EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 13.9.2017
JOIN(2017) 450 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

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

1. INTRODUCTION

Cybersecurity is critical to both our prosperity and our security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats: both civilian infrastructure and military capacity rely on secure digital systems. This has been recognised by the June 2017 European Council[1], as well as in the Global Strategy on Foreign and Security Policy for the European Union.[2]

The risks are increasing exponentially. Studies suggest that the economic impact of cybercrime rose fivefold from 2013 to 2017, and could further quadruple by 2019.[3] Ransomware[4] has seen a particular increase, with the recent attacks[5] reflecting a dramatic rise in cyber-criminal activity. However, ransomware is far from the only threat.

Cyber threats come from both non-state and state actors: they are often criminal, motivated by profit, but they can also be political and strategic. The criminal threat is intensified by the blurring of the border between cybercrime and "traditional" crime, as criminals use the internet both as a way to scale up their activities, and also as a source to find new methods and tools to commit crime.[6] Yet in the vast majority of cases, the chances of tracing the criminal are minimal, and the chances of prosecution smaller still.

At the same time, state actors are increasingly meeting their geopolitical goals not only through traditional tools like military force, but also through more discreet cyber tools, including interfering in internal democratic processes. The use of cyberspace as a domain of warfare, either solely or as part of a hybrid approach, is now widely acknowledged. Disinformation campaigns, fake news and cyber operations targeted at critical infrastructure are increasingly common and demand a response. For this reason, in its Reflection Paper on the Future of European Defence[7] the Commission stressed the importance of cyber defence cooperation.

Unless we substantially improve our cybersecurity, the risk will increase in line with digital transformation. Tens of billions of "Internet of Things" devices are expected to be connected to the internet by 2020, but cybersecurity is not yet prioritised in their design.[8] A failure to protect the devices which will control our power grids, cars and transport networks, factories, finances, hospitals and homes could have devastating consequences and cause huge damage to consumer trust in emerging technologies. The risk of politically-motivated attacks on civilian targets, and of shortcomings in military cyber defence, deepens the risk still further.

The approach set out in this Joint Communication will make the EU better placed to face these threats. It would build greater resilience and strategic autonomy, boosting capabilities in

---

1 http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.
2 http://europa.eu/globalstrategy/.
3 See for example McAfee & Centre for Strategic and International Studies "Net losses: Estimating the Global Cost of Cybercrime" 2014.
4 Ransomware is a type of malware that prevents or limits users accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.
5 In May 2017 the WannaCry ransomware attack affected more than 400,000 computers in over 150 countries. A month later, the "Petya" ransomware attack hit Ukraine and several companies worldwide.
6 EUROPOL's Serious and Organised Crime Threat Assessment 2017.
7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf.
8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, study for the Commission.

terms of technology and skills, as well as helping to build a strong single market. This needs the right structures to be in place to build strong cybersecurity and to react when needed, with the full involvement of all key actors. The approach would also better deter cyber-attacks, by stepping up work to detect, trace and hold to account those responsible. It would also recognise the global dimension by developing international cooperation as a platform for EU leadership on cybersecurity. These steps build on the approaches of the Digital Single Market, the Global Strategy, the European Security Agenda[9], the Joint Framework on countering hybrid threats[10] and the Communication on Launching the European Defence Fund.[11][12]

The EU is already working on many of these issues: it is now time to draw the various work streams together. In 2013, the EU set out a Cybersecurity Strategy launching a series of key workstreams to improve cyber resilience.[13] Its main goals and principles, to foster a reliable, safe and open cyber ecosystem, remain valid. But the continuously evolving and deepening threat landscape calls for more action to withstand and deter attacks in the future[14].

The EU is well placed to address cybersecurity, given the scope of its policies and the tools, structures and capabilities at its disposal. While Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity. This approach is designed to galvanise all actors – the EU, Member States, industry and individuals – to give cybersecurity the priority it needs to build resilience and deliver a better EU response to cyber-attacks. It will bring concrete steps to help detect and investigate any form of cyber incidents against the EU and its Member States and to respond appropriately, including by prosecuting criminals. It will enable EU external action to effectively promote cybersecurity on the global stage. The result will be a shift for the EU from a reactive to a proactive approach to protecting European prosperity, society and values, as well as fundamental rights and freedoms, through responding to both existing and future threats.

2. BUILDING EU RESILIENCE TO CYBER ATTACKS

Strong cyber resilience needs a collective and wide-ranging approach. This calls for more robust and effective structures to promote cybersecurity and to respond to cyber-attacks in the Member States but also in the EU's own institutions, agencies and bodies. It also requires a more comprehensive, cross-policy approach to building cyber-resilience and strategic autonomy, with a strong Single Market, major advances in the EU's technological capability, and far greater numbers of skilled experts. At the heart of this is a broader acceptance that cybersecurity is a common societal challenge, so that multiple layers of government, economy and society should be involved.

---

9 COM(2015) 185 final.
10 JOIN(2016) 18 final.
11 COM(2017) 295.
12 The approach is also substantiated by independent scientific advice provided by the European Commission's Scientific Advice Mechanism High Level Group of scientific advisors (see references below).
13 JOIN(2013) 1 final. An assessment of this strategy is available in SWD (2017) 295.
14 Unless otherwise stated, proposals in this Communication are budgetary neutral. Any initiative having budgetary implications will duly follow the annual budget procedures and cannot prejudge the next Multi-Annual Financial Framework post-2020.

2.1 Strengthening the European Union Agency for Network and Information Security

The **European Union Agency for Network and Information Security (**ENISA) has a key role to play in strengthening EU cyber resilience and response but is constrained by its current mandate. The Commission is therefore presenting an ambitious reform proposal, including a **permanent mandate for the agency**.[15] This will ensure that ENISA can provide support to Member States, EU institutions and businesses in key areas, including the implementation of the Directive on the Security of Network and Information Systems[16] (the "NIS Directive") and the proposed cybersecurity certification Framework.

The reformed ENISA will have a strong advisory role on policy development and implementation, including promoting coherence between sectoral initiatives and the NIS Directive and helping to set up Information Sharing and Analysis Centres in critical sectors. ENISA will raise the bar and enhance the European preparedness by organising yearly pan-European cybersecurity exercises combining response across different levels. It will also support EU policy development on information and communications technology (ICT) cybersecurity certification and play an important role in stepping up both operational cooperation and crisis management across the EU. The agency will also serve as a focal point for information and knowledge in the cybersecurity community.

