrity
Unauthorised access	⚠	⚠	⚠
Disclosure	🔒	⚠	🔒
Modification of Information	🔒	🔒	⚠
Destruction	⚠	🔒	🔒
Denial of service	⚠	🔒	🔒

Source: ECA modified from a European Parliament study[4]. Padlock = security not impacted; Exclamation mark = security at risk

Box 1

Types of cyber attacks

Every time a new device comes online or connects with other devices, the so-called cybersecurity "attack surface" increases. The exponential growth of the Internet of Things, the cloud, big data and the digitisation of industry is accompanied by a growth in the exposure of vulnerabilities, enabling malicious actors to target ever more victims. The variety of attack types and their growing sophistication make it genuinely difficult to keep pace[5].

Malware (malicious software) is designed to harm devices or networks. It can include viruses, trojans, ransomware, worms, adware and spyware. **Ransomware** encrypts data, preventing users from accessing their files until a ransom is paid, typically in cryptocurrency, or an action is carried out. According to Europol, ransomware attacks dominate across the board, and the number of ransomware types has exploded over the past few years. **Distributed Denial of Service** (DDoS) attacks, which make services or resources unavailable by flooding them with more requests than they can handle, are also on the rise, with one-third of organisations facing this type of attack in 2017[6].

Users can be manipulated into unwittingly performing an action or disclosing confidential information. This ruse can be used for data theft or cyberespionage, and is known as **social engineering**. There are different ways to achieve this, but a common method is **phishing**, where emails appearing to come from trusted sources trick users into revealing information or clicking on links that will infect devices with downloaded malware. More than half of Member States reported investigations into network attacks[7].

Perhaps the most nefarious of threat types are **advanced persistent threats** (APTs). These are sophisticated attackers engaged in long-term monitoring and stealing of data, and sometimes harbouring destructive goals as well. The aim here is to stay under the radar without detection for as long as possible. APTs are often state-linked and targeted at especially sensitive sectors like technology, defence, and critical infrastructure. Cyberespionage is said to account for at least one-quarter of all cyber incidents and the majority of costs[8].

How serious is the problem?

07 Capturing the impact of being poorly prepared for a cyberattack is difficult due to the lack of reliable data. The economic impact of cybercrime rose fivefold between 2013 and 2017[9], hitting governments and companies, large and small alike. The forecast growth in cyber insurance premiums from €3 billion in 2018 to €8.9 billion in 2020 reflects this trend.

08 While the financial impact of cyberattacks continues to grow, there is an alarming disparity between the cost of launching an attack and the cost of prevention, investigation and reparation. For example, a DDoS attack can cost as little as €15 a month to carry out, yet the losses suffered by the targeted business, including reputational damage, are considerably higher[10].

09 Although 80 % of EU businesses having experienced at least one cybersecurity incident in 2016[11], acknowledgement of the risks is still alarmingly low. Among companies in the EU, 69 % have no, or only a basic understanding, of their exposure to cyber threats[12], and 60 % have never estimated the potential financial losses[13]. Furthermore, according to a global survey, one-third of organisations would rather pay the hacker's ransom than invest in information security[14].

10 The global *Wannacry* ransomware and *NotPetya* wiper malware attacks in 2017 together affected more than 320 000 victims in around 150 countries[15]. These incidents led to something of a global awakening of the threat posed by cyberattacks, creating fresh momentum to bring cybersecurity into mainstream policy thinking. In addition, 86 % of EU citizens now believe the risk of falling victim to cybercrime is increasing[16].

The EU's action on cybersecurity

11 The EU became an observer organisation to the Council of Europe's Convention on Cybercrime Committee in 2001[17] (the Budapest Convention). Since then, the EU has used policy, legislation and spending to improve its cyber resilience. Against a background of an increasing number of major cyberattacks and incidents, activity has accelerated since 2013, as ***Figure 2*** shows. In parallel, Member States have adopted (and in some cases already updated) their first national cybersecurity strategies.

12 The main EU actors with responsibility for cybersecurity are described in ***Box 2*** and ***Annex I***.

Box 2

Who is involved?

The **European Commission** aims to increase cybersecurity capabilities and cooperation, strengthen the EU as a cybersecurity player, and mainstream it into other EU policies. The main Directorates-General (DG) responsible for cybersecurity policy are DGs **CNECT** (cybersecurity) and **HOME** (cybercrime), responsible for the Digital Single Market and the Security Union respectively. DG **DIGIT** is responsible for the IT security of the Commission's own systems.

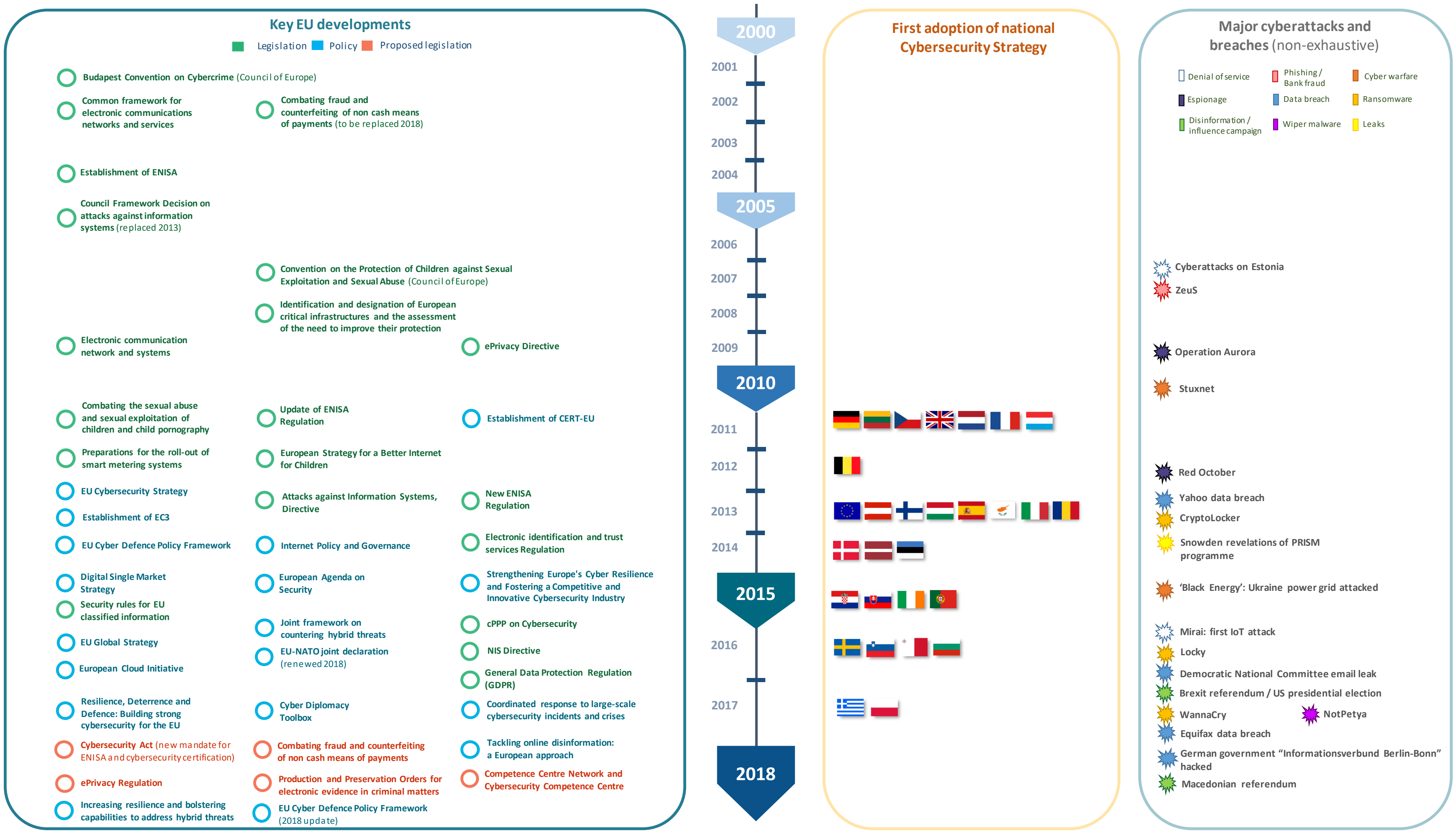
A host of EU agencies support the Commission, notably **ENISA** (European Union Agency for Network and Information Security), the EU's cybersecurity agency – a mainly advisory body that supports policy development, capacity-building and awareness-raising. Europol's European Cybercrime Centre (**EC3**) was established to strengthen the EU's law enforcement response to cybercrime. A Computer Emergency Response Team (**CERT-EU**), supporting all Union institutions, bodies and agencies, is hosted by the Commission.

The **European External Action Service** (EEAS) leads on cyber defence, cyber diplomacy and strategic communication, and hosts intelligence and analysis centres. The **European Defence Agency** (EDA) aims to develop cyber defence capabilities.

Member States are primarily responsible for their own cybersecurity and, at the EU level, act through the **Council**, which has numerous coordination and information-sharing bodies (amongst them the Horizontal Working Party on Cyber Issues). The **European Parliament** acts as co-legislator.

Private sector organisations, including industry, internet governance bodies, and academia, are both partners and contributors to policy development and implementation – including through a contractual public-private partnership (**cPPP**).

Figure 2 – An acceleration in policy development and legislation (as at 31 December 2018)



Key EU developments

🟩 Legislation 🟦 Policy 🟥 Proposed legislation

Budapest Convention on Cybercrime (Council of Europe)

Common framework for electronic communications networks and services

Combating fraud and counterfeiting of non cash means of payments (to be replaced 2018)

Establishment of ENISA

Council Framework Decision on attacks against information systems (replaced 2013)

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Council of Europe)

Identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Electronic communication network and systems

ePrivacy Directive

Combating the sexual abuse and sexual exploitation of children and child pornography

Update of ENISA Regulation

Establishment of CERT-EU

Preparations for the roll-out of smart metering systems

European Strategy for a Better Internet for Children

EU Cybersecurity Strategy

Attacks against Information Systems, Directive

New ENISA Regulation

Establishment of EC3

EU Cyber Defence Policy Framework

Internet Policy and Governance

Electronic identification and trust services Regulation

Digital Single Market Strategy

European Agenda on Security

Strengthening Europe's Cyber Resilience and Fostering a Competitive and Innovative Cybersecurity Industry

Security rules for EU classified information

Joint framework on countering hybrid threats

cPPP on Cybersecurity

EU Global Strategy

EU-NATO joint declaration (renewed 2018)

NIS Directive

European Cloud Initiative

General Data Protection Regulation (GDPR)

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

Cyber Diplomacy Toolbox

Coordinated response to large-scale cybersecurity incidents and crises

Cybersecurity Act (new mandate for ENISA and cybersecurity certification)

Combating fraud and counterfeiting of non cash means of payments

Tackling online disinformation: a European approach

ePrivacy Regulation

Production and Preservation Orders for electronic evidence in criminal matters

Competence Centre Network and Cybersecurity Competence Centre

Increasing resilience and bolstering capabilities to address hybrid threats

EU Cyber Defence Policy Framework (2018 update)

First adoption of national Cybersecurity Strategy

Major cyberattacks and breaches (non-exhaustive)

- Denial of service
- Phishing / Bank fraud
- Cyber warfare
- Espionage
- Data breach
- Ransomware
- Disinformation / influence campaign
- Wiper malware
- Leaks

Cyberattacks on Estonia

ZeuS

Operation Aurora

Stuxnet

Red October

Yahoo data breach

CryptoLocker

Snowden revelations of PRISM programme

'Black Energy': Ukraine power grid attacked

Mirai: first IoT attack

Locky

Democratic National Committee email leak

Brexit referendum / US presidential election

WannaCry

NotPetya

Equifax data breach

German government "Informationsverbund Berlin-Bonn" hacked

Macedonian referendum

Source: ECA.

Policy

13 The EU's cyber ecosystem is complex and multi-layered, cuts across an array of internal policy areas, like justice and home affairs, the digital single market and research policies. In external policy, cybersecurity features in diplomacy, and is increasingly part of the EU's emerging defence policy.

14 The cornerstone of the EU's policy is the **2013 Cybersecurity Strategy**[18]. The Strategy aims to make the EU's digital environment the safest in the world, while defending fundamental values and freedoms. It has five core objectives: (i) increasing cyber resilience; (ii) reducing cybercrime; (iii) developing cyber defence policies and capabilities; (iv) developing industrial and technological cybersecurity resources; and (v) establishing an international cyberspace policy aligned with core EU values.

15 The Cybersecurity Strategy interlinks with three subsequently adopted strategies:

— The **European Agenda on Security**'s (2015) objective is to improve law enforcement and the judicial response to cybercrime, mainly by renewing updating existing policies and legislation[19]. It also sets out to identify obstacles to criminal investigations on cybercrime and enhance cyber capacity-building.

— The **Digital Single Market Strategy**[20] (2015) aims to create better access to digital goods and services by creating the right conditions in which to maximise the digital economy's growth potential. Strengthening online security, trust and inclusion is essential to this end.

— The 2016 **Global Strategy**[21] aims to boost the EU's role in the world. Cybersecurity forms a core pillar through a renewed commitment to cyber issues, cooperation with key partners, and a resolve to address cyber issues across all policy areas, including the rebuttal of disinformation through strategic communication.

16 In recent years, as cyberspace has become increasingly militarised[22] and weaponised[23], it has come to be seen as the fifth domain of warfare[24]. Cyber defence shields cyberspace systems, networks and critical infrastructure against attack by military and other means. A **Cyber Defence Policy Framework** was adopted in 2014 and updated in 2018[25]. The 2018 updates identifies six priorities, including the development of cyber defence capabilities, as well as the protection of the EU Common Security and Defence Policy (CSDP) communication and information networks. Cyber defence also forms part of the Permanent Structured Cooperation Framework (PESCO) and EU-NATO cooperation.

17 The EU's **Joint Framework on countering hybrid threats** (2016) tackles cyber threats to both critical infrastructure and private users, highlighting that cyberattacks can be carried out through disinformation campaigns on social media[26]. It also notes the need to improve awareness and enhance cooperation between the EU and NATO, which was given substance in the Joint EU-NATO Declarations of 2016 and 2018[27].

18 In 2017 the Commission presented a new cybersecurity package, reflecting the growing urgency of digital protection. This included a new Commission communication updating the 2013 cybersecurity strategy[28], a blueprint for a quick and coordinated response to a major attack, and for the swift implementation of the Directive on Security of Network and Information Systems (NIS Directive)[29]. Furthermore, the package included a number of legislative proposals (see paragraph ***22***).

Legislation

19 Since 2002 legislation with varying degrees of relevance to cybersecurity has been adopted.

20 As the main pillar of the 2013 cybersecurity strategy, the legal centrepiece is the 2016 **Network and Information Security (NIS) Directive**[30], the first EU-wide legislation on cybersecurity. The directive, which was to be transposed by May 2018, aims to achieve a minimum level of harmonised capabilities by obliging Member States to adopt national NIS strategies and create single points of contact and computer security incident response teams (CSIRTs)[31]. It also sets security and notification requirements for operators of essential services in critical sectors and digital service providers.

