Council of the European Union

Brussels, 14 September 2017
(OR. en)

12210/17

CYBER 131
TELECOM 211
JAI 789
DROIPEN 122
COSI 201
JAIEX 63
POLGEN 119
RELEX 768
MI 634
IND 216
CSDP/PSDC 488
COPS 280
POLMIL 101

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	13 September 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2017) 295 final
Subject:	COMMISSION STAFF WORKING DOCUMENT ASSESSMENT OF THE EU 2013 CYBERSECURITY STRATEGY

Delegations will find attached document SWD(2017) 295 final.

Encl.: SWD(2017) 295 final

EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 295 final

COMMISSION STAFF WORKING DOCUMENT

ASSESSMENT OF THE EU 2013 CYBERSECURITY STRATEGY

Table of Contents

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

The purpose of this Staff Working Document is to present the achievements of the 2013 EU Cybersecurity Strategy[1]. While this is not an evaluation in the sense of the Better Regulation Guidelines, it is an assessment carried out in the spirit of Better Regulation. The Staff Working Document provides a short overview of the Strategy as conceived in 2013 and key-findings. The objective is to provide a set of lessons learnt to build on in the future work announced in the Digital Single Market Strategy Mid-Term Review[2].

The assessment covers the 5 objectives of the Strategy from the date of its adoption in 2013 until mid-2017.

The five policy objectives presented by Commission in the Strategy and endorsed by Member States through Council Conclusions in June 2013[3] are listed below:

1. Achieving Cyber Resilience;
2. Drastically reducing cybercrime;
3. Developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
4. Developing the industrial and technological resources for cybersecurity; and
5. Establishing a coherent international cyberspace policy for the European Union and promote core EU values.

An overview of the Strategy's objectives is presented by Figure 1.

The 2013 Strategy is a broad policy document addressing a wide range of issues and calling for action from a wide range of actors. It includes different types of initiatives, both legislative and non-legislative.

The Staff Working Document focuses on the Strategy as a political instrument to achieve its objectives and does not assess in detail individual actions identified in the Strategy. In terms of geographical scope, the present assessment does not cover cybersecurity related activities in Member States, but at the EU level.

[1] The 2013 EU Cybersecurity Strategy did not indicate the need to carry out a final evaluation as such. According to the Strategy, the progress was to be assessed through a high-level conference gathering together all relevant parties after 12 months since the Strategy adoption. Such a yearly progress conference took place both in 2014 and 2015. The progress was also monitored though regular meetings of the competent Council preparatory body - the Friends of Presidency on Cyber issues, where the Commission and other stakeholders were regularly provided updates on the progress made as requested by Council Conclusions on 2013 EU Cybersecurity Strategy. See: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT

[2] COM (2017) 0228

[3] See: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT

2 BACKGROUND AND CONTEXT

This section provides a brief description of the Cybersecurity strategy, including its objectives and the problems it was intended to solve.

2.1 DESCRIPTION OF THE EU CYBERSECURITY STRATEGY AND ITS KEY OBJECTIVES

In 2013, the Commission, together with the High Representative, put forward a Cybersecurity Strategy – "An Open, Safe and Secure Cyberspace"[4] – which represented the EU's comprehensive vision on how to best support Member States and other stakeholders in preventing and responding to cyber disruptions and attacks.

The vision was to foster European values of freedom and democracy and to ensure that the digital economy can safely grow. Specific actions aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cybersecurity and cyber defence policy.

The strategy articulates the EU's vision of cyber-security through five priorities as outlined in section 1.1 and Figure 1 and it is implemented via a series of instruments:

- **Legislative instruments**: A number of legislative instruments have been used to achieve the 2013 EU Cybersecurity Strategy objectives. Some of these legislative instruments existed already (e.g. cybercrime directives) but needed additional efforts related to transposition and implementation, while new legislation was also required (e.g. NIS Directive).
- **Non-legislative instruments:** This category included activities ranging from providing political steer and coordination facilities, supporting capacity building, to measures aimed at enhancing existing initiatives, mainstreaming cybersecurity issues into EU external relations and encouraging political dialogue.
- **Funding activities:** While a dedicated budget has not been established to support the strategy, it did benefit from a number of ongoing programmes/projects to support it at the level of the Commission or at the Member States. It has not been possible to estimate the total budget because of the correlation between cybersecurity–related investment in programmes and various information technology or information society projects.

The implementation and management of the Cybersecurity Strategy were located mainly under the responsibility of two Commission services – Directorate-General for Communications Networks, Content and Technology and Directorate-General for Migration and Home Affairs as well as of the European External Action Service. A number of suggested actions were also to be implemented by EU agencies and bodies (European Network and Information Security Agency – ENISA and EC3 of Europol) as well as by Member States and other stakeholders.

The Strategy envisaged that its progress would be assessed through a high-level conference gathering together all relevant parties 12 months after its adoption. Such a progress conference took place both in 2014 and 2015. The progress was also monitored through regular meetings of the competent Council preparatory body – firstly held in the format of the Friends of Presidency and then transformed into regular Horizontal Working Party on Cyber

[4] Joint Communication "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" JOIN (2013) 1 final, 7 February 2013.

issues, where the Commission and other stakeholders were regularly provided updates on the progress made as requested by Council Conclusions on 2013 EU Cybersecurity Strategy.[5]

[5] See: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT

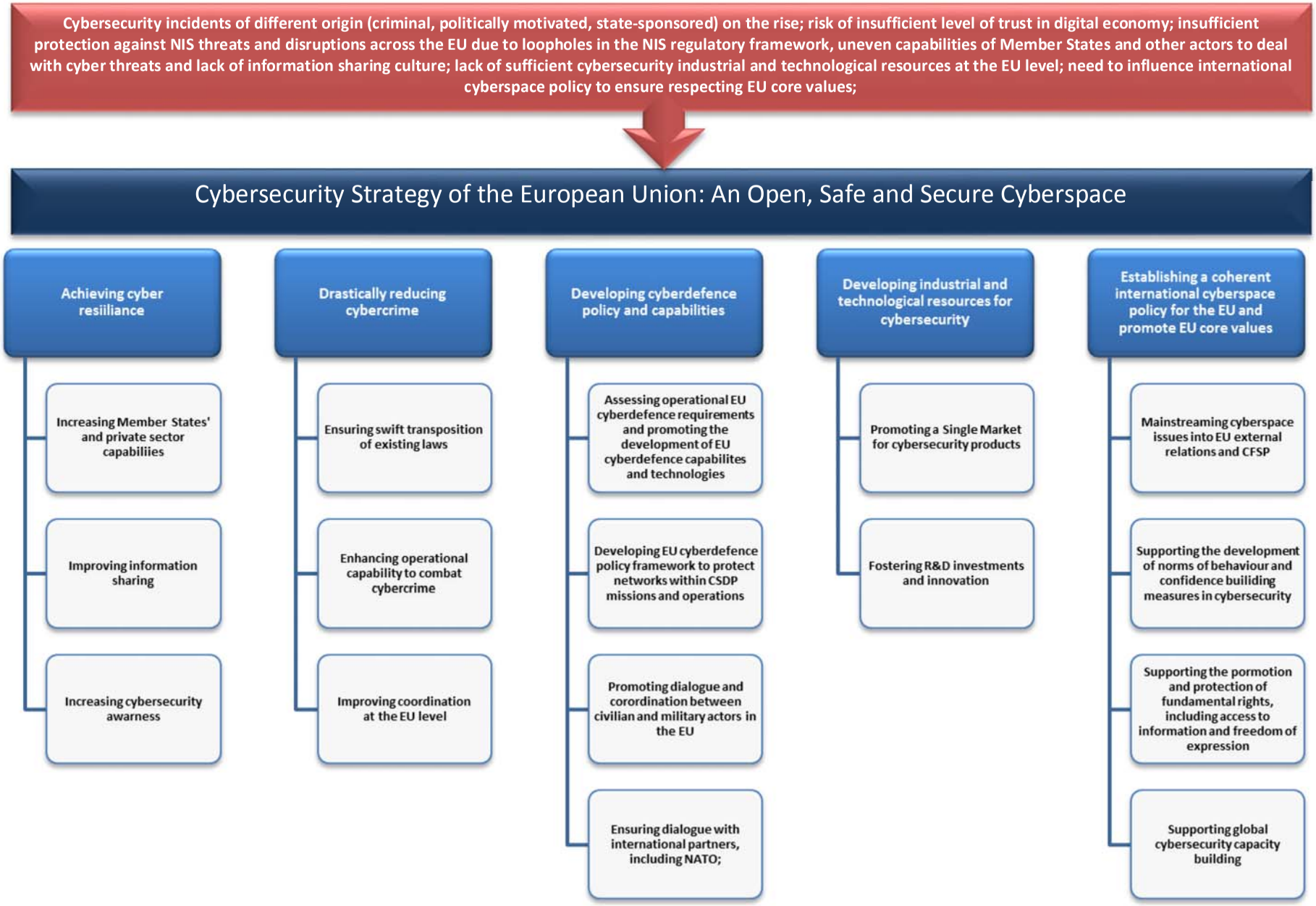

Figure 1: Overview of the Strategy Objectives

2.2 PROBLEMS THE CYBERSECURITY STRATEGY WAS INTENDED TO SOLVE

After a short overview of the general context, this section describes the specific challenges faced by Member States, the private sector and citizens, as well as the defence and international cooperation challenges.

General overview

Economies and societies have become reliant on Internet connections at an exponential rate. With this rise in Internet connections came the rise in cybercrime. While exact figures are difficult to establish, in 2013, cybercrime was causing a significant share of cybersecurity incidents and the approximate gain by cybercriminals reached around € 750 billion per year. According to Europol's Internet Organised Crime Threat Assessment (iOCTA), a sophisticated and self-sufficient digital underground economy had developed, in which data was a key commodity, including stolen personal and financial information. A range of new criminal activities had developed, such as phishing, pharming, crime ware distribution and the hacking of corporate databases, with a fully-fledged infrastructure of malicious code writers, specialist web hosts and individuals able to lease networks of many thousands of compromised computers to carry out automated attacks.[6] Whilst the monetary value of the cybercriminal economy as a whole was and remains difficult to establish, one estimate of global corporate losses at the time gave a figure of $1 trillion per year.[7] Cyber threats had started migrating from desktop computers – key targets in previous years – to mobile ecosystems[8].

On the legislative side, while a number of framework decisions already existed,[9] EU Member States' legislation on cybercrime was quite heterogeneous, making swift operational cooperation more challenging. Member States were in the process of implementation of the 2011 Directive to combat child sexual abuse and exploitation and child pornography, and about to adopt the Directive on Attacks against Information Systems.[10] Six Member States had not yet ratified the Budapest Convention, signed on 23 November 2001 with a view to address cybercrime by harmonising national laws, improving investigation and international cooperation.

A number of additional challenges existed for the organisation of the response to cybercrime, in particular in cooperation and information sharing. According to the Commission's

[6] https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011

[7] http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html

[8] While ENISA Threat Landscape for 2013 appeared after the publication of the EU Cybersecurity Strategy, it confirmed the trends mentioned in the SWD (2013) 32, which accompanied the proposal for a Directive concerning measures to ensure a high level of network and information security across the Union, which was one of the Strategy's key initiatives. Please check: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

[9] Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment; Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography; and Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems; and

[10] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework- Decision 2004/68/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Ajl0064

Feasibility Study for a European Cybercrime Centre[11], factors contributing to this situation were first, cultural and sociological. Member States were not forthcoming in sharing cybercrime information amongst each other or with Europol[12]. Reticence to use Europol as a focal point for information exchange was probably due to factors such as a policing culture that is cautious about sharing information, has low awareness and lacks knowledge. The second reason hampering the flow of information was of a more structural nature, as most Member States did not have structural links with the private sector for the purposes of fighting cybercrime. This meant that few cybercrime incidents reports reached the national law enforcement agencies.[13]

Furthermore, at the end of 2012, Europol had a limited number of resources dedicated to the fight against cybercrime, which effectively limited the number of operations it could support, with a total of 31 employees.[14]

The risk of cross-border services becoming unavailable, suspended or interrupted due to security breaches was also becoming more evident as proved for example by the case of an online market place – eBay, which had experienced web-based attacks that made all or portions of its websites unavailable for periods of time in 2010 and likewise PayPal, thereby affecting e-commerce in the internal market.[15] The situation and its worrying evolution called for joint efforts to reduce cybercrime by enhanced cooperation across Member States.

More and more actors across the EU and internationally began calling for stronger cyber resilience as a means to ensure that entities are able to continuously deliver the intended outcome despite malicious cyber activities.

The level of capabilities to tackle cyber threats was uneven, to say the least, both among private sector actors and Member States. In addition, no framework for trusted information sharing on security threats, risk and incidents amongst the Member States and between the private and the public sector existed.[16]

Challenges faced by Member States

As far as the national level of preparedness was concerned, Member States had very different level of capabilities and only a few Member States had adopted national cyber security strategies.[17]

A the same time, although the majority of Member States had established national/government Computer Emergency Response Teams (CERTs), there were significant

[11] Commission Staff Working Document Ex-Ante Evaluation: Resources needed to fulfil the tasks set forth in the Commission's Communication on the establishment of a European Cybercrime Centre (EC3) /* SWD/2013/0100 final */ http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013SC0100

[12] The European Union Agency for Law Enforcement Cooperation (Europol) was founded in 1998 in view of establishing cooperation between the relevant law enforcement authorities in Member States to combat international organised crime more efficiently.

[13] COM(2013) 100 final.

[14] COM(2013) 100 final.

[15] SWD(2013) 32 final.

[16] SWD(2013) 32 final.

[17] The first EU member state to do this was Germany, which adopted the “National Plan for Information Infrastructure Protection (NPSI)” already in 2005. The following year, Sweden developed a "Strategy to improve Internet security in Sweden". Following the severe cyber-attack on Estonia in 2007, the country was the first EU Member State to publish a broad national cyber security strategy in 2008. While progress could be observed in this regard, by 2012 only ten Member States developed official strategies, although some also had unofficial or informal documents considered as a national cybersecurity strategy.

differences regarding the power of their mandate (which in some cases was time-limited), their role in developing national cybersecurity strategies, the type of CERT (i.e., national, de facto, national/governmental, governmental), and the maturity status of the team. At the same time there were also some Member States with no national/governmental CERT established.

Public sector players dealing with network and information security (NIS) in EU Member States included a large variety of ministries, agencies and National Regulatory Authorities. This plethora of bodies, each with different competences and responsibilities, made it difficult for the Member States to identify their counterparts with whom to cooperate in other Member States. No EU-wide cooperation mechanism for Member States on cybersecurity-related issues existed to facilitate such cooperation.

This was also the case for national/government CERTs. Only some of them had been officially attributed the role of an official contact point for other Member States and this was not easily accessible information.[18]

The uneven level of capabilities was hindering the creation of trust among peers in the Member States, which in turn held up effective cooperation and information sharing.

In this context, cross-border cooperation took place in a closed circle of trust. The informal European Government CERTs (EGC) group, which performed operational tasks, comprised only 10 Member States, which were top performers. As indicated in the group's website: "*Its members effectively co-operate on matters of incident response by building upon a fundament of mutual trust and understanding due to similarities in constituencies and problem sets*".[19] No EU-wide mechanism for national/governmental CERTs existed at the time.

Cybercrime was beginning to emerge more prominently on the radar of national law enforcement and had been identified as a general priority crime area at EU level in 2011 in the context of the Policy Cycle, fostering operational cooperation across Member States.[20] The European Cybercrime Centre at Europol had just been launched on 1 January 2013.[21] Stable cross-border cooperation was still in its infancy and mostly limited to a number of more advanced players, as evidenced by the comparatively low number of cybercrime cases supported by Europol in 2013 (57 high-profile cases).

Due to a low level of awareness about cybersecurity risks across sectors and among end-users a large proportion of attacks went unnoticed or at best undisclosed. The underreporting of incidents, due to potential significant damages for the organisations involved, contributed to maintaining a patchy understanding of the general level of risks that public administration, businesses and citizens were exposed to.[22] At the time of the announcement of the EU Cybersecurity Strategy no framework for trusted information sharing on security threats, risk and incidents amongst the Member States and between the private and the public sector existed.

An overall insufficient level of protection against security incidents, risks and threats across the EU left governments, businesses and citizens vulnerable to disruption and fundamental rights exposed to abuse. Understanding that such vulnerabilities could not be accepted because they could seriously undermine the proper functioning of the internal market, fuel

[18] www.enisa.europa.eu/activities/cert/support/files/status-report-2012
[19] SWD(2013) 32 final.
[20] https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf
[21] https://www.europol.europa.eu/events/official-launch-of-new-european-cybercrime-centre-ec3-ceremony
[22] SWD(2013) 32 final.

distrust and prevent the EU from reaping the full benefits of the digital economy, was the basic premise behind the EU Cybersecurity Strategy.

Challenges faced by the Private sector

According to Eurostat[23], by January 2012, only 26 % of enterprises in the EU had a formally defined ICT security policy with a plan for regular review; this share rose to over 50% among those enterprises whose principal activity was information and communication activities. Enterprise in Sweden and Denmark were most frequently equipped with such policies, whereas the lowest shares of enterprises with a formally defined ICT security policy were recorded in Bulgaria, Hungary, Romania, Poland and Estonia.

At the same time businesses lacked effective incentives to conduct serious risk management, which involved the adoption of appropriate NIS measures. Companies often considered NIS as a purely technical matter and did not address it as a key component of their business strategy.[24]

Companies also lacked incentives to introduce security by design approach. From an economic perspective security was seen as an externality leading to a market failure i.e. the market players did not see the economic rationale to bear the full social costs of increasing the level of security but rather prioritise time-to-market or a low pricing for their product. [25]

While Europe possessed excellent research and development capacities, most of the global leaders providing innovative ICT products and services were located outside the EU. This resulted in a risk of the EU becoming excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers.

According to a pan-European study conducted for the European Commission the EU market had been dominated by a small group of global vendors, competing with a high number of smaller European suppliers. At the time of the study, while the levels of market concentration varied across market segments (hardware, software, services) the top five vendors controlled 20.4% of total market (and they all came from outside the EU). The EU suppliers, while showing a positive dynamism, remain mostly national or regional players. Their cumulative market share was estimated at round 16.5% of the total EU NIS market revenues.[26]

Historically, industrial development in this area had been stimulated by governmental purchase and some highly innovative European companies in this sector were still largely dependent on public procurement in their home country. A side effect of this situation was limited willingness for cross-border purchasing, which constituted a barrier to the development of a common cybersecurity market. This was also linked to the lack of trust between the supply and demand sides of cybersecurity products and solutions.

Challenges faced by Citizens

[23] http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

[24] OECD 2008 "Economics of malware: Security decisions, incentives and externalities" http://www.oecd.org/internet/interneteconomy/40722462.pdf

[25] OECD 2008 "Economics of malware: Security decisions, incentives and externalities" http://www.oecd.org/internet/interneteconomy/40722462.pdf

[26] The European Network and Information Security Market: Scenario, Trends and Challenges - A study for the European Commission, DG Information Society and Media; 2009. A new market study is being conducted by an external contractor for the European Commission at the moment and will feed into the cPPP creation process.

The results of the 2012 Special Eurobarometer on Cybersecurity[27] showed that most EU citizens (73%) had seen or heard something about cybercrime in the previous 12 months before the survey was conducted. At the same time most of them did not feel very or at all well informed about the risks of cybercrime (59%). There was a clear link between being well informed and feeling confident online. More than half of those who felt confident in their ability to do online banking or buying things online said they felt well informed about cybercrime (59%).

The same survey confirmed that internet users had changed their behaviour in a number of ways because of security concerns. 37% said that they were less likely to give personal information on websites, while 43% did not open emails from people they did not know. 51% had installed anti-virus software. However, more than half (53%) of internet users in the EU did not change any of their online passwords during the past year.

In 2013 a number of initiatives had already been implemented. ENISA had been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. In 2012 ENISA piloted the "European Cybersecurity Month" and the Safer Internet Programme had been funding a network of NGOs active in the field of child welfare online.

Defence and International Cooperation Challenges

Whereas NATO has adopted already two cyber defence policies in 2008 and 2011, the EU lacked its policy on Common Security and Defence Policy (CSDP) related cyber defence in 2013. Member States have repeatedly asked for a comprehensive policy for better cyber protection of European External Action Service's (EEAS) headquarters and CSDP missions and operations.

There were also calls for EU pooling and sharing efforts in cyber defence capability development within the European Defence Agency (EDA) framework. The EDA cyber defence project team that had started in 2012 needed a strategic guidance for its future efforts.

Finally, the relations with NATO were sporadic, and no regular format for EU-NATO cyber defence meetings existed in 2013.

In 2013, the EU also lacked coherent international cyber policy, and there were no common EU positions on Internet Governance, the application of existing international law in cyberspace, the development of voluntary norms of responsible state behaviour, confidence building measures or the protection of human rights and freedoms online. EU also had no diplomatic engagement with key partners on cyber issues with participation of Member States, cybersecurity was dealt with sporadically within sectorial dialogues.