A rapid and shared understanding of threats and incidents as they unfold is a prerequisite for deciding whether joint mitigation or response action supported by the EU is needed. Such information exchange requires the involvement of all relevant actors – EU bodies and agencies, as well as Member States – at technical, operational and strategic levels. ENISA, in cooperation with the relevant bodies at Member State and EU level, notably the network of Computer security incident response teams[17], CERT-EU, Europol and the EU Intelligence and Situation Centre (INTCEN), will also contribute to EU-level situational awareness. This can be fed into threat intelligence and policy-making in the context of regular monitoring of the threat landscape and effective operational cooperation, as well as in response to large-scale cross-border incidents.

2.2 Towards a Single Cybersecurity Market

The growth of the cybersecurity market in the EU – in terms of products, services and processes – is held back in a number of ways. A key aspect is the lack of cybersecurity certification schemes recognised across the EU to build higher standards of resilience into products and to underpin EU-wide market confidence. The Commission is therefore putting forward a proposal to set up **an EU cybersecurity certification framework**.[18] The Framework would lay down the procedure for the creation of EU-wide cybersecurity certification schemes, covering products, services and/or systems, which adapt the level of assurance to the use involved (be it critical infrastructures or consumer devices).[19] It would bring clear benefits to businesses by avoiding the need to go through several certification processes when trading across borders, thereby limiting administrative and financial costs. The use of schemes developed under this Framework would also help build consumers'

---

15 COM(2017) 477.

16 Directive 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.

17 As provided for in article 9 of the NIS Directive.

18 COM(2017) 477.

19 A level of assurance indicates the degree of rigour of the security assessment and is usually commensurate to the level of risk associated with this application areas or functions (i.e. higher level of assurance required for ICT products or services used in high risk application areas or functions).

confidence, with a certificate of conformity to inform and reassure purchasers and users about the security properties of the products and services they buy and use. This would make high standards for cybersecurity a source of competitive advantage. The result would build increased resilience as ICT products and services would be formally evaluated against a defined set of cybersecurity standards, which could be developed in close connection with the broader ongoing work on ICT standards.[20]

The Framework's schemes would be voluntary and would not create any immediate regulatory obligations on vendors or service providers. The schemes would not contradict any applicable legal requirements, such as the EU legislation on data protection.

Once the Framework is established, the Commission will invite the relevant stakeholders to focus on three priority areas:

- Security in critical or high-risk applications[21]: systems that we depend on in our daily activities, from our cars to the machinery in factories, from the largest of systems such as airplanes or power plants to the smallest such as medical devices, are becoming increasingly digital and interconnected. Therefore, core ICT components in such products and systems would require rigorous security assessments.

- Cybersecurity in widely-deployed digital products, networks, systems and services used by private and public sector alike to defend against attacks and apply regulatory obligations[22] – such as email encryption, firewalls and Virtual Private Networks; it is critical that the spreading use of such tools does not lead to new sources of risk or new vulnerabilities.

- The use of "security by design" methods in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things: schemes under the framework could be used to signal that the products are built using state of the art secure development methods, that they have undergone adequate security testing, and that the vendors have committed to update their software in the event of newly discovered vulnerabilities or threats.

These priorities should take particular account of the evolving cybersecurity threat landscape, as well as the importance of essential services such as transport, energy, health care, banking, financial market infrastructures, drinking water or digital infrastructure.[23]

While no ICT product, system or service can be guaranteed to be "100 %" secure, there are several well-known and well-documented defects in the design of ICT products that can be exploited for attacks. A "security by design" approach adopted by producers of connected devices, IT software and equipment would ensure that cybersecurity is addressed before putting new products on the market. This could be part of the "duty of care" principle, to be further developed together with the industry, which could reduce product/software vulnerabilities by applying a range of methods from design to testing and verification, including formal verification where applicable, long term maintenance, and the use of secure

[20] COM(2016) 176.

[21] The exception would be where mandatory or voluntary certification is governed by other Union acts.

[22] For example Directive (EU) 2016/1148, Regulation (EU) 2016/679, Directive (EU) 2015/2366 and other proposed pieces of legislation such as the European Electronic Communications Code, each require that organisations put in place appropriate security measures to address relevant cybersecurity risks.

[23] The sectors within the scope of Directive 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.

development lifecycle processes, as well as developing updates and patches to address previously undiscovered vulnerabilities and fast update and repair.[24] This would also increase consumers' trust in digital products.

Furthermore, the important role of third party security researchers in discovering vulnerabilities in existing products and services needs to be acknowledged and conditions to enable coordinated vulnerability disclosure[25] should be created across Member States, building on best practices[26] and relevant standards.[27]

At the same time, **specific sectors** face specific issues and should be encouraged to develop their own approach. In this way, general cybersecurity strategies would be complemented by sector-specific cybersecurity strategies in areas like financial services[28], energy, transport and health.[29]

The Commission has already highlighted the specific issues concerning **liability** raised by new digital technologies[30] and work is under way to analyse the implications; next steps will be concluded by June 2018. Cybersecurity raises issues around the attribution of damage for businesses and supply chains and failure to address these issues will hamper the development of a strong single market in cybersecurity products and services.

Finally, the development of the EU single market is also dependent on factoring cybersecurity into policy on trade and investment. The effect of foreign acquisitions on critical technologies – of which cybersecurity is an important example – is a key aspect in the framework for **the screening of foreign direct investment in the European Union**[31], which aims to enable the screening of investments from third countries on the grounds of security and public order. By the same token, cybersecurity requirements have already created trade barriers for EU goods and services in important sectors in a number of third country economies. The EU cybersecurity certification framework will further strengthen Europe's international position, and should be complemented by continued efforts towards the development of high-security global standards and mutual recognition agreements.

2.3 Implementing the Directive on the Security of Network and Information Systems in full

With the main tools to combat cybersecurity today in national hands, the EU has recognised the need to drive standards higher. Large-scale cybersecurity incidents rarely affect only one Member State due to the increasingly globalised, digitally-reliant and interconnected nature of key sectors such as banking, energy or transport.