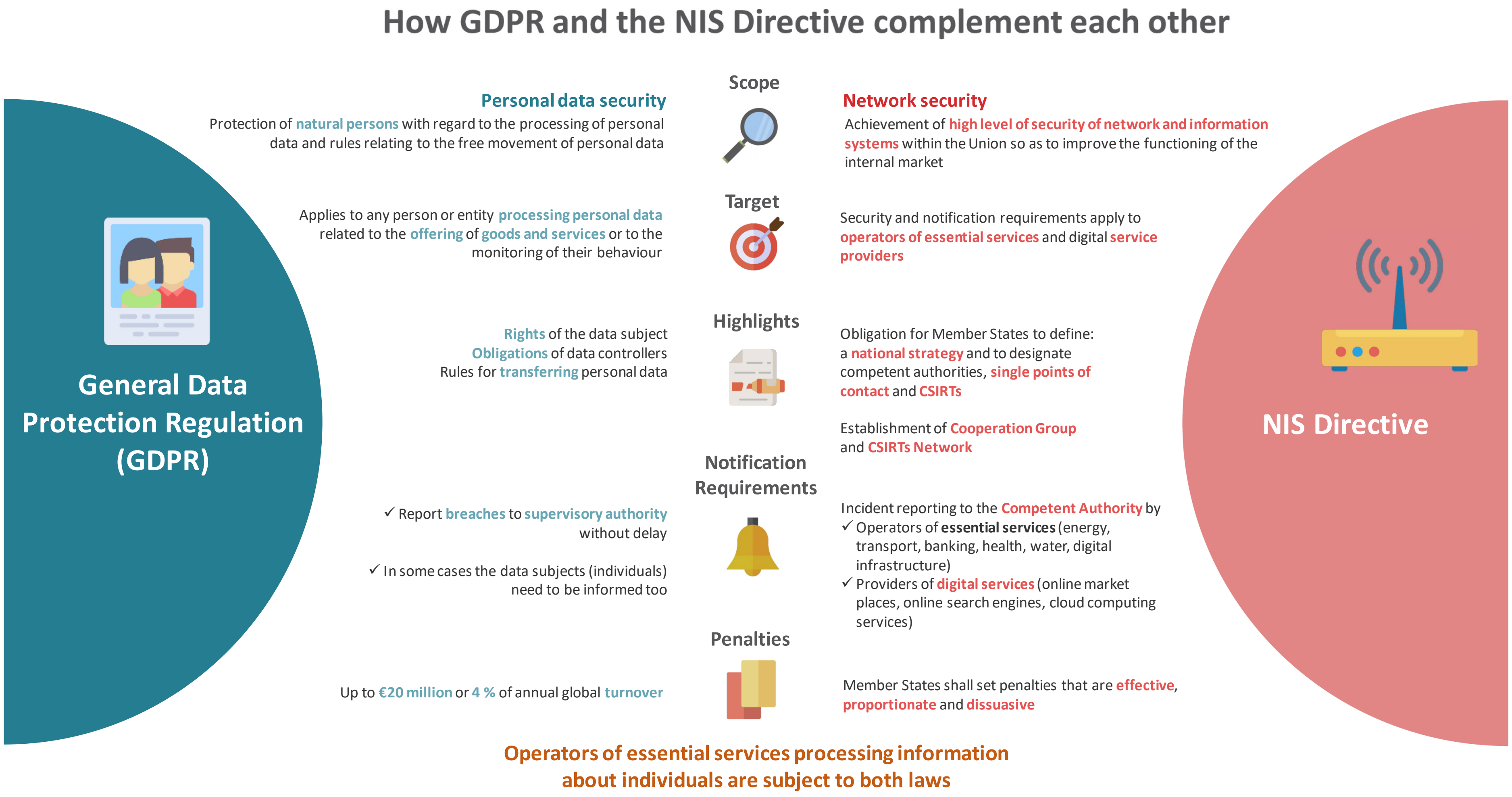
21 In parallel, the **General Data Protection Regulation**[32] (GDPR) came into force in 2016 and applied from May 2018. Its objective is to protect European citizens' personal data by setting rules on its processing and dissemination. It grants data subjects certain rights and places obligations on data controllers (digital service providers) regarding the use and transfer of information. It also imposes notification requirements in case of breach and, in some cases, can levy fines. ***Figure 3*** illustrates how the NIS Directive and the GDPR they complement each other in their aims to strengthen cybersecurity and safeguard data protection.

22 Draft legislation currently under discussion includes the proposed Cybersecurity Act to strengthen ENISA and establish an EU-wide certification mechanism[33], the proposed regulation on production and preservation orders for e-evidence[34], and the proposed directive on e-evidence[35]. The 2018 proposal for a European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (hereafter referred to as 'network of cybersecurity competence centres and a research competence centre') forms part of the 2017 cybersecurity package[36].

23 It can be difficult to get a sense of the breadth of the policy and legislative framework that touches on cybersecurity and how it affects our daily lives.

24 ***Figure 4*** attempts to chart the intersection of different legislative acts and other activities with the life of a fictitious European citizen.

Figure 3 – How the GDPR and the NIS Directive complement each other



How GDPR and the NIS Directive complement each other

General Data Protection Regulation (GDPR)

NIS Directive

Scope

Personal data security

Protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data

Network security

Achievement of high level of security of network and information systems within the Union so as to improve the functioning of the internal market

Target

Applies to any person or entity processing personal data related to the offering of goods and services or to the monitoring of their behaviour

Security and notification requirements apply to operators of essential services and digital service providers

Highlights

Rights of the data subject
Obligations of data controllers
Rules for transferring personal data

Obligation for Member States to define: a national strategy and to designate competent authorities, single points of contact and CSIRTs

Establishment of Cooperation Group and CSIRTs Network

Notification Requirements

✓ Report breaches to supervisory authority without delay

✓ In some cases the data subjects (individuals) need to be informed too

Incident reporting to the Competent Authority by

✓ Operators of **essential services** (energy, transport, banking, health, water, digital infrastructure)

✓ Providers of digital services (online market places, online search engines, cloud computing services)

Penalties

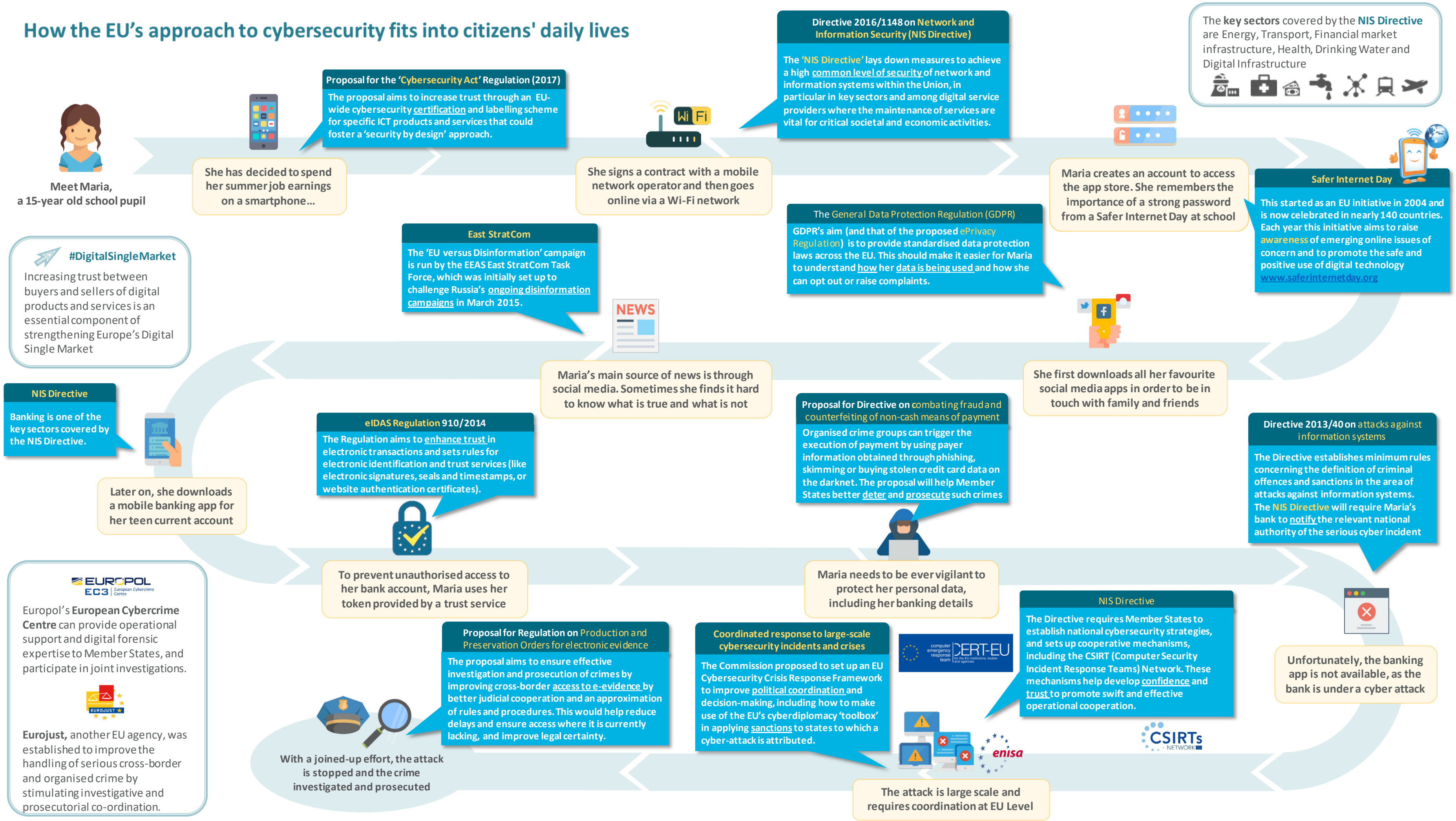
Up to €20 million or 4 % of annual global turnover

Member States shall set penalties that are effective, proportionate and dissuasive

Operators of essential services processing information about individuals are subject to both laws

Source: ECA.

Figure 4 – How the EU’s approach to cybersecurity fits into citizens’ daily lives



How the EU’s approach to cybersecurity fits into citizens' daily lives

Meet Maria, a 15-year old school pupil

She has decided to spend her summer job earnings on a smartphone…

Proposal for the ‘Cybersecurity Act’ Regulation (2017)

The proposal aims to increase trust through an EU-wide cybersecurity certification and labelling scheme for specific ICT products and services that could foster a ‘security by design’ approach.

She signs a contract with a mobile network operator and then goes online via a Wi-Fi network

Directive 2016/1148 on Network and Information Security (NIS Directive)

The ‘NIS Directive’ lays down measures to achieve a high common level of security of network and information systems within the Union, in particular in key sectors and among digital service providers where the maintenance of services are vital for critical societal and economic activities.

The **key sectors** covered by the **NIS Directive** are Energy, Transport, Financial market infrastructure, Health, Drinking Water and Digital Infrastructure

Maria creates an account to access the app store. She remembers the importance of a strong password from a Safer Internet Day at school

Safer Internet Day

This started as an EU initiative in 2004 and is now celebrated in nearly 140 countries. Each year this initiative aims to raise awareness of emerging online issues of concern and to promote the safe and positive use of digital technology www.saferinternetday.org

The General Data Protection Regulation (GDPR)

GDPR’s aim (and that of the proposed ePrivacy Regulation) is to provide standardised data protection laws across the EU. This should make it easier for Maria to understand how her data is being used and how she can opt out or raise complaints.

She first downloads all her favourite social media apps in order to be in touch with family and friends

Maria’s main source of news is through social media. Sometimes she finds it hard to know what is true and what is not

East StratCom

The ‘EU versus Disinformation’ campaign is run by the EEAS East StratCom Task Force, which was initially set up to challenge Russia’s ongoing disinformation campaigns in March 2015.

#DigitalSingleMarket

Increasing trust between buyers and sellers of digital products and services is an essential component of strengthening Europe’s Digital Single Market

NIS Directive

Banking is one of the key sectors covered by the NIS Directive.

Later on, she downloads a mobile banking app for her teen current account

eIDAS Regulation 910/2014

The Regulation aims to enhance trust in electronic transactions and sets rules for electronic identification and trust services (like electronic signatures, seals and timestamps, or website authentication certificates).

To prevent unauthorised access to her bank account, Maria uses her token provided by a trust service

Proposal for Directive on combating fraud and counterfeiting of non-cash means of payment

Organised crime groups can trigger the execution of payment by using payer information obtained through phishing, skimming or buying stolen credit card data on the darknet. The proposal will help Member States better deter and prosecute such crimes

Maria needs to be ever vigilant to protect her personal data, including her banking details

Directive 2013/40 on attacks against information systems

The Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. The NIS Directive will require Maria’s bank to notify the relevant national authority of the serious cyber incident

Unfortunately, the banking app is not available, as the bank is under a cyber attack

NIS Directive

The Directive requires Member States to establish national cybersecurity strategies, and sets up cooperative mechanisms, including the CSIRT (Computer Security Incident Response Teams) Network. These mechanisms help develop confidence and trust to promote swift and effective operational cooperation.

Coordinated response to large-scale cybersecurity incidents and crises

The Commission proposed to set up an EU Cybersecurity Crisis Response Framework to improve political coordination and decision-making, including how to make use of the EU’s cyberdiplomacy ‘toolbox’ in applying sanctions to states to which a cyber-attack is attributed.

The attack is large scale and requires coordination at EU Level

Proposal for Regulation on Production and Preservation Orders for electronic evidence

The proposal aims to ensure effective investigation and prosecution of crimes by improving cross-border access to e-evidence by better judicial cooperation and an approximation of rules and procedures. This would help reduce delays and ensure access where it is currently lacking, and improve legal certainty.

With a joined-up effort, the attack is stopped and the crime investigated and prosecuted

Europol’s **European Cybercrime Centre** can provide operational support and digital forensic expertise to Member States, and participate in joint investigations.

Eurojust, another EU agency, was established to improve the handling of serious cross-border and organised crime by stimulating investigative and prosecutorial co-ordination.

Wi Fi
NEWS
EUROPOL
EC3 European Cybercrime Centre
EUROJUST
computer emergency response team CERT-EU for the EU institutions, bodies and agencies
enisa
CSIRTs NETWORK

Source: ECA.

Constructing a policy and legislative framework

25 The EU's cyber ecosystem is complex and multi-layered, involving many stakeholders (see *Annex I*). Bringing together all of its disparate parts is a considerable challenge. Since 2013, there has been a concerted drive to bring coherence to the EU's cybersecurity field[37].

Challenge 1: meaningful evaluation and accountability

26 Establishing a causal relationship between the 2013 strategy and any changes seen is difficult, as the Commission has noted. The 2013 strategy's objectives were very broadly formulated, "expressing rather a vision than a measurable target"[38]. Developing action aligned to these broad aims is a challenge in the absence of measurable objectives. The updated cyber defence policy framework (2018) will aim to develop objectives setting the minimum level of cybersecurity and trust to be achieved. However, this will be limited to cyber defence; objectives defining the desired level of resilience for the EU as a whole have not been set.

27 Outcomes are rarely measured and few policy areas have been evaluated[39]. This is partly due to the recent implementation of many of the measures – legislative or otherwise – hindering a full evaluation of their impact. The challenge is to define meaningful assessment criteria that can help measure impact. Moreover, rigorous evaluation has not yet become the norm for cybersecurity generally. A shift is therefore needed towards a performance culture with embedded evaluation practices and standardised reporting. ENISA's current mandate does not extend to evaluating and monitoring the state of EU cybersecurity and readiness.

28 Evidence-based policymaking depends on the availability of sufficient reliable data and statistics to help monitor and analyse trends and needs. The absence of a compulsory and common monitoring system makes reliable data scarce. Indicators are often not readily available and are difficult to define[40]. Specific metrics have been developed in some areas though, such as the EU Policy Cycle, used for tackling serious and organised crime.

29 Few Member States regularly collect official data on cyber-related matters, hindering comparability. The EU has given to date little indication on the need to consolidate statistics at the European level[41]. There are also few independent EU-wide

analyses available covering key topics such as[42]: the economics of cybersecurity, including behavioural aspects (misalignment of incentives, information asymmetries); understanding the impact of cyber-failures and cybercrime; macro-statistics on cyber-trends and expected challenges; and the best solutions to address threats.

30 In light of the absence of specific objectives and scarcity of reliable data and well-defined indicators, assessment of the strategy's achievements has been largely qualitative to date. Progress reports often describe the activities carried out or milestones achieved, without a thorough measure of results. Furthermore, baselines for the assessment of systems' resilience have not yet been established. In addition, due to the lack of a codified definition of cybercrime it is nearly impossible to find relevant European indicators that would aid monitoring and evaluation.

31 Independent oversight of the implementation of cybersecurity policy differs between Member States. We surveyed national audit offices on their experience in auditing this field. Half of all respondents[43] had never audited the area. For those that had, the main focus of audits had been on: information governance; protection of critical infrastructure; information exchange and coordination between key stakeholders; incident preparedness, notification and response. Among the subjects less covered were awareness-raising measures and the digital skills gap. The results of these audits or evaluations are not always made public on the grounds of national security. A list of published audit reports by national audit offices is included in ***Annex III***.

32 Limitations in cyber-related skills (see also paragraphs ***82 to 90***) and difficulties in evaluating progress in cybersecurity were perceived as the main challenges to auditing government measures in this field.

Challenge 2: addressing gaps in EU law and its uneven transposition

33 The speed at which new technologies and threats emerge far outpaces the design and implementation of EU legislation. The Union's procedures were not designed with the digital age in mind: developing innovative and flexible procedures to ensure a policy and legal framework that is fit for purpose[44] to better anticipate and shape the future, is a critical priority[45].

34 Despite a drive for greater coherence, the legislative framework for cybersecurity remains incomplete (for some examples, see ***Table 1***). Fragmentation and gaps hamper achievement of the overall policy objectives and lead to inefficiencies. Gaps identified by the Commission in the strategy assessment included the Internet of Things, the balance of responsibilities between users and providers of digital products, and certain aspects left unaddressed by the NIS Directive. The proposed Cybersecurity Act attempts to address this in part by promoting security-by-design through an EU-wide certification scheme. Some stakeholders believe a clearly defined cyber industrial policy and a common approach to cyberespionage are still noticeably absent[46].