A systematic approach to capacity building in third countries was also lacking, with no proper political oversight, resulting in sub-optimal efforts, e.g. a model law for West African states where human rights safeguards were minimal. In the context of a broader lack of capacity, donors were nevertheless duplicating efforts in some cases.

[27] http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf

3 IMPLEMENTATION/CURRENT STATE OF PLAY (2017)

The present section provides a factual description of how the main instruments of the Cybersecurity Strategy have been implemented. It also covers the current state of play with regards to cybersecurity, paying particular attention to unexpected external factors.

3.1 IMPLEMENTATION OF THE KEY CYBERSECURITY STRATEGY INSTRUMENTS

NIS Directive transposition

In July 2016, the first EU-wide cybersecurity law – the so-called NIS Directive[28], which is one of the key instruments outlined in the Strategy - was formally adopted and entered into force on 8 August 2016. Member States have 21 months (until May 2018) to transpose the Directive into their national laws and 6 months more to identify operators of essential services.

Member States were required to:

- adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cyber security by 2018. At the time of drafting this document 25 Member States have either updated or developed a National Cyber Security Strategy and 2 have a draft in public consultation (compared to 12 Member States in 2013).
- designate a national competent authority for the implementation and enforcement of the Directive, as well as Computer Security Incident Response Teams (CSIRTs) responsible for handling incidents and risks by May 2018. Today, all Member States have a governmental/national CERT in place.

The Directive envisaged as well the creation of:

- The 'Cooperation Group' to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them. The Commission provides the secretariat for the Cooperation Group. The Group was successfully established in February 2017, is meeting regularly (every 2-3 months) and has started working on different work streams to deliver important guidelines/reference documents on the transposition and implementation of provisions concerning operators of essential services by the end of 2017.
- The network of Computer Security Incident Response Teams, known as the CSIRTs Network, to promote swift and effective operational cooperation on specific cyber security incidents and sharing information about risks. The Network has been established in February 2016.

Apart from obligations for Member States, the Directive put also certain obligations on the private sector:

- businesses with an important role for society and economy, referred in the Directive as *"operators of essential services"*[29], were required to take appropriate security measures and to notify serious incidents to the relevant national authority.

[28] The Directive on security of Network and Information Systems (EU) 2016/1148
[29] Sectors covered include energy, transport, banking, financial market infrastructures, health, water, digital infrastructure.

- important digital businesses, referred to in the Directive as *"digital service providers"* (DSPs) were asked to take appropriate security measures and to notify incidents to the competent authority. [30], The Commission and Member States are now working on the implementing act related to these obligations, which should be adopted in September 2017.

Implementation of soft-measures supporting the goal of achieving cyber resilience

The Cybersecurity Strategy also aimed to support the resilience of Member States and the private sector through soft measures. It tasked the European Network and Information Security Agency (ENISA) with capacity building and awareness raising support activities. A brief update on the state of implementation of key initiatives in this regard is presented below.

As requested by the Strategy ENISA continued organising bi-annual "Cyber Europe" exercises. Over the last years ENISA's exercises have given the opportunity to approximately 4000 cybersecurity experts from over 2000 different organizations to be trained to deal with difficult and complex cybersecurity crisis scenarios. Cyber Europe 2016 was the largest and most comprehensive EU cyber-security exercise to date involving more than 700 cyber-security professionals from all 28 Member States. The next edition of Cyber Europe is planned for 2018. Building on this experience, ENISA also supported the planning and execution of exercises for different EU institutions and bodies.[31]

Since 2014 ENISA actively supported the CERT community. It provided 19 different types of courses to improve the capacity of CERTs. Between 2014 and 2017, it delivered 114 training sessions, with an average of approximately 28 trainings per year. The Agency also organised workshops to facilitate the cooperation with the law enforcement services and collected good practices from mature CERTs in Europe on how such cooperation could be structured. ENISA also produced a number of studies[32] on information sharing and common taxonomies between CERTs and law enforcement to support the alignment on tools, methods and procedures across the EU.

Whereas the Strategy called on all stakeholders to promote cybersecurity awareness among end users, ENISA was tasked with coordinating a pan-European campaign in this regard. At least 18 Member States organise national awareness campaigns, usually aimed at the Public Sector (80%) followed by adults, children, adolescents and SMEs[33]. At EU level, since 2013, ENISA, together with partners in Member States and the European Commission, runs the European Cyber Security Month (ECSM), an EU advocacy campaign taking place in the month of October to raise awareness about cybersecurity issues and promote among citizens a sense of shared responsibility to practice safe and informed behaviours on the Internet[34]. A yearly evaluation of the Cybersecurity Month is conducted.

---

[30] DSPs include: online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online), cloud computing services, search engines.

[31] MultiLayer (ML) exercises by the European External Action Service (EEAS) in 2015 and 2016, the crisis management exercise CYBER 13 for Eurocontrol, the first ever exercise of the Integrated Political Crisis Response (IPCR) arrangements organised by the European Council in 2014, the strategic exercises for European Defence Agency in 2015 and 2016.

[32] See: www.enisa.europa.eu

[33] Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.

[34] ENISA provided the following data with regard to the ECSM for the period 2013 – 2016: i) the number of cybersecurity activities taking place in October across Europe rose by 296% between 2013 and 2016 and the online outreach of the

Since 2014 ENISA has been also organizing every year the European Cyber Security Challenge to help close the cybersecurity skills gap by identifying cyber security talents and developing human resources networks. In 2017 ENISA will conduct its first impact study of the European Cyber Security Challenge, the results of which should be available at the end of 2017.[35]

Transposition of cyber-crime related directives

Directive 2011/93/EU on combating child sexual abuse[36] addresses new phenomena such as online grooming and webcam sexual abuse, as well as online viewing of child abuse images without download. The Directive had a transposition deadline of 18 December 2013. By the deadline, only 12 Member States had notified the Commission of completed transposition of the Directive and it took until December 2016 for all Member States to complete transposition and notification.

Directive 2013/40/EU on attacks against information systems[37] covers the main offences related to cyber-attacks and introduces new offences such as the use or making available of tools to commit cyber-attacks. It approximates Member State's definitions of cybercrime offences, setting minimum maximum penalties and providing a framework for the exchange of information on these crimes between Member States, and for the collection of statistical information. The Directive, adopted in August 2013, had to be implemented by September 2015. As of now, two Member States still have not notified transposition.

Implementation of measures related to increasing accountability online

As foreseen by the Cybersecurity Strategy, the Commission has worked to ensure greater accountability of domain name registrants and accuracy of information on website ownership on the basis of the Law Enforcement Recommendations for the Internet Corporation for Assigned Names and Numbers (ICANN), in compliance with Union law, including the rules on data protection.

In 2013 a new Registrar Accreditation Agreement (RAA), and in 2014 a new gTLD Registry Agreement were adopted by ICANN and amended in May 2017, providing for a better definition of responsibilities and accountability of registrars and registries. Furthermore, in June 2015 the Public Safety Working Group (PSWG) of the ICANN Governmental Advisory Committee (GAC) was established, creating a more structured approach to public safety issues. The Commission supports the PSWG's work and currently co-chairs the group.

ICANN has launched a policy development process for domain name registration directory services which began its work in January 2016, with Commission participation.[38] In parallel,

---

campaign increased at annual growth rate of 41%; featured press articles of European Cyber Security Month increased at an annual growth rate of 44% reaching 429 articles.

[35] In 2014 only 2 Member States and Switzerland participated in the championship. The attendance has continuously expended with 150 young talents from 15 EU and EFTA countries planning to compete in Malaga, Spain in 2017.

[36] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[37] 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, OJ L 218/8 of 14.8.2013.

[38] https://gnso.icann.org/en/group-activities/active/rds

it has started its regular review of the current Registration Directory Services system in June 2017, again with Commission participation.[39]

The Commission is also actively involved in policy work aimed at ensuring high consumer protection safeguards in the domain names environment and supports ongoing work within ICANN to better monitor and gather data on DNS Abuse with a view to improve the security of the DNS.

Beyond the accuracy of the databases underlying the domain name system, in October 2016 the successful completion of the IANA stewardship transition to the global multistakeholder community and the accompanying measures to increase ICANN accountability towards such community marked an historical landmark in creating mechanisms to ensure more accountability in the management of critical internet resources in the global public interest.

The European Commission and EU Member States had been calling for such a transition for many years, including in Council Conclusions on Internet governance[40] and in Council Conclusions on the transfer of the stewardship of the IANA functions[41], recognising that the overall robustness and stability of the global Internet as well as the security and stability of the domain-name system should be maintained and strengthened.

The European Commission has also been striving to create a safer online environment within the .eu top level domain name (TLD). The .eu TLD is implementing the Domain Name Security Extensions (DNSSEC) protocol. DNSSEC is designed to protect Internet users from forged DNS data. DNSSEC can only reach its full potential if all the zones in the hierarchical DNS tree are signed. At the end of Q1 2017, there were 357,389 DNSSEC signed .eu domain names.

The .eu Registry has been applying measures to counter phishing and other types of malicious online behaviour on a daily basis, as well as providing regular assistance to law enforcement authorities, including the upholding of a regular dialogue with CERT-EU. The .eu Registry also signed a Memorandum of Understanding with Europol in December 2016, to engage in joint efforts related to fighting cybercrime, to exchange statistical data and trends pertaining to cybercrime, and to commit to cooperating on projects designed to combat cybercrime.[42]

Support for European Cybercrime Centre (EC3) at Europol

In 2013, the European Cybercrime Centre (EC3) was created as an integral part of Europol. The Strategy called for support to EC3 as a focal point in the fight against cybercrime. EC3 focuses on cybercrimes and serves as the nexus at European level:

- committed by organised crime groups, particularly those generating large criminal profits such as online fraud;
- which cause serious harm to their victims, such as online child sexual exploitation;
- affecting critical infrastructure and information systems in the Union (including cyber-attacks).

[39] https://www.icann.org/resources/reviews/specific-reviews/whois
[40] ST-16200/14-INIT
[41] ST-9855/15-INIT
[42] https://www.europol.europa.eu/newsroom/news/europol-enhances-cybercrime-and-internet-security-cooperation-signing-mou-eurid

The EC3 focuses on providing operational support of the Member States at the EU level for cross-border cybercrime, as well as specialised strategic and threat assessments. A regular production of strategic reports on emerging threats and trends was established to identify priorities.

The number of staff has risen from 31 on 31 December 2012 to 77 on 1 January 2017. This increase in staff – although not sufficient to cover all requests from Member States – allows EC3 to support Member States and link investigations in different Member States, either via direct contacts or the Joint Cybercrime Action Task Force (J-CAT) set up by Europol. J-CAT consists of police officers temporarily seconded by national authorities on a temporary basis to EC3 (for a period of up to 6 months). The main added value of this group lies in its ability to pool national intelligence related to a single cybercrime case - which is typically scattered across several Member States - in order to build an accurate picture of its scale and relevance for EU coordinated action.

The EC3 has also charted new territories in terms of strategic cooperation with the private sector, through the creation of its advisory groups.[43] Four dedicated advisory groups have been created in the areas of internet security, financial services, communication services and e-commerce in order to foster closer cooperation with its leading non-law enforcement partners.

EC3's most important contribution remains its operational support to Member States' law enforcement, which has expanded significantly since 2013. The number of high profile operations supported rose from 57 in 2013 to 131 in 2015 and 175 for the first two quarters of 2016.[44] In addition, the EC3 has also seen a strong rise in the strategic and knowledge products it has provided and which are rated highly by EC3's stakeholders: In 2013, 34 strategic and knowledge products were produced, and in the first two quarters of 2016, 91 were created.

Europol and RIPE NCC, one of the five Regional Internet Registries that manage the allocation and registration of internet number resources, signed a Memorandum of Understanding in December 2016 in order to enhance cooperation to tackle cybercrime and internet security[45]. Europol, together with other public safety agencies, has launched an globally coordinated initiative to improve the accuracy of the databases maintained by the five RIRs.

Implementation of the European Strategy for a Better Internet for Children and the Global Alliance against Child Sexual Abuse Online

The Strategy highlighted the role of the Global Alliance against Child Sexual Abuse Online as a tool to improve co-ordination at the EU level.

The Global Alliance Against Child Sexual Abuse Online was launched on 5 December 2012 by the European Commission and the US and it aimed to raise standards worldwide and unite efforts around the world to more effectively combat online sexual crimes against children.[46] It

[43] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board
[44] These figures are not to be accumulated across the years as some cases span across multiple years. Note that the 29 Europol operational teams and focal points together supported 1001 operations in total during 2016.
[45] https://www.europol.europa.eu/newsroom/news/ripe-ncc-and-europol-enhance-cooperation-to-tackle-cybercrime-and-internet-security
[46] https://ec.europa.eu/home-affairs/what-is-new/news/news/2012/20121130_02_en

gathered 54 countries, which committed to pursue concrete actions to enhance victim protection, identify and prosecute offenders, raise awareness, and reduce the availability of child pornography online and the re-victimization of children. In 2013, participating countries submitted concrete commitments in order to reach the four political targets, including by adapting their legal systems, improving cooperation and taking measures to ensure better victim protection.[47]

In 2015, a comprehensive threat assessment conducted by the Global Alliance secretariat revealed that child sexual abuse was still on the rise and criminals were increasingly availing themselves of the many opportunities to evade detection online.[48] In view of this assessment, Ministers and representatives from participating countries, experts from law enforcement authorities, the private sector, victim advocacy groups and frontline organisations assessed what progress has been made in the first two years of the Global Alliance and how to expand the fight against global proliferation of child sexual abuse online in the future. A Ministers' Declaration summarized the outcome of the conference[49] and in the aftermath, countries provided renewed updates on their progress towards achieving the Global Alliance's policy targets.[50]

Progress in developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

In 2014 the EU has adopted its first Cyber Defence Policy Framework as provided by the Strategy, has mainstreamed cyber defence into the Common Security Defence Policy (CSDP) missions and operations, as well as enhanced education, training and exercises. Many efforts have been implemented by the European Defence Agency Cyber Defence Project team to raise Member States' cyber defence capabilities.

The EU-NATO Joint Declaration signed at NATO's Warsaw Summit in July 2016 advanced further EU and NATO coordination on cyber security and defence as provided by the Strategy. Among the biggest successes in overall EU-NATO defence cooperation has been the signing of a Technical Arrangement between CERT-EU (Computer Emergency Response Team for the EU institutions) and NCIRC (NATO Computer Incident Response Capability) in 2016. The Technical Arrangement allows for operational information exchange between the two organisations, which is necessary in peacetime, and will be essential in times of crisis.

Cyber aspects were addressed within the Common Foreign and Security Policy exercises for the first time in 2016. The cyber-dimension has been effectively integrated in the Common Foreign and Security Policy exercise Multi-Layer (ML16)[51] and the Common Security and Defence Policy crisis management MILEX exercises that have taken place in 2016.

The 2014 EU Cyber Defence Policy Framework has provided a relevant and effective framework for strengthening cyber defence in the broader context of CSDP. The revised EU

[47] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_report_201312_en.pdf
[48] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_threat_assessment_en.pdf
[49] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_ministerial_statement_en.pdf
[50] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_2015_report_en.pdf
[51] Multi-Layer 16 and MILEX exercises tested the EU CFSP procedures in reacting to crises outside the EU, with the involvement of the EU Delegations, and CSDP operational headquarters.

Concept for Cyber Defence in EU-led Military Operations and Missions has been adopted. It aims to unlock further integration of cyber defence and security into CSDP missions and operations, also taking into account the need for intensified civil-military cooperation and coordination.

Progress in developing industrial and technological resources for cybersecurity

Promoting a Single Market for cybersecurity products

The Strategy highlighted a number of initiatives to help overcome this fragmentation by building trust between different actors of cybersecurity ecosystem. This was to be partly achieved through the development of security standards and assistance with EU-wide voluntary certifications schemes.

Some progress has been made in gaining knowledge of the different available standards – a necessary step towards ensuring interoperability. A Memorandum of Understanding has been signed between the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunication Standards Institute (ETSI) to facilitate cooperation in defining standards. However, this has not yet led to the development of a common approach at the EU-level.[52]

The relatively slow progress at the EU level related to standardisation and development of possible voluntary certification schemes was coupled with the emergence of a number of national certification schemes.

Fostering R&D investments and innovation

In July 2016, the Commission launched a cybersecurity contractual public private partnership to stimulate the competitiveness and innovation capacities of the digital security and privacy industry in Europe. The contract was signed with the European Cybersecurity Organisation (ECSO) with an end date of 31 December 2020. At the moment ECSO has more than 200 members, including large cybersecurity companies, SMEs and start-ups, research centres, universities, clusters and associations as well as local, regional and national administrations from the EU and European Economic Area (EEA) and the European Free Trade Association (EFTA) as well as Horizon 2020 associated countries[53].

The EU will invest €450 million in calls for proposal related to this partnership, under its research and innovation programme Horizon 2020 (Leadership in Enabling and Industrial Technologies (LEIT-ICT) and Societal Challenge Secure Societies - SC7).

Cybersecurity market players, represented by ECSO, are expected to invest three times more. The Commission expects the industry to complement the public funding with a strong leverage from private investment, including the financing of related research and innovation and market activities.

[52] Conclusions workshop held in the context of the NIS Directive Cooperation Group work on security measures gave the opportunity to Member State authorities to exchange views on how they approach the issue of cybersecurity standards

[53] The European Cyber Security Organisation (ECSO), which signed the contract with the Commission, was launched on 13 June in Brussels. ECSO is a fully self-financed non-for-profit association (ASBL) under Belgian law. The founding members are the European Organisation of Security, Alliance pour la Confiance Numérique, Guardtime acting for the Estonian Association of ICT, and Teletrust. See: www.ecs-org.com

Progress in mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy

In order to set a clear vision and guidance for its international cyber policy, the EU has adopted Cyber Diplomacy Council Conclusions in 2015, which prioritise the promotion of core EU values in cyberspace, the application of existing international law, developing cyber norms and confidence building measures, as well as advancing cybersecurity capacity building globally.

In its Council Conclusions on Internet Governance, the EU supports a multi-stakeholder governance model of the internet that is based on clear principles, in line with the "Netmundial principles"[54] endorsed by EU Member States.

In June 2017 the Foreign Affairs Council adopted the Council Conclusions on a "Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities"[55] The framework makes use of CFSP instruments for the EU to jointly respond to malicious cyber activities.

EU has also set up specific cyber dialogues with the technologically developed strategic partners and major emerging markets – the US, Japan, South Korea, India and China as well as with key international organisations:

- The **EU-U.S. Cyber Dialogue**[56] - the dialogue has effectively addressed politico-military and international security issues, including norms of state behaviour, the application of existing international law in cyberspace, and confidence building measures as well as co-ordination of efforts in cyber security capacity building in third countries. It also allowed taking stock of best practices in addressing cybercrime and raising cyber resilience.
- The **EU-China Cyber Taskforce** has made progress since 2012. The Taskforce has offered an opportunity to exchange views on international cyberspace issues, the economic aspects of IT security and cybersecurity with Chinese counterparts. In addition, a parallel non-governmental engagement between EU and China to discuss international cybersecurity and international law issues has been set up allowing for a better understanding between both parties. Furthermore, a non-governmental Expert Group on Economic Aspects of ICT Security was set up in 2016.
- The **EU-Japan Cyber Dialogue** has allowed addressing key international policy perspectives with Japan, which is a key strategic partner in Asia with significant influence in the region. Japan is a party to the Council of Europe Convention on Cybercrime (the Budapest Convention) and is among the 'like-minded States' when it comes to promoting the Convention. Japan is also a member of the We Protect Global Alliance to End Child Sexual Exploitation Online.
- The **EU-Republic of Korea Dialogue** has effectively addressed issues such as global cyber developments, cyber strategies and policies, international norms in Cyberspace and cyber confidence building measures. The Republic of Korea has several cyber capacity building programmes in Africa, Asia and Latin America, and acts as a broker between the different Asian countries on international security issues.

[54] http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
[55] Council Conclusions on "Joint EU diplomatic response on cyber operations".
[56] Dialogue has built on EU-US Working Group on Cybercrime and Cyber security, which priorities include awareness raising, standards for risk management, the strengthening of operational cooperation between EU and U.S. Computer Emergency Response Teams, the advancement of the Global Alliance against Child Sexual Abuse Online.

- Two **EU-India Cyber Dialogues** in 2013 and 2015 have identified many common areas of interest, and India has made progress in developing its international cyber policy. India has a growing interest in cybersecurity education and training. India will be the host of the fifth edition of the Global Conference on Cyber Space (GCCS) in 2017 and has been appointed as one of the two co-chairs of the Global Forum on Cyber Expertise at the beginning of 2017.
- Additionally, close consultations have taken place with the Council of Europe (CoE), the ASEAN Regional Forum (ARF), the Organisation for Security and Cooperation in Europe (OSCE), the United Nations (UN), the African Union (AU), and the Organisation for Economic Cooperation and Development (OECD).