---

[24] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017

[25] Coordinated vulnerability disclosure is a form of cooperation which facilitates and enables security researchers to report vulnerabilities to the owner or vendor of the information system, allowing the organisation the opportunity to diagnose and remedy the vulnerability in a correct and timely fashion before detailed vulnerability information is disclosed to third parties or the public.

[26] For example Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, ENISA, 2016.

[27] ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure.

[28] The Commission's forthcoming work on financial technology will cover cybersecurity for the financial sector.

[29] In the energy sector for instance, combining very old and cutting edge information technologies, particularly with the real-time requirements of the power grid.

[30] COM(2017) 228.

[31] COM(2017) 478.

The Directive on the Security of Network and Information Systems (the "NIS Directive") is the first EU-wide cybersecurity law.[32] It is designed to build resilience by improving national cybersecurity capabilities; fostering better cooperation between the Member States; and requiring undertakings in important economic sectors to adopt effective risk management practices and to report serious incidents to the national authorities. These obligations also apply to three types of providers of key internet services: cloud computing, search engines and online marketplaces. It aims for a stronger and more systematic approach and a better information flow.

Full implementation of the Directive by all Member States by May 2018 is essential to EU cyber resilience. The process is being supported by collective work from Member States which will result, by autumn 2017, in guidelines to support a more harmonised implementation, notably in relation to operators of essential services. The Commission is also issuing a Communication[33] as part of this cybersecurity package to support their efforts by providing best practice from the Member States relevant to the implementation of the Directive and guidance on how the Directive should be operating in practice.

An area where the Directive will need to be supplemented is information flow. For example, the Directive only covers key strategic sectors – but logically a similar approach by all stakeholders hit by cyberattacks would be necessary to have a systematic assessment of vulnerabilities and entry points for cyber attackers. In addition, cooperation and information sharing between the public and private sectors faces a number of obstacles. Governments and public authorities are reluctant to share cybersecurity-relevant information for fear of compromising national security or competitiveness. Private undertakings are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules.[34] Trust needs to be strengthened for public-private partnerships to underpin wider cooperation and sharing of information across a greater number of sectors. The role of Information Sharing and Analysis Centres is particularly important in creating the necessary trust for sharing information between private and public sector. Some first steps have been taken in respect of specific critical sectors such as aviation, through the creation of the European Center for Cybersecurity in Aviation,[35] and energy, by developing Information Sharing and Analysis Centres.[36] The Commission will contribute in full to this approach with support from ENISA, with an acceleration needed in particular with regard to sectors providing essential services as identified in the NIS Directive.

2.4 Resilience through rapid emergency response

When a cyber-attack takes place, a fast and effective response can mitigate its impact. This can also demonstrate that public authorities are not powerless in the face of cyber-attacks, and contribute to building trust. As regards the EU institutions' own response, in the first instance

---

[32] Directive 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.

[33] COM(2017) 476.

[34] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017. A specific issue concerns trade secrets, where the July 2016 Communication "Strengthening Europe's Cyber Resilience System" noted the reticence to report the cyber theft of trade secrets and the importance of trusted reporting channels ensuring confidentiality.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] These are non-profit, member-driven organisations formed by private and public entities to share information on cyber threats, risks, prevention, mitigation and response. See e.g. the European Energy Information Sharing and Analysis Centres (http://www.ee-isac.eu).

the cyber aspects should be mainstreamed into existing EU crisis management mechanisms: the EU integrated political crisis response, coordinated by the Presidency of the Council[37] and the EU's general rapid alert systems[38]. The need to respond to a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause.[39]

A fast and effective response also relies on a swift information exchange mechanism between all key players at national and EU level, which in turn requires clarity on their respective roles and responsibilities. The Commission has consulted institutions and Member States on a "Blueprint" to provide an effective process for an operational response at Union and Member State level to a large-scale cyber incident. The **Blueprint** presented in a Recommendation[40] in this package explains how cybersecurity is mainstreamed to existing Crisis Management mechanisms at EU level and sets out the objectives and modes of cooperation between the Member States as well as between Member States and relevant EU Institutions, services, agencies and bodies[41] when responding to large scale cybersecurity incidents and crises. The Recommendation also requests Member States and EU institutions to establish an EU Cybersecurity Crisis Response Framework to operationalise the Blueprint. The Blueprint will be regularly tested in cyber and other crisis management exercises[42] and updated as necessary.

Given that cybersecurity incidents might substantially impact the functioning of economies and the daily lives of people, an option would be to investigate the possibility of a **Cybersecurity Emergency Response Fund**, following the example of other such crisis mechanisms in other EU policy areas. This would allow Member States to seek help at the EU level during or following a major incident, provided that the Member State had put in place a prudent system of cybersecurity prior to the incident, including full implementation of the NIS Directive, mature risk management and supervisory frameworks at national level. Such a Fund, complementing existing crisis management mechanisms at EU level, could deploy a rapid response capability in the interests of solidarity and finance specific emergency response actions such as replacing compromised equipment or deploying mitigation or response tools, drawing on national expertise along the lines of the EU Civil Protection Mechanism.

2.5 A cybersecurity competence network with a European Cybersecurity Research and Competence Centre

The technological tools of cybersecurity are strategic assets, as well as being key growth technologies for the future. It is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society and democracy, to protect critical hardware and software and to provide key cybersecurity services.

The Public-Private Partnership on Cybersecurity[43] created in 2016 was an important first step, triggering up to EUR 1.8 billion of investment by 2020. However, the scale of the investment

---

37 This enables the coordination of responses to major cross-sectorial crises at the highest political level.

38 These enable internal information sharing and coordination on emerging multi-sectoral crises or foreseeable or imminent threats requiring action at EU level.

39 Under Article 222 of the Treaty on the Functioning of the European Union.

40 C(2017) 6100.

41 Including Europol, ENISA, the EU's Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) and the EU Intelligence and Situation Centre (INTCEN).

42 For example, those run by ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

43 C(2016) 4400 final.

under way in other parts of the world[44] suggests that the EU needs to do more in terms of investment and to overcome the fragmentation of capacities spread across the EU.