Table 1 – Gaps and uneven transposition in the legislative framework (non-exhaustive)

Policy area	Examples
Digital Single Market	o The present Consumer Sales Directive does not cover cybersecurity. The proposed directives on digital content[47] and online sales[48] aim to address this gap. o There are limited and diverse legal frameworks for duties of care in EU Member States, giving rise to legal uncertainty and difficulty in enforcing legal remedies[49]. o Policies on software vulnerability disclosures are being developed at different speeds across Member States, with no overarching legal framework at the EU level to enable a coordinated approach[50].
Strengthening network and information security	o Member States are free to include sectors omitted from the NIS Directive[51]. The accommodation industries, which are not covered, can be a gateway for other crimes, including human and drug trafficking and illegal immigration[52].
Fighting cybercrime	o Many Member States have not defined e-evidence in their national legislation[53] (see also paragraph *22*). o The current framework decision on non-cash payment fraud does not explicitly include non-physical payment instruments such as virtual currencies, e-money and mobile money, nor does it cover such acts as phishing, skimming and the possession and sharing of payer information[54]. o The Directive on Attacks against Information Systems does not directly address illegal data acquisition from the inside (e.g. cyberespionage), leading to challenges for law enforcement[55]. o In the wake of the Court of Justice of the European Union judgment on data retention[56], differences in the application of the legal framework among Member States has impeded law enforcement, potentially resulting in the loss of investigative leads and impairing effective prosecution of online criminal activity[57].

Source: ECA.

35 Applying some aspects of legislation remains voluntary both for national authorities and private operators. For example, within the framework of the Cooperation Group, evaluating the national strategies on the security of network and information systems and the effectiveness of CSIRTs is voluntary. Also, under the proposed certification scheme in the Cybersecurity Act, the application of certification for ICT products and services will be voluntary.

36 In the EU, cybersecurity is a prerogative of the Member States. Despite this, the EU has a critical role to play in creating the conditions for its Member States' capacities to improve, and for them to work together and generate trust. Yet given the wide differences among the Member States in terms of capacity and engagement[58], the provision of sensitive (national security) information will remain voluntary.

37 The inconsistent transposition of EU law among Member States can result in legal and operational incoherence, and prevents legislation from reaching its full potential. For example, Member States have differing interpretations of how dual-use export controls should be applied[59], with the result that some EU-based companies may be exporting technologies and services that can be used for cyber-surveillance and human rights violations through censorship or interception. The European Parliament has expressed concern about this[60].

38 In addition, protecting privacy and the freedom of expression calls for a tailored legislative response in order to strike the necessary balance between protecting fundamental values and achieving the EU's security imperatives. For example, how do we ensure end-to-end encryption while finding the best way to support law enforcement? Or how might we meet the aims of the GDPR while understanding its implications on publicly available information on registrants of domain names and holders of blocks of IP addresses? And how this can adversely affect law enforcement investigations[61]?

39 Legislation alone does not guarantee resilience. While the NIS Directive's objective is to achieve a high level of security across the EU, it explicitly focuses on achieving minimum, not maximum, harmonisation[62]. Gaps will continue to emerge as the cyber-landscape evolves.

Reflection points – policy framework

- What critical steps are needed to prompt a shift by policy-makers and legislators alike towards a stronger performance culture in cybersecurity, including defining overall resilience?
- How can research better contribute to generating the necessary data and statistics to enable meaningful evaluation?
- In what ways can the EU's legislative processes be adapted to be more flexible and take better account of the speed of technological and threat developments?
- How can the practice of developing metrics (indicators, targets) in the EU Policy Cycle be adapted, scaled-up and replicated for the cybersecurity domain as a whole?
- What can national audit offices learn from each other's approaches to auditing cybersecurity policies and measures?
- Which inconsistencies in the transposition and implementation of the EU legal framework are undermining a more effective response to cybersecurity gaps and cybercrime, and how could this be best addressed by Member States and EU institutions?
- How effective are EU export controls on cyber goods and services in preventing human rights abuses outside the EU?

Funding and spending

40 The EU has its sights set on becoming the world's safest online environment. Achieving this ambition requires significant efforts from all stakeholders, including a sound and well-managed financial footing.

Challenge 3: aligning investment levels with goals

Scaling up investment

41 Total global cybersecurity spending as a percentage of GDP is estimated to be about 0.1 %. In the United States[63], this rises to about 0.35 % (including the private sector). As a percentage of GDP, US federal government spending is around 0.1 %, or around $21 billion budgeted for 2019[64].

42 Spending in the EU has been low by comparison, fragmented and often not backed by concerted government-led programmes. Figures are hard to come by, but EU public spending on cybersecurity is estimated to range between one and two billion euros per year[65]. Some Member States' spending as a percentage of GDP is one-tenth of US levels, or even lower[66]. The EU and its Member States need to know how much they are investing collectively to know which gaps to close.

43 It is difficult to form a comprehensive picture in the absence of clear data owing to cybersecurity's cross-cutting nature and because cybersecurity and general IT spending are often indistinguishable[67]. Our survey has confirmed that it is difficult to obtain reliable statistics on spending in both the public and private sectors. Three-quarters of the national audit offices reported having no centralised overview of cyber-related government spending, and not one Member State obliged public entities to report cybersecurity expenditure separately in their financial plans.

44 Scaling up public and private investment in Europe's cybersecurity firms is a particular challenge. Public capital is often available for the initial phases, but less so for the growth and expansion stages[68]. Numerous EU funding initiatives exist but are not being taken advantage of, largely due to red tape[69]. Overall, EU cybersecurity firms underperform against their international peers: fewer in number, the average amount of funding they raise is significantly lower[70]. Ensuring effective targeting and funding of start-ups is therefore crucial to achieving the EU's digital policy objectives.

Scaling up impact

45 Closing the cyber investment gap needs to yield useful outcomes. For example, despite the strength of the EU's research and innovation sector, results are not sufficiently patented, commercialised or scaled up to help strengthen resilience, competitiveness and digital autonomy[71]. This is especially the case when compared with the EU's global competitors. The paucity of properly harnessed results stems from a range of factors[72], including:

- the lack of a consistent transnational strategy to scale up the approach to fit the EU's wider digital needs for competiveness and increased autonomy;
- the length of the value chain cycle, which means tools soon become obsolete;
- the lack of sustainability as projects typically end with the dissolution of the project team and a discontinuation of support, including updates and patching solutions.

46 The Commission's proposal to establish a network of cybersecurity competence centres and a research competence centre is an attempt to overcome fragmentation in the cybersecurity research field and to spur investment at scale[73]. In total, there are some 665 centres of expertise across the EU.

Challenge 4: a clear overview of EU budget spending

47 A centralised overview of spending is important for transparency and improved coordination. Without this, it is difficult for policymakers to see how spending aligns with needs for meeting priority goals.

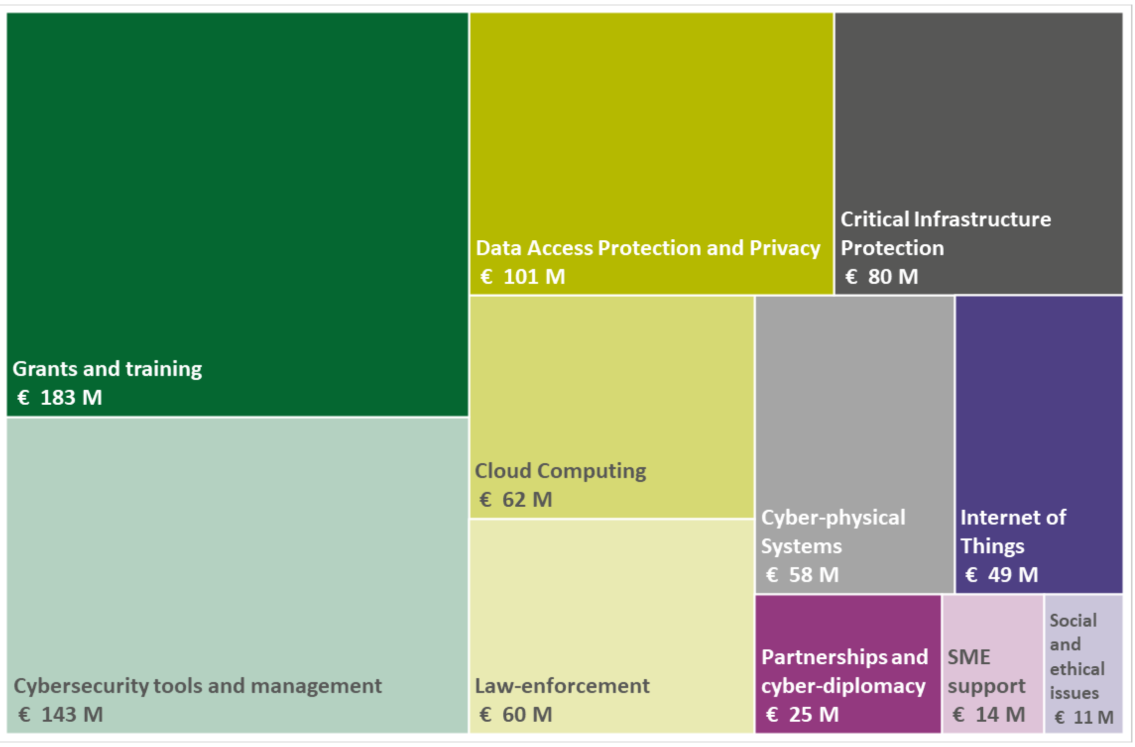
48 No dedicated budget funds the cybersecurity strategy. At the EU level, cybersecurity spending instead comes from the EU's general budget and Member States' co-funding. Our analysis reveals a complex set-up of at least ten different instruments under the EU general budget, but no clear picture of what money goes where (see ***Annex II***).

49 Establishing a clear spending overview of a topic that cuts across many policy areas is thus a sizeable challenge. Spending programmes are managed by different parts of the Commission, each with its own goals, rules and timetables. The picture is complicated further when factoring in Member States' co-financing, like under the Internal Security Fund (Police)[74].

Identifiable cybersecurity spending

50 In the 2014 – 2018 period, the Commission spent at least €1.4 billion implementing the Strategy[75], allocating the largest share to Horizon 2020[76] ('H2020'). H2020's funding is mainly channelled through the Secure Societies Challenge programme and in Leadership in enabling and industrial technologies projects[77]. We identified 279 contracted cybersecurity-related projects up to September 2018, with total EU-financing of €786 million[78]. ***Figure 5*** shows the typology of these projects based on this analysis.

Figure 5 – H2020 contracted cybersecurity research projects (€ millions)



Source: ECA.

51 A contractual public-private partnership (cPPP) was set up in 2016 to spur on the European cybersecurity industry. The aim was to channel €450 million from the H2020 programme into the cPPP and attract an additional €1.8 billion from the private sector by 2020. In the 18-month period to 31 December 2017, €67.5 million was channelled from H2020 into the cPPP and the private sector invested €1billion[79].

52 The fight against cybercrime is also supported by the Internal Security Fund – Police (ISF-P). The ISF-P supports studies, expert meetings, and communication activities; these amounted to nearly €62 million between 2014 and 2017. Member States can furthermore receive grants for equipment, training, research and data collection under shared management. Nineteen Member States have taken up these grants for €42 million.

53 Funds supporting judicial cooperation and the functioning of mutual legal assistance treaties, with a specific focus on the exchange of electronic data and financial information, amounted to €9 million under the Justice Programme managed by DG JUST.

54 The NIS Directive explicitly states that the CSIRTs must have adequate resources to effectively carry out their tasks[80]. Between 2016 and 2018, €13 million was available annually from the Connecting Europe Facility, to which Member States could apply to help implement the Directive's requirements. There has been no study determining the actual financial needs for the CSIRTs network and Cooperation Group to have an impact.

55 Several of the agencies' operational costs have been specifically aimed at cybersecurity or cybercrime activities. It is difficult, however, to extract any exact figures from the available public information.

56 The Budapest Convention (see paragraph *11*) has formed the backbone for EU external cyber spending. The EU spent around €50 million strengthening cybersecurity beyond its borders in the 2014-2018 period. Nearly half of this was through the Instrument contributing to Stability and Peace, with one main project – the €13,5 million GLACY+ – aiming to strengthen capacities worldwide to develop and implement cybercrime legislation and to increase international cooperation[81]. Elsewhere the focus of spending by other EU financial instruments was largely on the Western Balkans[82], as well the European neighbourhood, for example the Cybercrime@EaP project with the Eastern Partnership countries aims to improve international co-operation on cybercrime and e-evidence.

Other cybersecurity spending

57 It is not always possible to identify specific cybersecurity spending within EU programmes:

- H2020 funding has also been channelled through the Electronic Components and Systems for European Leadership (ECSEL) joint undertaking for cyber-physical systems. However, we were unable to determine what specifically related to cybersecurity from among the 27 projects totalling €437 million between 2015 and 2016.

- Up to €400 million is available for spending on cybersecurity and trust services under the European Structural and Investment Funds. This covers security and data protection investments to enhance interoperability and interconnection of digital infrastructure, electronic identification, and privacy and trust services.

58 In its 2018 operational plan, the European Investment Bank announced its intention to increase the financing of dual-use technology, cybersecurity and civilian security to up to €6 billion over a three-year period[83].

Looking ahead

59 The €2 billion cybersecurity component of the proposed new Digital Europe Programme[84] (DEP) for 2021-2027 is designed to strengthen the EU cybersecurity industry and overall societal protection, including by aiding implementation of the NIS Directive. The proposed network of cybersecurity competence centres and a research competence centre, which aims to lead to a more streamlined approach, is expected to form the main implementation mechanism for EU spending under the DEP.

60 Defence spending from the EU budget has recently increased through the European Defence Industrial Development programme, with €500 million to be allocated in 2019 and 2020[85]. This will focus on improving the coordination and efficiency of Member States' defence spending through incentives for joint development. It aims to generate a total of €13 billion of defence capability investment after 2020 through the European Defence Fund, some of which covers cyber defence[86].

Challenge 5: adequately resourcing the EU's agencies

61 The three core bodies at the heart of the EU's cybersecurity policy – ENISA, Europol's EC3, and CERT-EU (see ***Box 2***) are facing resourcing challenges at a time of heightened security-driven political priorities. The current allocation of human and financial resources in the EU agencies remains a challenge for them to meet expectations[87].

62 The agencies' requests for additional resources to meet rising demand have not been fully satisfied, potentially jeopardising the (timely) meeting of policy objectives. For example:

- Limited resources were a factor in preventing ENISA from fully achieving its objectives in 2017[88]. Additional resources were proposed in the 2017 package to match ENISA's new mandate.

- The supply of analysts and investment in ICT capabilities at Europol EC3 have not kept pace with demand[89]. Also, Europol EC's Joint Cybercrime Action Taskforce (J-CAT) is staffed by Member State and third country experts to support intelligence-led investigations. But the costs are largely borne by the sending states, discouraging the deployment of larger numbers of experts. A temporary, case-basis deployment has been devised with some Europol or EU Policy Cycle funding to permit participation by more countries.

63 Some constraints are self-inflicted. Many staff at CERT-EU and ENISA are contract agents, the recruitment procedures for which are typically slow. Others, such as attracting and retaining talent, stem from the agencies' inability to compete with private sector salaries or due to poor career progression prospects. ENISA therefore outsourced much of its work between 2014 and 2016[90].

64 Shortages in staff and the necessary tools can entail significant risks, especially concerning the gathering of threat intelligence. The volume of data from open and closed sources continues to swell and risks overwhelming analysts' abilities to conduct proper threat analyses. Without the right capabilities and tools in place to successfully integrate and interconnect such data, it will not effectively translate into usable threat intelligence that can be shared and analysed across the EU[91].

Reflection points – Funding and spending

- In what ways can the Commission and legislators streamline EU cybersecurity spending and more explicitly align it to clearly defined goals?

- How can the shortfalls in the resourcing of the EU agencies be addressed in an over-arching manner taking account of the Union's needs and goals?

- What measures are being identified at EU and Member State level to reduce barriers to SMEs taking up investment capital to scale-up their activities?

- What concrete and sustained results are H2020 funds delivering to produce cybersecurity solutions?

- How are EU capacity building exercises strengthening capacities beyond its borders in line with EU values?

Building a cyber-resilient society

65 Cybersecurity governance deals with the management of threats and risks, the strengthening of capacity and awareness, and coordination and information-sharing built on a foundation of trust.