Support to the development of norms of behaviour and confidence building measures in cybersecurity

The EU has been promoting the work of the UN Group of Governmental Experts (UN GGE) on developments in the field of information and telecommunications in the context of international security related to the application of existing international law and the development of voluntary norms for state behaviour to address existing and potential threats and contribute to stability in cyberspace. Six EU Member States were engaged in the 2016-2017 UN GGE work (United Kingdom, France, Germany, Estonia, Netherlands, Finland) and were regularly updating all 28 Member States on the progress made in the UN format. In 2017, UNGGE did not produce a report due to increasing differences in visions among major global players how cyberspace could be stabilised. Many important elements on the application of existing international law and a list of cyber norms were articulated in the UN GGE 2013 and 2015 reports[57].

In general, some useful steps have been taken towards better analysis on the application of existing international law to cyber conflicts, such as the preparation of the Tallinn Manuals[58] that constitute an academic analysis of international law applying in cyberspace during wartime and peacetime.

The EU has also made efforts to support the development of Cyber Confidence Building Measures in OSCE and the ASEAN Regional Forum. The EEAS, together with Malaysia and the Netherlands, supported by the EU Member States, organised a cybersecurity workshop on operationalising cyber confidence building measures in the framework of the ASEAN Regional Forum in March 2016.

[57] A/68/98 and A/70/174.

[58] The Tallinn Manual 2.0 is the most comprehensive analysis of how existing international law applies to cyberspace. Authored by nineteen international law experts, the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", the updated and considerably expanded second edition of the 2013 "Tallinn Manual on the International Law Applicable to Cyber Warfare", is an influential resource for legal advisers dealing with cyber issues. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence. See: https://ccdcoe.org/tallinn-manual.html

Support the promotion and protection of fundamental rights, including access to information and freedom of expression

On 12 May 2014 the Foreign Affairs Council adopted the EU Human Rights Guidelines "on freedom of expression online and offline". Building upon existing instruments and documents, these guidelines have helped to implement key human rights principles online.

The EU has, through its bilateral human rights dialogues that have taken place since the adoption of the guidelines, informed third countries of the adoption of the guidelines and encouraged them to take active steps to prevent censorship. The EU has also organised a number of events to promote the Guidelines by raising awareness on online freedoms via its Delegations and civil society organisations.

The EU has been actively engaged in debates at the Internet Governance Forum (IGF) and on the 10 year review of the World Summit on the Information Society (WSIS) and the Global Conference on Cyberspace with a view to promoting a human rights perspective. Council Conclusions on Internet Governance were adopted on 27 November 2014 (16200/14), where the EU reaffirmed the vision of the Internet as a single, open, neutral, free, un-fragmented network, subject to the same laws that apply offline, where individuals can benefit from their rights, and from judicial remedies when those rights are infringed; as well as its commitment to promote multistakeholder governance structures that are based on a coherent set of global Internet governance principles, consistent with human rights and fundamental freedom online.

In order to mainstream the protection and promotion of freedom of expression in all the EU's external actions, the EEAS and the Commission have created an informal inter service group to coordinate freedom of expression related topics. It has been very active in the drafting of the EU guidelines and in the preparation of the EU-NGO Human Rights Forums focused on Freedom of Expression online and offline.

Support global capacity-building in third countries by engaging with international partners and organisations, the private sector and civil society

The EU has successfully started capacity building efforts in third countries by developing an efficient model and allocating, together with the Council of Europe, increasing funds to address cybercrime globally.

Since 2010, the EU has used development cooperation funds in the fight against cybercrime in joint projects with the Council of Europe in Western Balkans and Eastern Partners. In 2013 the EU launched, together with the Council of Europe, a global initiative on cybercrime (GLACY), contributing three million Euro under the EU's Instrument Contributing to Stability and Peace. This initiative was also implemented with Europol and Member States (France, Romania). Another programme implemented by the Council of Europe and Interpol with the budget of nine million Euro started in mid-2016.

In addition to promoting the Budapest Convention, the EU programmes have concentrated on training law enforcement officials. New programmes have started in 2017 to strengthen technical and organisational cyber incident response capacity in developing countries.

3.2 THE CYBERSECURITY LANDSCAPE IN 2017

Cybersecurity threats

According to Eurostat data on Internet access and use statistics of households and individuals, 85% of European households had access to the Internet (fixed or mobile) from home in 2016 compared to 55% in 2007. A change in the use of devices to access the Internet can also be noted: there has been a dramatic rise in the proportion of people who access the Internet using smartphones, more than doubling from just over a third (35%) in 2013 to nearly eight in ten (79%) of those polled in the current survey. In 2016, 79% of individuals were regular users (at least weekly) of the Internet: 71% of individuals in the EU-28 accessed the Internet on a daily basis with a further 8% using it at least once a week (but not daily). Today, in the EU, 7 in 10 people access the Internet every day. The "Internet of Things revolution" has become a fact with fifty billion new devices expected to be connected to the Internet by 2020.

The cybersecurity threat landscape has substantially evolved and looks quite different in 2017 compared to 2013. The ever-increasing connectivity of poorly secured devices (reaching today the key systems that control citizens' cars, factories, homes, farms, hospitals and all critical infrastructures) have substantially increased the surface of possible cyber-attacks, eagerly used by cybercriminals[59]. Accordingly, the rate of growth of cybercrime has outpaced the rate of new connections to the Internet.

Cyber-attacks are, in fact, booming. A 2016 study by PwC[60] revealed that the number of security incidents across all industries rose by 38% in 2015, which is the biggest increase in the past 12 years. The study identifies that 80% of European companies have experienced at least one cybersecurity incident and in Q3 2016 alone, 18 million new malware samples were captured, that is an average of 200,000 per day.

In some Member States, it has been estimated that more than half of all crimes are cybercrimes[61]. Some of these cyber-attacks have aimed at high-profile targets, including power grids, important webmail services, central banks, telecom companies and electoral commissions. Moreover, a large share of cybersecurity incidents happens due to technical failures without malicious intent – products weak on security, lack of software updates or appropriate procedures – or some type of human error.

At the same time, the current cybersecurity threat landscape is also characterised by "the efficiency of cybercrime monetization" and this trend is likely to continue. Cyber-attacks including multiple channels and various layers seem to be the "state of the art", while robust,

[59] The October 2016 *Dyn* incident – a disturbed denial of service attack, which resulted in the break-down of some of the biggest websites in the world including Twitter, The Guardian, Netflix, Reddit, Aribnb and CNN is just one of many examples in the recent months of how these vulnerabilities can and are exploited.

[60] PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

[61] http:/www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

efficiently managed flexible cyberattack tools became a service widely available, even to low capability threat agents.[62]

The "ENISA Threat Landscape 2016" summarizes the top 15 cyber-threats and threat trends:

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	⊃	6. Phishing	⊃	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	⊃	8. Ransomware	⊃	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	⊃	↓
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	↓
11. Data breaches	⊃	11. Exploit kits	↑	↓
12. Identity theft	⊃	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 2: Overview and comparison of the current threat landscape 2016 with the one of 2015[63]

When it comes to cyber-attacks, the perpetrators often tend to collaborate internationally by sharing information, building their intelligence collectively, rapidly responding to possible counter-measures from the victims and practicing the same values and behaviours. Despite some progress made in the past years the level of cooperation and coordination on the side of public authorities and businesses in the EU has not kept pace, leaving us less well defended against a better coordinated and more sophisticated threat.

New unexpected threats have also emerged. The politically motivated use of cyber vectors to undermine democratic systems has become a significant threat to the security and integrity of European democracies, societies and businesses. These actors, directly or via proxies, leverage a significant amount of technical expertise, human and financial resources to gain political or commercial advantage.[64] Numbers relating to the exploitation of vulnerabilities in the Domain Name Servers are also concerning[65].

Awareness and skills gap

Technology has facilitated a continuous and increasingly intensive access to the Internet by a wide range of individuals whose cyber skills can range from near illiteracy to extensive experience in using IT.

[62] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
[63] ENISA Threat Landscape Report 2016: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[64] http://www.iss.europa.eu/uploads/media/Brief_30_Cyber.pdf
[65] https://www.icann.org/public-comments/sadag-final-2017-08-09-en

According to the most recent Eurobarometer study,[66] in the last three years, many Internet users in the EU have taken at least some action to increase their security and privacy online. 45% installed or changed antivirus software, 35% are opening emails only from known sources. One quarter started using different passwords for different websites and changing them regularly. The results show, however, that there are still vast groups of citizens who are not taking any action to increase their security and privacy online.

Opportunities for employment in the field of cybersecurity are growing. The total for Cybersecurity employment in Europe 2016 was 909,600[67]. This was an increase of 17% compared to the 2015 employment count of 775,700. This compares with a previous increase of 22% for the 2014-2015 period. The EU accounted for 25% of the global employment in the field of cybersecurity for 2016.

While there are opportunities for employment and European citizens who want to learn and/or specialize in cybersecurity can nowadays access almost 500 university courses and trainings across Europe,[68] the cybersecurity skills gap across all sectors remains a major challenge and talent pool is not keeping up the pace. The cybersecurity skills gap for cybersecurity professionals working in industry in Europe is predicted to be 350 000 (globally 1.8 million) by 2022. Two-thirds of the European security professionals surveyed for the 2017 Global Information Security Workforce Study said there was too few staff available in their field, a proportion in line with the worldwide figure, which rose from 62 percent worldwide in 2015.[69]

4 METHODOLOGY

The assessment of the Cybersecurity strategy started in 2017 and was overseen by an Inter-service Steering Committee composed of relevant Directorates-General within the European Commission and the European External Action Service. Work concluded in September 2017 with this Staff Working Document.

As detailed in Annex 2 to this document, the assessment was carried out, to the extent possible, using the triangulation technique - a common evaluation method that brings together at least three sources of data and tools for data collection, and is embedded in a structured approach.

Data and information was gathered through a literature review, stakeholder consultations and expert workshops (see below). No open public consultation was conducted for this initiative as the thematic was already covered by other public open consultations conducted in the context of the evaluation of the European Network and Information Security Agency (ENISA) as well as the contractual Public Private Partnership.

Assessing causality between the EU Cybersecurity Strategy and the results on the ground was not straightforward. Indeed, when it comes to the issue of cybersecurity, a large number of

[66] Special Eurobarometer 460, 2017
[67] Results of the Cybersecurity Market analysis conducted by LSEC and PwC, V2 2017 Draft Report, 30/06/2017 (Final report to be issued in October 2017).
[68] https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities
[69] 2017 Global Information Security Workforce Study commissioned by the Centre for Cyber Safety and Education and (ISC)2, was carried out from 22 June to 11 September, 2016, and surveyed 19,641 IT security professionals from 170 countries, including nearly 3,700 respondents in Europe, https://www.isc2.org/pressreleasedetails.aspx?id=14570

intervening factors are at play, making the isolation of the Strategy's impact a difficult exercise.

Coupled with the added limitation of the relatively recent implementation of the associated legislative instruments, it was evident that measuring its impact would prove challenging. Furthermore, data is difficult to obtain. Both primary and secondary sources are scarce. Currently there is little information and independent analyses available on key cybersecurity issues (such as the economics of cybersecurity, reliable trends of expected new challenges, the best solutions to face threats) that cover the whole EU. Ministries in most Member States responsible for cybersecurity do not collect on regular basis official data regarding cybersecurity.

The lack of a compulsory and common monitoring system also makes it very difficult to verify any progress made as a result of the application of the strategy.

Given the aforementioned challenges, it was clear from the outset that the methodology for this assessment would be based on a number of qualitative inputs gathered through different tools and stakeholder fora, including, among others:

- **Desk research** by relevant services of the European Commission and European External Action Service. It was undertaken in order to identify all contextual elements, issues and existing studies, including evaluations.
- **Monitoring activities (e.g. The Council's EU Cybersecurity Strategy Roadmap,** which monitors initiatives implemented by Member States.)
- **Member States' feedback** through Council Horizontal Working Party on Cybersecurity and a high-level Roundtable with Member States, as well as written submissions of Member States.:
- **The input of relevant agencies**, including the European Network and Information Security Agency and Europol (EC3).
- **Input from industry representatives** (through contractual Public Private Partnership and industry leaders input).
- **Public consultations:**
    - The 2016 public consultation on contractual Public Private Partnerships (cPPPs) on cybersecurity and accompanying measures, which included also questions related to the broader cybersecurity context; **Consultation gathered 241 responses ;**
    - The public consultation and evaluation process of the European Network and Information Security Agency (ENISA), and which included also forward looking questions on the EU cybersecurity needs. Consultation gathered 90 responses, including the input of the authorities of more than a half of Member States'.
- **Stakeholder events related to different elements that can be potentially addressed by the reviewed Strategy** (blueprint for cooperation workshop with Member States, certification workshops with Member States and other stakeholders).
- The Cybersecurity **Eurobarometer** studies conducted at regular intervals.

The full list of sources used for this assessment is provided in Annex 1. The synopsis report summarising the results of the different consultation activities is provided in Annex 2.

The wide range and high number of stakeholders consulted thanks to the outlined methodology ensured a satisfactory level of reliability of the results. As indicated above the lack of similar studies on this subject makes a comparative analysis difficult to conduct. ENISA's latest evaluation report contains some overlap with this assessment, the results of which appear to coincide. It can therefore be concluded that the data collected during this evaluation is valid and for the most part robust.

5 ASSSESSMENT OF THE 2013 CYBERSECURITY STRATEGY

5.1 OBJECTIVE 1 OF THE STRATEGY : CYBER RESILIENCE

The first objective of the strategy was to **achieve cyber resilience.** This was supposed to be achieved via 3 means: improved capabilities; improved cooperation and increased awareness. Twelve actions (1 legislative and 11 non-legislative) were linked to this objective.

The following sections examine whether this overall objective has been achieved, the extent to which the individual actions have effectively contributed to this objective and whether the objective is still relevant today. The assessment of the individual actions linked to this objective falls outside of the scope of this exercise.

5.1.1 To what extent has the objective been achieved?

The NIS Directive[70], adopted in July 2016, included a coherent set of measures calling for targeted action by Member States, who have the primary responsibility for cybersecurity, by key internet enablers and by critical infrastructure operators. The expectations are that this should result in a clear policy cybersecurity framework for the national level, helping all relevant stakeholders achieve the common goal of improving cyber resilience.

As described in Chapter 3, the Directive is currently subject to transposition into national law by Member States. It is therefore too early to assess its effectiveness and efficiency. Nevertheless, a series of observations can already be made on how the NIS transposition process influenced the capabilities, cooperation and information sharing mechanisms and hence the cybersecurity resilience.

Improved Capabilities

Today considerable discrepancies can still be observed between Member States' cybersecurity policies, legal frameworks and operational capabilities[71.] As a consequence, the effectiveness of the measures taken at national level by one or a few Member States can be affected by the lower level of protection in another Member State, potentially resulting in a "contagion" effect in case of serious disruptions affecting the "weakest links" in the EU community.

However, the instrument used by the Strategy – the NIS Directive – has already triggered positive developments. At the time of drafting this document, 25 Member States have either updated or developed a National Cyber Security Strategy and 2 have a draft in public consultation (compared to 12 Member States in 2013). Whereas the full assessment of the

[70] 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.
[71] Global Cybersecurity Index & Cyberwellness Profiles, ABI Research and ITU, 2015.

Strategies has not been conducted yet, these national Strategies are likely to achieve a certain level of alignment given that they need to address how to comply with the requirements of the NIS Directive. This should contribute to advancing towards the 2013 Strategy objective of strengthening Member States' resilience.

Some progress has been also noted in terms of building national operational capabilities. All Member States have now a governmental/national CERT in place requested by the NIS Directive. As highlighted in the ENISA's evaluation report, the Agency's work has contributed to enhanced capacities of CERTs, most notably the ones with more limited capabilities and resources in the area of cybersecurity. However, the level of CERTs' capacity across the EU is still uneven as proved by the Global Cybersecurity Index & Cyber-wellness Profiles 2017.[72] A number of Member States have well-resourced CERTs in place, whereas others have only recently created such structures, which are not yet fully operational. This is due, among others, limited financial and human resources devoted as well as difficulties in finding skilled experts. This has been also confirmed by the exchange of experience and discussions during the Cooperation Group and CSIRT network meetings. The recent global ransomware attacks, which were a stress-test for the CERTs, also confirmed these observations.

While the objective of reaching full capacities has not been achieved yet, it can be still concluded, that at this early stage of the Directive's implementation, Member States have already made some progress, which proves the added-value of the action at the EU level. In this context it needs to be noted that according to the recent public consultation conducted in the framework of ENISA evaluation[73] Member States and other stakeholders especially appreciate the bi-annual "Cyber Europe" exercises, which involved more than 4000 cybersecurity experts from over 2000 different organizations to date. This is also confirmed by the satisfaction surveys following the exercises, which show the level of satisfaction as high to very high for 99% of the participants. The relevance of this resilience capacity building activity was also confirmed by the view of a number of stakeholders[74] suggesting that such exercises should be both scaled up and conducted more frequently given the fast evolving nature of the cyber threats. This is, however, not feasible at the moment in view of the limited resources of the Agency.

The NIS Directive, once fully transposed and implemented, is expected to lead to increased capabilities of the private sector to manage risks and respond to cybersecurity incidents. However, it has to be noted that the requirements of the Directive concern only selected sectors and entities. In addition, the efficient and comprehensive identification of such entities will depend on each Member State's ability to do so. Therefore although it is too early to fully assess the effectiveness of this instrument, it can be assumed it not likely to directly impact some sectors leaving a clear gap that reduces the effectiveness of the Strategy in achieving its goal.

Finding 1: *Based on the desk research, a majority of Member States' have engaged in activities to develop their internal capacities and this despite the early stage of the NIS Directive transposition process. Stakeholders attribute this result to the recent actions taken at the EU level.*

[72] Global Cybersecurity Index & Cyber-wellness Profiles, ABI Research and ITU, 2017.
[73] Study on the Evaluation of the European Union Agency for Network and Information Security.
[74] Discussion in the Horizontal Working party on cybersecurity on 12 June 2017.

Finding 2: *Member States capabilities, despite progress made, are still uneven with some Member States having fully-operational CERTs in place while others are at the beginning of the process of creating real capacities. This is attributed, among others, to limited human and financial resources available in some Member States as well as difficulties in finding specialists due to a cybersecurity skills gap experienced across the EU and globally.*

Finding 3: *The Cybersecurity Strategy, via the NIS Directive, is likely to contribute to increased capacities and resilience of some private entities, which will be identified as essential operators. However, cybersecurity is not likely to directly impact the sectors not covered by the Directive, or the entities working within the sectors covered by it but not listed by Member States as "operators of essential services". This reduces the effectiveness of the Strategy as it negatively impacts the level of resilience of our economies and societies.*

Finding 4: *Capacity building support related to building resilience e.g. through trainings, bi-annual Cyber Exercises, has proved useful for both the private sector and public authorities. However, the usefulness of this support depends on the level of maturity of Member States, with less advanced Member States finding it particularly useful. At the same time some stakeholders argued that some of the capacity building activities e.g. Cyber Europe exercises should be scaled up and conducted more frequently given the fast evolving nature of the cyber threats. This is, however, not feasible at the moment in view of the limited resources of the Agency.*

Improved Cooperation and information exchange

Cooperation across Member States, between public and private actors and between the national and the EU level is gradually taking shape. Progress achieved in the cooperation at the EU level is quite substantial, if compared to the baseline scenario whereby neither the Cooperation Group nor CSIRT Network involving all Member States, existed, proving the added-value of action at the EU level.

However, it needs to be emphasised that the cooperation remains voluntary under the Directive, which might hamper the effectiveness of these mechanism. The trust deficit has not yet been overcome at this early stage of its implementation, which leads to resistance from the concerned actors to embrace collaboration on a topic that is perceived close to national security and for which a culture of cooperation is still not widespread.

In fact, the cooperation on operational matters, in particular on detection and response to cybersecurity incidents is still limited. The May 2017 ransomware attack presented a first opportunity for Member States to use the CSIRT Network - a mechanism created by the NIS Directive. This first "stress-test" highlighted the importance of the CSIRT Network although the cooperation still takes place in a smaller circle of Member States with well-developed capacities (informal European Government CERTs Group), which closely cooperated in real-time as the attack unrolled. This group took the leading role in providing timely guidance. This was then shared with the CSIRT Network and helped other Member States, whose capacities and resources do not yet allow for such a swift reaction. The CSIRT Network also proved very useful in terms of analyzing lessons learnt in its aftermath.

At the same time, as far as cross-border cooperation in case of a major cyber-incident is concerned, the EU still lacks an effective mechanism for coordinated crisis response. Despite

some progress made at the operational level as highlighted above there is not yet a coordinated reaction to a cyber crisis across the EU at a more strategic level. The NIS Cooperation Group, which provides more long-term strategic policy guidance, is not the right mechanism to ensure such response.

Cybersecurity is not mainstreamed in the current EU crisis response mechanisms such as e.g. the Council's Integrated Political Crisis Response[75], nor in relevant sectoral mechanisms or external EU Crisis Response Mechanism[76].