The EU has added value to provide, given the sophistication of cybersecurity technology, the large-scale investment required, and the need for solutions that work across the EU. Building on the work of Member States and the Public-Private Partnership, a further step would be to reinforce EU cybersecurity capability through a **network of cybersecurity competence centres**[45] with a **European Cybersecurity Research and Competence Centre** at its heart. This network and its Centre would stimulate development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level. The Commission will launch an impact assessment to examine available options – including the possibility of setting up a Joint Undertaking – with a view to set up this structure in 2018.

As a first step and to inform future thinking, the Commission will propose that a pilot phase is launched under Horizon 2020 to help bring national centres together into a network to create a new momentum in cybersecurity competence and technology development. It plans to propose a short-term injection of funding of EUR 50 million to this end. This activity will complement the ongoing implementation of the Public-Private Partnership on Cybersecurity.

Pooling and shaping research efforts would be at the core of the network and the Centre's initial focus. To support the development of industrial capabilities, the Centre could act as a capability project manager able to handle multinational projects. This would also give added impetus to innovation and competitiveness of the EU industry on the global scene in the development of next-generation digital technologies including artificial intelligence, quantum computing, blockchain and secure digital identities, as well as in ensuring access to mass data for EU based companies, all key to cybersecurity in the future. The Centre would also draw on the EU's work to scale up High Performance Computing infrastructure: this is essential for analysis of large quantities of data, rapid encryption and decryption of data, checking of identities, simulating cyber-attacks, and analysing video material.[46]

The network of competence centres could also have capabilities to support industry through testing and simulation to underpin the cybersecurity certification described in section 2.2. Its involvement in the full range of EU cybersecurity activity would ensure a continual updating of its targeting according to need. The Centre would aim to drive high cybersecurity standards not only in technology and cybersecurity systems but also in high-end skills development for professionals, through providing solutions and templates for national efforts to roll out digital skills. To that extent, it would also enhance cybersecurity capabilities at EU level and build on synergies notably with ENISA, CERT-EU, Europol, the possible future Cybersecurity Emergency Response Fund and national CSIRTs.

A particular focus of work by the competence network must be the lack of European capacity on assessing the **encryption** of products and services used by citizens, businesses and governments within the Digital Single Market. Strong encryption is the basis for secure digital identification systems that play a key role in effective cybersecurity[47]; it also keeps people's

---

[44] The US will invest 19 billion dollars in cybersecurity in 2017 alone, a 35 % increase compared to 2016. The White House, Office of the Press Secretary: 'Fact Sheet: Cybersecurity National Action Plan', 9 February 2016.

[45] The network would include existing and future cybersecurity centres set up in the Member States, whose members would typically be public research organisations and laboratories.

[46] COM(2012) 45 final and COM(2016) 178 final.

[47] The Commission will already launch under Horizon 2020 a new Horizon Prize challenge that will award EUR 4 million to the best innovative solution for seamless online authentication methods.

intellectual property secure and enables protecting fundamental rights such as freedom of expression and the protection of personal data, and ensures safe online commerce.[48]

As the EU civilian and defence cybersecurity markets share common challenges[49] and dual-use technology that call for close collaboration in critical areas, a second phase of the network and its Centre could be further developed with a cyber defence dimension, in full respect of the Treaty provisions related to the Common Security and Defence Policy. As well as its technological focus, the defence dimension could contribute to the cooperation between Member States in the area of cyber defence, including sharing of information, situational awareness, building expertise and coordinated reactions, and supporting Member States' development of common capabilities. It could also act as a platform, enabling Member States to identify the priorities for the EU's cyber defence, investigating common solutions, contributing to the development of common strategies, facilitating joint cyber defence training, exercises and testing at European level, and supporting work on cyber defence taxonomies and standards, with the Centre having a supporting and advisory role. To pursue the above activities, the Centre would need to work closely and in full complementarity with the European Defence Agency in the area of cyber defence, as well as with ENISA in the area of cyber resilience. This defence dimension would take into account the process launched by the Reflection paper on the future of European Defence.

The high level of resilience required in cyber defence calls for specific targeting of research and technology efforts. The cyber defence projects or technologies developed by undertakings could benefit from European Defence Fund financing when it comes to both the research and development phase.[50] Specific areas such as encryption systems based on quantum technologies, cyber situational awareness, biometric access control systems, Advanced Persistent Threats detection, or data mining could be particularly relevant in this context. The High Representative, the European Defence Agency and the Commission will support Member States in identifying areas where common cybersecurity projects could be considered for financing by the European Defence Fund.

2.6 Building a strong EU cyber skills base

There is a strong education dimension to cyber security. Effective cybersecurity relies heavily on the skills of the people concerned. But the cybersecurity skills gap for professionals working in the private sector in Europe is predicted to be 350,000 by 2022.[51] Cybersecurity education should be developed at all levels, starting from regular training of a cyber workforce, additional cybersecurity training for all ICT specialists, and new specific cybersecurity curricula. Strong academic competence centres should be established to meet the demands for accelerated education and training, which could draw on guidance from a European Cybersecurity Research and Competence Centre and ENISA. The goal should be that it becomes natural to design ICT products and systems which incorporate security principles from the very beginning. Cybersecurity education should not be limited to IT professionals, but should be mainstreamed in curricula for other areas, such as engineering, business management or law, as well as for sector-specific education tracks. Finally, teachers

[48] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017.

[49] "Study on synergies between the civilian and the defence cybersecurity markets"(Optimity; SMART 2014-0059).

[50] Already now the European Defence Industry Development Programme will give priority to cyber-defence projects and cyber defence will be one of the themes of the call for proposals that will be launched in 2018.

[51] Global Information Security Workforce Study 2017. The global shortfall is 1.8 million.

and pupils in primary and secondary education should be sensitised to cybercrime and cyber security when acquiring digital competences in schools.

The EU, together with the Member States, should also make a contribution to this work by building on the work of the Digital Skills and Jobs Coalition[52] and by putting in place, for example, apprenticeship schemes in cybersecurity for SMEs.

2.7 Promoting cyber hygiene and awareness

With some 95 % of incidents said to be enabled by "some type of human error – intentional or not",[53] there is a strong human factor at play. So cybersecurity is everyone's responsibility. This means personal, corporate and public administration behaviour must change to ensure everybody understands the threat, and is equipped with the tools and skills necessary to quickly detect and actively protect themselves against attacks. People need to develop cyber hygiene habits and businesses and organisations must adopt appropriate risk-based cybersecurity programmes and update them regularly to reflect the evolving risk landscape.

The NIS Directive not only sets out the responsibilities of Member States to exchange information on cyber-attacks at EU level but also to put in place mature national cybersecurity strategies and frameworks on the security of network and information systems. Public administrations at EU and national level should play a further leading role in driving these efforts forward.

First, Member States should maximise the availability of cybersecurity tools for businesses and individuals. In particular, more should be done to prevent and mitigate the impacts of cybercrime on end-users. An example already exists in the work of Europol with the 'NoMoreRansom' campaign[54], built up through close cooperation between law enforcement and cybersecurity companies to help users prevent ransomware infections and decrypt data if they are victims of an attack. Such schemes should be rolled out for other types of malware, in other areas and the EU should develop a **single portal to bring together all such tools in a one-stop-shop**, offering advice to users on prevention and detection of malware and links to reporting mechanisms.

Second, Member States should accelerate the **use of more cyber-secure tools in the development of e-government** and also draw full benefit from the competence network. The adoption of secure means of identification should be promoted, building on the EU framework of electronic identification and trust services for electronic transactions in the internal market, which has been in force since 2016 and provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, individuals and public authorities.[55] In addition, public institutions, especially those providing essential services, should ensure that their staff are trained in cybersecurity-related areas.

Third, Member States should make cyber-awareness a priority **in awareness campaigns**, including those targeting schools, universities, the business community and research bodies. The Cybersecurity month that takes place every year in October under the coordination of ENISA will be scaled up to achieve a greater reach as a common communication effort at EU

---

52 https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

53 IBM "The Cybersecurity Intelligence Index" 2014, referred to in Securitymagazine.com, 19 June 2014.

54 https://www.nomoreransom.org/.

55 The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014. Also, the European Commission is providing building blocks and tools for eID and e-Signature interoperability (e.g. Trusted Lists Browsers) through the Connecting Europe Facility Programme.

and national level. Awareness-raising in relation to online **disinformation campaigns and fake news** on social media specifically aimed at undermining democratic processes and European values is equally important. While the primary responsibility remains at national level – including for European Parliament elections – the pooling of expertise and sharing of experience at the European level has proven to be of value-added in providing a focus for action.[56]

There is also a strong role for **industry** in general, but with particular attention to digital services providers and manufacturers. It needs to support users (individuals, businesses and public administrations) with tools that allow them to take responsibility for their own actions online, making clear that maintaining cyber hygiene is an indispensable part of the offer to consumers[57]. To detect and remove vulnerabilities, industry should strive to have internal processes in place that deal with investigation, triage and resolution of vulnerabilities, regardless whether the source of potential vulnerability was external or inside the company concerned.

Key actions

- Full implementation of the Directive on the Security of Network and Information Systems;
- Swift adoption by the European Parliament and the Council of the Regulation setting out a new mandate for ENISA and a European framework for certification[58];
- A joint Commission/industry initiative to define a "duty of care" principle for reducing product/software vulnerabilities and promoting "security by design";
- Swift implementation of the blueprint for cross-border major incident response;
- Launch an impact assessment to study the possibility for a Commission proposal in 2018 to set up a Network of Cybersecurity competence centres and a European Cybersecurity Research and Competence Centre, building on an immediate pilot phase;
- Support Member States in identifying areas where common cybersecurity projects could be considered for support by the European Defence Fund;
- An EU-wide one-stop-shop to help victims of cyber-attacks, providing information on latest threats and bringing together practical advice and cybersecurity tools;
- Action by Member States to mainstream cybersecurity into skills programmes, e-government and awareness campaigns;
- Action by industry to step up cybersecurity-related training for their staff and adopt a "security by design" approach for their products, services and processes.

3. CREATING EFFECTIVE EU CYBER DETERRENCE

Effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers. As long as the perpetrators of cyber-attacks – both non-state and state – have nothing to fear besides failure, they will have little incentive to stop trying. A more effective law enforcement response focusing on detection, traceability and prosecution of cyber criminals is central to building effective

[56] An example is the East StratCom Task Force set up in 2015 by Member States and the High Representative to address Russia's ongoing disinformation campaigns. The team is engaged in developing communication products and campaigns focused on explaining EU policies in the Eastern Partnership region.

[57] Some manufactures are already used with this concept as some European product legislation (such as the Machinery Directive 2006/42/EC) prescribes principles for "safety by design".

[58] COM(2017) 477.

deterrence. Added to this is the need for the EU to support its Member States in the development of dual-use cybersecurity capabilities. We will only begin to turn the tide on cyber-attacks when we increase the chances of getting caught and sanctioned for committing them. Cyber-attacks should be promptly investigated and perpetrators brought to justice, or action taken to allow an appropriate political or diplomatic response. In case of a major crisis with an important international and defence dimension, the High Representative could present options for an appropriate response to the Council.

One step towards improving the criminal law response to cyber-attacks was already taken with the adoption in 2013 of the Directive on attacks against information systems.[59] This established minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and provided for operational measures to improve cooperation amongst authorities. The Directive has led to substantive progress in criminalising cyber-attacks at a comparable level across the Member States, which facilitates the cross-border cooperation of law enforcement authorities investigating these types of offences. However, there is still scope for the Directive to reach its full potential if Member States were to implement all of its provisions fully.[60] The Commission will continue to provide support to the Member States in their implementation of the Directive and currently sees no need to propose amendments to it.

3.1 Identifying malicious actors

In order to increase our chances of bringing perpetrators to justice, we need to urgently improve our capacity to identify those responsible for cyber-attacks. Finding useful information for cybercrime investigations, mostly in the form of digital traces, is a major challenge for law enforcement authorities. We therefore need to increase our technological capability to investigate effectively including by reinforcing Europol's cybercrime unit with cyber experts. Europol has become a key actor in supporting Member States' multi-jurisdictional investigations. It should become a centre of expertise for Member States' law enforcement on online investigations and cyber forensics.

The widespread practice of placing multiple of users – sometimes thousands of them – behind one IP address makes it technically very difficult to investigate malicious online behavior. It also makes it sometimes necessary, for example for serious crime such as child sexual abuse, to investigate large number of users in order to identify one malicious actor. The EU will therefore encourage the uptake of the new protocol (IPv6) as it allows the allocation of a single user per IP address, thus bringing clear benefits to law enforcement and cybersecurity investigations. As a first step to encourage uptake, the Commission will mainstream the requirement to move to IPv6 throughout its policies, including requirements in procurement, project and research funding as well as supporting the necessary training materials. In addition, Member States should consider voluntary agreements with Internet Service Providers to drive the take up of IPv6.

[59] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

[60] COM(2017)474.

Belgium leads the world[61] in the rate of IPv6 adoption also thanks to public-private cooperation: relevant stakeholders have considered limiting the use of one IP address to a maximum of 16 users as part of a voluntary self-regulatory measure, which incentivised IPv6 transition.[62]

More generally, online accountability should be further promoted. This means promoting measures to prevent the abuse of domain names for the distribution of unsolicited messages or phishing attacks. To this end, the Commission will work to improve the functioning of and the availability and accuracy of information in the Domain Name and IP WHOIS[63] systems in line with the efforts of the Internet Corporation for Assigned Names and Numbers.[64]

3.2 Stepping up the law enforcement response

Effective **investigation** and **prosecution** of cyber-enabled crime is a key deterrent to cyber-attacks. However, today's procedural framework needs to be better adapted to the internet age.[65] The speed of cyber-attacks can overwhelm our procedures, as well as creating particular needs for swift cooperation across borders. To this end, as announced under the European Agenda on Security, the Commission will in early 2018 put forward proposals to **facilitate cross-border access to electronic evidence**. In parallel, the Commission is implementing practical measures to improve cross-border access to electronic evidence for criminal investigations, including funding for training on cross-border cooperation, the development of an electronic platform to exchange information within the EU, and the standardisation of judicial cooperation forms used between Member States.

Another obstacle to effective prosecution is the different forensic procedures for the gathering of e-evidence in cybercrime investigations across Member States. This could be alleviated by working towards establishing common forensic standards. In addition, to support traceability and attribution, forensics capabilities need to be reinforced. One step would be to further develop forensic capability in Europol, adapting the existing budgetary and human resources at Europol's European Cybercrime Centre to meet the growing need for operational support in cross-border cybercrime investigations. Another would be to mirror the technological focus set out above for encryption by looking at how its abuse by criminals creates significant challenges in the fight against serious crime, including terrorism and cybercrime. The Commission will put forward the results of current reflections on the **role of encryption in criminal investigations**[66] by October 2017.[67]

Given the borderless nature of the internet, the framework for international cooperation provided by the Council of Europe **Budapest Convention on Cybercrime**[68] offers the

---

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 A query and response protocol that is widely used for querying databases that store the registered users or assignees of an internet resource.

64 The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the internet.

65 To cite just one example, the (virtual) central command and control server of the Avalanche botnet moved physical servers and domains every five minutes.

66 Presidency of the Council, "Outcome of the Justice and Home Affairs Council meeting of 8 and 9 December 2016, No. 15391/16.

67 Eighth progress report towards an effective and genuine Security Union of 29 June 2017, COM(2017) 354 final.

68 The Convention is the first international treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography

opportunity amongst a diverse group of countries to use an optimal legal standard for the different national legislation addressing cybercrime. A possible addition of a protocol to the Convention is now being explored[69], which could also provide a useful opportunity to address the issue of cross-border access to electronic evidence in an international context. Rather than the creation of new international legal instruments for cybercrime issues, the EU calls for all countries to design appropriate national legislation and pursue cooperation within this existing international framework.

The pervasive availability of anonymisation tools makes it easier for criminals to hide. The "**darknet**"[70] has opened up new ways for criminals to access child sexual abuse materials, drugs or firearms, often with little risk of being caught.[71] It is also now a key source of the tools used in cybercrime, such as malware and hacking tools. The Commission, together with relevant stakeholders, will analyse national approaches with a view to identifying new solutions. Europol should facilitate and support investigations on the darknet, assess threats and help to determine jurisdiction and prioritise high risk cases, and the EU can play a leading role in coordinating international action.[72]

One growing area of cybercrime activity is the fraudulent use of credit card details or other electronic means of payment. Payment credentials obtained through cyber-attacks against online retailers or other legitimate businesses are then traded online and can be used by criminals to commit fraud[73]. The Commission is presenting a proposal to boost deterrence through a **Directive on the combatting of fraud and counterfeiting of non-cash means of payment.**[74] This aims to update the existing rules in this area and to strengthen the ability of law enforcement to tackle this form of crime.

The cybercrime investigative capabilities of Member States' law enforcement authorities also need to be improved, as well as the understanding of cyber-enabled crimes and investigative options by prosecutors and the judiciary. Eurojust and Europol contribute to this objective and to enhanced coordination, in close cooperation with specialised advisory groups within Europol's Cybercrime Center and with the networks of chiefs of cybercrime units and of prosecutors specialised in cybercrime. The Commission will dedicate EUR 10.5 million funding to fight cybercrime, primarily under its **Internal Security Fund-Police Programme**. Training is an important element and a number of useful materials have been developed by the European Cybercrime Training and Education Group. These should now be widely rolled out for law enforcement professionals with the support of the European Union Agency for Law Enforcement Training (CEPOL).

---

and violations of network security. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 In 2017, 55 governments had ratified or acceded to the Council of Europe Convention on Cybercrime.

69 Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, T-CY (2017)3.

70 The darknet consists of content in overlay networks which use the internet but require specific software, configurations or authorization to access. The darknet forms a small part of the deep web, the part of the Web not indexed by search engines.

71 A notable exception is the recent takedown of two of the largest criminal Dark Web markets, AlphaBay and Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Europol already plays an important role in this area. For a recent example see: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

73 The proceeds of fraud are an important source of income for organised crime and therefore an enabler for other criminal activities such as terrorism, drug trafficking and trafficking in human beings.

74 COM(2017) 489.

3.3 Public-private cooperation against cybercrime

The effectiveness of traditional law enforcement mechanisms is challenged by the features of the digital world, which consists mostly of privately-owned infrastructure and numerous different players across a variety of jurisdictions. As a result, cooperation with the private sector, including industry and civil society, is fundamental for public authorities to fight crime effectively. In this context, the financial sector is also key and cooperation should be stepped up. For example, the role of Financial Intelligence Units[75] in the context of cybercrime should be strengthened.

Some Member States have already taken key steps. In the Netherlands, financial institutions and law enforcement authorities work side-by-side to address online fraud and cybercrime in the Electronic Crime Task Force. The German Competence Centre against Cyber Crime provides the operational hub for its members to exchange information in close collaboration with the German Federal Police Office and develop measures aimed at ensuring protection against cybercrime. 16 Member States[76] have created Cybercrime Centres of Excellence to facilitate cooperation between law enforcement authorities, academia and private partners for the development and exchange of best practices, training and capacity building.
The Commission supports the establishment of public-private partnerships and cooperation mechanisms through dedicated projects such as the Online Fraud Cyber Centre and Experts Network,[77] implementing information sharing model and standard in order to analyse and mitigate electronic crimes risks and online frauds.

In the context of cybercrime, private undertakings need to be able to share information on concrete incidents with law enforcement – including personal data – in full respect of data protection rules. The EU data protection reform, which will enter into application in May 2018, provides a common set of rules setting out the conditions under which law enforcement authorities and private entities can cooperate. The European Commission will work with the European Data Protection Board and relevant stakeholders to identify best practices in this area and, where appropriate, provide guidance.

3.4 Stepping up the political response

The recently adopted **framework for a joint EU diplomatic response to malicious cyber activities**[78] (the "cyber diplomacy toolbox") sets out the measures under the Common Foreign and Security Policy, including restrictive measures which can be used to strengthen the EU's response to activities that harm its political, security and economic interests. The framework constitutes an important step in the development of signaling and reactive capacities at EU and Member State level. It will increase our capacity to attribute malicious cyber activities, with the aim of influencing the behaviour of potential aggressors, while taking into account the need to ensure proportionate responses. Attribution to a State or a non-State actor remains a sovereign political decision based on all-source intelligence. Implementation work on the

[75] Financial Intelligence Units serve as national centres for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis.

[76] Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Greece, Ireland, Lithuania, Poland, Romania, Slovenia, Spain and the United Kingdom.

[77] The EU-OF2CEN initiative aims to enable the systematic, EU-wide sharing of internet fraud related information between banks and law enforcement services for the prevention of payments to fraudsters and money mules and for the investigation and prosecution of the perpetrators involved. It is co-funded by the EU (Internal Security Fund-Police Programme).

[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

Framework is currently ongoing with Member States and would also be taken forward in close coordination with the Blueprint to respond to large scale cyber incidents[79]. Situational awareness necessary for the use of measures within the framework should be fused, analysed and shared by INTCEN,[80] working closely together with the Member States and EU institutions.

3.5 Building cybersecurity deterrence through the Member States' defence capability

Member States are already developing cyber defence capabilities. In addition, given the blurring of lines between cyber defence and cybersecurity and the dual-use nature of cyber tools and technologies, as well as of the great variations between Member States' approaches, the EU is well placed to help promote synergies between military and civilian efforts.[81]

Those Member States with more advanced cybersecurity capabilities and willing to pull them together could consider, with support from the High Representative, the Commission and the European Defence Agency, to include cyber defence within the framework of a "Permanent Structured Cooperation" (PESCO). This could be underpinned by the work set out above to encourage EU industrial capacities and strategic autonomy. The EU can also promote interoperability, including by facilitating capability development, coordination of training and education and dual-use standardisation efforts.

Full use should also be made of the joint framework to respond to hybrid threats, which often involve cyber-attacks, notably through the EU Hybrid Fusion Cell and the recently established European Centre for Countering Hybrid Threats in Helsinki, whose mission is to encourage strategic dialogue and conduct research and analysis.

The EU will bring a renewed emphasis to the 2014 EU Cyber Defence Policy Framework[82], as a tool to further integrate cybersecurity and defence into Common Security and Defence Policy (CSDP). The cyber-resilience of CSDP missions and operations themselves is essential: standardised procedures and technical capabilities will be developed that could support both deployed civilian and military missions and operations as well as their respective Planning and Conduct Capability structures and EEAS information technology service providers. In order to advance Member States' cooperation and better guide EU efforts in this field, the European Defence Agency and the EEAS, in cooperation with Commission services, will facilitate strategic level engagement between Member States' cyber defence policymakers. The EU will also support the development of European cybersecurity solutions as part of its efforts in favor of a European Defence Technological and Industrial Base. This also includes the fostering of regional clusters of excellence in cybersecurity and defence.

The Commission services, working in close cooperation the EEAS, Member States and other relevant EU bodies, will be put in place by 2018 **a cyber defence training and education platform** to address the current skills gap in cyber defence. This will complement the work of the European Defence Agency in this area, helping address the current skills gap in cybersecurity and cyber defence.

Key actions

- A Commission initiative for cross-border access to electronic evidence (early 2018);

[79] C(2017) 6100.
[80] JOIN(2016) 018 final.
[81] The EU understands cyber space as a domain of operations like land, air and sea. Cyber defence efforts also include the protection and resilience of space assets and related ground infrastructures.
[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

- Swift adoption by the European Parliament and the Council of the proposed Directive on combatting fraud and counterfeiting of non-cash means of payment;
- The introduction of requirements on IPv6 in EU procurement, research and project funding; voluntary agreements between Member States and Internet Service Providers to drive up the uptake of IPv6;
- A renewed/expanded focus in Europol on cyber forensics and monitoring the darknet;
- Implementation of the framework for a joint EU diplomatic response to malicious cyber activities;
- Enhanced financial support to national and transnational projects improving criminal justice in cyberspace.
- A cybersecurity-related education platform to address the current skills gap in cybersecurity and cyber defence in 2018.

4. STRENGHTENING INTERNATIONAL COOPERATION ON CYBERSECURITY

Guided by the EU core values and fundamental rights such as freedom of expression and the right to privacy and protection of personal data, and the promotion of the open, free and secure cyberspace, the EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber stability, as well as contributing to Europe's strategic autonomy in cyberspace.

4.1 Cybersecurity in external relations

Evidence suggests that people from around the globe identify cyber attacks from other countries as among the leading threats to national security.[83] Given the global nature of the threat, building and maintaining robust alliances and partnerships with third countries is fundamental to the prevention and deterrence of cyber-attacks – which are increasingly central to international stability and security. The EU will prioritise the establishment of a strategic framework for conflict prevention and stability in cyberspace in its bilateral, regional, multi-stakeholder and multilateral engagements.