Challenge 6: strengthening governance and standards

Information security governance

66 Information security governance is about putting structures and policies in place to ensure data confidentiality, integrity and availability. More than just a technical issue, it requires effective leadership, robust processes, and strategies aligned with organisational objectives[92]. A subset of this is cybersecurity governance, which deals with all types of cyber-related threats, including targeted, sophisticated attacks, breaches or incidents that are difficult to detect or manage.

67 Cybersecurity governance models differ between Member States, and within them responsibility for cybersecurity is often divided among many entities. These differences could obstruct the cooperation needed to respond to large-scale, cross-border incidents and to exchange threat intelligence at the national – let alone the EU – level. Our survey of national audit offices revealed that weaknesses in public authorities' governance arrangements and risk management were perceived as the highest risks.

68 Although the consequences for private sector organisations can be severe, weaknesses in cyber governance abound. Nearly nine in ten organisations say their cybersecurity function does not fully meet their needs[93], and cybersecurity officers are often at least two levels removed from the board[94].

69 The EU's company law directives set no specific requirements on the disclosure of cyber risks. In the United States, the Securities and Exchange Commission recently issued non-binding guidance to assist public companies in preparing disclosures on cybersecurity risks and incidents[95]. The Joint Committee of the European Supervisory Authorities[96] (ESAs) warned of the increasing in cyber risks, encouraged financial institutions to improve fragile IT systems, and to explore inherent risks to information security, connectivity, and outsourcing[97].

70 Strengthening the information security governance of SMEs is especially difficult since, more often than not, they are unable to implement the appropriate systems. SMEs lack suitable guidelines on applying information security and privacy requirements and mitigating technology risks[98]. Key challenges are therefore better understanding their needs and providing the necessary incentives and support.

71 The lack of a coherent, international cybersecurity governance framework impairs the international community's ability to respond to and limit cyberattacks. It is important, therefore, to forge consensus on such a governance framework that best reflects the EU's interests and values[99]. Attempts to set binding international cyberspace norms are becoming increasingly fraught, as seen in the lack of consensus within the UN Group of Governmental Experts in 2017 on how international law should apply to state responses to incidents.

72 To strengthen its agenda on cyberspace governance, the EU has also formalised six cyber partnerships to establish regular policy dialogues aiming to build trust and common areas for cooperation[100]. Outcomes are mixed; but, overall, in the international domain, the EU cannot yet be considered a "major cybersecurity actor" although it has raised its profile[101].

Information security at the EU institutions

73 Each EU institution has its own information security governance rules. An inter-institutional agreement provides for information security assistance from the Commission for the other institutions and agencies. The EU institutions and bodies have recognised the need to develop their cyber capacities and risk management approaches in a coherent manner. The Commission, Council and EEAS are to present a report in 2020 to the Horizontal Working Party on Cyber Issues on governance and the progress made in clarifying and harmonising cybersecurity governance at the EU institutions and agencies[102].

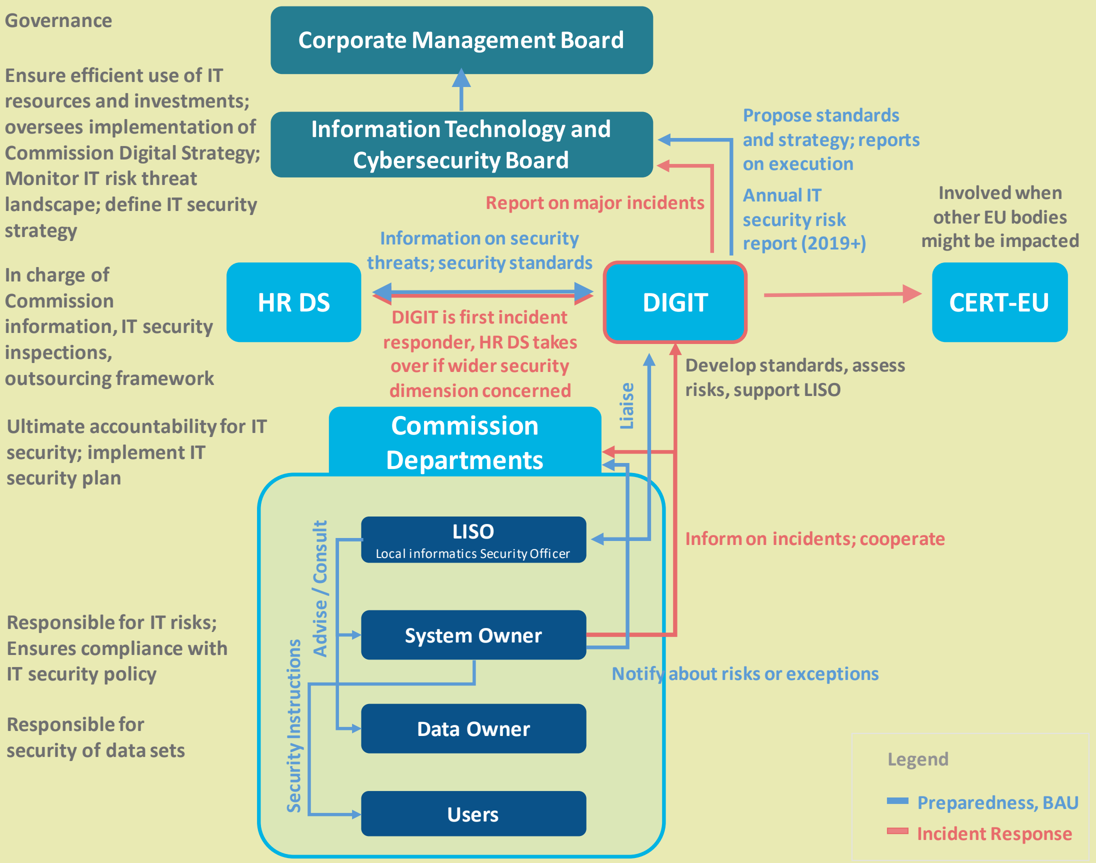
74 Within the Commission, the Directorate-General for Informatics (DIGIT) is responsible for the security of IT infrastructure and services (see ***Box 3***). The Commission's Digital Strategy's main IT security objectives are embedding IT security in management processes; provision of (cost-) effective infrastructure and resilience; widening the scope of incident detection and response; and integrating IT and security governance[103]. The Commission, under its provider contract, ensures that almost all software is actively maintained, and that only vendor-supported software is used[104].

75 The importance of protecting the institutions also stretches to the EU's CSDP missions and structures worldwide. One of the priorities of the EU's Cyber Defence Policy Framework (2018 update) is to enhance the protection of CSDP communication and information systems used by EU entities. An internal EEAS Cyber Governance Board is now in place and met for the first time in June 2017[105].

Box 3

Protecting the Commission's information systems

The Commission's roughly 1 300 systems and 50 000 devices are continuously targeted by cyberattacks. Responsibility for IT is decentralised, as illustrated in the figure below. Information and IT security are based on a common IT security plan set by DIGIT. The Information Technology and Cybersecurity Board acts as the Commission's de facto Chief Information Security Officer and links the operational side of IT security to the Commission's top management, represented by the Corporate Management Board.


Governance
Corporate Management Board
Ensure efficient use of IT resources and investments; oversees implementation of Commission Digital Strategy; Monitor IT risk threat landscape; define IT security strategy
Information Technology and Cybersecurity Board
Propose standards and strategy; reports on execution
Report on major incidents
Annual IT security risk report (2019+)
Involved when other EU bodies might be impacted
Information on security threats; security standards
In charge of Commission information, IT security inspections, outsourcing framework
HR DS
DIGIT
CERT-EU
DIGIT is first incident responder, HR DS takes over if wider security dimension concerned
Develop standards, assess risks, support LISO
Liaise
Ultimate accountability for IT security; implement IT security plan
Commission Departments
LISO
Local informatics Security Officer
Inform on incidents; cooperate
Advise / Consult
Responsible for IT risks; Ensures compliance with IT security policy
System Owner
Notify about risks or exceptions
Security Instructions
Responsible for security of data sets
Data Owner
Users
Legend
Preparedness, BAU
Incident Response

Source: ECA, based on Commission Decisions[106].

DG Human Resources and Security's (DG HR DS) main task is to protect the Commission's staff, information and assets. It also carries out security investigations of incidents that have a broader security dimension than IT only, thus feeding into its counter-intelligence and counter-terrorism activities.

DIGIT is responsible for IT security and hosts CERT-EU (Computer Emergency Response Team). Established in 2011, CERT-EU runs on an annual budget of about €2.5 million per year and has about 30 staff. It is the first responder in any information security incident that concerns several institutions yet does not operate on a 24/7 basis. It hosts an information-sharing platform. In 2018, CERT-EU signed a non-binding memorandum of understanding with ENISA, EC3 and the European Defence Agency to strengthen cooperation and coordination. It also has a technical agreement with NATO's computer incident response capability (NCIRC).

Threat and risk assessments

76 Well-founded and continuous threat and risk assessments are important tools for public and private organisations alike. However, there is no standard approach to classifying and mapping cyber threats or to risk assessments, meaning assessments' content varies considerably, posing a challenge to a coherent EU-wide approach to cybersecurity[107]. Furthermore, they often rely on the same sources or even other threat assessments, resulting in an echo chamber resounding with repeat findings[108], at the risk of paying insufficient attention to other threats. This is exacerbated by a continued reluctance to share information and under-reporting of incidents.

77 The Hybrid Fusion Cell[109] embedded within the EEAS was established to improve situational awareness and support decision-making through analysis-sharing but needs to broaden its expertise, including in cybersecurity. In parallel, CERT-EU provides EU institutions, bodies and agencies with reports and briefings regarding cyber threats targeted at them.

78 ENISA has noted in the past that many Member States have a qualitative understanding of threats and that there is a need for more cyber-threat modelling[110]. Monitoring capacity for strategic analysis will strengthen overall understanding. However, threat assessments could cover not only technological threats, but also socio-political and economic threats to ensure a more comprehensive picture, as well as threat drivers and actors' motives.

Incentives

79 There are still too few legal and economic incentives for organisations to notify and share information about incidents. Fearing reputational damage, many organisations still prefer to handle cyberattacks discretely or to pay off the perpetrators. It remains to be seen how effectively the NIS Directive will be in raising the level of notifications. The Commission expects improvements to materialise primarily at the national level, but the Cybersecurity Act will add an EU-wide view.[111]

80 By embedding certain standards in its procurement, public authorities have significant leverage over suppliers as buyers of digital products and services through public procurement, and research and programme funding (for example, by requiring the adoption of certain technical standards like Internet Protocol IPv6 to help in the fight against cybercrime). Currently, though, there is no joint procurement framework for cybersecurity infrastructure[112]. There is much that the Commission can do in this regard. The proposed DEP for the next multiannual financial framework aims to address the hitherto limited public sector investment in purchasing the latest cybersecurity technology.

81 Through its regulatory capacity, the Commission can ensure that the right standards are developed for widespread adoption to enhance security. The Commission and Europol work with internet governance bodies like ICANN (see paragraph ***38***) and RIPE-NCC[113], which is essential to putting the right cybercrime architecture in place to support law enforcement and the judicial authorities.

Challenge 7: raising skills and awareness

82 ENISA has pointed out that users play a critical role against cyberattacks and that strengthening skills, education and awareness is key to building a cyber-resilient society[114]. Individuals, at work or at home, who are well-versed in spotting the warning signs and armed with the right techniques can slow down or prevent attacks.

83 Of particular concern is the growing asymmetry between the know-how needed to commit a cybercrime or launch a cyberattack, and the skills needed to defend against it. The crime-as-a-service model has lowered the barriers of entry to the cybercriminal market: individuals without the technical knowledge to build them can now rent botnets, exploit kits or ransomware packages.

Training, skills and capacity development

84 The world faces a growing cybersecurity skills shortfall; the workforce gap has widened by 20 % since 2015[115]. Traditional recruitment channels are not meeting demand, including for managerial and interdisciplinary positions[116]. Nearly 90 % of the global cybersecurity workforce is male; the persistent lack of gender diversity restricts the talent pool further[117]. Moreover, at universities, cyber-related subjects are under-represented on non-technical programmes.

85 Training and education is needed across the board, among civil servants, law enforcement officers, judicial authorities, the armed forces and educators. For example, the judicial courts need to be able to deal with the fast-changing technical particularities of cybercrime and its victims[118]; there are currently no EU-wide standards for training and certification[119]. At the EU institutions, getting the right skills mix is important. Without the right skills mix in place, the institutions may be unable to properly define scope, identify the right partners and security needs, or lack the capacity to manage programmes. This in turn may undermine the effectiveness of EU programmes or policy development.

86 While Member States are responsible for education policies at the EU level, numerous training activities (see ***Table 2***) and exercises (see ***Box 4***) are already taking place. The EU can help work EU-wide standards into the learning curricula across all relevant disciplines[120]. In the area of digital forensics, for example, common training standards are necessary to facilitate the path to evidence admissibility in Member States. Due to the cross-border nature of cybercrime multiple jurisdictions can be involved, which requires training at the EU level. And yet, CEPOL, the EU's law enforcement training agency, has noted that more than two-thirds of Member States do not provide regular cyber training to law enforcement officials[121]. The EU can also potentially identify ways to synergise education and training between the civilian and military spheres[122]. That said, ENISA has found that while current training opportunities in critical sectors are extensive, they do not sufficiently target the resilience of critical infrastructure[123].

Table 2 – Some of the EU's cyber-related training initiatives

European Defence Agency projects, e.g. exercise support by the private sector and the Cyber Ranges project	European Security and Defence College network (providing civilian-military training), including Cyber Education, Training Exercise and Evaluation Platform	ENISA training, offering training programmes where the commercial market may fail to provide them
Europol, CEPOL, ECTEG[124] training programmes – including the Training Governance Model and Training Competency Framework (incl. certification)	Competence Centre Network and Research Competence Centre (proposed)	Measures on encryption proposed in the 11th Security Union Progress Report
EU-NATO cooperation on cyber-defence training and education	Military Erasmus Programme	European Judicial Training Network

Source: ECA.

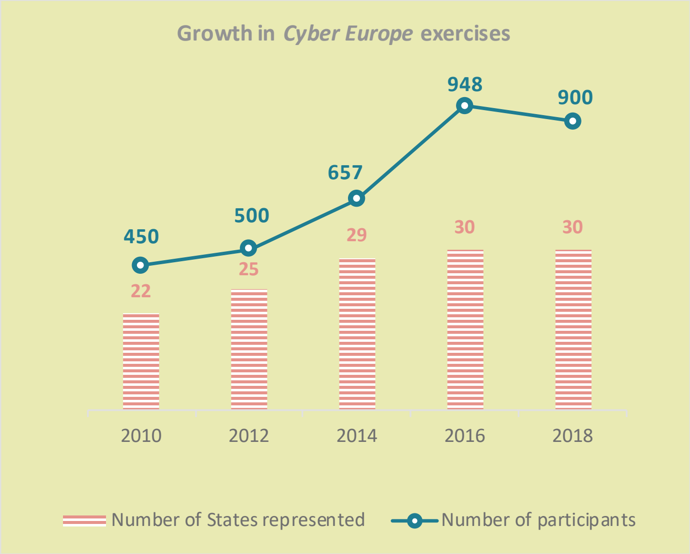
87 The EU has posted counter-terrorism and security experts to 17 delegations to reinforce the link between the EU's internal and external security[125]. Notwithstanding resource constraints, greater cyber know-how could help put in place the right projects, as well as identify synergies with other programmes or sources of funding[126]. It could also raise cybersecurity's profile in political dialogue, although it would have to compete with many other priorities, like migration, organised crime or returning foreign fighters.

Box 4

Exercises

Exercises are important elements of cyber education and training, offering prime opportunities to boost preparedness by testing capabilities, offering responses to real-life scenarios and building networks of working relationships. Since 2010, their frequency has increased markedly.

Participants take part on site or remotely. There are post-exercise assessments to identify lessons learned, although these may not yet be percolating fully between the strategic/political, operational and technical layers[127].



Source: ECA, based on ENISA documents.

EU and NATO's flagship exercises – the biennial Cyber Europe (operational) and the annual Locked Shields (technical) – garner over 1 000 participants from around 30 participating states. Both exercises focus on protecting and maintaining critical infrastructure in simulated attack scenarios. The exercises have increased in depth considerably, with both now including media, legal and financial policy elements to improve practitioners' situational awareness The parallel and coordinated PACE exercises (strategic) test EU-NATO interaction in a hybrid crisis scenario.

These are not the only international exercises. ENISA organises an annual cyber challenge, in which teams compete to solve security-related challenges like web and mobile security, crypto puzzles, reverse engineering, ethics and forensics. The first ministerial-level exercise, EU CYBRID, took place in September 2017, focusing on strategic decision-making. In 2018 the NATO-affiliated exercise, Crossed Swords, was launched to improve the offensive elements of its Locked Shields exercise. NATO also organises the Cyber Coalition exercises.