In case of a major cross-border incident, the communication between European institutions, relevant agencies and bodies (ENISA, EUROPOL, CERT-EU, CSIRT Network, EU INTCEN, the EU Intelligence and Situation Centre, the Commission services) is based more on informal relationships rather than on established procedures, as proved by the *modus operandi* experienced during recent incidents. No crisis response communication system is used for cybersecurity issues either e.g. the Commission ARGUS[77] general alert system does not cover cybersecurity either. In 2017, the EU Hybrid Fusion Cell was set up within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS) to offer a single focus for the analysis of external aspects of hybrid threats, including cyber threats. The Fusion Cell will receive, analyse and share classified and open source information from different stakeholders within the EEAS, the Commission and Member States specifically relating to indicators and warnings concerning these threats. The Cell enhances awareness and provides inputs to security risk assessment processes which support policy-making at national and EU levels.

However, numerous reports and stakeholder views[78] emphasise limited progress in achieving a fully coherent cybersecurity governance framework at the European level. Many organisations in the EU ecosystem are involved and some are gaining competence in cybersecurity. Apart from the European Commission[79] and the European External Action Service (EEAS), it is possible to identify four main actors dealing with cybersecurity, cybercrime and cyber defence (CERT of the EU institutions, agencies and bodies (CERT-EU), European Network and Information Security Agency – ENISA, EUROPOL/European Cybercrime Centre (EC3) and EU INTCEN, the EU Intelligence and Situation Centre and the European Defence Agency (EDA)). Sectorial agencies (transport and finance for examples) are also gaining competence in this field.

According to stakeholders and literature review[80], the large number of actors dealing with cybersecurity leads to fragmentation and duplication of efforts. Information and expertise are dispersed across several entities, and these entities often produce, collect and disseminate information and analyses, in some cases on the same topic and addressing the same public. Furthermore, the coordination mechanisms, where they exist, are not always adequate. For example, from the evaluation of ENISA and the stakeholder consultations we can conclude

[75] Integrated Political Crisis Response (IPCR) Arrangements are crisis arrangements agreed in 2013 by the Council.
[76] E.g. The EEAS Crisis Response System (CRS), which covers crises which may affect EU security and interests occurring outside the EU, including those affecting the EU delegations or any other EU asset or person in a third country. It equally covers crisis occurring inside the EU if those have an external dimension.
[77] ARGUS is the Commission's general alert system in place since 2005.
[78] European political Strategy Centre, 2017; ENISA evaluation report; discussions at the Horizontal Working Party for Cybersecurity – 7 June 2017.
[79] Within the European Commission two main Directorate Generals (DG CONNECT and DG HOME) are tasked with addressing overall cybersecurity and cybercrime while at least eight Directorate Generals have started initiatives at sectoral level.
[80] See ENISA public consultation and evaluation report, see also: European Political Strategy Centre Strategic Notes: Building an Effective European Cybershield - taking EU cooperation to the next level.

that a good level of cooperation and coordination has been achieved between ENISA and EC3: there is almost no overlap between the two organisations, which seem to cooperate well. On the other side, there is still room for improvement in the coordination between ENISA and sectorial agencies, and the European Commission and CERT-EU. In particular, the evaluation highlighted that in spite of different scope of their mandate (one EU-wide, the other targeted to EU institutions); there is a risk of overlap between ENISA and CERT-EU in the areas of direct support and assistance to Member States' CSIRTs and cross-border operational cooperation.

Last but not least, a significant gap relates to cooperation and information sharing between different stakeholders, including public-private cooperation. The level of this cooperation and approach to it still differs across the EU with only a few Member States having in place mature frameworks for public-private partnerships[81]. For example, only recently Information Sharing and Analysis Centres (ISACs) to support the protection of critical infrastructures are emerging in the EU. This is partly due to the lack of trusted reporting channels for the industry and financing mechanisms to support such initiatives. As information exchange is key to be able to prevent potential incidents, insufficient level of private-public cooperation in this regard hampers the possibility of full achievement of the Strategy goals.

[81] EU cybersecurity dashboard, BSA, 2015.

Finding 5: *The Cybersecurity strategy - via the NIS Directive - has laid the grounds for improved strategic and operational cooperation at the EU level, filling in the vacuum that existed before. As cooperation is voluntary in nature, the effectiveness of these measures will depend on the willingness of Member States to use them.*

Finding 6: *The operational cooperation mechanism (so-called CSIRTs Network), has made substantial progress since its establishment. However, not all Member States are yet equally engaged in its activities (largely due to different level of capacities and resources available) and the initial cooperation in case of a major cyber incident involved only some of Member States.*

Finding 7: *Desk research, survey results and experience of recent cross-border incidents have shown that the Cybersecurity Strategy and its instruments are limited in their capacity to deliver EU-level cooperation mechanism in case of a large-scale cross-border cyber incident. This is partially due to the fact that cybersecurity has not been yet mainstreamed in the existing crisis response mechanisms at the EU level.*

Finding 8: *In case of a major cross-border incident the communication between European institutions, relevant agencies and bodies (ENISA, EUROPOL, CERT-EU,* EU INTCEN, the EU Intelligence and Situation Centre*) is based more on informal relationships rather than on established procedures. No crisis response communication system is used for cybersecurity issues either. This might lead to inefficiencies and hamper the effectiveness of the EU support to Member States.*

Finding 9: *Numerous reports and stakeholder views emphasise limited progress in achieving a coherent cybersecurity governance framework at the European level, with overlaps of mandates and duties of different institutions and bodies. This leads to inefficiencies and less effective support to the efforts of Member States.*

Finding 10: *The level of information exchange between private stakeholders as well as between public and private sectors is not yet optimal due to lack of trusted reporting mechanisms and incentives to share information. As information exchange is key to effective cybersecurity prevention, insufficient level of private-public cooperation in this regard hampers the possibility of full achievement of the Strategy goals.*

Raising Cybersecurity Awareness

The 2013 EU Cybersecurity Strategy sought to support improving the level of cybersecurity awareness among the end-users. As, in line with the subsidiarity principle, the cybersecurity awareness raising is mostly promoted at the national level, the Strategy called Member States and the private sector to increase efforts in this regard. However, it also outlined a number of activities at the EU level to support Member States and other stakeholders in their efforts such as the European Cybersecurity Month (ECSM) and the Cybersecurity Challenge to help bridge the skills gaps.

At least 18 Member States organise national awareness campaigns, usually aimed at the Public Sector (80%) followed by adults, children, adolescents and SMEs[82].

At EU level, since 2013, ENISA, together with partners in Member States and the European Commission, runs the European Cyber Security Month (ECSM), an EU advocacy campaign taking place in the month of October to raise awareness about cybersecurity issues and

[82] Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.

promote among citizens a sense of shared responsibility to practice safe and informed behaviours on the Internet[83] Over the years, the ECSM outreach has extended to diversified audiences ranging from professional organisations, to users' organisations and the general public. More than 30 countries take part in the campaign. The progress of the campaign itself has been considerable with a number of cybersecurity activities taking place in October each year across Europe rising by 296% (from 115 to 455) between 2013 and 2016.[84]

At the same time it is clear that the level of engagement of different Member States differs a lot. The graph below illustrates the top ten countries with respect to the number of events registered during ECSM in October 2016:

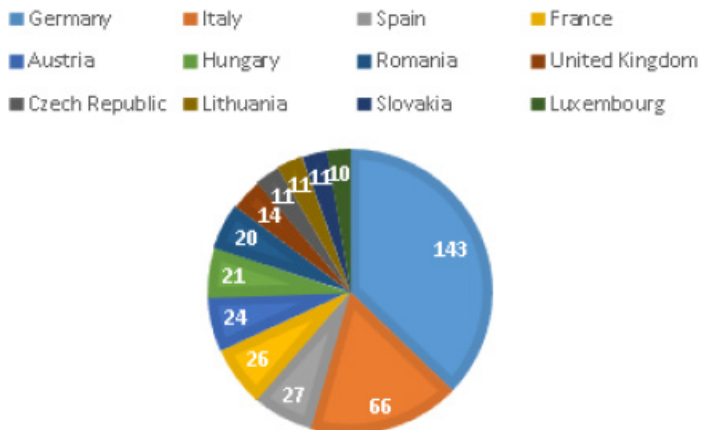

Figure 3: Top Ten countries with respect to the number of events during ECSM

All campaign partners that took part in the survey for the yearly evaluation report[85] stated that the campaign added value to their national campaigns and that it provided the support they needed and required for sharing ideas.

The added-value of this activity was also confirmed by the survey among Member States conducted in 2016 by the Council[86], which assessed cybersecurity awareness activities carried out across the European Union. In fact, the findings of the survey reveal that Member States authorities feel that cooperation needs to be extended more on a pan-European scale to harmonise learning and support and that the coordination role of ENISA and Europol should be strengthened, including the provision of more funds to these bodies for such activities.

While these sources confirm the relevance of activities supporting Member States and other stakeholders at the European level, the effectiveness of this activity in achieving the objective of raising general awareness especially for EU citizens, cannot be assessed given the inherent limitations of the current data gathering methods used to evaluate the campaign.[87] However,

[83] ENISA provided the following data with regard to the ECSM for the period 2013 – 2016: i) the number of cybersecurity activities taking place in October across Europe and the online outreach of the campaign increased at annual growth rate of 41%; featured press articles of European Cyber Security Month increased at an annual growth rate of 44% reaching 429 articles.

[84] European Cybersecurity Month Deployment Report 2016: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month

[85] European Cybersecurity Month Deployment Report 2016: https://www.enisa.europa.eu/publications/ecsm2016-deployment-report

[86] Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.

[87] European Cybersecurity Month Deployment Report 2016: https://www.enisa.europa.eu/publications/ecsm2016-deployment-report

given the limitations mentioned above (limited although growing engagement of Member States and limited resources devoted to the campaign), it can be assumed that the campaign alone, in its current form, although adding-value to Member States, is not sufficient to respond to the challenge of insufficient cybersecurity awareness across European Union.

At the same time it has to also be noted that the objective of raising awareness has been formulated in the Strategy in a non-quantitative manner. Striving to achieve this objective should be a continuous effort, given that threat landscape is changing rapidly exposing citizens to new threats.

However, despite cybersecurity getting increasingly higher in the political agenda, and in spite of the Member States and EU action, European citizens and companies still seem to have limited awareness and knowledge of cybersecurity issues, ranging from basic steps to secure one's online presence to key information on the financial impact of cyber incidents.

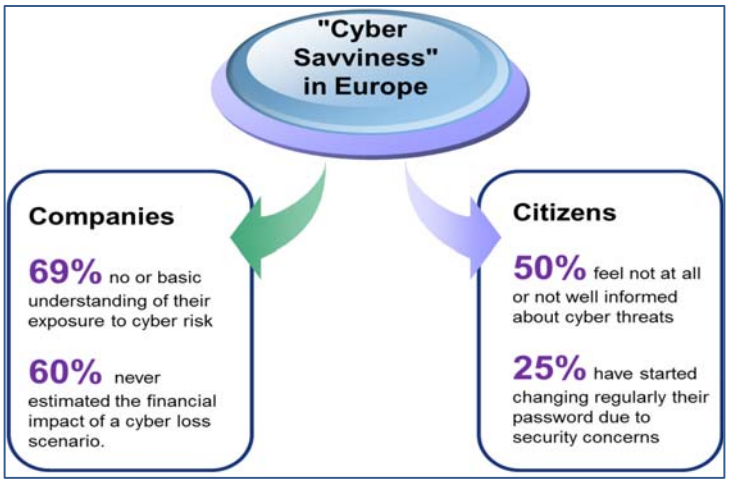

Figure 4: Some figures[88] on awareness and knowledge of cybersecurity issues in Europe

The most recent Eurobarometer Study[89] seems to suggest that despite the efforts made, cybersecurity awareness across the EU has not improved in the last three years. In fact, in 2017, a majority of respondents (51%) do not feel well informed about the risks of cybercrime (see figure 5 below). Moreover, a big majority of respondents (86%) believe that the risk of becoming a victim of cybercrime is increasing. Since 2014, there has been steady growth in the proportion of respondents concerned about different forms of cybercrime. This Eurobarometer (464) marks the first time where there is a majority of respondents feeling concerned about all forms of cybercrimes tested in the survey.

While increasing concern can be noted, the measures that can be taken to avoid becoming a victim of cybercrime do not seem well known to the Internet users. In fact, the EU average indicates that less than half (44%) of respondents claimed they felt able to protect themselves against cybercrime. In 2017, 42% of respondents have discovered malicious software on their device and over one in ten has been a victim of bank card or online banking fraud.

[88] "Cyber Security" Eurobarometer 2015, Attitudes towards the impact of digitisation and automation on daily life" Eurobarometer 2017, Continental European Cyber Risk Survey 2016 Report.
[89] Special Eurobarometer 464, 2017

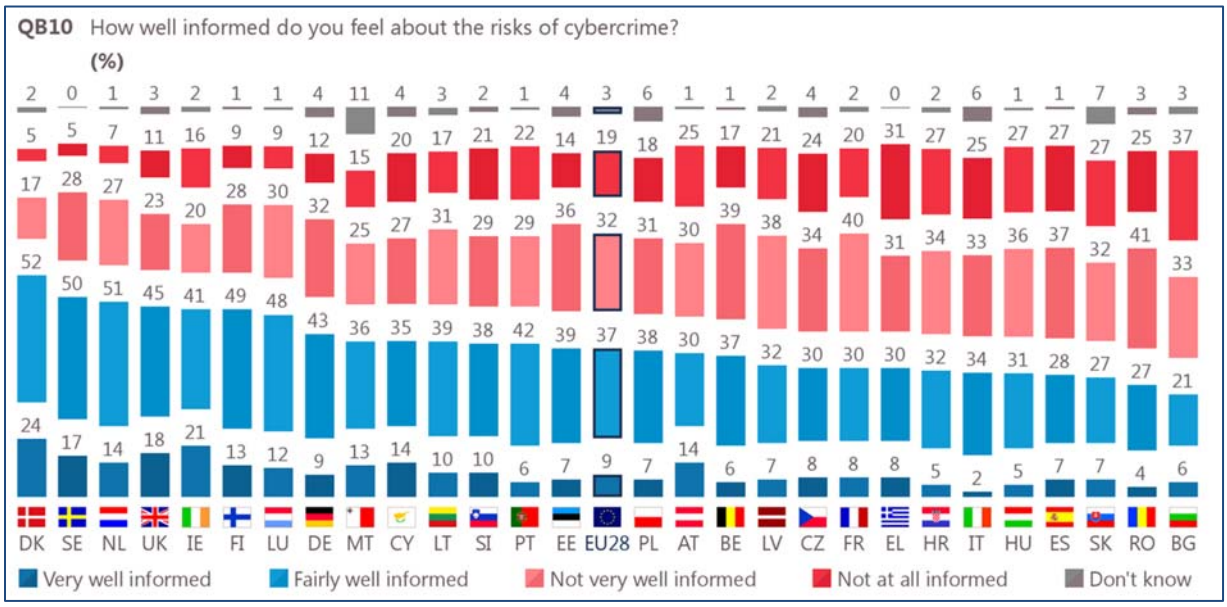

Figure 5: In average in the EU, 51% of respondents do not feel well informed about the risks of cybercrime

The proportion of Internet users in the EU who have taken at least some action to increase their security and privacy online remains comparable to 2013 levels. However, in 2013 45% of respondents stated they open emails only from known sources whereas in 2017[90] the same statement was chosen by only 35% of respondents. In 2017 a smaller proportion of respondents declared installing anti-virus software (45% compared to 51% in 2013) as well.

As far as the skills gaps is concerned, and as foreseen the 2013 Strategy, the Commission and ENISA have also organised a yearly cybersecurity championship - a European Cyber Security Challenge (ECSC) - leveraging on existing national competitions to promote cyber security amongst young students, European industries and the general public and help close the cybersecurity skills gap. Since 2014 the ECSC has managed to considerably expand its audience, with only 2 Member States and Switzerland participating in 2014 to 13 Member States and Switzerland in 2017, which is set to involve 150 students. The first impact study of ECSC will be conducted this year with results expected in Q4 2017.

However, as with the European Cybersecurity Month, while the growing interest in the initiative proves its added-value and relevance for the partners involved, this activity alone is not likely to fix the challenge of the yawning cybersecurity skills gap in Europe, which is predicted to achieve 350 000 (globally 1.8 million) by 2022.[91]

The EU Cybersecurity Strategy also aimed to encourage stepping up national efforts on NIS education and training by introducing training on NIS in schools, training on NIS and secure software development and personal data protection for computer sciences students;

Finding 11: *The Cybersecurity Strategy, despite having successfully triggered a series of awareness raising and skills building events (e.g. European Cyber Security Month, Cyber Challenge) is only partially effective in raising the awareness of citizens and businesses at national level. This is partly due to the magnitude of the task as well as the limited*

[90] Results of the Special Eurobarometer 460, 2017
[91] 2017 Global Information Security Workforce Study commissioned by the Centre for Cyber Safety and Education and (ISC)2, was carried out from 22 June to 11 September, 2016, and surveyed 19,641 IT security professionals from 170 countries, including nearly 3,700 respondents in Europe, https://www.isc2.org/pressreleasedetails.aspx?id=14570

resources available. The subsidiarity principle is also a key factor as raising awareness is primarily the task of Member States, whose engagement is still uneven and largely reflects the level of their cybersecurity capacities in general. The Cybersecurity Strategy, by its voluntary non-binding nature, only has limited means to influence Member States behaviour.

***Finding 12:** According to the evaluation of European Cyber Security Month, to the ENISA evaluation, as well to the results of the survey conducted by the Council among Member States, the latter would appreciate further/strengthened support from the EU institutions and bodies in coordination of awareness raising activities and increasing resources to support such activities.*

***Finding 13:** Awareness raising and skills development remain relevant Strategy objectives, for which continuous efforts at both national and EU level are needed. Cybersecurity awareness remains a challenge as the Eurobarometer 464 demonstrates that a majority of Internet users do not feel adequately informed about the risks of cybercrime, and about measures they can take to protect themselves. The cybersecurity skills gap is predicted to achieve 350 000 (globally 1.8 million) by 2022.*

5.1.2 To what extent is the objective to achieve resilience still relevant today?

In response to the 2013 challenges, the objective of achieving resilience was very relevant as strong resiliance is a first line of defence against cybercrime. However, it should be noted that the objective itself was formulated in a very broad manner, expressing rather a vision than a measurable target. Whereas full resilience cannot be achieved in real life, the Strategy identified relevant operational objectives of increasing capacities, stimulating cooperation and information exchange as well as raising awareness and skills, which are prerequisite for effective cybersecurity prevention.

As presented in the previous sections, progress has been achieved in both building capacities and improving cooperation and information sharing, which should help European society and economy be more resilient than before. This is, however, by no means a finished process but a first step in the right direction. The literature review and stakeholders' feedback suggest that the measures used by the 2013 Strategy to achieve these operational objectives were relevant but only partially effective. This is due to, among others, their scope and voluntary nature (e.g. parts of the NIS Directive), limited resources, the different levels of engagement of stakeholders (e.g. awareness raising activities) and the constantly changing threat landscape. It has to be noted that it is too early for the full assessment of some of them (e.g. NIS Directive).

The recent public consultation confirmed that indeed a number of gaps and challenges still exist. Among the top 4 (in a list of 16) areas for improvement mentioned by respondents were: cooperation across Member States; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks.

In the recent public consultation a large majority (88%) of respondents considered the current instruments and mechanisms available at the EU level to be insufficient or only partially adequate to address current challenges and gaps.

This is partly due to the fast evolving threat landscape, which requires constant efforts to adapt policy response. As the threat landscape has dynamically changed since 2013, the Strategy does not address a number of issues that are crucial to achieving resilience. The security of the Internet of Things devices and its implications for the whole digital ecosystem is just one example. The issues related to the balance of responsibilities between the end users (individual citizens, public and private organisations and enterprises) and the providers of products and services with embedded digital/connected components, software and hardware have not been tackled either. The Strategy also focuses predominantly on the critical sectors while the fast pace of the digital revolution made it clear that cybersecurity is and should be "everybody's business", regardless of the size and sectors the entities are operating in.

Finding 14: *The 2013 Strategy objective of achieving resilience was and remains relevant as strong resilience is a first line of defence against cybercrime. However, in 2013 the objective itself was formulated in a very broad manner, expressing rather a vision than a measurable target. Whereas full resilience cannot be achieved in real life, the Strategy identified relevant operational objectives of increasing capacities, stimulating cooperation and information exchange as well as raising awareness and skills, which are prerequisite for effective cybersecurity prevention.*

Finding 15: *While the objective remains relevant, according to stakeholders' feedback and literature review a number of challenges and gaps still exist. Among the top 4 (in a list of 16) areas for improvement in the recent consultation were: cooperation across Member States; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks.*

Finding 16*: The review of the literature and stakeholders' feedback suggest that the measures used by the 2013 Strategy to achieve operational objectives related to resilience (improved capacities, cooperation, information sharing and awareness) were relevant but only partially effective. This is due to, among others, their scope and voluntary nature (e.g. parts of the NIS Directive), limited resources and different level of engagement of stakeholders (e.g. awareness raising activities) as well as constantly changing threat landscape.*

Finding 17: *The Strategy measures are not sufficient anymore as they do not address a number of issues related to the changing threat landscape, which are crucial to achieving resilience (e.g. the security of the IoT devices and its implications for the whole digital ecosystem, the balance of responsibilities between the end users (individual citizens, public and private organisations and enterprises) and the providers of products and services with embedded digital/connected components, cybersecurity of sectors and entities not covered by the NIS Directive).*

5.2 OBJECTIVE 2 OF THE STRATEGY: DRASTICALLY REDUCING CYBERCRIME

The 2013 objective to reduce cybercrime focused in particular on making the response to cybercrime more effective and thus also creating a deterrent effect that should contribute to the prevention of cybercrimes. The measures can be categorized into three groups:

- measures to create a more harmonised legal framework by ensuring adoption and swift transposition of the EU directives and the Budapest Convention;
- measures to improve the operational response, e.g. by supporting the European Cybercrime Centre; and
- measures to improve coordination across the EU, e.g. by supporting the EU Policy Cycle.