The EU strongly promotes the position that international law, and in particular the UN Charter, applies in cyberspace. As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts[84]; it also encourages the development and implementation of regional confidence building measures, both in the Organisation for Security and Co-operation in Europe and other regions.

On a bilateral level, cyber dialogues[85] will be further developed and complemented by efforts to facilitate cooperation with third countries to reinforce principles of due diligence and state responsibility in cyberspace. The EU will prioritise international security issues in cyberspace in its international engagements, while also ensuring that cybersecurity does not become a pretext for market protection and the limitation of fundamental rights and freedoms, including the freedom of expression and access to information. A comprehensive approach to cybersecurity requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights Guidelines on online freedom.[86] In that

[83] Spring 2017 Global Attitudes Survey, Pew Research Centre.
[84] A/68/98 and A/70/174.
[85] In September 2017 EU had cyber dialogues with the US, China, Japan, the Republic of Korea and India.
[86] EU Human Rights Guidelines on Freedom of Expression Online and Offline.

regard the EU emphasises the importance of all stakeholders' involvement in the governance of the internet.

The Commission has also put forward a proposal[87] to modernise EU export controls, including the introduction of controls on the export on critical cyber-surveillance technologies that could cause violations of human rights or be misused against the EU's own security and will step up dialogues with third countries to promote global convergence and responsible behaviour in this area.

4.2 Cybersecurity capacity building

Global cyber stability relies on the local and national ability of all countries to prevent and react to cyber incidents and investigate and prosecute cybercrime cases. Supporting efforts to build national resilience in third countries will increase the level of cybersecurity globally, with positive consequences for the EU. Countering fast-evolving cyber threats would suggest a need for training, policy and legislation development efforts, as well as efficiently functioning Computer Emergency Response Teams and cybercrime units in all countries worldwide.

Since 2013, the EU has been leading on international cybersecurity capacity building and systematically linking these efforts with its development cooperation. The EU will continue to promote a rights-based capacity building model, in line with the Digital4Development approach.[88] The priorities for capacity-building will be the EU's neighborhood and developing countries experiencing fast growing connectivity and rapid development of threats. EU efforts will be complementary to the EU's development agenda in light of the 2030 Agenda for Sustainable Development and overall efforts for institutional capacity building.

In order to improve the EU's ability to mobilise its collective expertise to support this capacity-building, a dedicated EU Cyber Capacity Building Network should be set up, bringing together the EEAS, Member States' cyber authorities, EU agencies, Commission services, academia and civil society. EU Cyber Capacity Building guidelines will be developed to help offer better political guidance and prioritisation of EU efforts in assisting the third countries.

The EU will also work together with other donors in this field to avoid duplication of effort and facilitate more targeted capacity building in different regions.

4.3 EU-NATO cooperation

Building on the substantial progress already achieved, the EU will deepen EU and NATO cooperation on cybersecurity, hybrid threats and defence, as foreseen in the Joint Declaration of 8 July 2016.[89] Priorities include fostering interoperability through coherent cyber defence requirements and standards, strengthening cooperation on training and exercises, harmonising training requirements.

The EU and NATO will also foster cyber defence research and innovation cooperation, and build on the current technical arrangement on cybersecurity information sharing between their respective cybersecurity bodies[90]. Recent joint efforts on countering hybrid threats, in

---

87 COM(2016) 616.
88 SWD(2017) 157.
89 http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
90 CERT-EU and NATO Computer Incident Response Capability (NCIRC).

particular the cooperation between the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch should be further leveraged to strengthen resilience and response to cyber crises. Further cooperation between the EU and NATO will be fostered through cyber defence exercises, with the involvement of the EEAS and other EU entities and relevant NATO counterparts, including the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. For the first time, NATO and the EU will carry out parallel and coordinated exercises in response to a hybrid scenario with NATO taking the lead in 2017 and the EU reciprocating in a similar fashion in 2018. The next report on EU-NATO cooperation, to be submitted to the respective Councils in December 2017, will offer an opportunity to consider possibilities to further expand cooperation, notably by ensuring common, secure and robust means of communication between all relevant institutions and bodies involved, including ENISA.

Key actions

- Advance the strategic framework for conflict prevention and stability in cyberspace;
- Develop a new Capacity Building Network to support third countries' ability to address cyber threats and EU Cybersecurity Capacity Building Guidelines to better prioritise EU efforts;
- Further cooperation between EU and NATO, including participation in parallel and coordinated exercises and enhanced interoperability of cybersecurity standards.

5. CONCLUSION

EU cyber preparedness is central to both the Digital Single Market and our Security and Defence Union. Enhancing European cybersecurity and addressing threats to both civilian and military targets is a must.

The upcoming Digital Summit organised by the Estonian Presidency on 29 September 2017 provides an opportunity to show a common determination to put cybersecurity at the heart of the EU as a digital society. As part of this common commitment, the Commission calls on the Member States to pledge how they intend to act in areas where they have the primary responsibility. This should include strengthening cybersecurity by:

- Ensuring full and effective implementation of the NIS Directive by 9 May 2018, as well as the resources necessary for public authorities responsible for cybersecurity to effectively carry out their tasks;
- Applying the same rules to public administrations, given the role they play in society and the economy as a whole;
- Providing cybersecurity-related training in public administration;
- Prioritising cyber-awareness in information campaigns and including cybersecurity as part of academic and vocational training curricula;
- Using initiatives on the "Permanent Structured Cooperation" (PESCO) and the European Defence Fund to support the development of cyber defence projects.

This Joint Communication has set out the scale of the challenge, and the range of measures that the EU can take. We need a Europe that is resilient, which can protect its people effectively by anticipating possible cybersecurity incidents, by building strong protection in its structures and behaviour, by recovering quickly from any cyber-attacks, and by deterring those responsible. This Communication puts forward targeted measures that will further strengthen the EU's cybersecurity structures and capabilities in a coordinated manner, with the full cooperation of the Member States and the different EU structures concerned and respecting their competencies and responsibilities. Its implementation will provide a clear

demonstration that the EU and the Member States will work together to put in place a standard of cybersecurity equal to the ever-growing challenges faced by Europe today.