A key challenge is to ensure the active involvement of all important stakeholders and the coordination of all the exercises, to avoid duplication and share lessons learned efficiently.

Awareness

88 Citizens are often vectors for attacks and spreading disinformation, since they are likely to be unwittingly exposed to vulnerabilities in cheap and widely distributed devices and software or fall victim to social engineering. Awareness-raising is therefore essential to building effective cyber resilience, yet it is by no means an easy task since it is difficult for non-experts to understand cybersecurity's complexity and the associated risks.

89 The annual European Cyber Security Awareness Month (ECSM) and Safer Internet Day are examples of awareness-raising. Seven non-EU Member States have now joined the ECSM[128]. Europol's *Say No!* campaign aims to reduce the risk of children falling victim to sexual coercion and extortion online. Reducing the risk is important because at present, few attack victims currently report these crimes to the police[129].The Commission acknowledges that the cybersecurity strategy has been only "partially effective" in raising citizens' and businesses' awareness[130]. This is due to the scale of the task, limited resources, Member States' uneven engagement, and a lack of scientific evidence on how to best raise and measure awareness.

90 The challenge for the Commission and relevant agencies is to ensure that awareness-raising measures are: well-targeted and publicised; inclusive; follow the threat landscape; avoid unintended effects like "security fatigue"[131]; and develop evaluative methods and metrics to assess their effectiveness. This should apply in equal measure within the EU institutions themselves, where the culture of awareness needs improving[132].

Challenge 8: better information exchange and coordination

91 Cybersecurity requires cooperation between public and private sectors, primarily in terms of sharing information and exchanging best practices. Trust is essential at all levels to create the right environment for the sharing of sensitive information across borders. Poor coordination leads to fragmentation, duplication of efforts and a dispersal of expertise. Effective coordination can result in tangible successes, like the shutdown of darkweb marketplaces[133]. Despite the progress achieved in recent years, levels of trust are still "insufficient"[134] at the EU level and in some Member States[135].

Coordination among EU institutions and with Member States

92 One of the aims of the Cybersecurity Strategy, and the cooperative structures introduced by the NIS Directive, has been to strengthen trust among stakeholders. The assessment of the strategy recognised that a foundation for strategic and operational cooperation at the EU level had been laid[136]. Despite this, coordination in general is "insufficient"[137]. The challenge is to ensure that information exchange is not only meaningful but also permits a complete overview of the big picture. Reaching a common understanding based on accepted terminology is an important factor in this regard (see ***Box 5***).

93 The ENISA evaluation noted, however, that the EU's approach to cybersecurity was not sufficiently coordinated, resulting in a lack of synergies between ENISA's activities and those of other stakeholders. Cooperation mechanisms are still relatively immature[138]; the Cybersecurity Act intends to address this by strengthening ENISA's coordinating role. The desire to enhance cooperation was the rationale behind the memorandum of understanding signed in 2018 between ENISA, EDA, Europol EC3, and CERT-EU[139]. A priority for the Commission in the coming years will be to ensure proper alignment between policy initiatives, needs and investment programmes in order to overcome fragmentation and generate synergies[140].

94 Coordination functions are embedded within various institutional bodies. The Task Force on the Security Union was established to play a central role in coordinating the Commission's different Directorates-General with a view to supporting the Security Union's agenda[141]. DG CNECT chairs the Task Force's sub-working group on cybersecurity.

95 At the Council, cybersecurity is handled by the Horizontal Working Party on Cyber Issues (HWP), which coordinates strategic and horizontal cyber issues, and helps prepare exercises and evaluate their results. It works closely with the Political and

Security Committee, which has a central decision-making role in relation to any cyber-related diplomatic measures (see ***Box 6*** in next chapter). Since cybersecurity is a cross-cutting subject, coordinating all relevant interests is not straightforward: no fewer than 24 working parties and preparatory bodies have recently dealt with cyber-related issues[142].

96 The two latest legislative proposals on strengthening ENISA (2017) and on establishing a network of cybersecurity competence centres and a research competence centre (2018) are specifically designed to address the fragmentation and duplication of effort. A driving factor behind the network of cybersecurity competence centres and a research competence centre has been the need to fill the gap that the NIS Directive's cooperative structures do not fill, since they were not designed to support the development of "cutting edge" solutions.

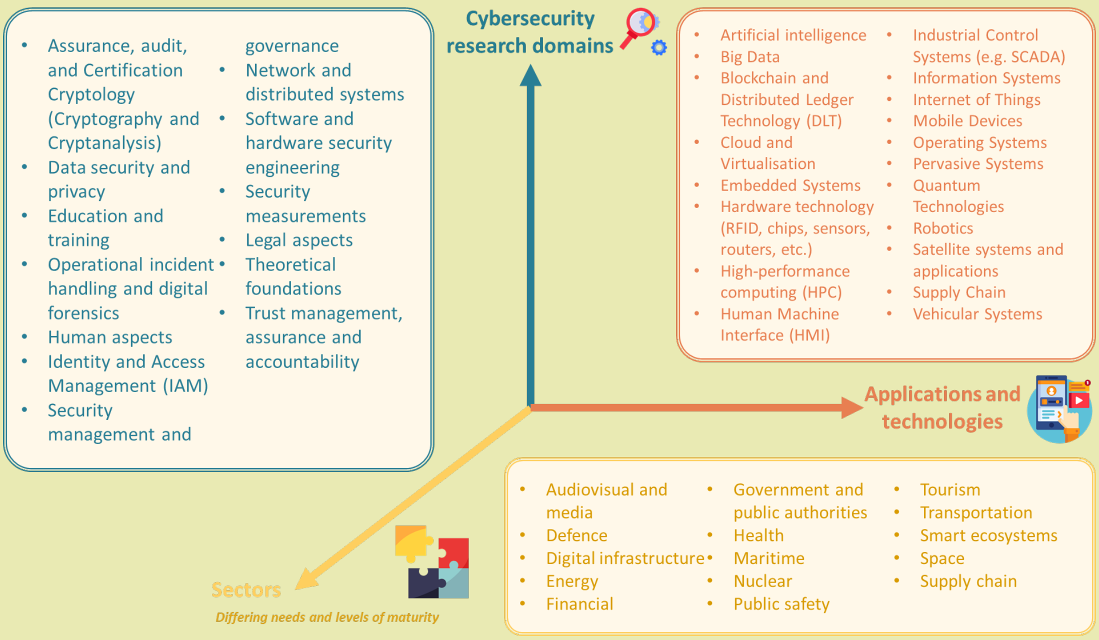
Box 5

Attempting to speak the same cyber language: *technological coherence*

Terminological clarity improves situational awareness and coordination[143] and helps establish precisely what constitutes a threat and a risk.

The Commission's Joint Research Centre (JRC) has recently developed a revised research taxonomy drawn from different international standards[144]. Its aims are to become a point of reference for use as an index by research entities across Europe.

Cybersecurity taxonomy



Cybersecurity research domains

- Assurance, audit, and Certification
  Cryptology (Cryptography and Cryptanalysis)
- Data security and privacy
- Education and training
- Operational incident handling and digital forensics
- Human aspects
- Identity and Access Management (IAM)
- Security management and governance
- Network and distributed systems
- Software and hardware security engineering
- Security measurements
- Legal aspects
- Theoretical foundations
- Trust management, assurance and accountability

Applications and technologies

- Artificial intelligence
- Big Data
- Blockchain and Distributed Ledger Technology (DLT)
- Cloud and Virtualisation
- Embedded Systems
- Hardware technology (RFID, chips, sensors, routers, etc.)
- High-performance computing (HPC)
- Human Machine Interface (HMI)
- Industrial Control Systems (e.g. SCADA)
- Information Systems
- Internet of Things
- Mobile Devices
- Operating Systems
- Pervasive Systems
- Quantum Technologies
- Robotics
- Satellite systems and applications
- Supply Chain
- Vehicular Systems

Sectors

Differing needs and levels of maturity

- Audiovisual and media
- Defence
- Digital infrastructure
- Energy
- Financial
- Government and public authorities
- Health
- Maritime
- Nuclear
- Public safety
- Tourism
- Transportation
- Smart ecosystems
- Space
- Supply chain

Source: ECA, adapted by from the European Commission.

Until recently, the EU institutions and agencies had no common definitions. This is changing. In the framework of its blueprint, the Cooperation Group devised an incident taxonomy with the aim of facilitating efficient cross-border collaboration.

Cooperation and information exchange with the private sector

97 Cooperation between public authorities and the private sector is essential for strengthening overall levels of cybersecurity. Despite this, in its 2017 assessment of the Cybersecurity Strategy, the Commission found that information exchange between private stakeholders and between public and private sectors was "not yet optimal" due to a "lack of trusted reporting mechanisms and incentives to share information"[145], hampering the attainment of strategic goals. The Commission has also noted the absence of an efficient cooperation mechanism by which Member States work together to strategically enhance lasting industrial capabilities at scale[146].

98 Information Sharing and Analysis Centres (ISACs) are organisations set up to provide platforms and resources to facilitate information sharing between the public and private sectors as well as to gather information on cyber threats. They aim to build trust through sharing experience, knowledge and analysis, especially about root causes, incidents and threats. National and sectoral ISACs already exist in many Member States, but at the European level, they are still relatively limited[147]. However, they come with a number of challenges (resourcing constraints, difficulties in evaluating their success, ensuring the right structures to engage both public and private sectors, getting law enforcement authorities involved) that will need to be overcome if they are to contribute to helping implement the NIS Directive and building security capabilities at a European-wide level[148].

99 Close cooperation with the private sector is particularly vital to combat complex cybercrime, but its efficiency is uneven across Member States and depends on the level of trust[149]. Europol EC3, however, has established a series of advisory groups with private sector operators, EU institutions and agencies, and other international organisations to improve collaboration through networking, strategic intelligence-sharing and cooperation. They work to plans aligned with the goals of the EU Policy Cycle[150]. The criminal abuse of encryption is another area ripe with challenges calling for more cooperation with the private sector. Europol EC3 is currently examining options to host case-specific short-term attachments to the J-CAT (see paragraph ***62***) for experts from the private sector and academia.

100 A lack of efficient cooperation mechanisms afflicts the civilian and defence communities – both public and private. Areas posing a common challenge include cryptography, secure embedded systems, malware detection, simulation techniques, network and systems communication protection and authentication technologies. Promoting civil-military cooperation and supporting research and technology (in particular by supporting SMEs) are two of the priorities in the updated EU Cyber Defence Policy Framework (2018 update).

Reflection points – Building resilience

- How can an appropriate balance be struck at EU level between the need to mainstream cybersecurity policy and ensure an efficient coordination between the various actors and dispersal of responsibilities?
- How well prepared are EU institutions and agencies for the next big attack launched directly against them?
- How can the EU cyber-relevant agencies be made more attractive to talent?
- What further steps are needed to ensure adequate capacity across EU institutions and agencies to enable a coherent risk and threat assessment framework?
- In what ways are the European supervisory authorities (European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority) addressing cyber vulnerabilities inherent in the financial sector, and what can be learned from this for other sectors?
- With the overall shortfall in expertise, how can EU technical assistance for public authorities best be utilised to have the maximum overall impact in improving cyber resilience?
- How can the EU and Member States ensure a meaningful presence in international discussions to shape cyberspace governance and standards and promote EU values?
- Which EU and Member State-level awareness raising measures (including prevention efforts) are really making a difference, and what can the EU do to scale these up?
- What role is there for the EU to help bring gender diversity in the cybersecurity field?
- How can the EU and Member States enhance synergies between the civilian and defence communities, in line with the Cyber Defence Policy Framework (2018 update)?

Responding effectively to cyber incidents

101 Devising an effective response to cyberattacks is fundamental to stopping them in their tracks as early as possible. It is especially important that critical sectors, Member States and EU institutions be able to respond in a swift and coordinated way. Essential to this is early detection.

Challenge 9: effective detection and response

Detection and notification

102 Common detection tools help defeat the vast majority of attacks on a daily basis[151]. Nevertheless, digital systems have become so complex that preventing each and every attack is impossible. Their sophistication means attacks often evade detection for prolonged periods. Experts say, therefore, that the focus should be on rapid detection and defence[152]. However, some detection tools –such as automation, machine learning and behavioural analytics, which look at reducing risks, and analysing and learning from system behaviour – suffer from low adoption rates by businesses[153]. This is in part due to the generation of false positives, whereby non-threatening activities are mistaken as malicious.

103 Once a breach has been detected and analysed, swift notification and reporting is necessary so that other public and private entities can take preventive action, and the relevant authorities can support those affected. Many organisations are reluctant to acknowledge and report cyber incidents[154]. The early involvement of law enforcement authorities in the initial response to suspected cybercrimes and proactive information exchange with CSIRTs is also essential.

104 The previous lack of common EU requirements on incident notification risked delaying the communication of breaches and hindering the response, which the introduction of the NIS Directive sought to address (see paragraph *20*). Following the 2017 Wannacry attacks, the Commission concluded that the CSIRT network system was “not yet fully operational”[155]. As the implementation of the Directive continues, it remains to be seen whether the guidance developed by the Cooperation Group will be effective in overcoming the reluctance to report incidents[156].

105 Operators of essential services in certain sectors have multiple notification obligations (including to consumers) under existing EU regulations, which may impair the efficiency of the process. For example, operators in the financial and banking sectors are subject to different notification criteria, standards, thresholds and time frames under the GDPR, the NIS Directive, the Payment Services Directive, ECB/SSM, Target 2 and the eIDAS Regulation[157]. It is therefore important to streamline these obligations since, aside from constituting an unnecessary administrative burden, such heterogeneity might lead to fragmented reporting.

Coordinated response

106 Development of a European cybersecurity crisis cooperation framework is still a work in progress. The related 'blueprint'[158] (see paragraph ***18***) was therefore introduced to inject a cyber-perspective into the Integrated Political Crisis Response (IPCR) mechanism, improve situational awareness and ensure better integration with other EU crisis management mechanisms[159]. The blueprint involves EU institutions, agencies and Member States. Seamlessly integrating all these crisis response mechanisms is challenging[160]. The current lack of a joint secure communications network across EU institutions is also an important shortcoming[161].

107 The EU's capacity to respond to cyberattacks at the operational and political level in the event of a large-scale, cross-border incident has been labelled "limited", partly because cybersecurity is not yet integrated into existing EU-level crisis response coordination mechanisms[162]. The NIS Directive did not address this.

108 The recently proposed reform of ENISA, which envisaged a greater operational role in handling large-scale cybersecurity incidents, was not supported by the Member States, preferring that the agency's role should support and complement their own operational action [163]. There are already many CERTs/CSIRTs at the Member State level, but their capacities vary considerably. This constitutes an obstacle to the effective cross-border cooperation needed for large-scale incident responses[164].

109 We tried to map the different roles assigned to the various actors identified in the blueprint, but there were gaps which will need to be filled as implementation advances. One initially under-addressed area was law enforcement, although the EU Law Enforcement Emergency Response Protocol took effect in December 2018[165]. Ensuring that the blueprint is practical and that all parties know what to do is key to its success; this will need extensive testing in the coming years.

110 Effective response is about more than damage containment; assigning responsibility for attacks is also pivotal. Tracking and identifying perpetrators, above all in a hybrid attack, can be very difficult due to the growing abuse of anonymisation tools, cryptocurrencies and encryption. This is known as the attribution problem. Remedying this problem is not just a technical issue; it is also a criminal justice challenge. Legal and procedural differences between countries may impede criminal investigations and the prosecution of suspects. Addressing the attribution problem will need a more formalised operational exchange of information through clearer procedures with Europol or Eurojust's European Judicial Cybercrime Network, for example.

111 At the political level, the cyber diplomacy toolbox (see ***Box 6***) has been developed in order to support the settlement of international disputes in cyberspace by peaceful means. The creation of cyber rapid response teams and an initiative for mutual assistance in cyber security are two projects fostering enhanced information sharing which are being developed under the PESCO framework[166].

Box 6

The cyber diplomacy toolbox

The EU Joint EU Diplomatic Response to Malicious Cyber Activities[167], or "cyber diplomacy toolbox", grew out of the 2015 Council conclusions on cyber diplomacy[168]. Cyber diplomacy aims to develop and implement a common and comprehensive approach to cyberspace based on EU values, the rule of law, capacity-building and partnerships, promotion of the multi-stakeholder model of internet governance, and the mitigation of cybersecurity threats and greater stability in international relations.