The present section assesses to what extent the three measures described above has been effective in achieving this objective, and whether the objective to reduce cybercrime is still relevant today.

5.2.1 To what extent has the objective been achieved?

Measures to create a more harmonised legal framework for cooperation

In the Strategy, the Commission committed to "ensure swift transposition and implementation of the cybercrime related directives". This contributes to the creation of a more harmonised legal framework and hence should facilitate operational cooperation, contributing in turn to a more effective response to cybercrimes which are typically trans-border in nature.

The recent Commission reports on the measures taken by Member States to **combat the sexual abuse and sexual exploitation of children and child pornography**[92] show that the Directive has led to substantive progress in the Member States by amending criminal codes, criminal procedures and sectorial legislation, streamlining procedures, setting up or improving cooperation schemes and improving the coordination of national actors. The Strategy contributed to that progress by including frequent contacts with Member States to encourage and facilitate swift and complete transposition of the measures. This substantive progress fulfils the Commissions intention to ensure that strong and effective legislation is in place to tackle cybercrime.

At the same time, there is still considerable scope for the Directive to reach its full potential through complete and correct implementation of all of its provisions by Member States. The analysis so far suggests that some of the main challenges for Member States could be related to prevention and intervention programmes for offenders, substantial criminal law and the assistance, support and protection measures for child victims. Also, there is room for improvement with regard to measures to remove child sexual abuse materials, as is evidenced by the fact that Europe has for the first time taken the lead in hosting child sexual abuse URLs identified by the Internet Watch Foundation globally in 2016, with the Netherlands hosting 37% and France 11%.[93] A 2015 threat assessment of the Global Alliance against Child Sexual Abuse online showed that the number of images in circulation worldwide had increased rather than decreased: 93% of respondents reported that the number had increased, while only 7% reported no change.

For the **Directive on Attacks against Information Systems**, the Commission is currently assessing the conformity of Member States' implementation. The Commission will adopt and submit to the Parliament and the Council a report on the extent to which Member States have taken the necessary measures in order to comply with the Directive in September 2017. Two

[92] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1486726102713&uri=CELEX:52016DC0871; http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1486726102713&uri=CELEX:52016DC0872
[93] https://www.iwf.org.uk/news/latest-internet-watch-foundation-report-shows-europe-now-hosts-60-of-child-sexual-abuse

countries still do not have transposition measures in place. The first comprehensive statistics will become available this year, enabling a better assessment of implementation.

The directives, in combination with other measures, have already facilitated closer cooperation between EU Member States on international cases, as is visible from the case statistics of Europol.[94] In terms of the gaps that remain, during the assessment of the transposition of the directives and through targeted stakeholder consultations, it has emerged that the focus of current measures on the substantive legal framework does not sufficiently address the challenges that arise in investigating cybercrimes which are more often than not cross-border in nature and challenge our traditional notions of sovereignty and territoriality.[95] Recent studies and expert processes have shown that the main challenges for Member States' law enforcement activities now lie in the investigative (procedural) area.[96] The lack of a possibility to actually take investigative measures has hampered a large number of cases, especially when it comes to illegal activity on the dark web. While the measures can therefore be considered largely effective when it comes to the substantive framework, gaps remain on procedural aspects.

***Finding 18**: The Strategy has contributed to a limited extent to the transposition of cybercrime related directives but the implementation of the Directive on Child Sexual Abuse and the Directive on Attacks against information Systems is not yet complete.*

***Finding 19**: While harmonised substantive law has facilitated cooperation across Member States, recent studies and expert processes have shown that the main challenges for Member States' law enforcement activities now lie in the investigative (procedural) area.*

Ratification of the Budapest Convention on Cybercrime by all Member States

The European Commission, through the Cybersecurity Strategy, has contributed significantly to the success of the **Budapest Convention on Cybercrime**, through constant promotion and support in all forums, including funding for Budapest Convention-based capacity building in third States. Since the adoption of the 2013 Cybersecurity Strategy, 14 additional States have ratified the convention, including four of the six Member States who had not yet ratified.[97] The measures of the Commission in this area, including the Strategy, can be considered mostly effective; in particular, the implementation plan of the Strategy obliged Member States to report on their efforts to ratify on a regular basis to the Council Working Group on Cyber Issues, which helped to keep the subject on national agendas The Strategy also lent additional weight and priority to the promotion of the Convention and was noticed also by many external partners; the political signal this sent was helpful.

While this action can be considered a success, there are still two EU Member States that have not yet ratified the Convention so that the efforts of the EU cannot be considered fully effective. In addition, given the sometimes open language of the Budapest Convention, there

[94] See below at 4.2.2.

[95] See the progress report and final technical report on cross-border access to electronic evidence: http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf; https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf;

[96] See documents available at https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

[97] Ireland is working on legislation that will enable it to ratify.

are divergent interpretations of some provisions and there is a perception that the Convention would need to be modernized to better address today's needs.[98]

Finding 20: *The Commission's urging of Member States to ratify the Budapest Convention, including through the call in the Strategy has resulted in a high number of ratifications both inside and beyond the EU. There are still two Member States that have not ratified the Convention.*

Measures to improve the operational response

The role of the European Cybercrime Centre (EC3) as the European nexus in the fight against cybercrime.

The Strategy highlighted the need to support the then recently created European Cybercrime Centre (EC3) as the European focal point in the fight against cybercrime. Since 2013, the European Cybercrime Centre has indeed become a very useful support resource to Member States.

As mentioned above, the number of high-profile cases[99] rose from 57 in 2013 to 175 in the first six months of 2016; in parallel, the number of staff in EC3 has risen to 77 as of December 2016. This is low compared to the RAND[100] estimates which that under the "high workload" scenario (8216 case per year) 158 functional staff would be needed (ratio of cases per functional staff, per year: 52). On the basis of this ratio, and taking into account that presently EC3 deals with 10736 cases per year, 206 functional staff would be needed, whereas the capacity is currently 56 (ratio of cases per functional staff, per year: 192). While the increase in staff shows that the Commission has been effective in supporting EC3 in obtaining additional resources in a time of overall reduction of resources, the raise in case ratios shows that this support has not been sufficiently effective to enable EC3 to have the resources it would ideally need, even if some of this additional burden is absorbed by more efficient approaches to cases.

In spite of these limitations, the EC3, in cooperation with EU Member States' law enforcement, has managed to successfully tackle a number of difficult cases, as outlined in its press releases.[101] Furthermore, in the area of prevention the EC3 has taken a number of measures, from its strategic knowledge products and alerts to the No More Ransom project[102] that have contributed to raising awareness of stakeholders and citizens.[103] The *NoMoreRansom* project alone has already helped more than 16,000 users decrypt their ransomed devices for free. In the absence of any comparable effort, these users would not have been able to decrypt their data or would have been forced to pay the ransom without the support organised by EC3. Overall, it can therefore be considered a significant success and

[98] Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY; https://rm.coe.int/16806a495e.
[99] High profile cases are cases which require at least three items from the Europol catalogue of products and services.
[100] http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf
[101] https://www.europol.europa.eu/newsroom
[102] https://www.nomoreransom.org/
[103] See also above under section on awareness raising.

Member States' feedback suggests as much. It has significantly contributed to the aim of the strategy to reduce cybercrime by enabling investigations that likely would not have succeeded as well absent EC3's involvement; it can therefore be considered an efficient measure.

Nonetheless, gaps remain. More effective cooperation requires further funding and an increase in human resources for EC3. The more operational EC3 becomes, the bigger the budgetary needs to cover for these operations. Based on the steady rise in high-priority cases in the last years (caseload has more than quadrupled between 2013 and 2016), it is likely that demands for EC3 support will increase in the future. In addition, Member States are looking to EC3 to become a centre of expertise for cyber-related criminal investigations, e.g. when encryption is involved.

Enhancing cooperation between Eurojust and Europol in information exchange, to increase their effectiveness in combatting cybercrime.

In the Strategy, Eurojust was asked by the Commission to identify the obstacles to judicial cooperation on cybercrime investigations and support Member States' coordination with third countries accordingly. The goal of this action is to support the prosecution of cybercrime both at the operational and strategic level. They have actively contributed to the Commission's work in this area and have helped to identify gaps that now need to be addressed, as well as possible solutions.[104] This action can therefore be considered effective. It has also contributed to the objective of reducing cybercrime at large as the identification of obstacles to cooperation is a precondition for addressing and removing these obstacles. In terms of practical measures, Eurojust has also volunteered to serve as the secretariat for the new European Judicial Cybercrime Network which brings together practitioners from all Member States to identify challenges and possible solutions and promote better operational cooperation.

In parallel, cooperation between Eurojust and Europol has significantly increased since 2013. Eurojust is involved in and supports Europol operations, and has posted a liaison officer to EC3. Eurojust participates in EC3's Programme Board and in the Joint Cybercrime Action Taskforce, and in turn EC3 is involved in the European Judicial Cybercrime Network.[105] This constant contact has greatly facilitated everyday cooperation and coordination and improved relations between the agencies. The action can therefore be considered mostly effective.

Finding 21*: The Cybersecurity Strategy envisaged an enhanced operational capability to combat cybercrime. The support to the at the time newly establishment European Cybercrime Centre at Europol has effectively contributed to the improved operational cooperation in the fight against cybercrime, as shown by the number of high-profile operations.*

Finding 22*: While the operational objective of supporting European Cybercrime Centre at Europol proved very relevant, a mechanism allowing for continuous resources adaptation was not envisaged, which resulted in EC3's resources being outpaced by Member States' needs for support.*

Finding 23*: The support provided by Eurojust has been effective in identifying obstacles to judicial cooperation.*

[104] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en; http://data.consilium.europa.eu/doc/document/ST-8634-2016-INIT/en/pdf.
[105] www.consilium.europa.eu/en/meetings/jha/2016/06/network--en_pdf/.

Increasing accountability online

A successful fight against cybercrime requires that Internet users are being made accountable for their actions. Therefore, efforts to increase accountability were part of the Strategy. The efforts of the Commission to become an active participant in the debate were effective and have resulted in concrete outcomes – appointment of a Commission co-chairperson for the relevant working group, adoption of a security framework for registries – the added value is still limited as the processes take a long time to complete and accountability online – while now increasingly being recognized as an issue – has not significantly increased over a five-year period. Therefore, while the action can be considered efficient by internet governance standards, it has not yet been able to significantly contribute to the overall goal of significantly reducing cybercrime.

In terms of effectiveness of these efforts to date, it remains a fact that the WHOIS[106] information is often inaccurate and does not serve to increase accountability online. On the basis of pilot studies it appears the new Agreements specifying responsibilities and accountability of registrars (2013 RAA) and registries (2014 gTLD Registry Agreement) have improved the situation slightly (2014, WHOIS ACCURACY REPORTING SYSTEM, University of Chicago). On the other hand, studies show that WHOIS information is still subject to abuse in many occasions (43.9% of registrants experience one or more types of misuse, 2014, WHOIS misuse study, Carnegie Mellon University). Similarly, EU Member State Data Protection Authorities have expressed concerns on the application of EU Data Protection Rules (WP29 letter of 8 January 2014 to ICANN).

***Finding 24**: The Cybersecurity Strategy has not been effective in increasing accountability online. There is a lack of publicly available and accurate data on registrants of domain names which creates opportunities for criminals to hide their activities; Commission initiatives in this area have only been moderately effective.*

The adoption of the European Strategy for a Better Internet for Children and the launching of the Global Alliance against Child Sexual Abuse Online.

In terms of concrete results, the **Global Alliance against Child Sexual Abuse Online**, envisaged in the Strategy as a tool to improve co-ordination at EU level,[107] has contributed to the continuous expansion of Interpol's International Child Sexual Exploitation (ICSE) database of known child abuse images, including the creation of a "worst-of" list of images illegal in every participating country. This will enable more effective monitoring and investigation of contraband files shared over peer-2-peer networks and facilitate the identification of more victims. 49 countries plus Europol are connected to the ICSE database and cooperate in the identification of child sexual exploitation victims and their abusers. By 1 January 2017, the ICSE database – funded by the EU – included data on more than 10,000

[106] A query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource.

[107] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm

identified victims from around the world, as well as data related to numerous unidentified victims, whose cases are yet to be investigated.[108] This is a steep increase from the pre-Global Alliance days, where 32 countries were connected[109] and the database contained images relating to 2,891 identified victims[110] of sexual exploitation from 41 countries: a more than 300% increase in identified victims and a more than 50% increase in connected countries. This can be attributed in part to the support of the Commission through both the strategy and the Global Alliance itself. The topic remains high on countries' political agendas because of the regular reporting mechanisms including in implementing the strategy, and meetings and high-level events in the context of the Global Alliance. Absent the Strategy, this topic likely would not have remained linked to the overall cybercrime and cybersecurity discussions to the same extent. The measure can therefore be considered effective in terms of improving victim identification and operational cooperation.

However, as the 2015 threat assessment report shows, the crimes are still on the rise and methods for criminals to disguise their actions are proliferating:[111] 81% reported an increase of the number of offenders trafficking in child pornography, 16% no change, and 3% a decrease. While the situation would likely have been even worse absent the Strategy and the Global Alliance, the action cannot be considered fully effective in terms of combating child sexual abuse online and hence reducing cybercrime.

Therefore, while there are some notable successes of the Global Alliance especially when it comes to measures of child- and victim-friendly justice systems and preventive measures, there is no evidence of a reduction of child sexual abuse. The most recent statistics by the Internet Watch Foundation (IWF), released in April 2017, are a case in point: 57,335 URLs contained child sexual abuse imagery and these were linked to using 2,416 domains worldwide. This is a 21% increase in just one year, from 1,991 in 2015.[112]

***Finding 25**: Operational cooperation between participants of the Global Alliance has increased, leading to a greater number of investigations and increasing the number of identified child victims. In turn, this increased the cooperation at EU level as envisaged by the Strategy. This can be attributed at least in part to the support by the Global Alliance and the Strategy framework, which was effective inasmuch as these indicators are concerned.*

***Finding 26**: The proliferation of child sexual abuse images online has not been halted; rather, the volume of available images has grown. While it is likely that growth would have been even steeper in the absence of the Strategy and the Global Alliance, there unfortunately has been no reduction in the overall number of child sexual abuse cases.*

[108] https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification
[109] https://www.interpol.int/News-and-media/News/2011/PR071
[110] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_2015_report_en.pdf
[111] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_threat_assessment_en.pdf.
[112] https://www.iwf.org.uk/news/latest-internet-watch-foundation-report-shows-europe-now-hosts-60-of-child-sexual-abuse

5.2.2 To what extent is the objective to reduce cybercrime still relevant today?

As described in Section 3.2, cybercrime remains a real and significant threat in 2017. Europol's most recent assessment[113] highlights the continuing expansion of cybercrime tools and techniques into other crime and threat areas as a growing range of threats, including trafficking in human beings[114] have become cyber-facilitated. This growth and expansion in scope threatens the security of citizens and undermines confidence in political processes, online tools and services, which can have a negative impact on economic growth and social well-being,[115] running counter to the core policy goals of the EU and its Member States.[116] As a result, the objective to more effectively counter and eventually reduce cybercrime remains more relevant than ever; the question is whether it is a realistic goal to aim for, in view of the developments over the last four years.

In addition to the overall growth in cybercrimes, other cross-cutting issues, such as the growing misuse of anonymity and encryption services and other legitimate tools for illegal purposes pose a serious impediment to detection, investigation and prosecution of criminals.[117] This further impedes the chances to effectively reduce cybercrime, adding to the doubts concerning the realistic nature of the target. However, this does not mean that we can afford to relax; on the contrary, while the target may have been overly ambitious, the objective behind it – to more effectively counter cybercrimes to ensure a better protection of all users and trust in the Digital Single Market – remains relevant.

***Finding 27**: Due to the growing number of devices connected to the Internet, the number of cyber-crime cases has increased massively since 2013 due to, among others, technological developments and changing cybercrime business models. Consequently, whereas the target of reducing cybercrime, in view of developments, may have been overly ambitious, the rationale behind it – to more effectively counter cybercrimes to ensure a better protection of all users and trust in the Digital Single Market – remains relevant.*

5.3 OBJECTIVE 3 OF THE STRATEGY: DEVELOPING CYBERDEFENCE POLICY AND CAPABILITIES RELATED TO THE COMMON SECURITY AND DEFENCE POLICY FRAMEWORK

This objective was expected to be achieved through cyber defence capability development, enhancing synergies between civilian and military approaches to protecting critical cyber

[113] Europol, `iOCTA The Internet Organised Crime Threat Assessment 2016', https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf, page 11.
[114] Europol, Situational Report (2016) Trafficking in human beings in the EU at https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/situational_report_trafficking_in_human_beings-_europol.pdf and Report on the progress made in the fight against trafficking in human beings (2016) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims (Brussels, 19.5.2016 COM(2016) 267 final) and its accompanying Staff Working Document (Brussels, 19.5.2016 SWD(2016) 159 final).
[115] https://www.forbes.com/sites/steveolenski/2016/08/03/the-effect-of-cyber-crime-on-online-shopping/#225be8ea2b87 ; http://www.econinfosec.org/archive/weis2014/papers/RiekBoehmeMoore-WEIS2014.pdf ; https://info.threatmetrix.com/rs/991-JSN-701/images/Q2_2016_Report.pdf
[116] See most recently the Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All, COM/2017/0228.
[117] 2017 Global Information Security Workforce Study commissioned by the Centre for Cyber Safety and Education and (ISC)2, was carried out from 22 June to 11 September, 2016, and surveyed 19,641 IT security professionals from 170 countries, including nearly 3,700 respondents in Europe. https://www.isc2.org/pressreleasedetails.aspx?id=14570

assets and exploring ways to complement the efforts of EU and NATO aiming at strengthening the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.

The following sections will examine whether this overall objective has been achieved, the extent to which the individual actions have effectively contributed to this objective and whether the objective is still relevant today. However, we have not addressed all actions linked to this objective but focused on the ones having potentially the most impact on the fulfilment of the objective.

Actions to implement this objective included 1) Support for Member States capability development, 2) cyber defence training and education, 3) advancing the cooperation between EU and NATO, 4) developing civilian and military synergies, and 5) increasing cyber defence of CSDP missions and operations.

5.3.1 To what extent has the objective been achieved?

Since the adoption of the 2013 Cybersecurity Strategy, the EU has adopted its first Cyber Defence Policy Framework in 2014, and has mainstreamed cyber defence into the CSDP missions and operations conduct, as well as enhanced education, training and exercises.

The EU Cyber Defence Policy Framework has provided a relevant and effective framework for strengthening cyber defence in the broader context of CSDP. The revised EU Concept for Cyber Defence in EU-led Military Operations and Missions has been adopted that aims to unlock further integration of cyber defence and security into CSDP missions and operations, also taking into account the need for intensified civil-military cooperation and coordination.

Some progress has been made towards the better protection of the CSDP missions and operations, especially for the military operations, However serious resources constraints and lack of dedicated personnel have been hindering the development of the cyber defence aspects in the civilian missions. The newly established EEAS Cyber Security Governance mechanism has started to address the cyber defence issues of civilian missions recently.

Development of cyber defence capabilities

A primary focus of the EU Common Defence policy Framework (CDFP) is the development of cyber defence capabilities made available by Member States for the purposes of the Common Security and Defence Policy.

Some progress has been achieved in this regard: in its fifth year of existence, the European Defence Agency's Project Team on Cyber Defence has met 3 times a year since 2013. Member States have actively participated in these meetings, and have benefitted from joint capability development, and training activities. For advancing cyber defence Research & Technology efforts, the European Defence Agency (EDA) started preparations for the establishment of a holistic Cyber Defence Joint Program with interested Member States.

To support Member States' cyber defence capability development, EDA also provided support through Cyber Ranges (exercises), and several projects, such as deployable cyber

situation awareness packages for CSDP Operational Headquarters, which allows to detect cyber threats in real time[118].

To improve situational awareness capability for the CSDP, the EU Intelligence Analysis Centre (INTCEN) has set up the EU Hybrid Fusion Cell in order to enable the early identification of hybrid threats affecting the EU's strategic activities and interests. The Hybrid Fusion Cell has contributed to improved analysis and early warning on cyber defence in the EEAS, the Commission and Member States.

Following the approval of the Cyber Defence Concept for the EU Military Operations in November 2016, EU Military Staff (EUMS) has reinvigorated the process of "mainstreaming" cyber within the CSDP. The intent is to incorporate the consideration of cyber defence aspects into routine processes and procedures, to ensure active engagement and contributions to enhance awareness of all EU Member States' military personnel.

The concept for integrating cyber security into the planning and conduct of civilian CSDP missions has started back to back with the EU Concept for Cyber Defence in Military Operations, but serious further efforts are necessary to improve the cyber protection of the civilian missions.

However, the effectiveness of all these measures was limited by the insufficient level of strategic guidance and different maturity levels of Member States.

Cyber Defence Training & Exercises

Modest progress has been achieved in the field of defence cyber training. The European Security and Defence College (ESDC) network is the only dedicated civilian-military training provider for CSDP structures, missions and operations at an EU level. The ESDC has identified synergies with the European Cybercrime Centre within Europol (EC3), ENISA and other relevant entities regarding the development of common civil-military training standards and curricula.

Some useful steps have been taken by both the Member States and EU structures. France and Portugal have launched a project to identify the CSDP Military Training Requirements for cyber defence. In the framework of the Military Erasmus initiative, an “EU module on cyber defence” was conducted as a pilot activity by France in 2015, with the support of Portugal and Belgium.

Cyber aspects were addressed within the CSFP exercises for the first time in 2016. The integration of an effective cyber-dimension to Common Foreign and Security Policy exercise Multi-Layer (ML16) and CSDP crisis management MILEX exercises in 2016 took place. The EU managed to improve exercise opportunities for the military by becoming an observer in multinational cyber defence exercises such as NATO’s CYBER COALITION since 2013 and LOCKED SHIELDS in 2016. However, the EU still lacks its own dedicated cyber defence exercise.

Identifying civil-military synergies

[118] The project addressed the need for pooling of Member States demands for training and exercises and advanced Persistent Threat Detection (APT-D).

Cyber remains a dual-use sector with both military and civilian technologies which offers many opportunities to develop synergies between these technologies. These potential synergies cover several aspects of cyber, from competence profiles to research. Progress in identifying civil-military synergies has been achieved thanks to the launch in 2015 of a dedicated study on "*Synergies between the civilian and the defence cybersecurity markets*"[119]. This study found examples of synergies between civilian and defence cybersecurity markets both on the supplier and the consumer side. The report concluded that over the last few years, the majority of the civilian market and civilian products and services were used on the defence market. This objective was also effectively supported by research projects[120], for which results can be used in support of current and future military cyber defence projects.

Enhancing cooperation with relevant international partners

There has been substantial progress towards enhancing cooperation with relevant international partners. The EU-NATO Joint Declaration signed at NATO's Warsaw Summit in July 2016 advanced further EU and NATO coordination on cyber security and defence. Among the biggest successes in overall EU-NATO defence cooperation has been the signing of a Technical Arrangement between CERT-EU (Computer Emergency Response Team for the EU institutions) and NCIRC (NATO Computer Incident Response Capability) in 2016. The Technical Arrangement allows for operational information exchange between the two organisations, which is necessary in peacetime, and will be essential in times of crisis.

Regarding cooperation between CERT-EU and the NATO Computer Incident Response Capability (NCIRC), a Technical Arrangement was agreed in February 2016. The agreement facilitates technical information sharing between NCIRC and CERT-EU to improve cyber incident prevention, detection and response in both organisations, in line with their decision making autonomy and procedures.

High level informal staff-to-staff consultations between the EU and NATO have been held regularly, with a new focus on the implementation of the Warsaw EU-NATO Joint Declaration. The further implementation of the EU-NATO Joint Declaration requires more efficient coordination efforts on the EU side in all major cooperation areas: concept development; training, education, and exercises, research and technology initiatives.

Finding 28: *Although mainstreaming of cyber issues into the CSDP daily management and decision-making has started, serious resource constraints continue to delay the delivery of the EU CDPF objectives. A dedicated CSDP cyber defence exercise remains a major objective of the EU, but at this stage the EEAS continues to lack the resources to do so. This highlights the need to include cyber defence and security in the existing cyber exercises organised by EEAS and the Member States.*

Finding 29: *Coordination of Member States defence forces' cyber preparedness is necessary for more successful CSDP interoperability. EU has started work on facilitating capability development, training and dual-use standardisation efforts, but efforts remain scattered and could use better strategic guidance by the Member States.*

Finding 30: *Several gaps have been identified in the training modules of EEAS, Commission and Member State end-users, in the framework of CSDP implementation. Intensifying the training opportunities is an urgent need where the EU could add value by developing an*

[119] https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets
[120] E.g. cyber-related Framework Programme 7 projects: *PANOPTESEC*,and *CyberROAD.*

enhanced Cyber Defence training capacity for its CSDP missions and Member States' military personnel.

Finding 31: *Ongoing cyber defence cooperation with NATO has been helpful in identifying the areas of concentration for both organisations and allow optimal use of resources.*

Finding 32: *Cooperation with the Commission services and the relevant agencies, such as the EDA, the ESDC, Europol's EC3 and ENISA, has started. The Political-Military Working Group in the Council has been a major forum to monitor and provide guidance on the implementation of the Cyber Defence Policy Framework. The EU Military Committee and other relevant Council working bodies, such as the Council Working Group on Civilian Missions have been informed about the relevant issues.*

5.3.2 To what extent is the objective of developing a cyber defence policy and capabilities relating to the CSDP still relevant?

As highlighted in the EU Global Strategy, geopolitical realities have significantly changed for the EU since 2013, with the evolving cyber threat environment calling for more strategic and robust action in terms of EU Member States cyber defence capability development and in the context of CSDP missions and operations. The objective has become even more relevant and its implementation requires serious structural efforts on behalf of the EU cyber defence community.

Finding 33: *As the implementation of the EU Cyber Defence Policy Framework moves forward within the CSDP, the Member States' involvement in EU defence efforts remains of very technical nature and lacks strategic dimension.*

5.4 OBJECTIVE 4 OF THE STRATEGY: DEVELOPING THE INDUSTRIAL AND TECHNOLOGICAL RESOURCES FOR CYBERSECURITY

The fourth objective of the strategy was to develop industrial and technological resources for cybersecurity**.** This was supposed to be achieved via two means: promoting a single market for cybersecurity products and fostering R&D investments and innovation. Twelve non-legislative actions were linked to this objective.

The following sections will examine whether this overall objective has been achieved, the extent to which the individual actions have effectively contributed to this objective and whether the objective is still relevant today.

5.4.1 To what extent has the objective been achieved?

Promoting a Single Market for cybersecurity products

The progress in achieving a single market for cybersecurity solutions has been modest and market supply for ICT security products and services in Europe remains fragmented. This is

partly due to historic reasons as industrial development in this area has been stimulated by governmental purchase and some highly innovative European companies in this sector are still largely dependent on public procurement in their home country.

A side effect of this situation is limited willingness for cross-border purchasing, which is a barrier to the development of a common cybersecurity market. Smaller, newer market players are having difficulties initiating their business in such limited country markets. They struggle with expanding internationally as buying behaviours can be biased towards established (often global) names that can leverage strong market presence and marketing budgets to protect their market share from new entrants.

The fragmentation of the cybersecurity market in Europe has been confirmed by a recent study for the European Commission[121]. It was also reflected in a number of studies conducted on a national level.[122] According to the Recommendations on Cybersecurity for Europe prepared by the European Cybersecurity Industry Leaders, the fragmentation of the European cybersecurity market is currently the main barrier to the creation of strong EU businesses in the field.[123]

The Strategy highlighted a number of initiatives to help overcome this fragmentation by building trust. This was to be partly achieved through the development of security standards and assistance with EU-wide voluntary certifications schemes. This approach brought mixed results so far. On the positive side, thanks to the actions of the Strategy, progress has been made in gaining knowledge of the different available standards – a necessary step towards ensuring interoperability. As reflected in section 3.1, a Memorandum of Understanding has been signed between the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunication Standards Institute (ETSI) to facilitate cooperation in defining standards. However, this has not yet led to the development of a common approach at the EU-level.[124] The lack of an EU-wide approach to cybersecurity standards hampers common efforts on the global standardisation stage where the EU's biggest competitors have an advantage in terms of scale and market size if the EU appears fragmented.

The relatively slow progress related to standardisation and development of possible voluntary certification schemes at the EU level was coupled with the emergence of a number of national certification schemes. Albeit important, these initiatives bear the risk of creating single market fragmentation and barriers for interoperability. An ICT vendor might need to undergo several certification processes to be able to sell in several Member States.[125] In a recent public consultation almost 40% of respondents expressed the view that existing certification schemes

[121] Cybersecurity Market analysis conducted by LSEC and PwC, V2 2017 Draft Report, 30/06/2017 (Final report to be issued in October 2017).
[122] Competitive analysis of the UK cyber security sector, A study for the A study for the Department for Business, Innovation and Skills, 2013; L'observatoire de la filière de la confiance numérique en France - Etude pour l'Alliance pour la Confiance Numérique (ACN), 2013; Der IT-Sicherheitsmarkt in Deutschland; Bundesministerium für Wirtschaft und Energie, 2014.
[123] Recommendations on Cybersecurity for Europe, A report to M Gunther Oettinger, European Commissioner for Digital Economy and Society, prepared by the European Cybersecurity Industry Leaders (Thales, Atos, Airbus Group, BBVA, BMW, Cyberentica, Deutsche Telekom, Ericsson, F-Secure, Infineon), January 2016 - https://ec.europa.eu/digital-agenda/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders
[124] Conclusions workshop held in the context of the NIS Directive Cooperation Group work on security measures gave the opportunity to Member State authorities to exchange views on how they approach the issue of cybersecurity standards.
[125] For example, smart meters manufacturers need to comply with three different certification schemes in three European countries (Germany, France and UK).

did not support the needs of Europe's industry, compared to only 17.5% of respondents, who felt that the existing schemes were sufficient.[126]

At the same time, the lack of a common EU-wide approach with regard to ICT security certification was identified in numerous consultations as one of key gaps in achieving the trust necessary for creating a well-functioning Digital Single Market. While the Strategy mentioned the need for support for the EU-wide voluntary certification schemes, more concrete actions to set-up a European certification framework were triggered only in 2016. This was largely due to the initial focus on the implementation of the resilience and cybercrime aspects of the Strategy.

Finding 34: *The progress in achieving a single market for cybersecurity has been modest and the market supply for ICT security products and services in Europe remains fragmented, which has been confirmed by a number of recent studies. Stakeholders' views confirm this constitutes one of key barriers to the creation of strong EU businesses in the field.*[127]

Finding 35: *The instruments suggested by the Strategy, although relevant, have been effective in addressing the need to achieve a single market for cybersecurity to a limited extent as the implementation progress of standardisation and certification efforts proved quite slow. This was largely due to the initial focus and prioritisation of the implementation of the resilience and cybercrime aspects of the Strategy.*

Finding 36: *The relatively slow progress at the EU level related to standardisation and development of possible voluntary certification schemes was coupled with the emergence of a number of national certification schemes. Albeit important, these initiatives bear the risk of creating single market fragmentation and barriers for interoperability. In fact, the lack of European framework for certification/labelling reinforces market fragmentation and can negatively impact the level of trust of businesses and citizens in digital single market hampering the possibility of achieving the Strategy's objectives.*

Fostering R&D investments and innovation

The Strategy also highlighted the need to foster R&D investment and innovation for cybersecurity. This was to be achieved not only through using available funds under the Horizon 2020 research programme but also through establishing mechanisms for better coordination of the research agendas of the EU institutions and Member States. As the EU cybersecurity industry was quite fragmented there was also a need to create a platform of dialogue with the industry.

Initially, the Strategy's instrument to build trust among different stakeholders was the NIS Platform (NISP), which had also a working group on research and innovation. The Group came up with the Strategic Research Agenda suggesting a coherent way forward for research and innovation in Europe. However, this platform was voluntary and its main mandate focused on supporting the work related to the implementation of the forthcoming NIS

[126] cPPP and accompanying measures consultation conducted in 2016, see SWD(2016) 215.
[127] Recommendations on Cybersecurity for Europe, A report to M Gunther Oettinger, European Commissioner for Digital Economy and Society, prepared by the European Cybersecurity Industry Leaders (Thales, Atos, Airbus Group, BBVA, BMW, Cyberentica, Deutsche Telekom, Ericsson, F-Secure, Infineon), January 2016 - https://ec.europa.eu/digital-agenda/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders

Directive. Although this Strategy instrument proved effective in triggering the initial dialogue, its limits had also been recognised as participation in meetings was often limited to Brussels-based audiences, with limited outreach at the national level. The EU cybersecurity industry representatives consulted by the Commission on a number of occasions[128] expressed a clear need for creating a more structured platform representing the cybersecurity industry as such, which would allow it to take up a continuous dialogue with the demand side and translate it into concrete projects linked to available research and innovation resources.

In view of this evolving situation, the contractual Public-Private Partnership (cPPP) on cybersecurity was signed with The European Cybersecurity Organisation[129] (ECSO) – the first ever pan-European cybersecurity association. The EU will invest €450 million in calls for proposal related to this partnership, under its research and innovation programme Horizon 2020 during the period 2017-2020. Cybersecurity market players, represented by ECSO, are expected to invest three times more bringing the total investment to 1.8 billion Euros over this period.[130]

It is too early to fully assess the effectiveness of this new instrument, given that it was launched only a year ago. The first positive results of this measure, can be, however, already observed. The cPPP involves more than190 members from all over the European Union, with members including large European companies, SMEs and start-ups, research centres, universities, clusters and associations as well as local, regional and national administrations. The Working Group 6 of the cPPP provided timely input for the Commission's work on the Horizon 2020 Work Programme for the years 2018-2020. The cPPP has also become an effective cooperation and structured dialogue platform on other issues relevant for the cybersecurity community such as certification, market development, awareness raising, skills development.

At the same time the review of the literature suggests that the resources involved in supporting cybersecurity in Europe remain much smaller than the investment by other major players around the world. In addition, cybersecurity competences and expertise are still dispersed across Europe, which hampers the possibility of achieving the critical mass of investment to stimulate world-class innovation.

Finding 37: *The Strategy triggered initiatives which led to a more structured and coherent approach to research and innovation in the field of cybersecurity across the EU. The initial instrument used for this purpose - the NIS Platform - proved effective but reached its limits in terms of possibility to attract a wide range of stakeholders and stimulate a structural dialogue. A new, more adapted instrument – the contractual public private partnership (cPPP) - was then established to continue the work. The first progress report assessing the effectiveness of this instrument will be presented in 2018.*

Finding 38: *Progress in achieving the Strategy objective of increasing investment in research and innovation was partly achieved through the set-up of the above cPPP, which will invest €450 million under the Horizon 2020 programme between 2017-2020. The industry has committed to top it up with additional investment of €1.35 billion. At the same*

[128] See SWD(2016) 215.
[129] The European Cyber Security Organisation (ECSO), is a fully self-financed non-for-profit association (ASBL) under Belgian law. It is industry-led, with members including large European companies, SMEs and start-ups, research centres, universities, clusters and associations as well as local, regional and national administrations from the EU and European Economic Area (EEA) and the European Free Trade Association (EFTA) and Horizon 2020 associated countries.
[130] Under H2020 the EU has already invested additional €150 million between 2014-2016.

time the review of the literature and stakeholders' feedback suggest that the resources involved in supporting cybersecurity in Europe still remain much smaller than the investment by other major players around the world.

***Finding 39**: Cybersecurity competences and expertise are still dispersed across Europe, which hampers the possibility of achieving the critical mass of investment to stimulate world-class innovation.*

5.4.2 To what extent is the objective of developing industrial and technological resources for cybersecurity still relevant?

In response to the 2013 challenges, the objective of developing industrial and technological resources for cybersecurity was very relevant. It should be noted that, as it is the case for other objectives of the Strategy, it was formulated in a very broad manner, expressing more a vision than a measurable target.

Progress towards achieving this objective was modest, especially as far as promoting a single market for cybersecurity products is concerned. The recent European cybersecurity market study[131] suggests that while the EU Cybersecurity Market is growing at fast pace, it is also increasingly fragmented as countries seem to specialise in different areas of cybersecurity.

EU Cybersecurity Market size and Fragmentation

According to the market study, 60, 250 cybersecurity companies in the EU were involved in the delivery of Cybersecurity products and services in 2016. This indicates an increase of 18% compared to the 2015 company count of 50,446 and marks an increase of 22% for the 2014-2015 period. The EU accounted for 27% of the global companies for 2016.

Figure 6 demonstrates that the most significant difference across EU countries relates to the number of Micro and Small businesses involved in delivering Cybersecurity as they make up for the majority of EU Cybersecurity companies. This is generally expected for an emerging sector and reflects the trend for skilled individuals and entrepreneurs to set up new businesses. It is a reasonable assumption that the future growth of the Cybersecurity sector will depend upon a) new micro businesses entering the market and b) current micro businesses becoming medium- sized enterprises. The difficulty to compete on the European and global level often leads to mergers and acquisitions of Europe's SMEs by non-European actors, weakening the European sector and leaving Europe also more vulnerable and technologically dependent on others in this strategically important area.[132]

[131] Cybersecurity Market analysis conducted by LSEC and PwC, V2 2017 Draft Report, 30/06/2017 (Final report to be issued in October 2017).
[132] Cybersecurity Market analysis conducted by LSEC and PwC, V2 2017 Draft Report, 30/06/2017 (Final report to be issued in October 2017).

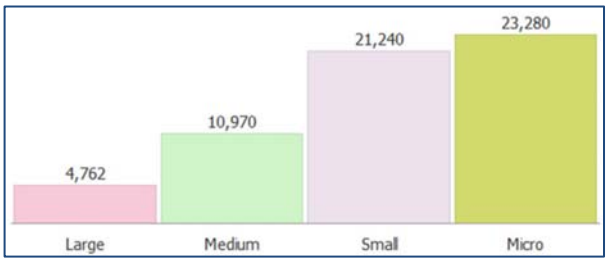

Figure 6: EU Cybersecurity Company Size Ranges 2016

Cybersecurity is also something of a hybrid sector, in that its roots extend into companies in diverse sectors such as ICT, Defence and Security. The cybersecurity business mix differs by country. For example, Figure 7 shows Situational Awareness (systems providing insight on an enterprise's security and threat environment) as 21% of sales across the EU, but at the country level the range is 16% (Netherlands and Latvia) to 27-28% (Croatia, Poland and Portugal).

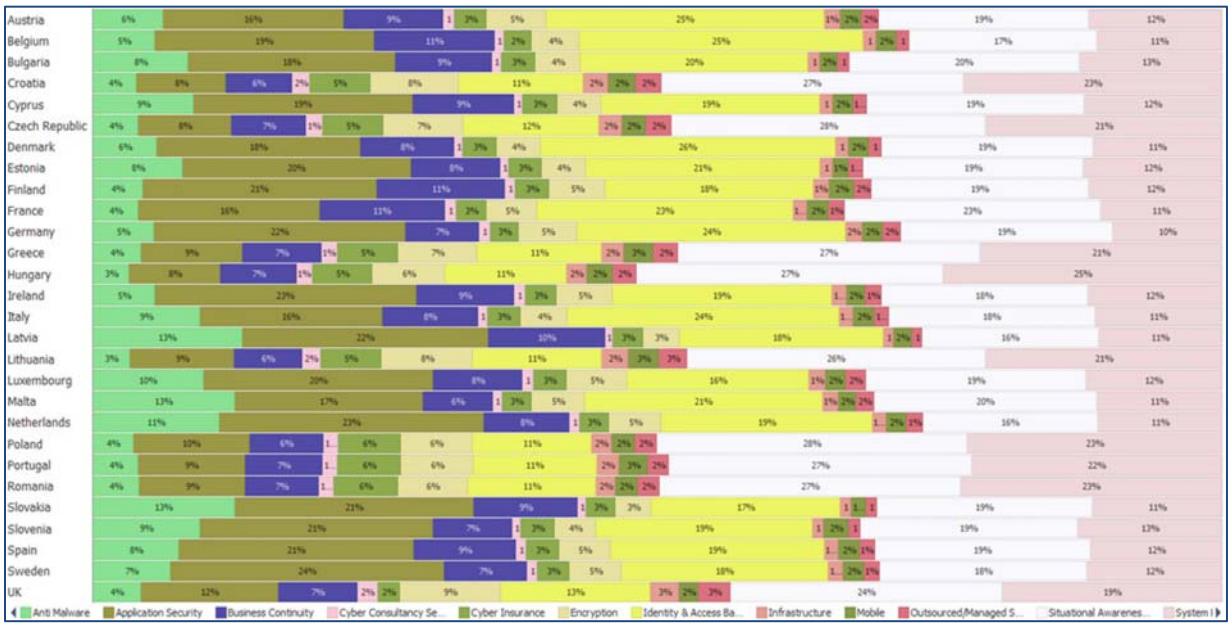

Figure 7: EU Cybersecurity Sales per Country, per Sub-category

Similar patterns are evident for other measures- companies and employment- suggesting that each country is developing different specialisations in Cybersecurity or responding to different challenges, resulting in market fragmentation. A possible explanation for this is the different level of maturity of Cybersecurity in the specific Member states.