The toolbox allows the EU and its Member States to mount a joint diplomatic response to malicious cyber activities making full use of measures within the Common Foreign and Security Policy. These can include preventive (e.g. awareness-raising, capacity-building), cooperative, stability and restrictive measures (e.g. travel bans, arms embargoes, freezing funds), or support to Member States' responses[169]. The idea is that further cooperation to mitigate threats and clearly signalling the likely consequences of a joint response may deter (potentially) aggressive behaviour.

A joint EU response to malicious cyber activities would be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity.

Integral to the success of the toolbox will be how well it is interwoven with the blueprint and IPCR (see paragraph ***106***), how well situational awareness is established through the quick and continuous sharing of information (including on elements of attribution)[170] and, finally, effective cooperation. Also key to the toolbox's successful deployment is effective and coordinated communication. So far, the toolbox has been used twice: to start a dialogue with the United States after the *Wannacry* attack[171], and to develop Council conclusions condemning the malicious use of ICT[172]. The operationalisation of the toolbox is ongoing; it remains to be seen how effective it will be in achieving its objectives.

Challenge 10: protecting critical infrastructure and societal functions

Protecting infrastructure

112 Much of the EU's critical infrastructure is operated through industrial control systems (ICS)[173]. Many of these were designed as stand-alone systems, with limited connectivity to the outside world. As components of ICS have been connected to the internet, they have become more vulnerable to outside interference. Maintaining and patching existing systems may no longer be possible, but upgrading them does not come quickly or cheaply. Efforts to enhance the security of critical infrastructure must therefore include the upgrading of ICS.

113 As industry continues to digitise (commonly known as "Industry 4.0"), the impact of a large-scale incident in one industrial sector may have knock-on effects elsewhere. ENISA has noted the importance of mapping the impact of critical sectors' mutual dependencies[174]. This is essential to understanding the potential spread of an incident and underpins well-coordinated responses.

114 The NIS Directive aims to enhance readiness in key sectors responsible for critical infrastructure. However, not all sectors are covered (see ***Table 1***)[175], which "reduces the effectiveness of the strategy"[176]: of particular concern in this regard is protecting the democratic integrity of elections from interference in electoral infrastructure and disinformation (see ***Box 7***). Aside from revising existing legislation, therefore, a key challenge will be seeing how to engage these sectors in effective responses to large-scale incidents.

115 Vulnerabilities in critical infrastructure do not stop at Europe's borders. A particular challenge for the Commission is encouraging candidate countries to adopt the same standards as Member States, for example in such areas as cyber-related legislation or the protection of critical infrastructure.

Box 7

Protecting critical societal functions: *fighting election interference*

In May 2019, some 400 million voters will go to the polls in the European parliamentary elections, the first to take place under the GDPR. These come in the wake of scandals surrounding the abuse of personal data for political micro-targeting and unprecedented coordinated disinformation ("Fake News") campaigns. The Commission has warned of likely cyber interference in these elections[177]; fighting this will require a whole-of-government and whole-of-society approach.

Election infrastructure

Organising elections is complex, and ensuring their protection and integrity is the Member States' responsibility. Interference in elections and electoral infrastructure may seek to influence voter preferences, turnout or the election process itself, including actual voting, and vote tabulation and communication. In the European Parliament elections, protecting the so-called "last mile" (the communication of results from the national capitals to Brussels) is a particularly critical challenge, given that no common security approach exists or has been tested for this[178].

The Commission's recent election package included measures to strengthen electoral cybersecurity, such as the appointment of national contact points to coordinate and exchange information in the run-up to the election. The sharing of best practices and lessons learned is of particular importance[179].

Election systems are not considered part of critical infrastructure[180], nor are they covered by the NIS Directive. Despite this, the Cooperation Group has developed practical guidance on election technology security to support public authorities. The national contact points are expected to meet in early 2019[181]. Member States are also encouraged to perform risk assessments on cyber threats to their electoral processes.

Disinformation

Disinformation is an increasingly important element of hybrid attacks that involves cyberattacks and the hacking of networks. These can be used to divide societies, sow mistrust and undermine confidence in democratic processes or other issues (for example, anti-vaccination or climate change). It has grown in scale, speed and range, and poses a genuine security threat to the EU.

The EU has taken a number of measures to address disinformation. Starting in 2015, the EEAS-based East StratCom Task Force was set up to challenge Russian disinformation campaigns[182]. Experts have praised its work in promoting EU policies, supporting independent media in the Neighbourhood, and forecasting, tracking and tackling disinformation.[183]. Still, the Task Force's resources are limited relative to the scale and complexity of disinformation campaigns[184]. A more systematic interaction with existing EU structures and improved strategic communication cooperation is needed[185] A new action plan[186] was endorsed by the European Council in December 2018.

More recently, the Commission, on the back of its April 2018 communication on tackling online disinformation[187], has developed a voluntary, self-regulatory code of practice[188], based on existing policy instruments, to which online platforms and the advertising industry have signed up[189]. Action includes helping to increase the trust-worthiness of content and supporting efforts to increase media and news literacy. An independent European network of fact-checkers has also been launched.

The Commission has stated that further regulatory measures may follow if the code of practice is not observed. Determining the effectiveness of measures will prove crucial, particularly deciding how to measure improvements in trust, transparency and accountability.

Another challenge will be finding ways to improve the detection, analysis and exposure of disinformation[190]. Active and strategic monitoring and analysis of open data sources is also needed[191]. Attempts to gain a better understanding of the threat environment should also cover emerging trends, such as “deepfakes” (fake videos made with the help of artificial intelligence and deep machine learning), as well as the tools needed to detect them.

Enhancing autonomy

116 The EU is a net importer of cybersecurity products and services, increasing the risk of technological dependence on, and vulnerability to, non-EU operators[192]. In particular, this reality undermines the security of the EU’s critical infrastructure, which is also supported by complex global supply chains. The risk is further exacerbated where non-EU operators acquire European cybersecurity firms. Member States are responsible for screening Foreign Direct Investments (FDI), and there is currently no EU-wide screening mechanism[193].

117 Greater strategic autonomy is an objective in the EU Global Strategy and the 2017 communication *Resilience, Deterrence and Defence*[194]. Addressing the myriad challenges presented in this report will help enhance this desired autonomy. No single measure will achieve this by itself.

Reflection points – Effective response

- How has the NIS Directive improved notification of cyber incidents in critical sectors and beyond?
- How well are the EU institutions internalising crisis response coordination for a major cyber incident?
- How can cyber diplomacy play a more prominent role in the EU external actions?
- Are the current EU structures and actions to tackle disinformation proportionate to the scale and complexity of the problem?

Concluding remarks

118 In recent years the EU and its Member States have advanced cybersecurity up the agenda in order to improve overall cyber resilience. Yet achieving a greater level of cybersecurity in the Union remains a monumental undertaking. In this briefing paper, we have sought to highlight some of the main challenges to the EU's ambition of becoming the world's safest digital environment.

119 Our review shows that a shift towards a performance culture with embedded evaluation practices is needed to ensure meaningful **accountability and evaluation**. Some **gaps in the law remain, and existing legislation is not consistently transposed by Member States**. This can make it difficult for legislation to reach its full potential. Another challenge identified concerns the **alignment of investment levels with the strategic goals**, which calls for the scaling up of investment levels and its impact. This is more demanding when the EU and its Member States do not have a **clear overview of EU spending** in cybersecurity. There are also reported **constraints in the adequate resourcing of the EU's cyber-relevant agencies,** including difficulties attracting and retaining talent.

120 Available studies conclude that **cybersecurity governance can be strengthened** to boost the global community's ability to respond to cyberattacks and incidents. At the same time, preventing all attacks is impossible. Therefore, **rapid detection and response** and the **protection of critical infrastructure and societal functions**, together with better **Information exchange and coordination** between the public and private sectors are key challenges to be addressed. Finally, the growing global cybersecurity skills shortfall means that **raising skills and awareness** across all sectors and levels of society is also a vital challenge.

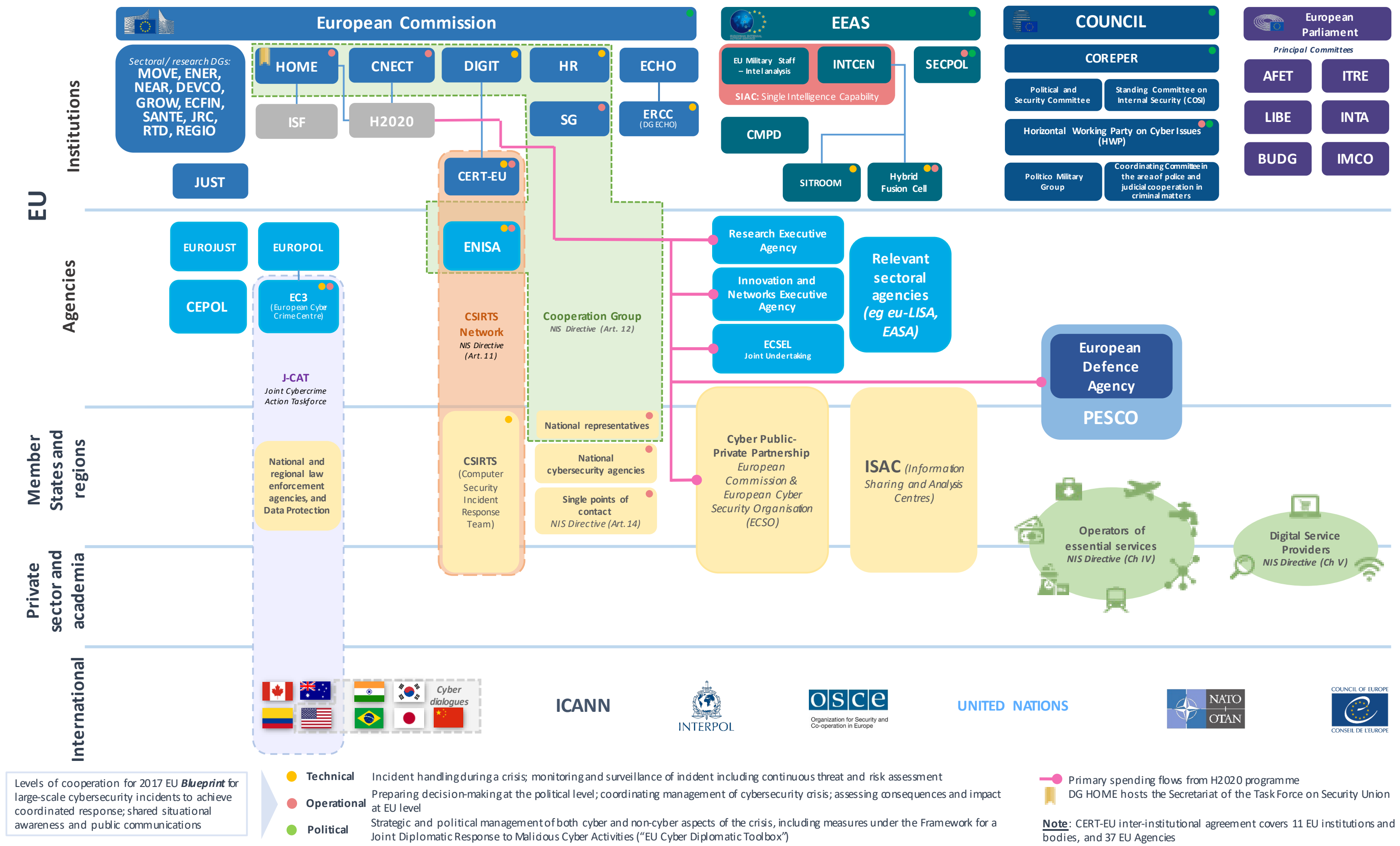
121 These challenges posed by cyber threats facing the EU and the broader global environment require continued commitment and an ongoing steadfast adherence to the EU's values.

This Briefing paper was adopted by Chamber III at its meeting of 14 February 2019.

For the Court of Auditors

Klaus-Heiner Lehne
President

Annex I — A complex, multi-layered landscape with many actors


EU
Institutions
Agencies
Member States and regions
Private sector and academia
International
European Commission
Sectoral/ research DGs:
MOVE, ENER, NEAR, DEVCO, GROW, ECFIN, SANTE, JRC, RTD, REGIO
JUST
HOME
CNECT
DIGIT
HR
ECHO
ISF
H2020
SG
ERCC
(DG ECHO)
CERT-EU
EEAS
EU Military Staff – Intel analysis
INTCEN
SIAC: Single Intelligence Capability
SECPOL
CMPD
SITROOM
Hybrid Fusion Cell
COUNCIL
COREPER
Political and Security Committee
Standing Committee on Internal Security (COSI)
Horizontal Working Party on Cyber Issues (HWP)
Politico Military Group
Coordinating Committee in the area of police and judicial cooperation in criminal matters
European Parliament
Principal Committees
AFET
ITRE
LIBE
INTA
BUDG
IMCO
EUROJUST
EUROPOL
CEPOL
EC3
(European Cyber Crime Centre)
J-CAT
Joint Cybercrime Action Taskforce
ENISA
CSIRTS Network
NIS Directive (Art. 11)
Cooperation Group
NIS Directive (Art. 12)
Research Executive Agency
Innovation and Networks Executive Agency
ECSEL
Joint Undertaking
Relevant sectoral agencies (eg eu-LISA, EASA)
European Defence Agency
PESCO
National and regional law enforcement agencies, and Data Protection
CSIRTS
(Computer Security Incident Response Team)
National representatives
National cybersecurity agencies
Single points of contact
NIS Directive (Art. 14)
Cyber Public-Private Partnership
European Commission & European Cyber Security Organisation (ECSO)
ISAC (Information Sharing and Analysis Centres)
Operators of essential services
NIS Directive (Ch IV)
Digital Service Providers
NIS Directive (Ch V)
Cyber dialogues
ICANN
INTERPOL
OSCE
Organization for Security and Co-operation in Europe
UNITED NATIONS
NATO
OTAN
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Levels of cooperation for 2017 EU ***Blueprint*** for large-scale cybersecurity incidents to achieve coordinated response; shared situational awareness and public communications

●	Technical	Incident handling during a crisis; monitoring and surveillance of incident including continuous threat and risk assessment
●	Operational	Preparing decision-making at the political level; coordinating management of cybersecurity crisis; assessing consequences and impact at EU level
●	Political	Strategic and political management of both cyber and non-cyber aspects of the crisis, including measures under the Framework for a Joint Diplomatic Response to Malicious Cyber Activities ("EU Cyber Diplomatic Toolbox")

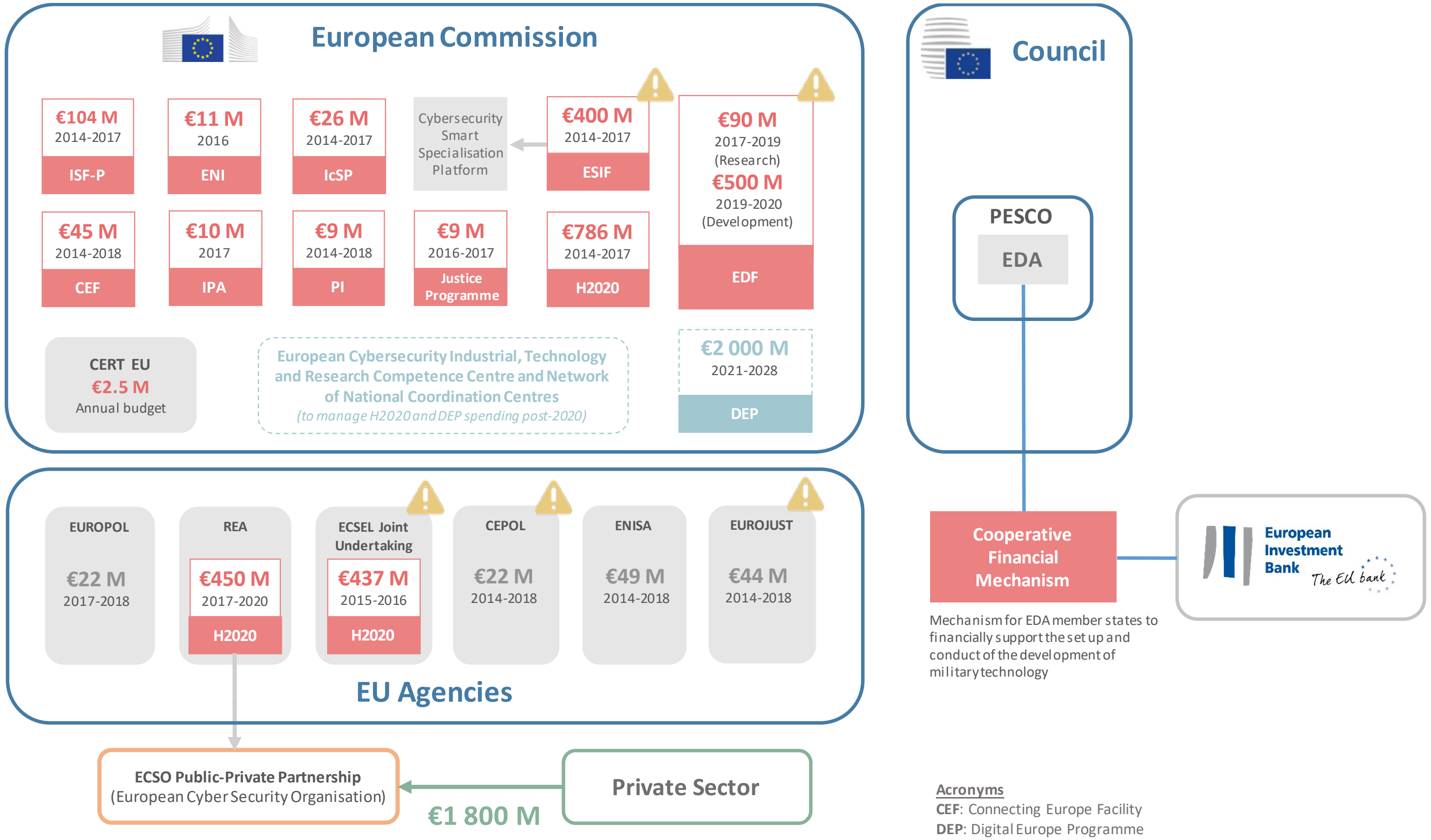
Primary spending flows from H2020 programme

DG HOME hosts the Secretariat of the Task Force on Security Union

Note: CERT-EU inter-institutional agreement covers 11 EU institutions and bodies, and 37 EU Agencies

Source: ECA.

Annex II — EU spending on cybersecurity since 2014



European Commission

€104 M 2014-2017 ISF-P

€11 M 2016 ENI

€26 M 2014-2017 IcSP

Cybersecurity Smart Specialisation Platform

€400 M 2014-2017 ESIF

€90 M 2017-2019 (Research) €500 M 2019-2020 (Development) EDF

€45 M 2014-2018 CEF

€10 M 2017 IPA

€9 M 2014-2018 PI

€9 M 2016-2017 Justice Programme

€786 M 2014-2017 H2020

CERT EU €2.5 M Annual budget

European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres *(to manage H2020 and DEP spending post-2020)*

€2 000 M 2021-2028 DEP

Council

PESCO

EDA

Cooperative Financial Mechanism

Mechanism for EDA member states to financially support the set up and conduct of the development of military technology

European Investment Bank *The EU bank*

EUROPOL €22 M 2017-2018

REA €450 M 2017-2020 H2020

ECSEL Joint Undertaking €437 M 2015-2016 H2020

CEPOL €22 M 2014-2018

ENISA €49 M 2014-2018

EUROJUST €44 M 2014-2018

EU Agencies

ECSO Public-Private Partnership (European Cyber Security Organisation)

€1 800 M

Private Sector

🟥 Instruments

- - - Under proposal

⚠ Figures incl. non cybersecurity-related spending

- For Europol, amounts are based on activity A.4 "Combatting Cybercrime" from multi-annual programming documents
- For ENISA, amount represents portion of agency budget funded by the EU budget
- For CEPOL and EUROJUST amounts presented relate to operational expenditure only

Acronyms

CEF: Connecting Europe Facility
DEP: Digital Europe Programme
EDF: European Defence Fund
ENI: European Neighbourhood Instrument
ESIF: European Structural and Investment Funds
H2020: Horizon 2020 programme
IcSP: Instrument contributing to Stability and Peace
IPA: Instrument for Pre-accession Assistance
ISF-P: Internal Security Fund – Police
PI: Partnership Instrument

Source: ECA, based on European Commission and EU agencies' documents

Annex III — EU Member State audit office reports

Type	Title (with hyperlink)	Year	MS
Compliance audits	Internal Control assessment note	2014	FR
	Certification Report for the accounts of the General Social Security Scheme (defence, foreign affairs)	2016	FR
	Certification of the State accounts	2016	FR
	Ensuring the security and preservation of Estonian national databases of critical importance	Fin. 2018 / not yet published	EE
	Effectiveness of internal controls in the protection of personal data in national databases	2008	EE
Performance / Value-for-money audits	Report on mitigation of cyber attacks	2013	DK
	RiR 2014:23 Information security in the civil public administration	2014	SE
	Report on the government's processing of confidential data on persons and companies	2014	DK
	The National Cyber Security Programme	2014	UK
	Report to the Budget Committee of the German Federal Parliament in accordance with § 88, paragraph 2, of the Federal Budget Code (BHO) – IT consolidation, Federal Government	2015	DE
	Report on access to IT systems that support the provision of essential services to Danish society	2015	DK
	Plaine de France Public Planning Authority	2015	FR
	'Cybersecurity Environment in Lithuania' a Lithuanian version a summary translated into English	2015	LT
	Public bodies' performance of cyber-security tasks in Poland (in PL)	2015	PL
	RiR 2015:21 Cybercrime – police and prosecutors can be more efficient.	2015	SE
	Digital Skills Gap in Government (Survey)	2015	UK
	Report to the Federal Parliament: Federal finance: collection of inheritance tax	2016	BE
	Report on management of IT security in systems outsourced to external suppliers	2016	DK
	Audit report of the loan activity of the Official Credit Institute 2016	2016	ES
	Steering of the Government Security Network	2016	FI
	Ensuring the security of IT systems used for public tasks	2016	PL
	Prevention and combat of cyber-bullying among children and young people	2016	PL
	Information security work at nine agencies - Another audit of information security in the state. RiR 2016:8	2016	SE
	Protecting Information across government	2016	UK
	Report on the protection of IT systems and health data in three Danish regions	2017	DK

Type	Title (with hyperlink)	Year	MS
	Note on the results of the international parallel audit "Effectiveness of internal controls in the protection of personal data in national databases".	2017	EE
	Cyber protection arrangements	2017	FI
	Steering of the operational reliability of electronic services	2017	FI
	Chambers of Agriculture network (synthesis)	2017	FR
	Vaucluse Chamber of Commerce and Industry (by the Regional Audit Chamber PACA)	2017	FR
	Ensuring the security and preservation of Estonian national databases of critical importance	Fin. 2018 / not yet published	EE
	'State Electronic Communications Infrastructure Development' a Lithuanian version a summary translated into English)	2017	LT
	Information Technology Audit: Cyber Security across Government Entities	2017	MT
	The national registries system: security, performance and usability	2017	PL
	The WannaCry incident	2017	UK
	Online Fraud	2017	UK
	Report on protection against ransomware attacks	2018	DK
	Arpajon Hospital (by the Île-de-France Regional Chamber)	2018	FR
	'Critical State Information Resources Management'	2018	LT
	'Electronic Crimes'	2019	LT
	Information security in Poland	2019	PL
Other	Database of public bodies	n/a	BE
	Questionnaire on security and risk analysis policy (ongoing)	n/a	BE

Acronyms and abbreviations

CERT: - EU: Computer Emergency Response Team

cPPP: contractual Public-Private Partnership

CSDP: Common Security and Defence Policy

CSIRT: Computer Security Incident Response Team

DDoS: Distributed Denial of Services

DEP: Digital Europe Programme

DG CONNECT: Communications Networks, Content and Technology

DG HOME: Directorate-General Migration and Home Affairs

DG JUST: Directorate-General Justice and Consumers

DIGIT: Directorate-General for Informatics

EC3: Europol's European Cybercrime Centre

ECA: European Court of Auditors

ECSEL: Electronic Components and Systems for European Leadership

ECSM: European Cyber Security Awareness Month

ECSO: European Cyber Security Organisation

EDA: European Defence Agency

EEAS: European External Action Service

ENISA: European Agency for Network and Information Security

ESA: European Supervisory Authority

ESIF: European Structural and Investment Fund

EU: European Union

FDI: Foreign Direct Instruments

GDPR: General Data Protection Regulation

HWPCI: Horizontal Working Party on Cyber Issues

ICS: Industrial Control Systems

ISF - P: internal Security Fund - Police

ISSB: Information System Security Steering Board

JRC: Joint Research Centre

LISO: Local Information Security Officer

NAO: National Audit Office

NCIRC: NATO's computer incident response capability

NIS Directive: Network and Information Security Directive

PESCO: Permanent Structured Cooperation Framework

SME: Small Medium Enterprise

Glossary

Access data: Information on a user's log-in and log-out activity to access a service, such as time, date and IP address.

Adware: Malicious software displaying advertising banners or pop-ups that include code to track victims' online behaviour.

Availability: Ensuring timely and reliable access to and use of information.

Botnet: A network of computers infected with malicious software and controlled remotely, without users' knowledge, to send spam emails, steal information or launch coordinated cyberattacks.

Cloud computing: The delivery of on-demand§ IT resources – such as storage, computing power or data-sharing capacity – over the internet, through hosting on remote servers.

Confidentiality: The protection of information, data or assets from unauthorised access or disclosure.

Crime-as-a-service (Caas) model: A criminal business model that drives the digital underground economy, providing a wide range of commercial services and tools enabling unskilled, entry-level cybercriminals to commit cybercrime.

Critical infrastructure: Physical resources, services and facilities of which the disruption or destruction would have a serious impact on the functioning of the economy and society.

Cryptocurrency: A digital asset which is issued and exchanged using encryption techniques, independently of a central bank. It is accepted as a means of payment among the members of a virtual community.

Cyberattack: An attempt to undermine or destroy the confidentiality, integrity and availability of data or a computer system through cyberspace.

Cybercrime: Various criminal activities involving computers and IT systems as either a primary tool or primary target. These activities include: traditional offences (e.g. fraud, forgery and identity theft); content-related offences (e.g. online distribution of child pornography or incitement to racial hatred); and offences unique to computers and information systems (e.g. attacks against information systems, denial of service attacks and malware).

Cyber defence: A subset of cybersecurity aiming to defend cyberspace with military and other appropriate means in order to achieve military-strategic goals.

Cyber-dependent crime: A crime that can only be committed using IT devices.

Cyber ecosystem: A complex community of interacting devices, data, networks, people, processes, and organisations, and the environment of processes and technologies influencing and supporting these interactions.

Cyber-enabled crime: A traditional crime committed on a larger scale by using IT systems.

Cyber incident: An event that directly or indirectly harms or threatens the resilience and security of an IT system and the data it processes, stores or transmits.

Cyber resilience: The ability to prevent, prepare for, withstand and recover from cyberattacks and incidents.

Cybersecurity: All the safeguards and measures adopted to defend IT systems and their data against unauthorised access, attack and damage to ensure their availability, confidentiality and integrity.

Cyberspace: The intangible global environment in which online communication occurs between people, software and services via computer networks and technological devices.

Digital content: Any data – such as text, sound, images or video – stored in a digital format.

Disinformation: Verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.

Distributed Denial of Service (DDoS): A cyberattack preventing legitimate users from accessing an online service or resource by flooding it with more requests than it can handle.

Electoral infrastructure: Includes campaign IT systems and databases, sensitive information on candidates, voter registration and management systems.

Encryption: The transformation of readable information into unreadable code for its protection. To read the information, the user must have access to a secret key or password.

Exploit kit: A type of toolkit cybercriminals use to attack vulnerabilities in network and information systems so they can distribute malware or perform other malicious activities.

Hacktivist: Individuals or groups who gain unauthorised access to information systems or networks with a view to furthering social or political ends.

Hybrid threat: An expression of hostile intent which adversaries make using a mix of conventional and non-conventional warfare techniques (i.e. military, political, economic and technological methods) in forceful pursuit of their objectives.

Information security: The set of processes and tools protecting physical and digital data from unauthorised access, use, disclosure, disruption, modification, recording or destruction.

Integrity: Guarding against the improper modification or destruction of information, and guaranteeing its authenticity.

Internet of Things: The network of everyday objects fitted with electronics, software and sensors so that they can communicate and exchange data over the internet.

Legacy system: An obsolete or outdated computer system, application or programming language that is still in use, but for which upgrades and vendor support may not be available, including security support.

Malware: Malicious software. A computer programme designed to harm a computer, server or network.

Network security: A subset of cybersecurity protecting data sent via devices on the same network, to ensure that the information is not intercepted or changed.

Patching: Introducing a set of changes to software or to update, fix, or improve it, including fixing security vulnerabilities.

Personal data: Information relating to an identifiable individual.

Phishing: The practice of sending emails purporting to originate from a trusted source in order to deceive recipients into clicking malicious links or sharing personal information.

Ransomware: Malicious software that denies victims access to a computer system or makes files unreadable, usually through encryption. The attacker then normally blackmails the victim by refusing to restore access until a ransom is paid.

Skimming: The theft of credit or debit card data when entered online.

Social engineering: In information security, psychological manipulation to deceive people into performing an action or divulging confidential information.

Text vectorisation: The process of converting words, sentences or entire documents into numeric vectors so that machine-learning algorithms can use these.

Trust services: Services that enhance the legal validity of an electronic transaction, such as electronic signatures, seals, time stamps, registered delivery and website authentication.

Vulnerability management: An integral part of computer and network security to proactively mitigate or prevent the exploitation of system and software vulnerabilities through their identification, classification, and remediation.

Wiper malware: A class of malware whose intention is to wipe the hard drive of the computer it infects.

[1] In the draft EU Cybersecurity Act, it has been defined as "all activities necessary to protect network and information systems, their users, and affected persons from cyber threats" The Act is expected to be adopted by the European Parliament and the Council in early 2019.

[2] Europol, *Internet Organised Crime Threat Assessment 2017*.

[3] European Cyber Security Organisation (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, June 2016.

[4] European Parliament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, Study for the LIBE Committee, September 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18 January 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018*.

[7] Europol, *Ibid.*, 2018.

[8] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper No 2/18, February 2018.

[9] European Commission, President's State of the Union 2017.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, press release, 25 April 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017*.

[12] European Commission factsheet on cybersecurity, September 2017.

[13] Costs could include: lost revenue; costs for repairing damaged systems; potential liabilities for stolen assets or information; customer retention incentives; higher insurance premiums; increased protection costs (new systems, employees, training); potential settlement of compliance costs or litigation.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] The *Wannacry* ransomware exploited vulnerabilities in a Microsoft Windows protocol enabling the remote takeover of any computer. A patch was issued by Microsoft after it had discovered the vulnerability. However, hundreds of thousands of computers had not yet been updated, and many of these were subsequently infected. Source: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19 December 2017.

[16] European Commission, *Europeans' attitudes towards cybersecurity*, Special Eurobarometer 464a, September 2017. A follow-up survey is expected to be published in early 2019.

[17] The Budapest Convention is a binding international guideline for countries developing legislation against cybercrime. It provides a framework for international cooperation between state parties. The Commission, the Council of the European Union, Europol, ENISA and Eurojust currently represent the EU.

[18] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final, 7 February 2013.

[19] European Commission, *The European Agenda on Security*, COM(2015) 185 final, 28 April 2015.

[20] European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, 6 May 2015.

[21] EEAS *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, June 2016.

[22] Centre for European Policy Studies, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, November 2018.

[23] The malware behind the Wannacry ransomware attack which was attributed to North Korea by the United States, the UK and Australia, was originally developed and stockpiled by the US National Security Agency to exploit vulnerabilities in Windows. Source: A. Greenberg, ibid., WIRED, 19 December 2017. In the wake of the attacks, Microsoft condemned the stockpiling of software vulnerabilities by governments and repeated its call for the need for a Digital Geneva Convention.

[24] In addition to land, sea, air and space.

[25] EU Cyber Defence Policy Framework (2018 update), 14413/18, 19 November 2018.

[26] European Commission/European External Action Service, *Joint Framework on countering hybrid threats: a European Union response*, JOIN(2016) 18 final, 6 April 2016.

[27] Joint declaration by the Presidents of the European Council and the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 8 July 2016 and 10 July 2018.

[28] European Commission/European External Action Service, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450 final, 13 September 2017.

[29] 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 (OJ L 194, 19.7.2016, p. 1).

[30] 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.

[31] These are integrated into cooperative structures established by the directive, the CSIRTS Network (a network composed of EU Member States' appointed CSIRTs and CERT-EU; ENISA hosts the secretariat) and the Cooperation Group (supports and facilitates the strategic cooperation and information exchange among Member States for which the Commission hosts the secretariat)

[32] 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[33] European Commission, *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")*, COM(2017) 477 final, 13 September 2017.

[34] European Commission, *Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM(2018) 225 final, 17 April 2018.

[35] European Commission, *Proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*. COM(2018) 226 final, 17 April 2018.