The stakeholders' feedback also clearly indicates the need for further efforts in terms of certification and building trust to overcome market fragmentation. The lack of trust and clear rules is a barrier for European companies to compete and grow their businesses across borders in Europe but also on a global scale. While European companies tend to be strong and innovative, their size and capacity (mostly SMEs with few larger actors) are smaller in comparison to their US, Israeli, Chinese, South-Korean, Japanese or Russian counterparts as they experience difficulties in expanding beyond national borders.

EU Cybersecurity Imports

Cybersecurity imports are a measure of the products and services that enter the EU from outside of its geographic borders. Global imports for 2016 are estimated at EUR 48,000 million, of which EUR 12,100 million or 25% arrived in the EU. Table 14 shows EU imports divided into imports from within the EU and from outside of the EU. The overall values of non-EU imports is EUR 8,504 million or 70%, with 30% of imports from within EU countries. The highest volume importers are Germany, France, Italy and the UK.

The percentage of imports from within the EU varies greatly by country. In fact, for the UK it is as low as 17%, while for France it is as high as 53%. The strongest inter-trading relations within the EU for Cybersecurity include France, Italy, Spain, Netherlands, Austria, Belgium and Germany.

EU Cybersecurity Exports

Cybersecurity exports are a measure of the products and services that leave the EU for countries outside of its geographic borders. Global exports for 2016 are estimated at EUR 48,000 million (the same value as global imports), of which the EU exported EUR 9,718 million or 20% of the total. This makes the EU a net importer of Cybersecurity products and services.

Figure 8 below ranks the top 12 global exporters, with China the leading Cybersecurity exporter at EUR 14,287 million. Four EU countries- Germany, UK, France and Italy- are within the top 12.

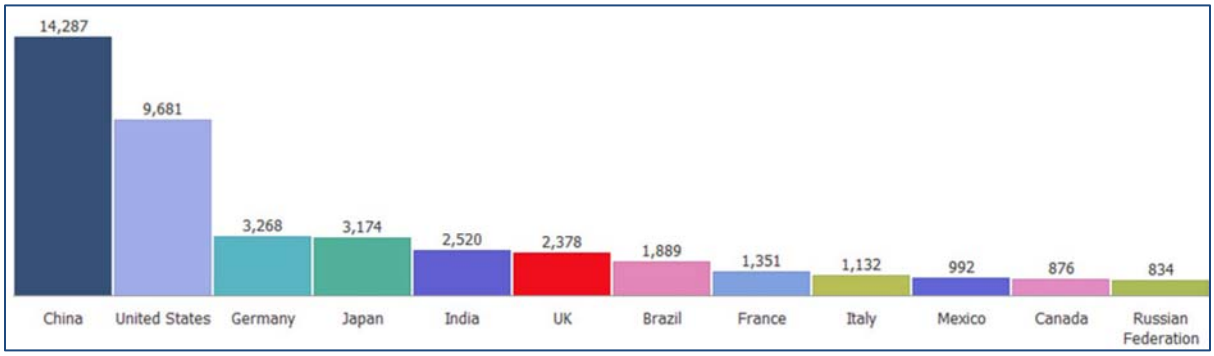

Figure 8: Top Global Exporting Nations 2016 EUR million

The above confirms that the objective remains relevant.

Finding 40: *The 2013 Strategy objective of developing industrial and technological resources was and remains relevant. Even though the whole value chain of digital technologies may not be mastered in Europe, it is in the EU's strategic interest to ensure that EU retains and develops certain essential capacities of securing its digital economy and society. In addition to certification framework, an effective industrial policy is needed to enable the development of European cybersecurity supply chain capable of securing critical hardware, software and providing key cybersecurity services.*

5.5 OBJECTIVE 5 OF THE STRATEGY: ESTABLISHING A COHERENT INTERNATIONAL CYBERSPACE POLICY FOR THE EUROPEAN UNION AND PROMOTING EU CORE VALUES

The fifth Strategy objective relates to establishing a coherent international cyberspace policy for the European Union and promoting EU core values. This was supposed to be achieved via two means: by mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy and developing capacity building on cybersecurity and resilient information infrastructures in third countries.

The following sections will examine whether this overall objective has been achieved, the extent to which the individual actions have effectively contributed to this objective and whether the objective is still relevant today. However, we have not addressed all actions linked to this objective but focused on the ones having potentially the major impact on the fulfilment of the objective. Major actions stemming from this objective include 1) promoting existing international law in cyberspace, the development of voluntary norms for responsible state behaviour and cyber confidence building measures within regional fora, 2) setting up EU cyber dialogues with six strategic players, 3) launching the Human Rights Guidelines, 4) adopting Council Conclusions on Cyber Diplomacy, 5) introducing several cyber capacity building programmes through global and regional instruments, 6) adopting Council Conclusions on a Joint EU Diplomatic Response to Malicious Cyber Activities.

As with the previous objectives it has to be noted that also this one was defined in a very general terms, showing the direction the EU should follow. Therefore the assessment looks at the degree of progress made without the assumption that the objective could have been fully met. It has also to be noted that due to the nature of diplomatic efforts, these are not easily quantifiable.

5.5.1 To what extent has the objective been achieved?

Working towards a coherent EU international cyberspace policy and mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy

One of the key operational objectives was to make progress towards a coherent EU international cyberspace policy. Thanks to the efforts triggered by the Strategy, the EU has been able to achieve a convergence of Member States' positions on different cyber diplomacy and Internet governance topics and present a coherent approach in major global cyber debates. This has helped also Member States to guide their foreign policy in this new and complex field.[133]

Another objective of the Strategy was to mainstream cyberspace issues into the EU's external relations and Common Foreign and Security Policy by advancing bilateral cyber efforts. The Strategy aimed at increased engagement and stronger relations with key international players and a special focus was to be put on like-minded partners that share EU values. Substantial

[133] See e.g. Cyber Diplomacy Council Conclusions from 2015, which prioritise the promotion of core EU values in cyberspace, applying existing international law, developing cyber norms and confidence building measures, as well as advancing cyber security capacity building globally.

progress in this regard was achieved as the EU has managed to build up specific cyber dialogues with the U.S., Japan, India, South Korea and China.

The dialogues, although at different levels of maturity, have helped to fulfil the Strategy's commitment of promoting the application of existing international law and voluntary norms of responsible state behaviour. Dialogues have also tackled technical cyber issues and have been assessed by Member States and international partners as effective when being comprehensive cross-cutting dialogues on all EU policies. Many Justice and Home Affairs as well as internal market issues have been discussed at dialogues including addressing cybercrime, sharing best practices on cyber security and exchanging cyber threat information. Setting up EU cyber dialogues was mostly appreciated by mid-size and smaller EU Member States that have had an opportunity to be involved in discussions with strategic players on cyber issues. At the same time, the effectiveness of the dialogues was hampered to a certain extent by staying at formal level, and having annual meetings only, with the lack of activities between formal dialogue sessions that could involve more stakeholders.

Council Conclusions on a Framework for a "Joint EU Diplomatic Response on Malicious Cyber Activities ("cyber diplomatic toolbox") that aims to influence the behaviour of potential aggressors in cyberspace and able the EU to jointly respond to malicious cyber activities were adopted in June 2017.

The major EU added value and relevance of the actions aimed at achieving the high-level objective set by the Strategy is making the EU's Internet governance and international cyber policy more coherent across the European Union. The fact that this objective is being attained was very visible in major global debates with other international organisations since 2013. Many Member States have mainstreamed cyber policy into their diplomatic services and have increased national resources on cyber diplomacy.

Support the development of norms of behaviour and confidence building measures in cybersecurity

In accordance with the objectives of the Strategy, the EU has consistently promoted the understanding that the existing international law applies in cyberspace and that norms of responsible state behaviour in cyberspace and regional cyber confidence building measures need to be developed.

EEAS has been effectively supporting international discussions on norms of responsible state behaviour as requested by the Strategy and has played a valuable role in supporting Member States in their efforts of resisting a new legal instrument at UN level. In this regard, the cyber dialogues described in the section above, proved to be a useful tool to address this topic with likeminded partners.

Member States, in particular the ones which have been members of the UN Group of Governmental Experts (UN GGE), have contributed greatly to the efforts of defining how international law applies in cyberspace and the EU has been promoting and supporting this important work contributing to peace and stability in cyberspace.

The Strategy also called for an active support of cybersecurity confidence building measures. Major progress has been achieved in this regard in international efforts to promote cyber confidence building measures, also thanks to the EU's substantive supporting role in the process. Two sets of confidence building measures, more specifically cooperation and transparency measures, were adopted by the OSCE participating States in 2013 and 2016,

which should be still fully implemented. In order to raise the level of trust and confidence between Asian countries, the EU has actively supported a similar process in the ASEAN Regional Forum.

While progress in this field has been achieved, some gaps related to active engagement remain as a number of larger Member States expect the EU to become more vocal on international security, confidence building and cyber norms issues. The efforts in this regard were, however, hampered by insufficient human resources and the lack of a clearer mandate by all 28 Member States for the EEAS to become more active in this field.

Enhancing the protection of fundamental rights, including access to information and freedom of expression

The Strategy highlighted the need of ensuring that the human rights law is also enforced in cyberspace. Since 2013, through the presence in international for a and discussions, the EU has been effective in promoting the notion that State behaviour should follow the long established principles of existing international human rights law, such as the legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of fundamental rights.

The progress towards achieving the objective was possible thanks to successful efforts to come up with a coherent EU position and guidelines (e.g. EU Human Rights Guidelines "on freedom of expression online and offline" and Council Conclusions on Internet Governance), which have helped to implement key human rights principles online and mainstream them into all cyber related areas.

Support global capacity building in third countries by engaging with international partners and organisations, the private sector and civil society.

Substantial progress has been achieved in capacity building activities in the third countries, making the EU a very relevant global player in this field. The EU has developed an efficient model[134] and has been allocating increasing funds to addressing cybercrime globally, together with the Council of Europe. The capacity building efforts have played a key role in building strong partnerships with third countries and helped to promote the notion of open, free and secure cyberspace. In order to avoid duplications of cyber capacity building efforts, at the Global Conference on Cyber Space in 2015 in The Hague, the Global Forum on Cyber Expertise (GFCE) has been launched. The GFCE is an initiative for policymakers, practitioners and experts from different countries and regions to identify gaps in global cybersecurity capacities, to complement existing efforts in capacity building and share experiences. The GFCE contributes to coordination of capacity building donor on a global level.

At the same time the effectiveness of the efforts was limited by the lack of mechanisms to mobilise Member States' collective expertise to assist efforts to build national cyber resilience in third countries. A clear political guidance and prioritisation of EU efforts in assisting the third countries was also lacking.

[134] The importance of this model was stressed in the 2015 Council Conclusions on Cyber Diplomacy and the EU Agenda on Security. It has been strongly linked with the EU's development agenda in light of the 2030 Agenda for Sustainable Development (*SDG 9a on resilient infrastructure and SDG 16a on combatting crime)* and overall efforts for institutional capacity building.

Finding 41: *The Strategy triggered initiatives, which led to establishing a coherent EU voice on global cyber affairs. This was key for conducting international cyber policy efforts more effectively. However, several gaps remain where global community and Member States expect more EU engagement. Some larger Member States expect the EU to become more vocal on international security, confidence building and cyber norms issues. This was hampered so far by insufficient resources and the lack of clear mandate by 28 MSs for EEAS to become more active in this field.*

Finding 42: *As the Strategy requested placing a renewed emphasis on dialogue with third countries, EU has set up six annual cyber dialogues. Although this is seen positively by Member States, the dialogues could bring more added-value if coherent between all cyber domains and complemented by inter-sessional activities tailored specifically towards each dialogue partner. The involvement of civil society and academia on both sides could be encouraged within these inter-sessional activities.*

Finding 43: *The EU has started efforts to mainstream cyber security into its CSFP engagement, but further work is necessary to organise awareness raising events on cyber norms, international law and cyber confidence building measures in other regions, and assist other regional organisations to adopt cyber confidence building measures.*

Finding 44: *Substantial progress has been made in reaching the Strategy's objective to enhance cyber capacity building in third countries. However, the effectiveness was limited by the lack of mechanisms to mobilise Member States' collective expertise to assist these efforts. The lack of clear political guidance and prioritisation of EU efforts in assisting the third countries was also limiting the effectiveness of the efforts.*

5.6 TO WHAT EXTENT IS THE OBJECTIVE OF ESTABLISHING A COHERENT INTERNATIONAL CYBERSPACE POLICY FOR THE EU AND PROMOTING EU CORE VALUES STILL RELEVANT?

The objective is still relevant as the borderless nature of the Internet makes the need for international cooperation indispensable. To preserve an open, safe and secure cyberspace the EU must further contribute to protecting the open internet and to global stability in cyberspace, while deepening our cooperation with strategic partners and other international organisations.

Continuous efforts by like-minded countries on raising global awareness of the application of existing international law in cyberspace and more efforts on how it is applying are needed to further resist the tendencies to increase government control over the Internet and through that hamper economic and societal development and limit Internet freedom;

Cybersecurity capacity building in third countries also remains relevant as the EU's resilience depends also on the ability to limit the vectors of incidents coming from outside its borders. Further joint efforts by the diplomatic, development and cyber communities of the EU Member States and institutions are also necessary to mobilise the expertise for capacity building and to contribute to more efficient donor coordination globally, which would allow more effective absorption of increased cybersecurity funding available through different development instruments.

***Finding 45**: The Strategy objective is still relevant as the borderless nature of the internet makes the need for international cooperation indispensable. To preserve an open, safe and secure cyberspace the EU must further contribute to protecting the open internet and to global stability in cyberspace, while deepening our cooperation with strategic partners and other international organisations Cybersecurity capacity building to third countries also remains relevant as the EU's resilience depends also on the ability to limit the vectors of incidents coming from outside its borders.*

6 CONCLUSION

The present **assessment** of the 2013 EU Cybersecurity Strategy focused on the relevance of the five objectives and on the progress introduced by the Strategy compared to the *status quo ante*.

Overall, the assessment found that the five original objectives of the 2013 Strategy are as **relevant** today as when the Strategy was first proposed. However, the Strategy no longer addresses the challenges caused by the new threat landscape and technological developments (e.g.: challenges related to security of the Internet of Things devices and its implications for the whole digital ecosystem, the balance of responsibilities between the end users (individual citizens, public and private organisations and enterprises) and the providers of products and services with embedded digital/connected components; the cybersecurity of sectors and entities which is not covered by the NIS Directive; evolving cybercrime business models; crisis management in case of a large-scale attack).

Regarding **effectiveness**, the Strategy appears to have only partially achieved its main objectives. This is, among others, due to the fact, that the objectives were formulated in a very broad, high-level manner (e.g. achieve cyber resilience), expressing rather the direction the EU should follow than a target that could be fully met. The degree to which the EU was able to follow the vision expressed by these objectives differed depending on a number of factors such as e.g. resources available, different level of engagement and ownership of stakeholders responsible for the implementation of specific actions, external factors impacting the cybersecurity ecosystem (e.g. changing threat landscape and technological developments). The summary of key conclusions for each of the objectives is presented below.

Achieving cyber resilience

The assessment found that the objective of achieving resilience was and remains relevant as strong resilience is a first line of defence against cybercrime. However, it should be noted that the objective itself was formulated in a very broad manner, expressing rather a vision than a measurable target. Whereas full resilience cannot be achieved in real life, the Strategy identified relevant operational objectives of increasing capacities, stimulating cooperation and information exchange as well as raising awareness and skills, which are prerequisite for effective cybersecurity prevention.

However, the Assessment found that the Strategy has only partially contributed to increased cyber resilience in the EU. On the one hand, the Strategy has, via the NIS Directive and

supporting non-legislative actions (e.g. Cyber Exercises), contributed to enhanced capacity building in Member States and improved cooperation and information sharing at the EU level. On the other hand, the Strategy mechanisms were limited in their capacity to deliver an EU-level cooperation mechanism in case of a large-scale cross-border cyber incident. Cooperation amongst Member States remains voluntary; cooperation between Member States and the private sector, and within the private sector, remains in its early stages of development; and cooperation between European institutions, relevant agencies and bodies in such a case is based to a large extent on informal relationships rather than established procedures, which reduces its effectiveness.

The Cybersecurity Strategy, despite having successfully triggered a series of awareness raising and skills building events (e.g. European Cyber Security Month, Cyber Challenge) is only partially effective in raising the awareness of citizens and businesses at national level. The assessment found that this is partly due to the magnitude of the task in comparison to the limited resources available both at the EU and Member States' level. The subsidiarity principle is also a key factor as raising awareness is primarily the task of Member States, whose engagement is still uneven and largely reflects the level of their cybersecurity capacities in general. The same finding was relevant for the skills gap, where the shortfall of 350,000 specialists by 2022, is expected.

Drastically reducing cybercrime

The assessment found that the objective of drastically reducing cybercrime has not been achieved. In addition to the overall growth in cybercrimes, other cross-cutting issues, such as the growing misuse of anonymity and encryption services and other legitimate tools for illegal purposes pose a serious impediment to detection, investigation and prosecution of criminals. This further impedes the chances of effectively reducing cybercrime, adding to the doubts concerning the realistic nature of the target. However, while the target of drastically reducing cybercrime may have been overly ambitious, the objective behind it – to more effectively counter cybercrimes to ensure a better protection of all users and trust in the Digital Single Market – was and remains relevant.

The assessment found that, whereas harmonised substantive law has facilitated cooperation across Member States, the main challenges for law enforcement now lie in the investigative (procedural) area. While the Strategy rightly identified the need to support the European Cybercrime Centre at Europol to enable it to effectively contribute to improving operational cooperation in the fight against cybercrime, its resources are now outpaced by Member States' need for support. The assessment also flagged remaining difficulties in accessing information from the private sector.

The assessment concluded that the measures taken based on the Cybersecurity Strategy have not been sufficiently effective in increasing accountability online. Certain data on registrants are inaccurate. This issue shall be addressed, ensuring at the same time that personal data are protected. While it is likely that growth would have been even steeper in the absence of the Strategy and the Global Alliance, there unfortunately has been no reduction in the overall number of child sexual abuse cases.

Developing industrial and technological resources for cybersecurity

The progress towards fulfilling the Strategy's objective to achieve a single market for cybersecurity has been modest and the market supply for ICT security products and services in Europe remains fragmented. The relatively slow progress at the EU level related to

standardisation and development of possible voluntary certification schemes was coupled with the emergence of a number of national certification schemes. Albeit important, these initiatives bear the risk of creating single market fragmentation and barriers for interoperability.

The assessment concluded that the set-up of the contractual Public-Private partnership on cybersecurity in 2016 can be seen as an important milestone towards achieving the Strategy's objective of increasing investment in research and innovation. The total investment, between public and private funds, is expected to reach €1.8 billion from 2017 to 2020. At the same time the assessment suggests that the resources involved in supporting cybersecurity in Europe still remain much smaller than the investment by other major players around the world (e.g. the USA). In addition, cybersecurity competences and expertise are still dispersed across Europe.

Developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

The assessment concludes that some progress has been made in implementing the defence policy objectives through the EU Cyber Defence Policy Framework, but a systematic approach to the Member States' capability building and CSDP operation and missions' protection has not yet been achieved. Member States' involvement in EU cyber-defence efforts remains low, efforts are scattered and there is a need for improvement in the cyber protection of CSDP missions and operations.

Regular consultations between EU and NATO, as well as the cyber defence information sharing agreement have been set up. However, further implementation of the EU-NATO Joint Declaration requires more efficient coordination efforts on the EU side across all major cooperation areas: concept development; training, education, and exercises, research and technology initiatives.

Establishing a coherent international cyberspace policy

The assessment concludes that progress has been made in establishing a coherent international cyberspace policy, as the EU has been able to present a coherent approach on major global cyber debates, with a convergence of Member States' positions on different cyber diplomacy issues. A major achievement in international cyber policy has been the establishment of six annual cyber dialogues with strategic players and the development of cyber security confidence building measures, where the EU has played an important role.

Against the background of global polarization on whether existing international law applies to cyberspace, the EU has been able to raise awareness on the application of existing international law. However, global consensus on this issue is currently fast disintegrating and there are increased efforts to call for new international legal instruments that could further hamper economic and societal development and freedom of expression online.

Although the EU has been relatively successful in kicking off capacity building programs to fight cybercrime globally, it still lacks a mechanism to mobilise its collective expertise to assist efforts to build national cyber resilience in third countries. In addition, there is a lack of mechanisms to mobilise Member States' collective expertise to assist efforts to build national cyber resilience in third countries.

Strategy relevance in view of fast changing Cybersecurity landscape

The assessment noticed that the five original objectives of the 2013 Strategy are as **relevant** today as when the Strategy was first proposed. However, as the threat landscape rapidly evolved since 2013, the cybersecurity context in which the 2013 Strategy has been created is substantially different in 2017. The "Internet of Things revolution" has become a fact with fifty billion new devices expected to be connected to the Internet by 2020.The ever-increasing connectivity of poorly secured devices (reaching today the key systems that control citizens' cars, factories, homes, farms, hospitals and all critical infrastructures) have substantially increased the surface of possible cyber-attacks, eagerly used by cybercriminals.

Cyber-attacks are, in fact, booming. The number of security incidents across all industries rose by 38% in 2015, which is the biggest increase in the past 12 years[135]. In addition, at least 80% of European companies have experienced at least one cybersecurity incident. In the third quarter of 2016 alone, 18 million new malware samples were captured: that is an average of 200,000 per day[136].

In some Member States it has been estimated that more than half of all crimes are cybercrimes. Some of these attacks have aimed at high-profile targets, including power grids, important webmail services, central banks, telecom companies and electoral commissions.

At the same time, the current cybersecurity threat landscape is also characterised by "the efficiency of cyber-crime monetization". That is to say, the selling of cybercrime related services online is becoming a lucrative activity and this trend is likely to continue. Attacks including multiple channels and various layers seem to be the "state of the art", while robust, efficiently managed flexible cyberattack tools became a service widely available, even to low capability threat agents.

New threat actors have also emerged. The politically motivated use of cyber vectors to undermine democratic systems has become a significant threat to the security and integrity of European democracies, societies and businesses. These actors, directly or via proxies, leverage a significant amount of technical expertise, human and financial resources to gain political or commercial advantage.

[135] PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

[136] PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

ANNEX 1 : SOURCES OF THE STAFF WORKING DOCUMENT ON THE ASSESSMENT OF THE 2013 EU CYBERSECURITY STRATEGY

INTRODUCTION

The assessment was carried out, to the extent possible, according to the triangulation technique - a common evaluation method that brings together at least three sources of data and tools for data collection, and is embedded in a structured approach. Annex 2 presents the list of sources used for this assessment. Sources have been categorized according to the nature of the documents: EU official documents, Reports issued by EU institutions and bodies, Reports issued by other entities, online sources and internal reports to the EU institutions and bodies.

1. EU OFFICIAL DOCUMENTS

- Joint Communication "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" JOIN (2013) 1 final, 7 February 2013.
- Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All, COM/2017/0228.
- Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.
- Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.
- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
- Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework- Decision 2004/68/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Ajl0064
- Commission Staff Working Document Ex-Ante Evaluation: Resources needed to fulfil the tasks set forth in the Commission's Communication on the establishment of a European Cybercrime Centre (EC3) SWD/2013/0100 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013SC0100
- COM(2013) 48 final. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union.
- SWD (2013) 32 final: Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union.

- 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, OJ L 218/8 of 14.8.2013.
- Cyber Diplomacy Council Conclusions, 10 February 2015. http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf
- Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"). 16 May 2017. http://data.consilium.europa.eu/doc/document/ST-7923-2017-REV-2/en/pdf
- Council conclusions on the European Judicial Cybercrime Network, 9 June 2016. www.consilium.europa.eu/en/meetings/jha/2016/06/network--en_pdf/
- 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.
- EU Cybersecurity Strategy: Road map development 6183/4/15 REV 4 of 20 September 2016.
- SWD (2016)216 final :Commission Staff Working Document: Contractual Public Private Partnership on Cybersecurity & Accompanying Measures Accompanying the document Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research an innovation between the European Union, represented by the Commission, and the stakeholder organisation.
- SWD (2016) 215 final: Report on the public consultation and other consultation activities of the European Commission for the preparation of the EU Cybersecurity contractual Public-Private Partnership and Accompanying Measures.
- COM (2016) 410 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.
- Ministers' Declaration Facilitating International Cooperation in Online Child Sexual Abuse Investigations, 30 September 2014. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_ministerial_statement_en.pdf
- Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT
- Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf
- Council Presidency. Standing Committee on Operational Cooperation on Internal Security (COSI) Note on Effective operational cooperation in criminal investigations in cyberspace, 11 May 2016. http://data.consilium.europa.eu/doc/document/ST-8634-2016-INIT/en/pdf
- Report from the Commission to the European Parliament and to the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. COM/2016/0871

final.http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1486726102713&uri=CELEX:52016DC0871

- Council Conclusions on Internet governance ST-16200/14-INIT.

- Council Conclusions on the transfer of the stewardship of the IANA functions ST-9855/15-INIT.
- Report on the progress made in the fight against trafficking in human beings (2016) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims (Brussels, 19.5.2016 COM(2016) 267 final) and its accompanying Staff Working Document (Brussels, 19.5.2016 SWD(2016) 159 final).

2. REPORTS ISSUED BY EU INSTITUTIONS AND BODIES

- Special Eurobarometer 390, 2012 on Cybersecurity. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf
- Special Eurobarometer 423, 2015 on Cybersecurity. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf
- Special Eurobarometer 460, 2017 on attitudes towards the impact of digitisation and automation on daily life. https://data.europa.eu/euodp/en/data/dataset/S2160_87_1_460_ENG
- Special Eurobarometer 464, 2017 on public attitudes to the European Union's role in emergency response. http://ec.europa.eu/echo/eurobarometer_en
- Cybersecurity Market analysis conducted by LSEC and PwC, V2 2017 Draft Report, 30/06/2017 (Pending validation before final report).
- ENISA evaluation report and ENISA public consultation.
- Europol. Threat Assessment on Internet Facilitated Organised Crime (IOCTA), 2011: https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011
- ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
- ENISA, Deployment of Baseline Capabilities of n/g CERTs- Status Report 2012: www.ensia.europa.eu/activities/cert/support/files/status-report-2012
- The European Network and Information Security Market: Scenario, Trends and Challenges - A study for the European Commission, DG Information Society and Media; 2009. A new market study is being conducted by an external contractor for the European Commission at the moment and will feed into the cPPP creation process.
- Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.
- Europol The Internet Organised Crime Threat Assessment (IOCTA) 2016: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

- Study on the Evaluation of the European Union Agency for Network and Information Security (ENISA).
- European Political Strategy Centre Strategic Notes: "Building an Effective European Cybershield - taking EU cooperation to the next level".
- EU cybersecurity dashboard, BSA, 2015.
- Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.
- European Cybersecurity Month Deployment Report 2016: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month
- Progress report and final technical report on cross-border access to electronic evidence: http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf;
- European Commission, Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf
- Feasibility study for a European Cybercrime Centre: http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf
- ENISA Annual activity report 2014:

  https://www.enisa.europa.eu/publications/corporate/enisa-annual-activity-report-2014
- ENISA Annual activity report 2015 https://www.enisa.europa.eu/publications/corporate/enisa-annual-activity-report-2015
- ENISA ECSM 2016 Deployment Report (December 2016).
- ENISA, Education Map: Data Base on available courses and certification programmes linked to Network and Information Security: https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities
- SecCord FP7 ICT Trust & Security Projects Handbook Version I, March 2015: http://www.euromils.eu/downloads/FP7HandbookbySECCORD.pdf
- Council Working Party on the Article 29. Letter of Jacob Kohnstamm, Chairman to Dr. Steve Crocker and Mr. Akram Atallah Chairman and interim CEO of the Board of Directors Internet Corporation for Assigned Names and Numbers (ICANN) , 26 September 2012. See: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf
- Europol, Situational Report (2016) Trafficking in human beings in the EU at https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/situational_report_trafficking_in_human_beings-_europol.pdf

3. REPORTS ISSUED BY OTHER ORGANIZATIONS AND BODIES

- Global Alliance against Child Sexual Abuse Online, 2015 Threat Assessment Report: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_threat_assessment_en.pdf
- OECD 2008 "Economics of malware: Security decisions, incentives and externalities" http://www.oecd.org/internet/interneteconomy/40722462.pdf
- United Nations. General Assembly November 2013. Report on Developments in the field of information and telecommunications in the context of international security. UN GGE 2013 A/68/98 https://disarmament-library.un.org/UNODA/Library.nsf/efed7557accf263185257b1000501036/830c33fdd673ad4a85257c2a0046c6b9/$FILE/A%2068%20406.pdf
- United Nations. General Assembly, July 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report on Developments in the field of information and telecommunications in the context of international security. UN GGE 2015 A/70/174: https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf
- The "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", the updated and considerably expanded second edition of the 2013 "Tallinn Manual on the International Law Applicable to Cyber Warfare". See: https://ccdcoe.org/tallinn-manual.html
- PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/
- National Crime Agency (NCA) NCA Strategic Cyber Industry Group .Cyber Crime Assessment 2016. See: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
- 2017 Global Information Security Workforce Study commissioned by the Centre for Cyber Safety and Education and (ISC)2 https://www.isc2.org/pressreleasedetails.aspx?id=14570
- Cloud Evidence Group, Criminal justice access to electronic evidence in the Cloud: Recommendations for consideration by the T-CY https://rm.coe.int/16806a495e
- Global Cybersecurity Index & Cyberwellness Profiles, ABI Research and ITU, 2015.
- Global Cybersecurity Index & Cyber-wellness Profiles, ABI Research and ITU, 2017.
- ThreatMetrix,Q2 2016 Cybercrime Report https://info.threatmetrix.com/rs/991-JSN-701/images/Q2_2016_Report.pdf
- Steve Olensky "The Effect of CyberCrime on Online Shopping", August 2016. https://www.forbes.com/sites/steveolenski/2016/08/03/the-effect-of-cyber-crime-on-online-shopping/#225be8ea2b87
- Markus Riek, Rainer Bohme University of Munster, Department of Information System "Understanding the influence of cybercrime risk on the e-service adoption of European Internet users" Working Paper, 2014. See: http://www.econinfosec.org/archive/weis2014/papers/RiekBoehmeMoore-WEIS2014.pdf
- Competitive analysis of the UK cyber security sector, A study for the Department for Business, Innovation and Skills, 2013.

- L'observatoire de la filière de la confiance numérique en France - Etude pour l'Alliance pour la Confiance Numérique (ACN), 2013.
- Der IT-Sicherheitsmarkt in Deutschland; Bundesministerium für Wirtschaft und Energie, 2014.
- Recommendations on Cybersecurity for Europe, A report to M Gunther Oettinger, European Commissioner for Digital Economy and Society, prepared by the European Cybersecurity Industry Leaders (Thales, Atos, Airbus Group, BBVA, BMW, Cyberentica, Deutsche Telekom, Ericsson, F-Secure, Infineon), January 2016. See: https://ec.europa.eu/digital-agenda/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders
- Jakob Bund, "Cybersecurity and democracy Hacking, leaking and voting" European Union Institute for Security Studies (EUISS), November 2016. http://www.iss.europa.eu/uploads/media/Brief_30_Cyber.pdf
- MARSH, Continental European Cyber Risk Survey 2016 Report. See: https://www.marsh.com/content/dam/marsh/Documents/PDF/eu/en/Continental%20European%20Cyber%20Risk%20Survey%202016%20Report.pdf

4. Online Sources

- https://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html
- https://www.europol.europa.eu/events/official-launch-of-new-european-cybercrime-centre-ec3-ceremony
- www.enisa.europa.eu
- https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board
- https://ec.europa.eu/home-affairs/what-is-new/news/news/2012/20121130_02_en
- https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_report_201312_en.pdf
- www.ecs-org.com
- https://www.iwf.org.uk/news/latest-internet-watch-foundation-report-shows-europe-now-hosts-60-of-child-sexual-abuse
- https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en
- https://www.europol.europa.eu/newsroom
- https://www.nomoreransom.org/
- https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en;
- http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm
- https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification
- https://www.interpol.int/News-and-media/News/2011/PR071

- https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_threat_assessment_en.pdf.
- https://www.iwf.org.uk/news/latest-internet-watch-foundation-report-shows-europe-now-hosts-60-of-child-sexual-abuse
- https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets
- ICANN-GNSO Generic Names Support Organisation website: https://gnso.icann.org/en/group-activities/active/rds
- Internet Corporation for Assigned Names and Numbers (ICANN). Registration Directory Service (RDS) Review (formerly WHOIS Review) https://www.icann.org/resources/reviews/specific-reviews/whois
- https://www.europol.europa.eu/newsroom/news/europol-enhances-cybercrime-and-internet-security-cooperation-signing-mou-eurid
- https://www.europol.europa.eu/newsroom/news/ripe-ncc-and-europol-enhance-cooperation-to-tackle-cybercrime-and-internet-security
- https://www.icann.org/resources/pages/ksk-rollover
- http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

ANNEX 2 OF THE STAFF WORKING DOCUMENT ASSESSING THE EU 2013 CYBERSECURITY STRATEGY : STAKEHOLDERS' CONSULTATION

INTRODUCTION

As Cybersecurity is a broad, cross-sectoral topic, the Commission used numerous consultation methods in order to make sure that the Union's general public interest – as opposed to special interests of a narrow range of stakeholder groups – is well reflected in the assessment of the initiative. This method ensures transparency and accountability in the Commission's work.

In order to identify the most appropriate mix of consultation methods, the first step has been to identify the relevant stakeholder groups and the best way to consult them in order to gather relevant input.

The Commission pays attention to differentiate data gathering tools and adapts them to different types of contributions the stakeholders might have. Furthermore, to allow for wide participation, the consultation period spanned over a long period - from July 2016 to July 2017 approximately.

No open public consultation was conducted specifically for this assessment as the thematic was already covered by other public open consultations conducted in the context of the evaluation of the European Network and Information Security Agency (ENISA) in 2017 as well as the contractual Public Private Partnership on cybersecurity and accompanying measures (2016).

1. IDENTIFICATION OF GROUPS OF STAKEHOLDERS CONSULTED, MEANS OF CONSULTATION, AND CONSULTATION TOPICS

1.1. WHOM HAS THE COMMISSION CONSULTED?

A list of stakeholders that have been consulted either directly, or through consultation efforts related to ENISA and certification initiatives, includes the following bodies:

- The EU Member States national authorities;
- European Commission's services;
- The European External Action Service;
- Other EU Agencies and bodies, such as ENISA, Computer Emergency Response Team for the EU institutions (CERT-EU), Europol and its European Cybercrime Centre (EC3), European Defence Agency, Body of European Regulators for Electronic Communications (BEREC), European Agency for the Operational

Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA);

- Trade associations and industry representatives, including the European Cybersecurity Organisation (ECSO), Alliance for Internet of Things Innovation (AIOTI), Digital Europe, and the Enterprise Europe Network (in particular for small and medium enterprises (SMEs);
- Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) (mostly regarding ENISA);
- Stakeholders relevant for certification aspects of the Strategy (standardisation bodies; Senior Officials Group – Information Systems Security (SOG-IS) members (mostly regarding certification);
- Citizens.

1.2. HOW HAS THE COMMISSION CONSULTED STAKEHOLDERS?

Different tools and methods were used in order to conduct the consultation.

- Public Consultations:
  - In 2016, a 12-week online public consultation was carried out at the occasion of the launch of the contractual public-private partnership on cybersecurity, which included specific questions / section on the general cybersecurity ecosystem, as well as on a number of initiatives building on the Strategy - public private partnership and certification (approx. 240 respondents).
  - In 2017, a 12-week online public consultation was carried out to seek views from the wider public (approx. 90 respondents) on ENISA evaluation and review. The consultation included also questions on the future needs and priorities in the area of cybersecurity;
- Workshop on the future contribution of ENISA to EU cybersecurity, where questions on current cybersecurity ecosystem were also asked (22 March 2017).
- High Level Roundtable chaired by Vice President Ansip on Cybersecurity Strategy on 25 April 2017.
- Council Horizontal Working Party meetings (2017: meetings on 19 April, 12 May, 07 June, 03 July, 12 July).
- Bilateral meetings with Member States' national cybersecurity authorities.
- Direct dialogue with individual stakeholders reaching out to the Commission on the review of the 2013 Cybersecurity Strategy, ENISA and certification.
- Special Eurobarometer 464, which interviewed *28,093* citizens across all Member States.

2. LEARNINGS FROM THE CONSULTATION PROCESS

2.1. LEARNINGS FROM THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF ENISA

The open public consultation on the evaluation and review of ENISA took place between 18 January and 12 April 2017. The public consultation aimed to gather the views of stakeholders on evolving needs and challenges in the cybersecurity landscape and to evaluate ENISA's overall performance. The results of this consultation were insightful for the purpose of the assessment as they highlighted gaps and challenges in the current cybersecurity ecosystem identified by the stakeholders, and their perception on the progress achieved since 2013.

Main results related to the questions related to the broad cybersecurity ecosystem:

- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU; in particular the top 5 (in a list of 16) were: cooperation across Member States in matters related to cyber security; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks; skills development, education and training of professionals.

- Respondents were also asked if the current instruments and mechanisms at the European level are adequate to promote and ensure cybersecurity in relation to the needs previously identified. Only 6% of the respondents judged the current instruments and mechanisms at the European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be "fully adequate" to promote and ensure cybersecurity. 83% of respondents regarded them as either "partially" or only "marginally adequate" and 5% found them "not at all adequate". National authority respondents appear to be more positive about the adequacy of these instruments and mechanisms in comparison with representatives of private enterprises or business associations and "other" respondents.

2.2. CONSULTATIONS WITH MEMBER STATES

HIGH LEVEL ROUNDTABLE ON THE REVIEW OF THE 2013 CYBERSECURITY STRATEGY CHAIRED BY VICE PRESIDENT ANSIP

Vice President Ansip held a high level Roundtable on 25 April 2017 focusing on the review process of the 2013 Cybersecurity Strategy. The Council, the Commission, European External Action Service EEAS also participated to the meeting. All 28 Member States were present at the roundtable.

This meeting was insightful for the purpose of assessing the 2013 Strategy as Member States pointed out the remaining gaps in building a secure cyberspace despite the progress made since 2013.

The main gaps identified by Member States were:

- Insufficient trust and cooperation among stakeholders;
- Cybersecurity not being sufficiently mainstreamed in EU internal and global policies;
- Cybersecurity awareness and skills gap in the population;
- An insufficient level of investment in Research and Development;
- The lack of a culture of security by design;
- Insufficient Member States' and EU capacity to respond to cyber threats;
- Limited law enforcement access to e-evidence and lack of prosecution of cybercrimes; and
- Limited capacity building support to third countries.

The consultation process has then continued at the meetings of the Council Horizontal Working Party (HWP) on Cyber issues. A number of thematically focused meetings (e.g. resilience, cybercrime, international aspects in cyber) took place between April and July 2017. Member States' discussions expressed their views on, among others, what worked well so far and where gaps exist in the response to cybersecurity challenges at the European level. A number of Member States have also submitted their position papers related to the review process of Cybersecurity Strategy.

2.3. LEARNINGS FROM THE SPECIAL EUROBAROMETER 464 RESULTS

The results of the Special Eurobarometer have been useful in assessing whether the objectives set under the 2013 Cybersecurity Strategy have been achieved as they allowed for a comparison with the 2013 context (by comparing with the results of the Eurobarometer 460). *28,093* citizens were interviewed for the Special Eurobarometer 464, over the period of *13th to 26th June 2017*. Regarding Cybersecurity results, the survey conducted focused on the Internet Use of citizens, their perception and (potential) experiences of cybercrime.

Internet Use

Overall, 7 in 10 people use the Internet every day in EU. Internet usage is increasing on a daily basis. A change in the use of devices since 2013 can be noted: there has been a 44% increase on the use of smartphones to access the Internet when comparing with the results of the Special Eurobarometer 460.

Concerns about Internet transactions

45% of respondents' are concerned about someone misusing their data when making secure online payments. Regarding measures people took as a precaution: there is a positive trend to change passwords for online banking accounts, but devolution in changing passwords for email accounts.

Awareness and Experience of Cybercrime

A majority of respondents (51%) do not feel well informed about the risks of cybercrime despite the rising internet use. Denmark and Sweden are most likely to feel well informed, compared to Bulgaria and Romania which do not feel well informed. In average in the EU, less than half (44%) of respondents claimed they felt able to protect themselves against cybercrime.

A big majority of respondents (86%) believe that the risk of becoming a victim of cybercrime is increasing. 9 out of 10 people avoid disclosing personal information online.

In 27 Member States, a majority is concerned that online personal information is not kept secure by websites. Estonia is the exception, with less than half (47%) feeling concerned.

The proportion of respondents who have been a victim of malicious software is significantly higher than in most of the other cases of cybercrime, but there are still substantial country-level differences. In Finland, over half (53%) of respondents have experienced this problem, and in the Netherlands nearly six in ten (59%) have. In all other countries, a minority of respondents have been affected by this, but this ranges from nearly half of those polled in Luxembourg (49%), France, Estonia and Sweden (all 48%) to only just over a fifth (21%) of respondents in Slovakia.

It is clear that there are high and increasing levels of concern about cybersecurity across the EU, with respondents particularly concerned about malicious software, identity theft, and online and banking fraud. Since 2013, there has been steady growth in the proportion of respondents concerned about different forms of cybercrime. This Eurobarometer marks the first time where there is a majority of respondents feeling concerned about all the forms of cybercrimes tested in the survey.

Three trends clearly come out of this report: first, an increasing proportion of Europeans are making daily use of the Internet; second, they are increasingly doing so on a variety of devices; third, they are increasingly using these devices to perform tasks – such as shopping and online banking – which carry risks of exposing personal data.