[36] European Commission, *Proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres,* COM(2018) 630 final, 12 September 2018.

[37] H. Carrapico and A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, Vol. 55, No. 6, 2017.

[38] European Commission, ibid., SWD(2017) 295 final, 13 September 2017.

[39] European Parliamentary Research Service, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, December 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27 November 2014.

[41] An exception being Article 14 (‘Monitoring and statistics’) of the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[42] European Economic and Social Committee, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, March 2018. CEPS-ECRI Task Force, Cybersecurity in Finance: Getting the policy mix right!, June 2018.

[43] 24 of 28 national audit offices replied to our survey.

[44] This means principles-based and as technology-neutral as possible.

[45] European Commission Scientific Advice Mechanism Scientific Opinion 2/2017, 24 March 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, September 2018. European Centre for Political Economy, ibid., Occasional Paper No 2/18, February 2018.

[47] European Commission, *Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content*, COM(2015) 634 final, 9 December 2015.

[48] European Commission, *Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods*, COM(2017) 635 final, 9 December 2015.

[49] Dutch Cyber Security Council, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force*, June 2018.

[51] European Commission, *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*, COM(2017) 476 final/2, 4 October 2017.

[52] Europol, ibid., 2017.

[53] Council of the European Union, *Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime"*, 12711/1/17 REV 1, 9 October 2017.

[54] European Commission, Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment, SWD/2017/0298 final, 13 September 2017. Political agreement on the new legislation was reached in December 2018, and is expected to be adopted in early 2019.

[55] Europol, ibid., 2017.

[56] C- 362/14: Maximillian Schrems v. Data Protection Commissioner (Ireland), 6 October 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime*, 7021/17, 13 March 2017.

[58] European Commission, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD (2017) 295 final, 13 September 2017.

[59] European Parliamentary Research Service, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, PE589.832.

[60] European Parliament resolution, *Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries*, (2014/2232(INI)), 8 September 2015. Dual-use goods and services, which include software and technology, can have civilian and military applications.

[61] The publically available information is stored in the WHOIS database, managed by ICANN (Internet Corporation for Assigned Names and Numbers). ICANN maintains the Domain Name System. Misuse of domain names facilitates cybercrime.

[62] Article 3, NIS Directive, ibid.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10 September 2015.

[64] The White House, *Cybersecurity spending fiscal year 2019*.

[65] European Commission, *Commission Staff Working Document: Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'*, SWD(2018) 305 final, 6 June 2018.

[66] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, December 2016.

[67] European Commission, ibid., COM(2018) 630 final, 12 September 2018.

[68] European Parliamentary Research Service Scientific Foresight Unit, *Achieving a sovereign and trustworthy ICT industry in the EU*, December 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31 July 2017.

[70] European Parliamentary Research Service Scientific Foresight Unit, ibid., December 2017.

[71] Ibid.

[72] European Commission, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 final (Part 1/4), 12 September 2018.

[73] European Commission, ibid., COM(2018) 630 final, 12 September 2018.

[74] ECA Special Report No 13/2018: "Tackling radicalisation that leads to terrorism".

[75] Figures cited in this section come from publicly available Commission documents, except for the €42 million in paragraph ***51***, which the Commission provided to us directly.

[76] Horizon 2020 is the EU's €80 billion research and innovation programme, supporting the Innovation Union, which is aimed at securing the EU's global competitiveness.

[77] Horizon 2020 Societal Challenge 7 "Secure and Innovative Societies: protecting freedom and security of Europe and its citizens".

[78] We analysed H2020 projects from the CORDIS dataset. We performed text vectorisation on each project's description, using the JRC cybersecurity taxonomy (see ***Box 5*** in next chapter), to identify projects that were likely to be cybersecurity-related. We then manually checked and analysed the results.

[79] European Cyber Security Organisation, *ECS cPPP Progress Monitoring Report 2016-2017*, 29 October 2018.

[80] Article 9(2), NIS Directive, ibid.

[81] GLACY+ (the Global Action on Cybercrime+) is a joint project with the Council of Europe. It supports twelve countries in Africa, Asia-Pacific, and Latin America and the Caribbean region, which may in turn serve as hubs to share their experience within their respective regions.

[82] The European Political Strategy Centre (EPSC), the Commission's think tank, has commented on the risk of a "digital blind spot" arising if the gap between the EU and its western Balkan neighbours continues to grow. Countries such as China and Russia are

investing significant amounts in the region, which risks marginalising the EU as a cyber-actor in the region. Source: EPSC, *Engaging with the Western Balkans: an investment in Europe's security*, 17 May 2018.

[83] European Investment Bank, *The EIB Group Operating Framework and Operational Plan 2018*, 12 December 2017.No further information was available at the time of drafting.

[84] European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027*, COM(2018) 434 final, 6 June 2018.

[85] European Commission, *Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry* (OJ L 200, 7.8.2018, p. 30). In addition, a preparatory action on defence research, totalling €90 million for 2017-2019 and funded by H2020, has been set up in 2017. It is unclear whether this includes cyber-related spending.

[86] A separate briefing paper by the ECA on EU defence is planned for publication in 2019.

[87] The Europol EC3, ENISA, the EEAS, the European Defence Agency and CERT-EU have a combined workforce of 159. This total does not include cyber-related staff at the European Commission or in the Member States. Source: Centre for European Policy Studies, ibid., November 2018.

[88] *ENISA evaluation*, 2017.

[89] Europol requested an annual staff increase of 70 temporary agents in its 2018-2020 multiannual plan, yet an increase of only 26 was approved for 2018. In the next draft multi-annual plan for 2019-2021, Europol factored in a modest increase, "assuming that a bigger resource demand would not be met". Source: Consultation on draft Multiannual Programming 2019-2021, submitted to the Joint Parliamentary Scrutiny Group, A 000834, 1 February 2018.

[90] *ENISA evaluation*, 2017. Between 2014 and 2016, around 80 % of ENISA's operational budget was used for procuring studies.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, December 2017.

[92] ISACA (formerly known as the Information Systems Audit and Control Association), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd ed., 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017*, p.16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, July 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21 February 2018.

[96] A forum for cooperation between the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority.

[97] European Securities and Markets Authority, *Joint Committee report on risks and vulnerabilities in the EU financial system*, April 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, December 2015.

[99] Referring to the EU's Member States, the Commission's Scientific Advice Mechanism has noted the "substantial and unique level of agreement on fundamental principles and values, as well as a shared strategic interest which can be at the heart of effective EU cybersecurity governance". Source: Scientific Opinion 2/2017, 24 March 2017.

[100] United States, China, Japan, South Korea, India and Brazil.

[101] European Security and Defence College (T. Renard and A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 23 November 2018.

[102] Council of the European Union, *Action Plan for implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, 15748/17, 12 December 2017.

[103] European Commission, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final, 21 November 2018.

[104] Commissioner Gabriel's reply to written parliamentary question (E-004294-17), 28 June 2017.

[105] Council of the European Union, *Annual Report on the Implementation of the Cyber Defence Policy Framework*, 15870/17, 19 December 2017.

[106] Decisions 2015/443, 2015/444 and 2017/46 govern the security of the Commission's communications and information systems. Commission Decision C(2018) 7706 of 21 November 2018 establishes an Information Technology and Cybersecurity Board, which merges the previous IT Board and Information System Security Steering Board.

[107] European Economic and Social Committee, ibid., March 2018.

[108] European Parliament, ibid., September 2015.

[109] The Hybrid Fusion Cell was established in 2016 within the EU Intelligence and Situation Centre of the EEAS. It receives and analyses classified and open source information from different stakeholders concerning hybrid threats.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, November 2013.

[111] European Commission, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final (Part 1/6), 13 September 2017.

[112] European Commission, ibid., SWD(2018) 403 final, 12 September 2018.

[113] Résaux IP Européens Network Coordination Centre, the regional internet registry for Europe, which oversees the allocation and registration of internet number resources.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs*, November 2012 .

[115] The Centre for Cyber Safety and Education, in partnership with Booz Allen Hamilton, Alta Associates and Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] European Economic and Social Committee, ibid., March 2018.

[117] House of Lords, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19*, 16 July 2018.

[118] Europol/Eurojust, *Common challenges in combatting cybercrime*, 7021/17, 13 March 2017.

[119] Europol/Eurojust, ibid., 7021/17, 13 March 2017.

[120] European Commission, ibid., SWD(2018) 403 final, 12 September 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022*, On 20 November 2018.

[122] For example, cooperation between the EEAS, Member States, agencies and bodies like CEPOL, ECTEG or the EDSC.

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, December 2017.

[124] European Cybercrime Education and Training Group.

[125] European Commission, Thirteenth progress report towards an effective and genuine Security Union, COM(2018) 46 final, 24 January 2018.

[126] Based on observations in Special Report No 14/2018, ibid.

[127] European Parliament resolution of 13 June 2018 on cyber defence (2018/2004(INI)). Council of the European Union, ibid., 15870/17, 19 December 2017.

[128] Switzerland, FYROM, Ukraine, Bosnia-Herzegovina, Kosovo (this designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence), Turkey and the United States.

[129] Europol, *Internet Organised Crime Threat Assessment 2018*.

[130] European Commission, ibid., SWD(2017) 295 final, 13 September 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman and S. Furman, *Security Fatigue*, "IT Professional", vol. 18, no. 5, 2016, pp. 26-32. See also NIST.

[132] European Commission/European External Action Service, *Increasing resilience and bolstering capabilities to address hybrid threats*, JOIN(2018) 16 final, 13 June 2018.

[133] For example, the shutdown of AlphaBay and Hansa in joint operations led by the FBI and the Dutch national police with the support by Europol. These were two of the largest

marketplaces for the trading of illicit goods like drugs, firearms and cybercrime tools, such as malware. Source: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, Press Release, 29 May 2018.

[134] European Commission, ibid., SWD(2018) 403 final, 12 September 2018.

[135] Council of the European Union, ibid., 12711/1/17 REV 1, 9 October 2017.

[136] European Commission, ibid., SWD(2017) 295 final, 13 September 2017.

[137] European Commission/European External Action Service, ibid., JOIN(2018) 16, 13 June 2018.

[138] European Commission, SWD(2017) 500 final, 13 September 2017.

[139] *Memorandum of Understanding – ENISA, EDA, Europol EC3, and CERT-EU*; 23 May 2018.

[140] European Commission, Call for tender: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*, 27 October 2017.

[141] Jean-Claude Juncker, Mission letter for the Commissioner for the Security Union, 2 August 2016. Defence is not within the task force's remit.

[142] Council of the European Union, *EU cybersecurity roadmap*, 8901/17, 11 May 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues*, 5th ed., November 2017.

[144] JRC Technical Reports, European Cybersecurity Centres of Expertise Map: *Definitions and Taxonomy*. Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres, SWD(2018) 403 final, 12 September 2018.

[145] European Commission, ibid., SWD(2017) 295 final, 13 September 2017.

[146] European Commission, ibid., SWD(2018) 403 final, 12 September 2018.

[147] For example, the European Financial Institutes ISAC includes financial sector representatives, national CERT's, law enforcement agencies, ENISA, Europol, European Central Bank, the European Payments Council and the European Commission.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14 February 2018.

[149] Council of the European Union, ibid., 12711/1/17 REV 1, 9 October 2017.

[150] https://www.europol.europa.eu/empact.

[151] A 2018 study by Accenture across 15 countries found that 87 % of focused cyber attacks were being prevented: *2018 State of Cyber Resilience*, 10 April 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, Oxford University Politics Blog, 14 September 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14 July 2017.

[154] European Economic and Social Committee, *Ibid.*, March 2018.

[155] European Commission, *Eighth progress report towards an effective and genuine Security Union*, COM(2017) 354 final, 29 June 2017.

[156] See the various NIS Cooperation Group publications.

[157] PSD2: Payment Services Directive 2; ECB/SSM: European Central Bank/Single Supervisory Mechanism; Target 2: Trans-European Automated Real-time Gross settlement Express Transfer system (2nd Generation), Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Source: CEPS-ECRI Task Force, ibid., June 2018.

[158] European Commission, *Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises*, C(2017) 6100 final, 13 September 2017.

[159] European Commission, ibid., SWD(2017) 295 final, 13 September 2017. There are several crisis management mechanisms, including the Integrated Political Crisis Response mechanism (IPCR), Argus (the Commission's crisis response mechanism), the EEAS Crisis Response Mechanism, the Union Civil Protection Mechanism and the EU Law Enforcement Emergency Response Protocol.

[160] In addition, this may also prompt Article 42(7) of the Treaty on the European Union (mutual assistance clause) or Article 222 Treaty on the Functioning of the European Union (solidarity clause) to be invoked.

[161] European Commission/European External Action Service, ibid., JOIN(2018) 16, 13 June 2018. In December 2018, alleged hacks of the the EEAS' diplomatic communications network, COREU, were reported in the media (source: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*; 18 December 2018). The matter is currently under investigation.

[162] Cooperation over early warnings and mutual assistance need further development as well: *Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, 10085/18, 26 June 2018.

[163] European Parliamentary Research Service, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, September 2018.

[164] European Economic and Social Committee, ibid., March 2018.

[165] Council of the European Union, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, 14893/18, December 2018.

[166] Cyber Rapid Response Teams and Mutual Assistance in Cyber Security; Cyber Threats and Incident Response Information Sharing Platform. Source: Council of the European Union, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*, 19 November 2018.

[167] Council of the European Union, Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, 9916/17, 7 June 2017.

[168] Council of the European Union, *Council Conclusions on Cyber Diplomacy*, 6122/55, 11 February 2015.

[169] Council of the European Union, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.

[170] Attributing responsibility for an incident remains a sovereign political decision for the Member States, and not all of the toolbox's measures require attribution.

[171] The toolbox did not lead to joint action; individual Member States adopted the US position.

[172] Council of the European Union, *Conclusions on malicious cyber activities*, 7925/18, 16 April 2018.

[173] Computer systems used to control processes in diverse industries, such as utilities, chemical and industrial manufacturing, food processing, transportation systems and hubs, and logistical services.

[174] ENISA, ibid., December 2017.

[175] For example, public administration, the chemical and nuclear industries, manufacturing, food processing, tourism, logistics and civil protection.

[176] European Commission, ibid., SWD(2017) 295 final, 13 September 2017.

[177] Speech by Commissioner Jourová at Plenary Session of the European Parliament on *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign*, 14 November 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23 May 2018.

[179] European Political and Strategy Centre (L. Past), Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses, in: "Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts", 2018.

[180] According to Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[181] European Commission, Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final, 12 September 2018.

[182] European Council Conclusions, EUCO 11/15, 20 March 2015. Two additional Task Forces have been added since, for the Western Balkans and the Neighbourhood South.

[183] An Atlantic Council report called for the EU to require all Member States to send national experts to the Task Force. See: D. Fried and A. Polyakova, *Democratic Defense Against Disinformation*, 5 March 2018.

[184] Originally lacking its own budget, in 2018 it was awarded €1.1 million for a "StratCom Plus" Preparatory Action by the European Parliament.

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), ibid., 23 May 2018.

[186] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Action Plan against Disinformation*, JOIN(2018) 36 final. The plan focuses on: improving EU institutions' capabilities to detect, analyse and expose disinformation; strengthening coordinated and joint responses; mobilising the private sector; and raising awareness and improving societal resilience.

[187] European Commission, *Tackling online disinformation: a European Approach*, COM(2018) 236 final, 26 April 2018.

[188] Not to be confused with the code of conduct for countering illegal online hate speech.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, April 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* April 2018

[191] European Political and Strategy Centre (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, in: ibid, 2018.

[192] European Commission, ibid., SWD(2018) 403 final, 12 September 2018.

[193] The proposed Regulation (COM(2017) 487 final, 13 September 2018) for FDI screening, submitted in September 2017, is currently making its way through the legislative process. It specifically covers critical technologies, which include artificial intelligence, cybersecurity and dual-use applications.

[194] European Commission/European External Action Service, ibid., JOIN(2017) 450 final, 13 September 2017.

ECA team

This briefing paper *Challenges to effective EU cybersecurity policy* was adopted by Chamber III External actions/Security and justice, headed by ECA Member Bettina Jakobsen. The task was led by ECA Member Baudilio Tomé Muguruza, supported by Daniel Costa de Magalhaes, Head of Private Office and Ignacio Garcia de Parada, Private Office Attaché; Alejandro Ballester-Gallardo, Principal Manager; Michiel Sweerts, Head of Task; Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha, auditors and Johannes Bolkart, intern. Hannah Critoph provided linguistic support.

From left to right: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

CURIA RATIONUM

EUROPEAN
COURT
OF AUDITORS

Publications Office

EUROPEAN COURT OF AUDITORS
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Enquiries: eca.europa.eu/en/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors