

Handbook on Cybersecurity

The Common Security and Defence Policy
of the European Union



Volume V
2nd edition

Handbook on Cybersecurity

**The Common Security and Defence Policy
of the European Union**

edited by
Jochen Rehrl

with forewords by

Federica Mogherini
High Representative of the Union for Foreign Affairs and Security Policy and
Vice-President of the Commission
and
Mario Kunasek
Federal Minister for Defence of the Republic of Austria



This document has been produced with the financial assistance of the European Union.

Imprint

Publication of the Federal Ministry of Defence of the Republic of Austria

Editor: Jochen Rehrl
Idea and concept: Jochen Rehrl

Published by:
Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria
Rossauer Lände 1, 1090 Vienna/Austria

Photo credits for the front page: HBF/Daniel Trippolt, NATO CCD COE/Kristi Kamenik, Austrian Armed Forces/Carina Karlovits, Austrian Armed Forces/Maximilian Fischer, Austrian Armed Forces/Maniecka, European Security and Defence College/Michael Chia, European Commission, ENISA, Pixabay (CC0 Creative Commons)

Layout: Armed Forces Printing Centre

Printed and bound by: Armed Forces Printing Centre, Vienna/Austria, 2019 (18-01988)

© Federal Ministry of Defence of the Republic of Austria and Jochen Rehrl

ISBN: 978-3-902275-48-6



AT/028/048



Printed according to the Austrian
Ecolabel for printed matter
UW-Nr. 943

Disclaimer:

Any views or opinions presented in this handbook are solely those of the authors
and do not necessarily represent those of the European Union
or the Austrian Federal Ministry of Defence.

Contents

Forewords.....	6
Preface of the editor.....	10
List of abbreviations.....	13

1 Strategies, policies and concepts

1.1 Two generations of EU cybersecurity strategies.....	18
1.2 International law of cyber defence.....	27
1.3 Military concept for cyber defence in CSDP.....	35
1.4 Integrating cybersecurity in civilian CSDP missions.....	43
1.5 Cyber resilience as a key challenge for the EU and its Member States.....	52
1.6 Data protection and digital security in the cyber age.....	60

2 Stakeholders

2.1 European Commission: the role of the European Commission in cyberspace.....	74
2.2 European Defence Agency: cyber defence capability development.....	92
2.3 EUROPOL: the role of Europol in cyberspace.....	100
2.4 European Centre of Excellence for Countering Hybrid Threats: cyber in the realm of hybrid threats.....	112
2.5 The European Security and Defence College: Cyber Education, Training, Evaluation and Exercise platform.....	118
2.6 ENISA – the European Union Agency for Network and Information Security.....	125
2.7 CERT-EU: European CERT cooperation.....	136

2.8 Other cyber stakeholders.....	151
2.8.1 Security Policy Directorate within the EEAS (SECOPOL).....	151
2.8.2 EU Institute for Security Studies (EUISS).....	152
2.8.3 European Cybercrime Training and Education Group (ECTEG).....	153
2.8.4 The European Union Agency for Law Enforcement Training (CEPOL)....	154

3 Cyber challenges

3.1 Emerging cybersecurity challenges.....	156
3.2 Cyber reservists: a flexible solution to address peaks in malicious cyber activities.....	168
3.3 Gender and cyberspace.....	175
3.4 The EU as a partner in cyber diplomacy and defence.....	182
3.5 The human layer of cybersecurity – the art of social engineering.....	192
3.6 Social media: manipulating people.....	203

Annexes

Joint Communication: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.....	214
Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.....	234
List of authors.....	255
Previously published handbooks.....	261

Foreword



Photo: Jennifer Jacquemart / EC - Audiovisual Service

Federica Mogherini

High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission

The internet has been a global force for human development since the early days of its inception. Yet, in recent times, we are all increasingly aware of the threats circulating on the web. I am convinced that cyberspace can be at the same time safe and open, and that the opportunities of global connectivity outnumber its dangers by far. If we want to preserve and expand these opportunities, we must also invest in the security and the governance of our cyberspace.

Getting prepared is essential: cyber-attacks have already caused huge economic loss, and directly affected thousands of Europeans' daily lives. This is why we have recently updated the European Union's Cybersecurity Strategy. Our main focus is what we call 'resilience'. We want to prevent cyber-attacks, to make sure that we know how to react, and to minimise their impact. To do so, we are investing in better capabilities, more research, more training and exercises on how to respond to an attack.

We all know that this is essentially a national competence. But we also know that cybersecurity transcends borders by definition. Cyber-attacks easily spread from one country to the next. European cooperation is essential, for at least two good reasons. First of all, cooperation is the best way to ensure higher cybersecurity standards all across our Union: in cyberspace, we are as strong as the weakest link of the chain. Secondly, joint investment and research among European Member States can help us develop more advanced capabilities, in a field where technological progress is constant and incredibly fast.

Over the last year, we have set up a number of tools to help Member States invest together, so that the impact of their investments can be maximised. The European Security and Defence College is currently working on a 'Cyber education, training, evaluation and exercise platform', in close cooperation with the EU institutions, Member States and NATO. And there is a strong focus on cybersecurity in the first set of cooperative projects launched in the framework of the new permanent structured cooperation we have established on defence.

Cybersecurity is also central to our cooperation with NATO: we share threat alerts and briefings, we work together on training, and we coordinate our exercises on hybrid threats.

The present handbook gives an overview of the state of affairs in European cybersecurity. It was edited and published by the Ministry of Defence of Austria during the Austrian Presidency of the Council of the European Union. It is the fifth handbook in the series of CSDP publications – an important step forward towards the creation of a common European security culture.

In a global context where security is never just a matter of traditional defence and where the real world merges with the cyberworld, cybersecurity is a collective responsibility. It calls on each and every one of us, citizens of Europe, to invest in the most powerful tool we have to exercise our sovereignty, advance our interests and stand by our values: our European Union.

Foreword

Photo: Harald Minich / Federal Ministry of Defence



Mario Kunasek

Federal Minister for Defence
of the Republic of Austria

When the digital era began, the positive prospects were overwhelming: new possibilities for communication, more opportunities for businesses, easier access for everyone to everything without borders. But very soon, challenges, risks and threats also developed in cyberspace. Viruses, worms and Trojans, to name but a few, were targeting private as well as public networks, companies and individuals. Over time, cyberspace has become more sophisticated, more imaginative and international.

The same actors are present in cyberspace as in the real world: the military, criminals, individuals, terrorists, diplomats, hackers, the police and so on. Several areas of expertise have developed over time: cyber defence, cyber diplomacy, cyberterrorism, cybercrime. What is common to cyber threats and risks is their borderlessness and the global spread of users. Whereas early cyber threats focused on hacking computers (criminal intent), present-day cyber-attacks ranging from cyber-war to manipulating behaviour (political intent) have completed the picture. In other words, there is a wide range of 'cyber-enabled' security challenges which are rooted in or accelerated by technology.

Hitherto at least, human beings are involved in most activities in cyberspace. With artificial intelligence, this picture may well change – which does not necessarily mean that the risks and threats will diminish.

The basic building blocks of the response to system threats are well known: reducing the likelihood of attacks by making them harder to carry out, increasing public awareness, and increasing the chances of getting caught, while at the same time reducing the impact of attacks through effective networks, procedures and protocols and better-designed systems and software.

To achieve all these goals, training and education in the cyber domain is essential. Austria therefore very much welcomes the establishment of the new Cyber Education, Training, Evaluation and Exercise (ETEE) platform within the European Security and Defence College, which will provide basic to advanced-level training for officials from EU Member States and partner countries. The Cyber ETEE platform will not be able to score quick wins, but in the medium to longer term it will provide our Member States with the knowledgeable personnel needed to tackle the threats encountered on the internet.

In the academic year 2017/18 Austria remained the main supporter of the ESDC, and I am proud therefore to present the fifth handbook in this publication series, which is provided by the Austrian Ministry of Defence for the students of the college. The handbook series is an exemplary means of transferring knowledge, sharing best practices and stimulating discussions on CSDP-related subjects, now even in cyberspace.

I wish the readers of this publication all the best in their professional work, good luck in future deployments and a pleasant experience reading the articles by various European experts on cyber- and security-related issues.

Preface of the editor



Jochen Rehrl

National Expert at the
European Security and
Defence College

The development of the internet can be seen as a milestone in the new digital era. We live in an age of ever greater interconnectivity, and are ever more dependent on online services. Without the internet many critical services, including public administration, would not function. Our societies rely on the confidentiality, integrity and availability of our systems. There are many social and economic benefits to this interconnectivity, but it also brings new risks – in new forms but also crucially on a new scale.

To protect our societies, we must focus on cybersecurity. But cybersecurity lies at the interface between internal/external, public/private and civil/military, which makes it complex and challenging. At the same time, the number of cyber-professionals is not growing at the same speed as the digital market.

Europe is facing a cybersecurity skills gap, with an expected shortfall of 350 000 people by 2022. Addressing this skills gap is central to ensuring effective resilience. So cyber must be mainstreamed and prioritised in education and training. The European Security and Defence College (ESDC) is ready to make its contribution. The newly established Cyber Education, Training, Evaluation and Exercise (ETEE) platform within the ESDC family will facilitate this joint endeavour.

Recent years have seen one eye-opening event after another: in Estonia, an orchestrated attack on the whole country in 2007; Stuxnet, the first big cyber-attack in the digital battlefield, which targeted Iran and was uncovered in 2010; ransomware (e.g. Cryptolocker, WannaCry, NotPetya), which has affected private and public sector IT systems around the world; the Sony hack, a cyber-attack on commercial infrastructure in 2014; the Snowden affair, which highlighted the need to strengthen privacy in cyberspace; the Cambridge Analytica scandal, which brought the vulnerability of our democracies to our attention, to name but a few. We have learned that cyber-attacks are becoming more strategic and can endanger our critical infrastructure and – perhaps to an even greater extent – our democratic institutions.

The cross-border nature of these threats and risks means that cooperation has never been more important; the private and public sectors and civilian and military sectors

need to work together, swiftly and efficiently. The European Union has a clear role to play in leading efforts both at home and internationally. There are essentially two types of threat which have to be addressed: those based on systems ('physical' cyber threats, i.e. the hacking of electronic tools, systems and databases) and those based on behaviours (e.g. hacks and leaks designed to change public opinion, use of fake news, misuse of targeted messaging). The latter – in my view – pose a greater challenge to our societies, to our democratic values and therefore to our way of life.

Democracy is based on citizens' participation in the political process. In the future, electoral campaigns will increasingly be fought online in a way that would have been hard to imagine even a few years ago. Never has it been easier for political parties to get their messages across using the internet and social media, tools which have made it possible not only to reach large numbers of people but also, increasingly, to micro-target individuals with tailor-made messages.

The public is becoming more aware of the challenge posed by cyber-attacks and cyber-interference, which have become more frequent and more damaging, are too easy to perpetrate and at the same time too hard to trace and attribute. But is the public also ready to draw the necessary conclusions? Some 95 % of successful attacks are enabled by some type of human error. Cybersecurity begins at home, with simple cyber-hygiene practices such as choosing safe passwords, checking attachments and backing up. Not rocket science, but these things can make a real difference.

This handbook gives a snapshot of the state of affairs at European level (chapters 1 and 2), but also gives some food for thought on topics which are relevant in our daily lives (chapter 3). When putting it together, I was again able to rely on experts from all over Europe with a broad range of professional backgrounds, who are willing and able to share their knowledge and experience. They are the ones to be thanked for this publication. Saying 'thank you' is just a small sign of appreciation for their tremendous contribution, not only in the transfer of knowledge but also in facilitating the establishment of a common European security culture.

In particular, I would like to thank:

- Lt Gen. Franz Leitgeb, Head of the Austrian Military Representation in Brussels, and his team;
- Maj. Gen. Johann Frank, Defence Policy Director of the Austrian Ministry of Defence and Sports, and his Directorate for Security Policy;
- Mr Oliver Rentschler, Ms Federica Mogherini's Deputy Head of Cabinet;
- Mr Gabor Iklody, Director of the Crisis Management and Planning Directorate;
- the English editing service of the General Secretariat of the Council;
- Mr Roman Bartholomay, head of the Austrian print shop, and his team, in particular Mr Axel Scala and Ms Eva Kutika;
- Mr Dirk Dubois, Head of the ESDC, and my colleagues in the ESDC Secretariat, in particular Ms Alexandra Katsantoni.

Lastly, I am more than grateful for the support of my family, my wife Bernadeta and my children Julia and Maximilian. I would like to thank them for their patience and understanding, in particular during the 2018 summer holidays and the following weekends because the vast majority of the work has been done outside office hours.

I hope that this new publication in the handbook series of the Austrian Ministry of Defence will meet your expectations and will again serve as a reference document for present and future cyber-experts on the common security and defence policy of the European Union.

List of abbreviations

A		C		D		E	
AHWG	Ad-hoc Working Group	CPCC	Civilian Planning and Conduct Capability				
AP	Analysis project	CS	Cybersecurity				
APT	Advanced persistent threats	CSA	Child sexual abuse				
Art.	Article	CSDP	Common Security and Defence Policy				
AT	Austria	CSIRT	Computer Security Incident Response Team				
		CSRA	Cyber Defence Strategic Research Agenda				
		CV	Curriculum vitae				
B		C		D		E	
BE	Belgium	CyCon	Cyber conference				
BG	Bulgaria	CySAP	Cyber Situation Awareness Package				
BMLV	Bundesministerium für Landesverteidigung (Austrian Federal Ministry of Defence)	CZ	Czech Republic				
CA	Cyber attack	DCEC2	Deployable Cyber Evidence Collection and Evaluation Capacity				
CAGR	Compound annual growth rate	DDoS	Distributed denial of service				
CCDCOE	Cooperative Cyber Defence Centre of Excellence	DE	Germany				
CD	Cyber defence	DEA	Drug Enforcement Agency (US)				
CD	Council Decision	DESI	Digital Economy and Society Index				
CD TEXP	Cyber Defence Training and Exercise Coordination Platform	DG	Directorate-General				
CDC	Cyber Defence Concept	DG CNECT	Directorate-General for Communications Networks, Content and Technology				
CDO	Cyber Defence Organisation	DG DIGIT	Directorate-General for Informatics				
CDP	Capability development plan	DG GROW	Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs				
CDPF	Cyber Defence Policy Framework	DG HOME	Directorate-General for Migration, Home Affairs and Citizenship				
CEF	Connecting Europe Facility	DK	Denmark				
CEO	Chief Executive Officer	DNS	Domain name system				
CEPOL	European Union Agency for Law Enforcement Training	Doc	Document				
CERT	Computer Emergency Response Team	DSG	Deputy Secretary-General				
CFSP	Common Foreign and Security Policy	DSG CSDPCR	Deputy Secretary-General for CSDP and Crisis Response				
CI	Critical infrastructure						
CIA	Confidentiality, integrity, availability						
CIS	Communication and information system						
CMO	Crisis management operation	EAB	Executive Academic Board				
CMPD	Crisis Management and Planning Directorate	EC	European Commission				
CoE	Centre of Excellence	EC3	European Cybercrime Centre				
COM	European Commission	ECSC	European Cybersecurity Challenge				

ECSM	European Cybersecurity Month	FIRST	Forum for Incident Response and
ECTC	European Counter-Terrorism Centre		Security Teams
ECTEG	European Cybercrime Training and Education Group	FR	French
EDA	European Defence Agency	FR	France
EDPS	European Data Protection Supervisor		G
EE	Estonia	G7	Group of Seven
EEAS	European External Action Service	GAAD	Global Airline Action Days
EFTA	European Free Trade Association	GDPR	General Data Protection Regulation
EGC	European Government CERTs group	GOV	Government
EGS	EU Global Strategy	GPS	Global positioning system
eID	Electronic identification		H
eIDAS	Electronic Identification, Authentication and Trust Services	HoM	Head of Mission
EL	Greece	HQ	Headquarters
EMMA	European Money Mule Action	HR	High Representative of the Union for Foreign Affairs and Security Policy
EMSC	European Migrant Smuggling Centre		
EN	English	HR	Human rights
ENISA	European Union Agency for Network and Information Security	HR/VP	Croatia
EP	European Parliament	HU	High Representative/Vice-President
EPRS	European Parliamentary Research Service		
ES	Spain		I
ESDC	European Security and Defence College	ICDS	International Centre for Defence and Security
ESOCC	European Serious Organised Crime Centre		
ESS	European Security Strategy	ICT	Information and communications technology
ETEE	Education, training, evaluation and exercise		
EU	European Union	IE	Ireland
EU CA	EU Cybersecurity Agency	INTCEN	Intelligence and Situation Centre
EU IRU	EU Internet Referral Unit	INTERPOL	International Criminal Police Organisation
EU ISS	EU Institute for Security Studies	IOCTA	Internet Organised Crime Threat
EU MS	EU Member States		Assessment
EUIPO	EU Intellectual Property Office	IOS	Operation In-Our-Sites
EUMC	EU Military Committee	IoT	Internet of Things
EUMS	EU Military Staff	IP	Internet Protocol
EUR	Euro (currency)	IPC3	Intellectual Property Crime Coordinated Coalition
EUROPOL	European Police Office		
		IPR	Intellectual property rights
		IPTV	Internet protocol television
F			
FBI	Federal Bureau of Investigation (US)	IT	Italy
FHQ	Force headquarters		
FI	Finland		

J		P	
J-CAT	Joint Cybercrime Action Taskforce	P	Page
JHA	Justice and Home Affairs	PESCO	Permanent structured cooperation
JOIN	Joint Communication	PL	Poland
L		PSD2	
LAW	Lethal autonomous weapons system	PT	Portugal
LT	Lithuania		
LU	Luxembourg		
LV	Latvia	R&T	Research and technology
M		Rev	Revision
M2M	Machine-to-machine	RO	Romania
MFA	Ministry of Foreign Affairs		
MHQ	Mission headquarters	SB	Steering Board
MILEX	Military exercise	SC	Steering Committee
MIT	Massachusetts Institute of Technology	SCO	Shanghai Cooperation Organisation
MOD	Ministry of Defence	SE	Sweden
MOI	Ministry of the Interior	SECD	Sino-European Cyber Dialogue
MOJ	Ministry of Justice	SECPOL	Security Policy and Conflict Prevention
MoU	Memorandum of understanding		Directorat
MPCC	Military Planning and Conduct Capability	SF	Standard form
MS	Member State(s)	SG	Secretary-General
MT	Malta	SGBV	Sexual and gender-based violence
N		SI	Slovenia
NATO	North Atlantic Treaty Organisation	SK	Slovakia
NCIRC	NATO Computer Incident Response	SLA	Service level agreement
	Capability	SOC	System and organisation controls
NIS	Network and information security	SOC	Security operation centre
NL	The Netherlands	SOCTA	Serious and Organised Crime Threat
No	Number		Assessment
NOC	Network operations centre	SOP	Standard operating procedure
O		T	
OC(G)	Organised crime (group)	TA	Technical arrangement
OES	Operator of essential services	TE-SAT	Terrorism Situation and Trend Report
OHQ	Operation headquarters	TEU	Treaty on European Union
OPLAN	Operational plan	TF	Task force
OSCE	Organisation for Security and	TFEU	Treaty on the Functioning of the
	Cooperation in Europe	TPP	European Union
			Tactics, techniques and procedures

U

UK	United Kingdom
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UN(O)	United Nations (Organisation)
UNIDIR	UN Institute for Disarmament Research
US(A)	United States (of America)
USD	US Dollar

V

VAWG	Violence against women and girls
VIDTF	Victim Identification Taskforce
Vol	Volume
VP	Vice-President of the European Commission

W

WEF	World Economic Forum
-----	----------------------

1

Strategies, policies and concepts

1.1 Two generations of EU cybersecurity strategies

by Heli Tiirmaa-Klaar

The EU began work on its first comprehensive cybersecurity strategy in 2012-2013. The development of the strategy took place in the wider context of the 'cyber awakening' in 2010-2013, when many advanced economies realised the gravity of cybersecurity challenges for their national security and economies – and the EU was no exception.

Compared to NATO, which produced its first cyber-defence policy as early as 2008 and adopted its second policy in 2011, the EU strategy came into being relatively late, in 2013. Whereas NATO's cyber-policy process was mostly limited to the protection of its own networks, the EU strategy process in 2012-2013 included all major EU competence areas and could be viewed as an authoritative whole-of-government cyber policy.

2013 Cybersecurity Strategy

Prior to the 2012-2013 strategy process, the EU had already produced several Council conclusions and a number of other policy documents on sectoral topics, the results of which were most notable in the Justice and Home Affairs policies on harmonising the fight against cybercrime. The EU Cybersecurity Strategy 2013, which took the form of a Joint Communication entitled '**Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace**', was one of the first joint efforts by the European Commission (EC) and the High Representative of the Union for Foreign Affairs and Security Policy (HR) in the post-Lisbon era, showcasing the EU's ability to work in a truly interinstitutional manner.

The strategy managed to bring together very different cyber policy areas under a single umbrella document and articulate the direction of EU policies on cybersecurity to the wider public. As a tangible added-value element, the first strategy was accompanied by the Commission legislative initiative that resulted in the Directive on Security of Network and Information Systems, which set the minimum requirements for Member States' cyber preparedness and included compulsory cyber protection of most critical services and infrastructures.

In addition, the strategy articulated the EU's international cyber-policy and cyber-defence objectives for the first time. It also established clear guidance on how to further address cybercrime. The five chapters of the document were drafted by various Commission departments and the EEAS according to their respective areas of competence – DG CNECT in the internal market, DG HOME in justice and home affairs and the EEAS in Common Foreign and Security Policy.

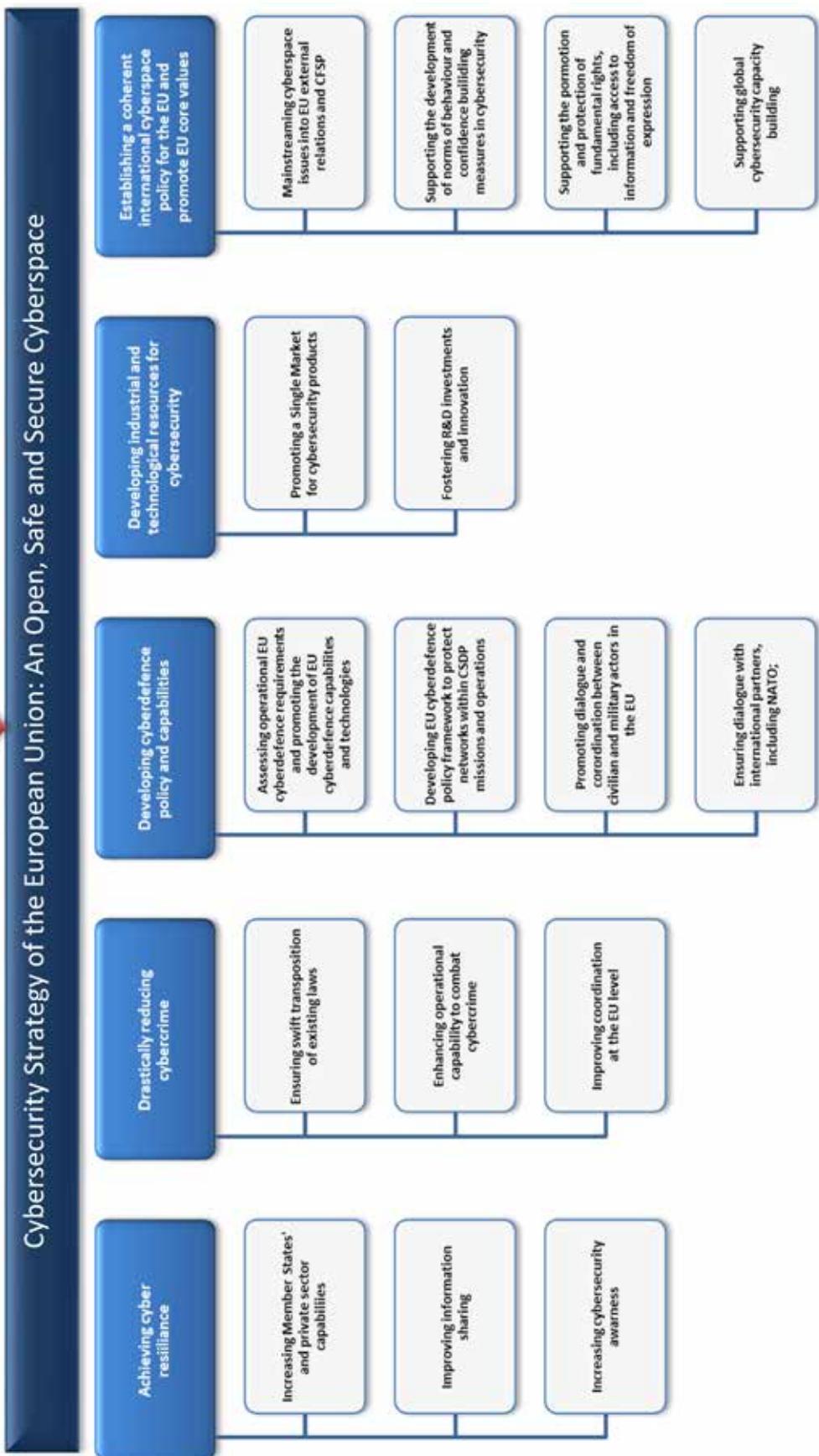


The cybersecurity strategy of 2013 was accompanied by the Commission legislative initiative that resulted in the Network and Information Security (NIS) Directive.

Photo: European Commission

Cybersecurity incidents of different origin (criminal, politically motivated, state-sponsored) on the rise; risk of insufficient protection against NIS threats and disruptions across the EU due to loopholes in the NIS regulatory framework, uneven capabilities of Member States and other actors to deal with cyber threats and lack of information sharing culture; lack of sufficient cybersecurity industrial and technological resources at the EU level; need to influence international cyberspace policy to ensure respecting EU core values;

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace



The strategic objectives of the 2013 Cybersecurity Strategy.

Graphic: European Commission

Roles and responsibilities

Responsibility for implementing the first EU Cybersecurity Strategy was divided between the departments involved. DG CNECT was responsible for activities related to new cyber legislation, industrial policies, research and development and awareness-raising. DG HOME was in charge of updating EU policies on addressing cybercrime, and facilitating cooperation between the national law enforcement authorities' cybercrime units. As a major addition to the EU cyber landscape, the European Cybercrime Centre, or 'EC3', was established within Europol shortly after the adoption of the first strategy in 2013. This allowed for better police coordination on cyber issues and strengthened operational ties between the relevant national entities, as well as enhancing the EU's ability to conduct large-scale operations to fight cybercrime.

Cyber-Defence Policy Framework

The EEAS had responsibility for cyber defence and international cyber-policy-related objectives. As a notable achievement, the EU Cyber-Defence Policy Framework was adopted in 2014, with five objectives:

1. supporting the development of Member States' cyber-defence capabilities related to CSDP;
2. enhancing the protection of CSDP communication networks used by EU entities;
3. promoting civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies and the private sector;
4. improving training, education and exercise opportunities;
5. enhancing cooperation with relevant international partners, especially NATO.

EU-NATO cooperation

The EU-NATO Joint Declaration from summer 2016 set specific objectives for furthering cyber-defence cooperation.

EU-NATO Joint Declaration: implementation

6 December 2016
Council of the EU and North Atlantic Council endorse

40+ proposals in 7 areas

hybrid threats operational cooperation, including maritime issues cyber security defence capabilities

industry and research exercises capacity building

Graphic: European Union



Council of the European Union
General Secretariat

© European Union, 2016.
Reproduction is authorised, provided the source is acknowledged.

In the area of EU-NATO cooperation, annual high-level consultations and staff-to-staff meetings have been taking place since 2012. In February 2016, the EU and NATO signed a technical arrangement (TA) between CERT-EU, the Computer Emergency Response Team of the EU, and NCIRC, NATO's Computer Incident Response Capability. The TA aims at facilitating technical information sharing to improve cyber-incident prevention, detection and response in both organisations. The EU-NATO Joint Declaration from summer 2016 set specific objectives for furthering cyber-defence cooperation: fostering interoperability of cyber defence in missions and operations; strengthening cooperation on training and exercises; promoting cooperation on cyber-defence research and technology innovation; and mainstreaming cyber aspects into crisis management.

The EU's international cyber policy

The first strategy also established the EU's international cyber policy which, in addition to protecting a free and open internet, had the objectives of promoting existing international law, norms of responsible state behaviour and confidence-building measures in cyberspace and advancing cooperation with the EU's strategic partners. Six cyber dialogues were launched with the US, China, Japan, South Korea, India and Brazil. Topics covered during the dialogues included, *inter alia*, international security in cyberspace, cyber resilience, addressing cybercrime, internet governance and cybersecurity standards.

An important landmark in helping to guide the EU's collective efforts in relation to global cyber policy and offer more detailed objectives in foreign policy issues was the adoption of the Council conclusions on cyber diplomacy in 2015.

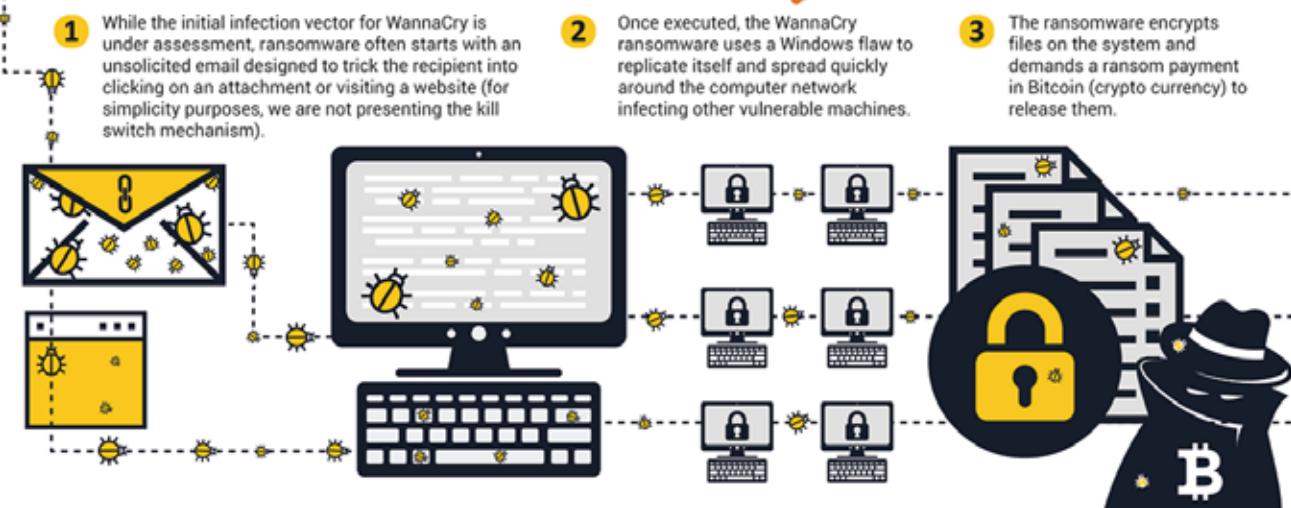
The EU's cybersecurity capacity-building programmes

Lastly, possibly the most remarkable achievement at global level was the successful launch of the EU's cybersecurity capacity-building programmes. Since 2013, the EU has invested around EUR 80 million in cybersecurity capacity building, contributing significantly to the strengthening of global cybersecurity. The EU has developed an efficient model and has been allocating an increasing amount of funds to addressing cybercrime globally, together with the Council of Europe. In addition to promoting the Budapest Convention on Cybercrime and training law enforcement officials, new programmes have started to strengthen technical and organisational cyber-incident response capacities in developing countries. The capacity-building efforts have also played a key role in building strong partnerships with third countries and have helped to promote the notion of open, free and secure cyberspace.

Upgrading the EU Cybersecurity Strategy in 2017

Although not all the objectives set by the first strategy had been attained by 2017, the global cyber-threat environment had evolved in 2016-2017. Disruptive cyber operations against critical infrastructures, democratic institutions and the 'Internet of Things' (IoT), massive botnet attacks and global ransomware cases like 'WannaCry' and 'NotPetya' raised awareness around cyber risks. It became quite clear that the EU needed to adapt to the new reality and take a more pro-active approach to cyber threats.

HOW DOES THE WANNACRY RANSOMWARE WORK?



Thanks to the leadership of Commission Vice-President Andrus Ansip, a reviewed EU Cybersecurity Strategy was adopted in September 2017, together with a package of new proposals. The updated strategy, also known as the HR and EC's Joint Communication on **'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'**, focuses on the creation of new technological capabilities via research, innovation and skills development and on the improvement of cooperation at EU level.

An ambitious path ahead

Substantive support from the Commission to Member States was provided for by the establishment of the EU Network of Cybersecurity Research and Competence Centres, with dual-use technology development aspects included. Ambitious plans for upgrading ENISA, the European Network and Information Security Agency, were announced, and a proposal was made to set up a certification framework for assessing cybersecurity of ICT products. The regulative steps of certification and IoT security are not only important standard-setting activities for both civilian and defence-related cyber technologies; they could also potentially have an impact on the overall European cybersecurity environment. In the field of defence, the cyber-defence training and education platform was identified as a key priority in addressing the Member States' current skills gap in the area of cyber defence.

In June 2017, under the work stream of deterrence, Foreign Affairs Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities (the 'Cyber Diplomacy Toolbox') were adopted, together with implementation guidelines that aimed to facilitate the decision-making process, including the process for collectively assessing the information, and implement a coherent EU approach to using CFSP measures to respond to malicious cyber activities. The EEAS coordinates and prepares regular exercises on toolbox implementation. In April 2018, the Foreign Affairs Council adopted Council conclusions condemning recent malicious activities, including WannaCry and NotPetya. The conclusions stressed the need for the application of international law in cyberspace and for adherence to norms of responsible state behaviour in order to maintain international peace and stability in cyberspace.

Building national cyber resilience

The strategy review also provided for an increase in EU support for building national cyber resilience in third countries. In order to better mobilise the EU's collective expertise, a capacity-building network should be set up, comprising the Member States' cyber authorities, the EEAS, COM, EU agencies, academia and civil society. For better political guidance and prioritisation of EU efforts in assisting third countries, Council conclusions on EU cyber capacity-building guidelines were adopted in 2018 as a follow-up document to the strategy. The universalisation of the Budapest Convention on Cybercrime would be a key outcome of these efforts.

Conflict prevention and stability in cyberspace

At international level, the EU will continue to promote a strategic framework for conflict prevention and stability in cyberspace. It will focus on the strict application in cyberspace of international law, in particular the UN Charter and international humanitarian law, the full implementation of universal non-binding cyber norms, rules and principles of responsible state behaviour, and the development and implementation of regional confidence-building measures. The OSCE is the most advanced regional organisation in this regard, with two sets of practical transparency and cooperation measures under implementation.

The cornerstone of EU-NATO cooperation remains the technical arrangement on cybersecurity information sharing between NCIRC and CERT-EU.



EU-NATO cyber-defence cooperation remains a key priority as regards ensuring civil-military synergies and complementarity of efforts. Priorities include fostering interoperability in terms of cyber-defence requirements and standards, strengthening cooperation on training and exercises, and harmonising training requirements. Both organisations will also foster cyber-defence R&T innovation cooperation and liaise on crisis-management-related cyber issues. The cornerstone of EU-NATO cooperation remains the technical arrangement on cybersecurity information sharing between NCIRC and CERT-EU.



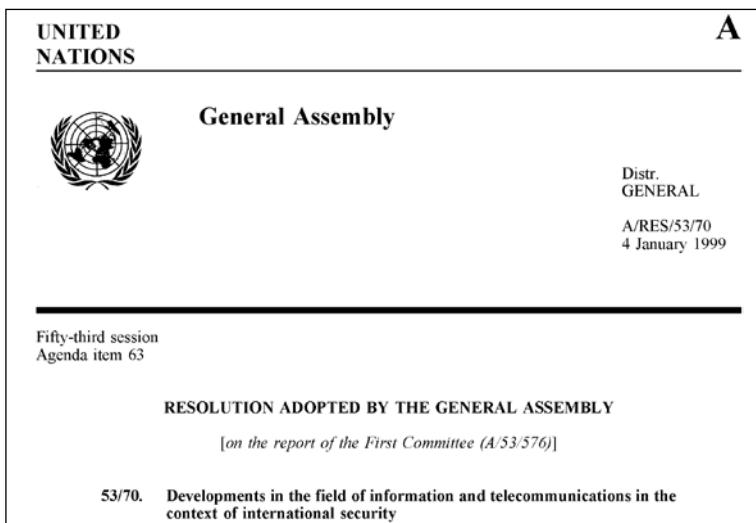
1.2 International law of cyber defence

by Liis Vihul

The application of international law to cyberspace is amongst the most highly controversial and politicised issues in international cybersecurity. This was most clearly illustrated in 2017, when 25 governmental experts forming the ‘United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (UN GGE) were unable to agree on the text of their joint report due to a disagreement over whether certain international law concepts apply in the cyber context. In the absence of a common understanding of the legal rules that bind the actions of states in this domain, disputes regarding the lawfulness of states’ cyber operations, or responses thereto, are likely to continue.

Evolution of cybersecurity as a national security issue

Cybersecurity emerged as an international security issue in 1998, when the Russian Federation introduced a draft resolution entitled ‘Developments in the field of information and telecommunications in the context of international security’ at the United Nations General Assembly’s First Committee.¹ Upon the recommendation of the First Committee, the General Assembly adopted the resolution in 1999.²



- 1 Russian Federation, revised draft resolution ‘Developments in the field of information and telecommunications in the context of international security’, U.N. Doc. A/C.1/53/L.17/Rev.1 (2 November 1998).
- 2 Developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/RES/53/70 (4 January 1999).

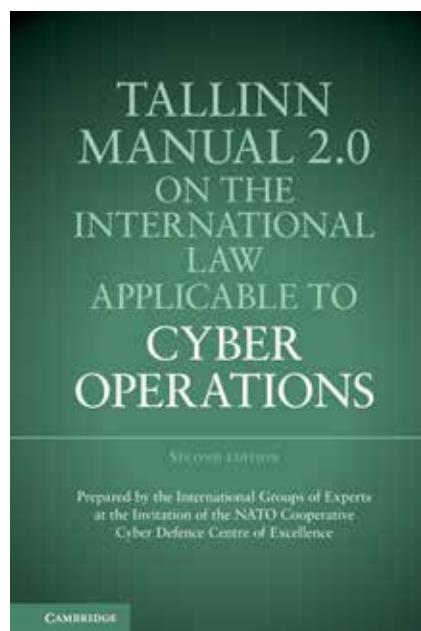
Although it is not directly apparent, the text is widely considered to be the first attempt by Russia to fashion a global regime for the control of cyber arms. Unconvinced of the sincerity of the Russian proposal and lacking a sense of urgency in dealing with cyber issues, other states treated it with relative indifference. It was only in 2007, after Estonia was targeted by a two-month distributed denial of service campaign, that cybersecurity, including the question of how international law applies to cyber activities, became a mainstream international relations topic.

The international community, including both states and academia, soon began to query whether the use of cyber capabilities to harm other states or entities was consistent with international law and to consider how victim states were entitled to defend themselves. Global discussions on those matters took place predominantly under the United Nations umbrella in the format of the UN GGE. In the Euro-Atlantic space, both the European

Union and NATO issued several statements on the applicability of international law to cyber activities. Additionally, some states have unilaterally set out their views on the interpretation and application of international law to the cyber domain.

Insofar as academic efforts to articulate the legal rules governing cyber activities are concerned, the most comprehensive resource is the '*Tallinn Manual 2.0 on the International Law of Cyber Operations*', produced by an international group of legal scholars and practitioners at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence in 2009-2017.

Liberal democracies committed to the rule of law approach the issue from the premise that cyber activities are subject to pre-cyber international law. In other words, to the extent that international law is technology-agnostic – and most of its principles and rules governing politico-military activities are – there is no reason to exclude cyber activities from its ambit. In its 2013 Cyber Security Strategy, the European Union committed to applying existing international law in cyberspace. Likewise, NATO's Wales Summit Declaration of 2014 recognised that international law applies to cyber activities. Both organisations, as well as many likeminded individual countries, continue to maintain this position.



Is international law applicable in cyberspace?

At the global level, in 2013 the UN GGE, which comprised national experts from 15 nations, concurred that '*International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.*'³ Two years later the subsequent UN GGE, consisting of representatives from 20 states, affirmed this position.⁴ Both groups included experts from the UN Security Council's five permanent members and the reports of each were subsequently 'noted' and 'welcomed' by the UN General Assembly. Thus, at least as of late 2015, there appeared to be global consensus that cyber activities were subject to extant international law, although additional work was needed to understand precisely how international law governed them.

An expanded UN GGE of 25 nations met in 2016-17. Despite the broad consensus cited above, international law proved to be the one discussion item that ultimately prevented the group from reaching agreement and issuing a consensus report. This was significant since, up to that point, the so-called 'Western approach' - rejecting the need for a cyber treaty - had tended to dominate the international law narrative. Yet, this Western approach had never been universally embraced. In 2009, under the auspices of the Shanghai Cooperation Organisation (SCO), Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan adopted the Agreement on Cooperation in the Field of International Information Security. Moreover, in 2011 and 2015, four and six SCO member states, respectively, submitted an 'International code of conduct for information security' to the UN General Assembly for adoption. Although the voluntary code was never adopted by the General Assembly, it suggested that the UN should play a prominent role in '*encouraging the development of international legal norms for information security,*'⁵ thereby making it clear that, in the estimation of Russia, China, and their likeminded partners, extant international law was inadequate to govern the cyber domain.

During the 2016-17 UN GGE, Russia and China did not deny the applicability of international law to cyber activities, since doing so would have directly contradicted their earlier position. The liberal democracies in the UN GGE nevertheless took the view that

3 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paragraph 19, U.N. Doc. A/68/98 (24 June 2013).

4 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paragraphs 24-29, U.N. Doc. A/70/174 (22 July 2015).

5 Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, paragraph 2(12), U.N. Doc. A/69/723 (13 January 2015).

the opposition to the report's text regarding international law undid previous progress. Accordingly, consensus could not be achieved and the fifth UN GGE collapsed.

Today, it is difficult to clearly identify where the international community stands with respect to applying international law in the cyber domain. On the macro level, liberal democracies are likely to continue to insist on the applicability of existing law, while refusing to open the door to cyber treaty negotiations. Yet, for extant law to play a meaningful role in preventing cyber conflict and ensuring international peace and security, mere acceptance that the law applies will not suffice. In particular, states will need to articulate the parameters of certain key international law rules and principles more clearly. Some of those rules and principles have been accepted by all states, whereas others have prompted heated debates within the UN GGE. This obstacle aside, the broader question is where Russia, China and their likeminded partners are going with their apparent desire to craft new legal rules, in particular a treaty regime.

At the Cyber Conference 2018 in Tallinn, one panel was dedicated to international law in cyberspace. In the picture: Mr Erki Kodar, Ms Liis Vihul, Ms Ianneke Borgersen Karlsen and Dr Asaf Lubin.



Photo: NATO Cooperative Cyber Defence Centre of Excellence / Kristi Kamenik

The normative significance of sovereignty

With respect to the uncertainty regarding the substantive rules of international law, one of the most-referenced international law concepts in the 2013 and 2015 UN GGE reports is that of sovereignty. As such, at least on the surface, sovereignty appears uncontroversial. Yet states understand 'sovereignty' in different ways: this facilitates references to sovereignty in the consensus reports, but renders its practical application difficult. Authoritarian and other states that are concerned about the transmission of information from foreign sources into, or made available in, their territories generally interpret sovereignty as a right to be free from outside interference and influence. For them, sovereignty protects their so-called information space.

For liberal democracies, such an understanding of sovereignty is unacceptable from a policy perspective because it is contrary to their commitment to human rights, in particular freedom of expression. Rather, liberal democracies view sovereignty as a foundational principle of international law. It entails sovereign equality, whereby all states are equal before the law. Other international law rules and principles, such as the rules regarding jurisdiction, the prohibition of intervention, and the obligation of due diligence are also derived from the principle of sovereignty.

From an operational perspective, the most pressing question with regard to sovereignty is whether it acts as a stand-alone legal 'rule' that places substantive limits on states' cyber activities. This issue has been addressed in some detail by academics, but only by a handful of states thus far. If, as in the United Kingdom, it is decided that this is not the case, the threshold at which offensive cyber activities violate international law will be relatively high: unless they constitute a prohibited intervention or use of force, they are likely to be held as lawful. According to the opposing view, certain cyber operations that would not amount to an unlawful intervention or use of force, may nevertheless constitute a violation of sovereignty. The first position legitimises many cyber operations that would be qualified as unlawful according to the second. Thus, while the former provides greater operational leeway, the latter can be said to contribute more meaningfully to cyber stability by requiring greater restraint on the part of states.

A derivative of the principle of sovereignty, the obligation of due diligence, is likewise controversial. The obligation requires that states do not knowingly allow the use of their territories for cyber activities that are harmful to other states. Should a malicious cyber activity that seriously harms another state be underway, the territorial state would be obligated to take all reasonably available measures to put an end to the cyber operation. Several major cyber powers, including Russia, China, the United States and the United Kingdom, appear hesitant to accept or even reject the legally binding nature of the due diligence obligation. However, numerous others, including France, Germany, Finland, the Netherlands and Spain, recognise due diligence as an international law rule. Nevertheless, while states disagree over whether due diligence forms a part of the corpus of international law, they seem to agree that, as a policy matter, it is desirable for states to take action vis-à-vis malicious cyber activities that originate from their territories. This was affirmed in the 2015 UN GGE report, which stated that '*States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.*'⁶

⁶ Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paragraph 13(c), U.N. Doc. A/70/174 (22 July 2015).

The applicability of two further international law rules that stem from the principle of sovereignty, the prohibition of intervention and prohibition of the use of force, is uncontested in the cyber context. According to the former, states are not allowed to coercively interfere in the internal or external affairs of other states. This would be the case, for instance, if election results in another country were altered by cyber means. The prohibition of the use of force, a customary international law rule codified in Article 2(4) of the UN Charter, is generally understood to at least proscribe states' cyber operations where such operations result in injury to or the death of persons, or physical damage or the destruction of objects. With regard to damage, states that have addressed the matter publicly appear to be comfortable extending the prohibition beyond physical consequences, although they have not definitively set forth their threshold of unlawfulness with respect to non-physical consequences.

Countermeasures

Whereas a degree of controversy surrounds the aforementioned international law obligations, certain key rights are even more contentious. In particular, disagreement over whether states are permitted to engage in 'countermeasures' in response to unlawful cyber activities, or act in self-defence when subjected to cyber 'armed attacks' - topics that had proven to be difficult discussion points in earlier UN GGE sessions - led in part to the collapse of the GGE's most recent iteration.

Countermeasures are acts that would otherwise be unlawful, but are deemed not to be unlawful to the extent that they are undertaken in the context of a response to another state's unlawful conduct. They are a means of self-help designed to enable a state that has suffered from a violation of the law to return the situation to one of lawfulness. By way of example, if a state has unlawfully intervened in another state's internal affairs by directing a large-scale distributed denial of service operation against its governmental information systems during an ongoing referendum, the target state is entitled to employ countermeasures in order to induce the wrongdoing state to terminate the cyber operations in question. The countermeasure in such a situation could entail a 'hack back' that would otherwise be unlawful, or, for instance, denying the malicious state's civil aircraft landing or overflight rights that the victim state would otherwise be obliged to confer pursuant to an international agreement.

Self defence

Provided for in Article 51 of the UN Charter, a state's right to self defence arises in the cyber context when a hostile cyber operation amounts to an 'armed attack'. An armed attack is generally considered to be a higher threshold than that of the use of force:

only 'the most grave' use of force constitutes an armed attack. In other words, the injury, death, damage, or destruction that a malicious cyber operation results in must be significant. Faced with a cyber armed attack, the victim state is permitted to resort to force, including cyber operations at the 'use of force' level, to defend itself.

Despite the fact that both countermeasures and self defence are permissible only in exceptional circumstances and subject to numerous restrictions, some states refuse to acknowledge their applicability in the cyber context. The debate over their applicability has become highly politicised. Most 'Western powers' see a deterrent value in a common understanding that certain malicious cyber operations may be met with robust responses. Other states view insistence on the recognition of countermeasures and self-defence as an attempt to legitimise their potential responses to what they perceive to be malicious cyber activity.

'Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.'

Art. 51 of the UN Charter, Chapter VII — Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression.

Applicability of international humanitarian law

Finally, a debate that is devoid of legal merit, but which nevertheless persists in cyber diplomacy, concerns the applicability of international humanitarian law to cyber operations conducted during armed conflicts. Cyber operations will increasingly manifest on the battlefield, as illustrated, for instance, by Israel's alleged manipulation of the Syrian air defence system in 2007 as part of Operation Orchard/Operation Out of the Box, Russia's use of cyber operations in its ongoing armed conflict in Ukraine and its conflict with Georgia in 2008, and the United Kingdom and the United States' cyber operations against Da'esh. Because they occurred in the context of either international or non-international armed conflicts, all were governed by international humanitarian law.

Countries that object to the applicability of international humanitarian law allege that its endorsement legitimises cyber warfare. They contend that, rather than focusing on how to wage wars, states should focus on preventing them. This line of argument ignores the reality that wars do break out and that limits must be imposed on the cyber operations that are certain to occur as a result thereof.

Despite the fact that the 2016-17 UN GGE was unsuccessful, primarily due to disagreements over international law, discussions at the multilateral level are likely to continue. The challenge for states committed to the rule of law will be to maintain the current international legal architecture and prevent its further erosion. Additionally, those states hoping to reduce the range of cyber activity must be more open to accepting the obligations of international law, such as due diligence, restrictions on their own cyber activities, and the requirement to respect the sovereignty of other states. Finally, all states, whether acting unilaterally or via international organisations, must be more forthcoming as to their interpretation of international law in the cyber context if international law is to have a meaningful effect in cyberspace.

1.3 Military concept for cyber defence in CSDP

by Neil Powell

In our everyday lives, we have become increasingly aware of the prevalence of cyber threats, be they from criminals or hacktivists or potentially state-sponsored. Major incidents such as the distributed denial-of-service (DDoS) attack on the managed DNS provider Dyn in October 2016, which left several major US and European sites, including PayPal, Spotify, and Twitter, inaccessible for hours, and the global 'WannaCry' ransomware attack in June 2017 have highlighted vulnerabilities and the wide-ranging effects of attacks through cyberspace.

The CIA principle



Graph: Jochen Rehrl

From a military perspective, communication and information systems (CIS) are a critical enabler for all operational domains and nearly every capability has become dependent on the confidentiality, integrity and availability of ICT-based systems. The use of and open access to a safe and secure cyberspace (mostly seen as the internet) is also fundamental and critical for EU CSDP operations and missions. Operational success and mission assurance are reliant on having available functioning and uncontested CIS. At the same time, various kinds of adversaries are conducting cyber operations directly or indirectly against the EU's critical communications networks (including missions and operations) to impair the functioning and decision-making ability of CSDP structures. Therefore, appropriate cyber measures and capabilities have to be put in place to face and counter these threats. Cyber resilience and preparedness is a major task for CSDP operations and missions.

The EU cyber defence concept

The EUMS, as the EU and EEAS' provider of military expertise, developed a new version of the EU Concept for Cyber Defence for Military Operations and Missions, which was endorsed by the EUMC in November 2016. The aim of the concept was to reflect the specific organisational and procedural aspects of military planning and military force generation as well as addressing the requirements for MS' provision of cyber capabilities for CSDP activities. Subsequently, a complementary concept for the implementation of cybersecurity for civilian missions was developed by the Civilian Planning and Conduct Capability (CPCC). In September 2017, the European Commission and EEAS issued a Joint Communication entitled 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'. This was, in essence, a significant update to the original 2013 EU Cybersecurity Strategy affirming, *inter alia*, the importance of cyber resilience for CSDP.

Before proceeding, it is useful to understand that the EU and the EEAS use the term 'cybersecurity' as a general term primarily related to the civilian context, whereas 'cyber defence' is generally used for military cyber aspects. Nevertheless, the two concepts are closely connected as they address the same threats, follow the same basic principles and require similar measures and procedures.

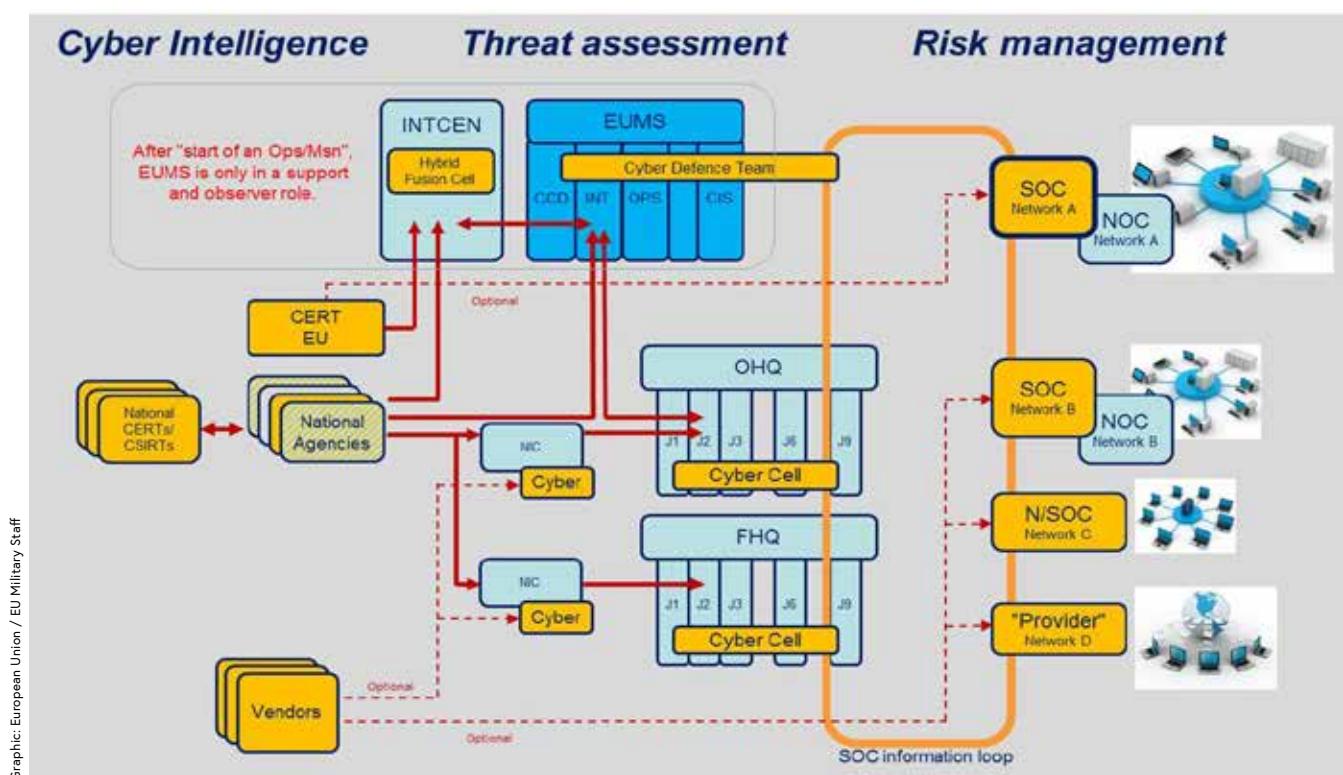
Cyber defence in planning

The first principle for ensuring effective cyber security and defence is to consider cyber aspects as early as possible within the EU's crisis management and planning processes. Cyber aspects must therefore be included in the overall threat evaluation when planning a potential operation or mission. Cyber threat intelligence should be provided by the EU's strategic intelligence structures, based around EEAS INTCEN, including the Hybrid Fusion Cell, and the EUMS Intelligence Directorate, and supported by information sharing with other trusted organisations; these could include the EU's cyber information hub (CERT EU), military partners, such as NATO, and of course MS' own cyber information providers.

Together with intelligence experts, the EUMS cyber defence team will assess the information provided and support the operation/mission planning teams, inserting a cyber narrative into initial planning documents (notably the Crisis Management Concept and the Initiating Military Directive). This provides a sound basis for further detailed planning by the designated operation or mission commander and their staff – supported by further intelligence and a more in-depth analysis of threats and risks from cyberspace in the area of operations. The commander is then able to make an informed decision on the importance of cyber defence and to define, in the concept of operations and the operation or mission plan, how an effective defence against potential threats from

cyberspace can be achieved. The necessary resources and capabilities can then be requested to ensure the resilience and protection of the enabling CSDP IT systems and networks.

As the EUMS does not provide or deploy any operational cyber capabilities, these must first be requested from MS supporting the CSDP activity through the force generation process. If MS are unable to provide the required expertise or systems, other options, including requesting EU partners' assistance or outsourcing to commercial providers, will need to be considered.



Cyber defence organisation within the Common Security and Defence Policy.

Cyber defence in conduct

The implementation of cyber defence in CSDP involves much more than simply providing some protection mechanisms in the networks. The term 'capabilities' has therefore been considered in the Cyber Defence Concept in a broader context, covering doctrinal, organisational, training/exercise, material, leadership, personnel, facilities and interoperability aspects (using the DOTMLPF-I scheme). Besides 'simple' material protection it is primarily concerned with the preparation of systems, structures, procedures and, in particular, the personnel involved, in order to ensure their awareness

of and education on threats from cyberspace. This cyber resilience and the related capabilities must be established and sustained so that they are available, tested and able to deploy prior to the start of any planning process for a new operation or mission.

As during the planning phase, organisational elements and procedures to ensure effective cyber defence must also be put in place during the conduct phase of operations and missions. Therefore, structures known as 'cyber cells' should be established within every OHQ/FHQ, to provide a continuous assessment of the cyber threat information received from the supporting intelligence structures. A cyber cell should advise decision-makers in the HQ, providing agreed and appropriate actions or reactions. Therefore, the cells work closely with the security operation centres (SOCs), which are responsible for running the risk management for the mission's networks, observing the networks and identifying, prioritising and mitigating risks. Standard operating procedures (SOPs) are needed to complement these organisational elements, and will ensure that both the strategic and the operational level of missions and operations act and react in a timely and effective manner.

Under the responsibility of the Council and of the High Representative

Political and Security Committee

shall exercise the political control and strategic direction

EU Military Committee

shall monitor the proper execution of the military mission/operation and the Chairperson EUMC shall act as the primary point of contact with the EU Mission/Operation Commander

Operation Headquarters (OHQ)

Option 1

NATO SHAPE
Berlin plus



FHQ

Option 2

EU OHQ
offered by
EU Member States



FHQ

Option 3

EU OpsCen
integrated in the
EUMS



FHQ

Option 4

Mission Planning
and Conduct
Capability (MPCC)



MFHQ

Military command
and control
structures.

There is also an important distinction between CSDP military operations and missions. For an operation, an OHQ will be nominated from one of the permanently offered HQs by certain MS (or NATO under Berlin+ arrangements). The relevant MS will then be responsible, *inter alia*, for the establishment and support of appropriate cyber-defence measures for the OHQ and subordinate FHQs. However, with the formation of the Military Planning and Conduct Capability (MPCC) in 2017, within the EUMS structure, the MPCC Director (the second hat of DG EUMS) is now responsible for military missions and therefore for ensuring that cyber-defence aspects are properly addressed for the HQ, in Brussels, as well as for subordinate mission force HQs (MFHQs).

Next steps for cyber defence in CSDP

Capability development

The Cyber Defence Concept addresses various aspects of an effective cyber-defence capability at a high level and this has to be translated into actionable work packages. One major aspect is the development of more tangible requirements and cyber capability packages which can be implemented by potential providers – including MS and commercial providers. During the major work to develop the new Requirements Catalogue (2017), which is used to identify the full range of CSDP military requirements across a number of illustrative scenarios, the need for cyber-defence capabilities emerged as a high priority.



Subsequently, this has provided the basis for the development of specific cyber-defence capabilities led and supported by studies carried out by the European Defence Agency (EDA) and its cyber-defence project team. In addition, specific cyber-defence capabilities have been proposed for development by MS through the permanent structured cooperation (PESCO) initiative.

“

We have activated a Permanent Structured Cooperation on Defence – ambitious and inclusive. 25 Member States have committed to join forces on a regular basis, to do things together, spend together, invest together, buy together, act together. The possibilities of the Permanent Structured Cooperation are immense.

Federica Mogherini

High Representative/ Vice-President (December 2017)



Graphic: Fact sheet 'Permanent Structured Cooperation' 2018

SOP development

Whilst the Cyber Defence Concept provides the basic understanding for appropriate preparatory actions and responses to cyber threats, the next step is to develop SOPs between the EUMS and operational stakeholders at HQ level. Consequently, the development of the EU 'Standard Operating Procedure (SOP) for Cyber Defence at HQ Level' has already started under the lead of the EUMS and is expected to be completed by the end of 2018. The SOP is based on lessons identified in various EU military operations and missions and best practices derived from other organisations. Its aim is to provide a set of procedures and best practice examples which will be valid for all HQ levels and for all phases of an operation/mission. A core element of this SOP is a 'Cyber Incident Response and Reporting Regime' which will include: detailed guidance and examples on how to establish a Cyber Defence Organisation for CSDP and how to prepare for, detect and analyse, react to and recover from cyber incidents; a Cyber Incident Criticality Matrix; and a structured and mandatory reporting mechanism for cyber incidents, coherent with civilian missions and other EU institutions.

Education, training and exercises

The most important aspect of resilience is to prepare the people involved, since the human element is the most common 'cyber-vulnerability'. Consequently, education, training and exercises are essential components of cyber resilience. This not only includes basic education for ICT users and training for deep specialists ('the geeks') but also training for others who need to better understand the cyber environment for CSDP. This includes decision-makers, operational planners and legal and political advisers.

Consequently, with the support of the EUMS and the MS, the Cyber Discipline within the EU Military Training Working Group, the European Security and Defence College (ESDC) and the EDA are working together on new initiatives to design, develop, conduct and evaluate training activities and exercises; these range from awareness training up to courses for high-level decision-makers. There is also now a clear expectation in exercises, such as the MILEX annual exercises, that cyber play will be a key component.

Cooperation with partners

Cooperation with civilian and military partners is essential, to share information and exchange ideas. While cyber expertise from industry and academia is linked into the processes mainly by the EDA and the ESDC, the EUMS interacts closely with NATO on military aspects of cyber defence both informally as well as formally via the EU-NATO Joint Declaration Implementation Plan, adopted by Council conclusions in December 2016. This gives huge impetus not only to the common use and development of training and exercises by the two organisations, but also to exchanges and involvement in cyber policy work and cyber information sharing, to increase synergies, avoid duplication and allow the organisations to understand each other's mechanisms. The EU-NATO Parallel and Coordinated Exercises (PACE) also have cyber security and defence as essential components for exercise play. Furthermore, mutual participation in cyber-focused exercises including the ENISA-organised CYBER EUROPE and NATO CYBER COALITION has now started.



Graphic: ENISA, Cyber Europe Poster 2018

Conclusion

The success of cyber security and defence in CSDP operations and missions remains dependent on a combination of state-of-the-art technology, organised and effective structures and procedures and, of course, educated, aware and competent staff. These capabilities will need continual investment to maintain their effectiveness. Moreover, in this dynamic and evolving environment, these capabilities need to be underpinned by close cooperation and information-sharing, both with external partners, such as NATO, and internally across MS and other EU institutions. Taken together, this will provide the basis for strong cyber resilience for CSDP: being prepared to deter and counter cyber threats and also able to respond and recover quickly and effectively in order to ensure operational effectiveness.

Cyber resilience for CSDP means: being prepared to deter and counter cyber threats and able to respond and recover quickly and effectively to assure operational effectiveness.



Photo: Austrian Armed Forces / Maximilian Fischer

1.4 Integrating cybersecurity in civilian CSDP missions

by Enrico Introini

In the last few years we have all experienced the recurrent feeling of living in a digital age, where everything is connected and needs to be synchronised online: we are more and more dependent on internet services in our offices, when we travel and in our private life. That is clearly bringing many economic benefits and faster communications, though also new risks which need to be taken into account properly.

The European Union started working on countering those risks back in 2013 with the first EU Cybersecurity Strategy. Since then a number of directives have been drafted to translate the general strategy into the various EU policy areas with their more specific and operational requirements. One of the first areas was the EU's Common Security and Defence Policy activities, which include civilian and military missions and operations. As soon as 2014 the European External Action Service (EEAS) developed the EU Cyber Defence Policy Framework (CDPF), which has been the main guide for strengthening cyber defence resilience and capabilities in the CSDP through the introduction of better governance for the different stakeholders working in the EEAS universe.

Photo: Austrian Armed Forces / Carina Karlovits



The EU's mission personnel as well as the host country's personnel must receive continuous training to develop the necessary level of preparedness and cyber resilience.

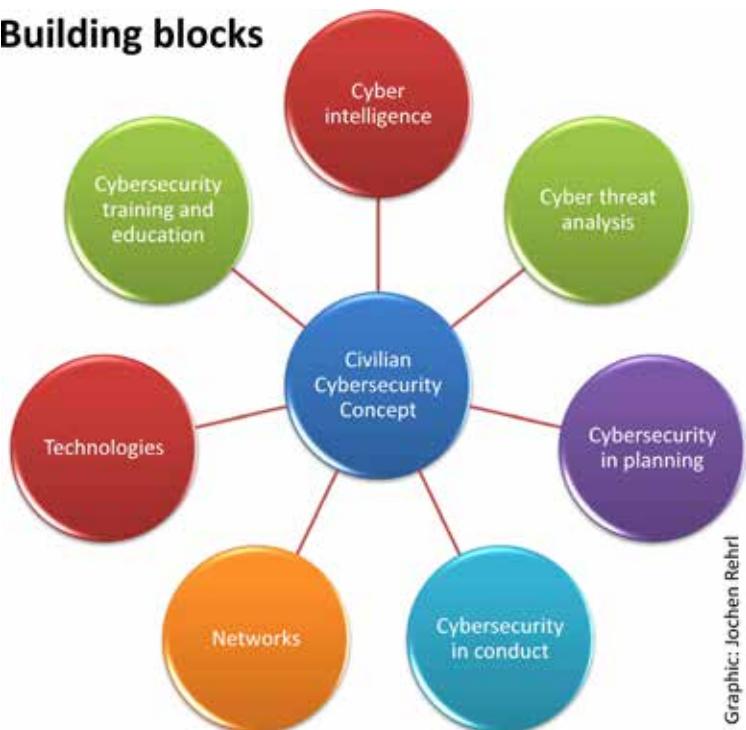
It also quickly became clear that the specific characteristics of military and civilian missions required further work on adapting the general policy and associated requirements to the environment and governance specific to CSDP missions. In November 2016, the 'EU Concept on Cyber Defence for EU-led Military Operations and Missions' was the first attempt to tackle the need for specific guidelines to strengthen the capabilities of CSDP military missions and operations in cyber defence.

There was still the need to cover the specific nature of civilian CSDP activities and their different needs in terms of cybersecurity to those of military missions. In order to meet this need during 2017, the EEAS working document 'Integrating cyber security in the planning and conduct of civilian CSDP missions' was drafted and eventually endorsed by the Political and Security Committee (PSC) on 12 July 2017.

EU concept paper on cybersecurity in civilian missions

The EEAS working document on integrating cybersecurity in civilian missions mainly complements the concept paper on military CSDP (cyber defence in EU-led military operations and missions), by highlighting the importance of translating high-level commitments to strong cybersecurity into concrete operational steps. The aim of the concept paper is to set the parameters for enhanced cybersecurity in civilian missions and promote a greater emphasis on cyber issues from mission planning right through to execution.

Building blocks



Graphic: Jochen Rehrl

Many of the challenges addressed in the military concept are also applicable to civilian missions and so have been discussed in the document, such as the need for cyber intelligence and cyber threat analysis, for integrating cybersecurity in the planning and conduct of missions and operations, for developing appropriate networks and technologies, and for training.

There are also some significant differences, of course, like the fact that Member States are responsible for providing equipment in military operations, whereas civilian missions acquire equipment through the CFSP budget. On the military side, the lead nation ensures that the CIS used in a given mission meets a certain minimum level of interoperability and security requirements, while this is not yet the case in all civilian missions. Another difference is that there is no single interconnected network for civilian CSDP missions, but a collection of separate and standalone CIS, one for each mission.

The vision behind the document is that strategic planners and heads of mission should first be able to identify areas where cyber-attacks may impair mission conduct, security of personnel or fulfilment of mission mandates and then ensure that necessary steps are taken to provide the mission with the capabilities to prevent, react, mitigate and recover quickly from such attacks.

Cyber intelligence and cyber threat assessment

Intelligence reports with information about cyber threats that a mission could possibly face should be an integral part of the preparation phase before the mission is launched. In the CSDP area, the main providers of this type of information are the EEAS INTCEN, the Intelligence Directorate of the EU Military Staff (EUMS) and the Hybrid Fusion Cell, all acting together in the Single Intelligence Analysis Capability (SIAC) format. They are supported by Member States' intelligence structures, CERT-EU expertise and information about cyber threats.

A cyber threat assessment should be available early in the planning phase to define a cybersecurity risk profile that will help with determining the needs of the mission in terms of setting up the correct cyber protection. This analysis should include the presence of hostile actors and their cyber capabilities in the area where the mission will operate. As a first step the general regional threat assessment that INTCEN provides about the security in the area of operations of the CSDP mission should include an assessment of the cyber threats with an indication of the threat level.

Cybersecurity in the planning process

It is very important to start considering the cybersecurity requirements as soon as possible from the beginning of the planning process. The main reason is to have cyber aspects included in the CSDP planning documents and in particular in the crisis management procedures. The analysis to assess the security situation and required measures should include an evaluation of the requirements for cybersecurity based on input from INTCEN.

Afterwards, the budget impact statement (BIS) should include details of the cyber threat level and the overall security situation (based on a cyber threat assessment), the required level of classification for communications, the required level of protection of information assets and the interoperability and classification levels needed for cooperation with other international stakeholders (EU DEL, Europol, Frontex, military CSDP operations/missions). All those details and requirements will help in establishing the mission's needs in terms of cybersecurity and their budgetary impact.

In order to implement cybersecurity best practices at mission level, it could be helpful to introduce further cyber-related requirements directly in the operation plan (OPLAN), one of the main planning instruments for each mission. This will in turn require designating a focal point for cybersecurity in each mission, establishing pre-deployment training including cyber awareness elements, defining general procedures for all staff members concerning cybersecurity and an SOP on cyber hygiene, or requesting the establishment of a communication plan for cybersecurity incidents and the creation of an SOP for incident reporting.

Cybersecurity in the conduct phase

In general, the new and continuous developments in the cyber area, such as zero-day vulnerabilities, exposure of weaknesses in CIS components, new modes of attack and new methods of protection, mean that the parties involved need to follow these developments closely through continuous training, so that they can develop the necessary level of preparedness and cyber resilience.

Handling of EU classified information (EUCI) requires providing physical security for the civilian mission premises corresponding to the given level of classification. In particular, EUCI data must be stored in accordance with the security rules of the EEAS applicable to each classification level and this should be reflected in the architecture of the mission's network (e.g. segregation of networks using physical and logical architectures).

Under the responsibility of the Council and of the High Representative

Political and Security Committee

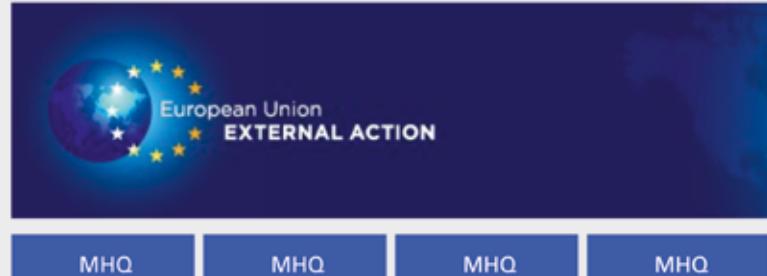
shall exercise the political control and strategic direction

**Committee for Civilian Aspects
of Crisis Management (CIVCOM)**

is NOT included in the chain of
command of civilian CSDP missions

Civilian Operation Headquarters (OHQ)

Civilian Planning and Conduct Capability (CPCC)
is the permanent headquarters
for ALL civilian CSDP missions



Graphic: Handbook on CSDP, 3rd edition, 2017. P 80. / Jochen Rehrl

Civilian command
and control
structures.

A number of technical requirements and basic architectural design considerations should be implemented following the agreed IT security standards set out inter alia in Council document 10578/12 'Information Assurance Security Guidelines on Network Defence'. These include the need to protect the local intranet from a direct connection to the internet, the need for a network-wide strong password policy, the requirement to have an accurate and updated inventory of permitted IT equipment and software, the need for a unique sign-on mechanism covering all the systems used, permanent monitoring of all logging on to the network and proper procedures for the arrival and departure of normal and privileged users.

These will always be non-exhaustive requirements, which is why the concept paper recommends also putting in place all feasible technical protection measures, including device-oriented and boundary-oriented methods for intrusion detection and intrusion prevention, security-hardened firewalls, web filtering against dangerous content and a malware and antivirus protection policy on removable media. Another important point

Awareness of cybersecurity will not be enough if the right equipment is not available.



Photo: EUAM Iraq

tackled in the EEAS working paper is the establishment of a regular campaign on security audits, penetration testing, application vulnerability assessment, and security awareness raising for mission staff.

Security governance is also important in the conduct phase, so a business continuity plan (BCP) and a disaster recovery plan should be developed and implemented to ensure the continuation of the mission and rapid recovery in the event of a disaster occurring. Cyber attacks and incidents should be analysed and associated standard operating procedures (SOPs) are needed in order to provide appropriate reporting to the relevant hierarchy and to the broader EU cyber community.

As regards the implementation of technical protection measures in mission networks, further collaboration and support could be sought through the advanced services offered by CERT-EU, which could progressively be extended to cover all civilian missions. It is also understood that the CIS and the measures to ensure cybersecurity in the mission itself will often be provided in the form of contracted services, including in the fields of cyber threat intelligence, penetration testing and vulnerability assessment, security audit, monitoring services and logging analysis. Any such purchased services must comply with the standards and requirements needed by the CSDP structures, including civilian missions, and must in all circumstances operate under the appropriate EU security



Civilian CSDP missions have established security standards and minimum requirements for CIS networks and interconnected IT systems.

clearances. In the longer run the needs of civilian CSDP missions could be included in ongoing work with the EUMS on civ-mil cooperation aimed at establishing security standards and minimum requirements for CIS networks and interconnected IT systems.

Way ahead

The 10 civilian missions currently active are independent legal entities with their own budget and independent IT network (not interconnected with those of other missions). The Civilian Planning and Conduct Capability (CPCC) in the EEAS holds the main responsibility for the planning and conduct of CSDP civilian missions and one of its current objectives is to harmonise and standardise the IT architecture and the cybersecurity posture of CSDP missions. This objective is complex mainly owing to the governance and budgetary constraints related to the CSDP missions that have, over the years, produced a range of different IT architectures and cyber security solutions.

The work of standardisation was started in 2018, through a cybersecurity survey in the missions aimed at establishing a central inventory of the different solutions and equipment used in the cybersecurity area. The CPCC is also involved in the work on establishing a cybersecurity capability maturity model (C2M2), which would be offered as a service under the inter-institutional cyber framework contract to all European institutions and would be a powerful tool for measuring and then harmonising the different levels of cybersecurity maturity in CSDP civilian missions.

CPCC's objective is to harmonise and standardise the IT architecture and cybersecurity posture.



The EEAS concept paper on cybersecurity for civilian missions has suggested creating a focal point for cyber issues in the CPCC structure to ensure that cybersecurity in missions is planned, implemented and monitored in a satisfactory manner. In line with this, the CPCC appointed a new officer in September 2017 who deals mainly with cyber-defence capabilities enforcement and cybersecurity coordination for civilian missions. According to the concept paper, there is also a need to designate focal points for cybersecurity in each civilian mission embedded in the mission security department structure; based on this advice, a number of missions have already nominated their local focal point. In the longer run, consideration should be given to creating dedicated 'cyber cells' in the context of civilian crisis management both at HQ and mission level.

During the last months of 2017, the CPCC supported the adoption of the new inter-institutional cyber framework contract within all missions, thereby making CSDP civilian missions formal participants in the contract. The CPCC has been monitoring the harmonisation of its use in the different missions. A number of civilian missions already procured a number of services (IT security audits, cybersecurity products and services) under this framework contract during 2018.

A number of missions have already signed a specific service level agreement (SLA) with CERT-EU in order to benefit from their advanced services of network surveillance, penetration testing and incident handling. The CPCC will promote and support the spreading of CERT-EU advanced services amongst all the other civilian missions in the next few years.

The implementation of the measures suggested in the concept paper ‘Integrating cyber security in the planning and conduct of civilian CSDP missions’ is also progressing thanks to the current review of the OPLAN of civilian missions and the inclusion of a special paragraph related to cybersecurity. This new paragraph has already been inserted in the updated OPLAN of several missions and the process will be extended to other missions in the coming months.

Significant improvements have also been secured on cybersecurity governance at HQ level, with the civilian CSDP missions permanently represented in the EEAS Cyber Task Force and in the EEAS Cyber Governance Mechanism. This will definitely help with presenting the needs and requirements of civilian CSDP missions at corporate level, with a view to including them in the global governance of cybersecurity at European level. Several benefits could derive from this inclusion, including the possibility to extend standardised procedures on incident management, participation in European cybersecurity exercises for civilian CSDP missions, access to jointly developed cyber-awareness or technical cyber security online training, better inclusion of civilian CSDP missions in common cybersecurity projects (e.g. the USB Kiosk sanitising project, and next-generation classified networks projects).

1.5 Cyber resilience as a key challenge for the EU and its Member States

by Arnold Kammel

Connected society and the Internet of Things (IoT) continue to challenge the status quo of information security practices for states and citizens. The number of transactions conducted via the internet is steadily increasing, with millions of citizens participating and making use of the possibilities of the virtual world. However, besides its positive impact on the daily lives of citizens, the misuse and vulnerability of the internet have gained importance for policy-makers including within the EU policy framework, and the concept of cybersecurity has become an issue. Already in 2008, the Implementation Report on the European Security Strategy named cybersecurity as a key challenge and called for a comprehensive EU approach.¹ Today, as cybersecurity incidents such as

European citizens and businesses rely on digital services and technologies:

Europeans believe that digital technologies have a positive¹ impact on:



86% of Europeans believe that the risk of becoming a victim of cybercrime is increasing.²

Sectors like **transport, energy, health and finance** have become increasingly dependent on network and information systems to run their core businesses.

The **Internet of Things (IoT)** is already a reality. There will be **tens of billions** of connected digital devices in the EU by 2020.³

Cyber incidents and attacks are on the rise:

+4,000 ransomware attacks per day in 2016.

In some Member States 50% of all crimes committed are cybercrimes.

Security incidents across all industries rose by **38%** in 2015 – the biggest increase in the past 12 years.

80% of European companies experienced at least one cybersecurity incident last year.⁴

+150 countries and +230,000 systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including **hospitals and ambulance services**.

Graphic: European Commission - Factsheet on cybersecurity 2017

¹ Report on the implementation of the European Security Strategy, 'Providing Security in a Changing World', S407/08, 5.

Awareness and knowledge

Despite the growing threat, awareness and knowledge of cybersecurity issues is still insufficient.



69% of companies
have no or basic
understanding of their
exposure to cyber risks



60% of companies
have never estimated the
potential financial losses
from a major cyber-attack⁶



**51% of European
citizens** feel not at all
or not well informed
about cyber threats⁷

malicious attacks are increasing rapidly, cyberspace appears more and more vulnerable. Cybercrime is consistently listed as a top concern of CEOs worldwide. According to the European Commission, in 2016 there were more than 4 000 ransomware attacks per day and 80 % of European companies experienced at least one cybersecurity incident. The economic impact of cybercrime has risen five-fold over the past four years alone.²

Generally it can be witnessed that cyber-attacks are not only increasing in number but also in sophistication. Contrary to that development, awareness and knowledge of cybersecurity is still insufficient. 51 % of European citizens feel uninformed about cyber threats and more than two thirds of companies have no basic understanding of their exposure to cyber risks.³

For years, the threat of being a victim of a cyber-attack was either ignored or was addressed simply with basic IT solutions, such as antivirus or anti-malware programs and firewalls. As cyber incidents became more evident, organisations responded with more investment in prevention, which meant developing more robust IT solutions designed to keep malware and other malicious activities out of networks and to avoid a possible total blackout of not only the IT, but also possibly critical, infrastructure. However, it has become obvious that measures related to cybersecurity alone are not enough, and cyber resilience has become a key topic. The idea of resilience is an analysis of what happens before, during and after a digitally networked system encounters a threat. Having resilient systems therefore means being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world. Cybersecurity is therefore an important element of resilience; however, cyber-resilient organisations recognise that operating safely online goes far beyond just technical measures.

2 http://europa.eu/rapid/press-release_IP-17-3193_en.htm

3 <http://www.consilium.europa.eu/en/policies/cyber-security/>

The EU's approach to cyber resilience – an overview

In a more interconnected and globalised world, cyberspace does not stop at national borders either and thus no Member State is able to tackle the challenge of cyber-attacks and crimes on its own. The EU therefore provides a logical and efficient solution to the challenge facing Member States of how to best tackle cybersecurity threats.⁴

Institutionally, this approach was followed mainly by the setting up of the European Network and Information Security Agency (ENISA) in 2004 and the European Cybercrime Centre (EC3) at Europol in 2013. In the same year, the EU adopted its first cybersecurity strategy⁵ aiming to improve the resilience of both the public and private sector to cyber threats by encouraging a higher degree of cooperation between all stakeholders, greater investment in national and private-sector capacities to respond to attacks, further development of cyber-defence capabilities, and increased engagement with international partners. From that time on, cybersecurity has been among the EU's top priorities in the political field. The strategy presents five key priorities:

1. increase cyber resilience
2. drastically reduce cybercrime;
3. develop EU cyber-defence policy and capabilities;
4. develop the industrial and technological resources for cybersecurity;
5. establish an international cyberspace policy for the EU and promote core EU values.⁶

The cybersecurity strategy was complemented by the European Agenda on Security 2015-2020, which set the fight against cybercrime as one of its three priorities. Also, the EU Global Strategy focuses, among other things, on building cyber resilience, including through strong cooperation with partners such as NATO.

Furthermore, in September 2017, a Joint Communication by the European Commission and the HR entitled 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'⁷ was published, calling for strong cyber resilience. In order to properly deal with this challenge, more robust and effective structures to promote cybersecurity and

4 Council of the European Union. (16 March 2005). Council Framework Decision on Attacks against Information Systems. Official Journal of the European Union. L 69/67.

5 European Commission and HR. (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013) 1 final.

6 European Commission, 'EU Cybersecurity Initiatives - Working towards a More Secure Online Environment', 2 January 2017, http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.



EUROPEAN
COMMISSION

Strasbourg, 28.4.2015
COM(2015) 185 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL
COMMITTEE AND THE COMMITTEE OF THE REGIONS**

The European Agenda on Security

to respond to cyber-attacks in the Member States but also in the EU's own institutions, agencies and bodies are therefore needed. A more comprehensive, cross-policy approach to building cyber resilience and strategic autonomy is also required, with a strong digital single market, major advances in the EU's technological capability, and far greater numbers of skilled experts.

In June 2018, the Council agreed on an upgrade of the current European Union Agency for Network and Information Security (ENISA) into a permanent EU agency for cybersecurity as well as on a mechanism for setting up common European cybersecurity certification schemes for specific ICT processes, products and services.

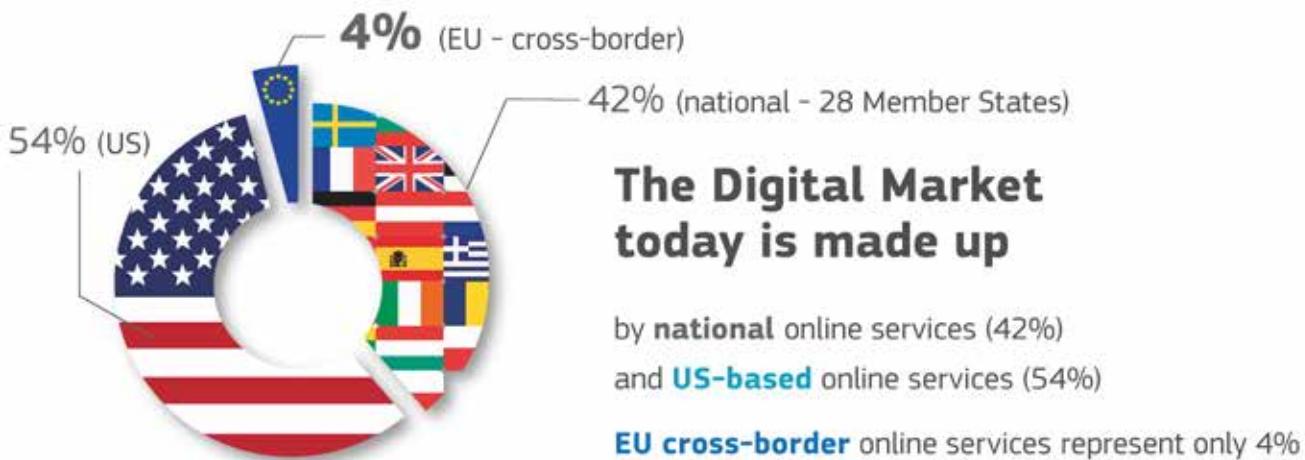
In addition to the cybersecurity dimension, an important decision improving the criminal law response to cyber-attacks was taken with the adoption in 2013 of the Directive on attacks against information systems.⁸ The Directive contains minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and provides for operational measures to improve cooperation between authorities, thus facilitating cross-border cooperation by law enforcement authorities. Furthermore, a blueprint for how Europe and Member States can respond quickly, operationally and jointly in the event of a large-scale cyber-attack was recommended in 2017. It sets out the objectives and modes of cooperation between the Member States and EU institutions in responding to such incidents and crises.

⁷ European Commission and HR. (2017). Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN (2017) 450 final.

⁸ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.



Graphic: Factsheet of the European Commission: Why we need a Digital Single Market 2015



In general, in accordance with Article 4 TFEU cybersecurity policy constitutes a 'shared area of competence' between Member States and the EU, which implies that when the EU decides to regulate, EU law takes primacy over any adopted national law. A significant amount of digital legislation and policies related to cybersecurity thus originates at the EU level.

The NIS Directive and resilience

In 2016, the European Commission proposed the EU's first ever cybersecurity regulatory framework. The Directive on security of network and information systems (NIS Directive) was adopted by the European Parliament in July 2016 and provides legal measures to enhance and strengthen the overall level of cybersecurity across the EU. It is designed to build resilience by improving national cybersecurity capabilities; fostering better cooperation between the Member States; and requiring undertakings in important

RISK MANAGEMENT
Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

SECURITY MEASURES

NOTIFICATION OF MAJOR INCIDENTS

Not all cyber incidents can be **prevented**, but they can be **mitigated**. Member States will have to identify by **9 November 2018** operators of essential services that will be in the scope of the **Directive**. These are businesses that operate in sectors that are vital for our economy and society and rely massively on **ICTs**.

••BLACKOUT

Imagine: A ransomware can infect computers of a major supplier of electric power, **blocking access** to their data and **shutting down** the industrial systems used for electricity distribution. The incident can result in a **huge blackout** shutting down all basic services.

Under the **NIS Directive**, as a major supplier of electricity, the company would be identified by its national authority as an operator of essential services. This means the company has to have in place **measures to prevent risks ensure security** of its network and information systems and **handle incidents**.

IF an incident nonetheless occurs, the electric power company has to **notify** it to its relevant **national authority**. Information sharing is key to receive support and to **prevent future incidents**. The company would also receive **operational assistance** from the national **Computer Security Incident Response Team** and thus be able to shorten the recovery time.

economic sectors to adopt effective risk mitigation and to report serious incidents to the national authorities.

The Directive aims to achieve a high standard of network and information systems security across the EU. It focuses primarily on regulating 'OES - operators of essential services' (transport, energy, banking, healthcare) and 'DSPs - digital service providers' (cloud services, online marketplaces and search engines), and was to be transposed into national law by 9 May 2018. For these organisations the NIS Directive highlights two primary obligations to ensure the continuity of essential services and avoid large-scale blackouts⁹:

1. to take appropriate technical and organisational measures to manage threats to networks and information systems
2. to notify the authorities 'without undue delay' of any significant security incident.

As it stands, the implementation of the NIS Directive is expected to lead to an overall increase in cybersecurity across those sectors that are considered vital for the economy and the state.

⁹ NIS Directive, recitals 47 and 49.

WHAT DOES THE NIS DIRECTIVE MEAN FOR THE EU CITIZENS?

The EU is reinforcing its cybersecurity so that everyone can enjoy greater safety and comfort, across all areas of our digital lives

AT WORK



AT HOME



ON THE MOVE



HOW?



GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.



COOPERATION

Increased EU-level cooperation

NATIONAL COMPUTER SECURITY
INCIDENT RESPONSE TEAM
(CSIRT)

NATIONAL NIS STRATEGY

NATIONAL NIS AUTHORITY

EU MEMBER STATES
COOPERATION GROUP
(STRATEGIC)

EMERGENCY TEAMS
(CSIRTS) NETWORK
(OPERATIONAL)

EU MEMBER STATES; EUROPEAN COMMISSION;
EUROPEAN UNION AGENCY FOR NETWORK AND
INFORMATION SECURITY

EU MEMBER STATES; CERT-EU; EUROPEAN
UNION AGENCY FOR NETWORK AND
INFORMATION SECURITY

Graphic: European Commission: What does the NIS Directive mean for the EU citizens? 2018

The NIS Directive requires all Member States to set up a national/governmental incident response team, the Computer Emergency Response Team (CERT). CERTs help governments protect critical information infrastructure and play a key role in coordinating incident management with the relevant stakeholders at national level. Thus, the directive sets out the responsibility of Member States not only to exchange information on cyber incidents at EU level but also to develop and implement appropriate national cybersecurity strategies and frameworks for the security of network and information systems.¹⁰

10 See Joint Communication (2017), 11.

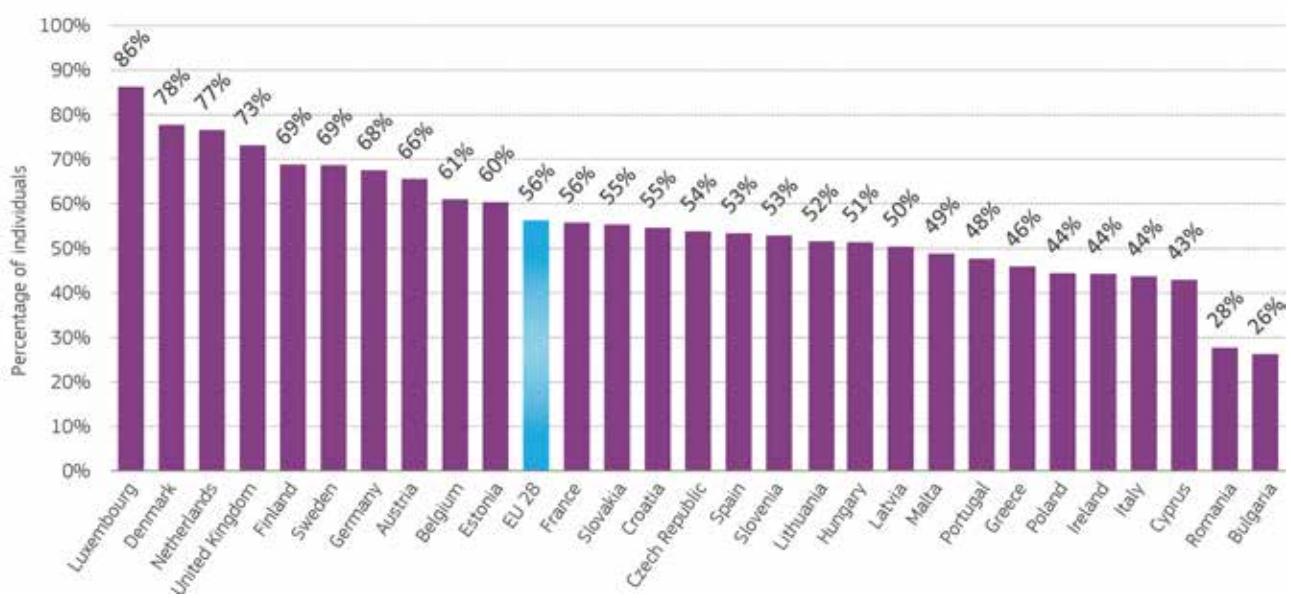
Conclusion

As the Joint Communication of 2017 states, EU cyber preparedness is central to both the digital single market and the security and defence union. Therefore the need for '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'¹¹ has been identified. This also requires effective deterrence, which means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers. It furthermore calls for close cooperation and coordination among EU Member States. Although all Member States have a cybersecurity strategy, the levels of maturity of adequate incident response capabilities vary among them¹² and the measures established do not fully overcome the fragmentation between individual Member States.

Finally, in order to effectively tackle the challenge posed by cyber-attacks, not only do proper deterrence and cybersecurity measures need to be in place, but resilient societies and systems are also particularly important. Besides all the technical developments and counter-strategies, this requires above all a high degree of self-awareness regarding this top security challenge of the 21st century, which needs to be jointly addressed by the EU and its Member States.

Basic digital skills in the EU

Graphic: Factsheet Tallinn Digital Market: Digital Skills in Europe. 2017



11 Ibid., 20.

12 ENISA, 'CSIRTs in Europe — ENISA', Topic, European Union Agency for Network and Information Security, accessed 20 September 2017, <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities?tab=details>.

1.6 Data protection and digital security in the cyber age

by Emese Savoia-Keleti

In today's cyber age, data protection is like a railway guard or conductor on a high-speed train of data flows, who is responsible for control and safety duties related to the actual operation of the train. This responsibility for protecting personal data plays a crucial role when it comes to cybersecurity. Safeguarding individuals' data and ensuring privacy are basic requirements and recognised as fundamental rights.

Introduction to cyber data security

The European Union lays an emphasis on the importance of a connected, open, stable and secure cyberspace, in which human rights, fundamental freedoms and the rule of law are fully respected and contribute to the social well-being, prosperity and integrity



of a democratic society. It should be stressed that cybersecurity is closely interlinked with human and fundamental rights, such as the rights to freedom of expression and the protection of personal data.

Cybersecurity encompasses all activities necessary to protect network and information systems and their users from cyber threats as outlined in a proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'). Thus cybersecurity also comprises the protection of personal data.

Ensuring security in cyberspace also involves taking precautions: avoiding, handling and mitigating security incidents. A data breach can be described as a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or misused by an unauthorised individual. If the data set contains personal information, it becomes a personal data breach, which needs to be dealt with by applying appropriate damage control measures, just like when following up on other cybersecurity incidents.

When referring to data protection, personal data is defined as information through which a natural person can be identified or made identifiable. This not only includes names or email addresses, but also medical records, search and driving habits, CVs and political interests as well as GPS location data. The combination of profession, organisation and country of origin could be considered personal data if those details could be used to identify the individual. Personal information can be used in ways we are not always aware of. Data protection may seem to be an abstract notion, but it is not as detached from our everyday lives as we think. Simply by using the internet, sending an email or connecting to social and professional network sites, we are disclosing personal data.

At work, too, data on employees and third parties is collected and traces can be tracked. Any EU institution, body, office or agency, or CSDP mission or operation, may process personal data when organising a meeting or conference or creating or updating a contact list, and would handle data in the course of a human resources or procurement procedure, as well as in a crisis situation.

The collection, processing, transmission and retention of personal data may entail certain privacy risks such as excessive data collection, the use of personal information for a purpose other than that originally specified, unauthorised access or even identity theft. Compliance with data protection rules is mandatory: the rules constitute an efficient tool for addressing and mitigating such risks.

European data protection for the digital era



Better protection for personal data

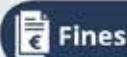


More opportunities for business



More consistent application and effective enforcement

- Individuals and businesses can have their cases dealt with by a data protection authority and a court close to them
- A one-stop shop for individuals and businesses in cross-border cases thanks to the cooperation of national data protection authorities



Fines



up to €20 million

OR



4% of global annual turnover



Council of the European Union
General Secretariat

© European Union, 2019
Reproduction is authorised, provided the source is acknowledged

Legal aspects

Data protection is never about prohibiting data handling; rather, it provides a framework to control what needs to be done in accordance with the applicable principles and rules. The right to the protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, which provides that '*everyone has the right to the protection of personal data concerning him or her*'. The European Convention on Human Rights also guarantees the right to respect for private and family life, home and correspondence. Accordingly, CSDP missions and operations are to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy and data protection with respect to the processing of personal data. This protection is to be guaranteed for staff employed by the CSDP missions and operations as well as for any third party.

General Data Protection Regulation

The General Data Protection Regulation (GDPR)¹, adopted on 27 April 2016, is applicable for EU Member States as of 25 May 2018. It also applies to organisations, authorities or companies not established in the EU which provide services or offer goods to individuals in the EU or monitor their behaviour, regardless of whether or not the processing takes place in the EU. The GDPR creates new rights for individuals in the digital sphere. Regulation (EC) No 45/2001 currently regulates the processing of personal data by EU institutions, bodies, offices and agencies. It is to be replaced by a new regulation before the end of 2018², aligned with the GDPR. The new regulation will reinforce the protection of personal data.

On the basis of Regulation (EC) No 45/2001, the High Representative of the Union for Foreign Affairs and Security Policy adopted a decision, on 8 December 2011, on the rules regarding data protection for the European External Action Service. Accordingly, the EEAS implements the necessary measures to protect personal data with regard to activities involving the collection, processing and retention of such data.

-
- 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – the General Data Protection Regulation (GDPR).
 - 2 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.



A new era for data protection in the EU

What changes after May 2018

The Facebook/Cambridge Analytica revelations show the EU has made the right choice to propose and carry out an ambitious data protection reform through the General Data Protection Regulation (GDPR).

The General Data Protection Regulation rules will apply as of 25 May 2018. They will bring several improvements to deal with data protection violations in the future:

CLEAR LANGUAGE	
TODAY	TOMORROW
Often businesses explain their privacy policies in lengthy and complicated terms	Privacy policies will have to be written in a clear, straightforward language

Graphic: European Commission

CSDP missions and operations

It must be highlighted that the abovementioned legal instruments do not apply to CSDP missions and operations. Article 2(2)(b) of Regulation (EU) 2016/679 (GDPR) provides that '[t]his Regulation does not apply to the processing of personal data: [...] (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU'. Moreover, Recital 15 of Regulation (EC) No 45/2001³ determines that '[w]here such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid

³ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union'. In addition, Recital 10a of the successor of Regulation (EC) No 45/2001 provides that '[t]his Regulation does not apply to the processing of personal data by missions referred to in Articles 42(1), 43 and 44 of the TEU, which implement the common security and defence policy. Where appropriate, relevant proposals should be put forward to further regulate the processing of personal data in the field of the common security and defence policy'. The Council has not yet adopted a decision laying down rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities pursuant to Article 39 of the Treaty on European Union.



Personal data must be processed fairly and lawfully.

Photo: EEAS DPO

However, data protection measures relevant for CSDP missions and operations have been introduced and are being implemented. Those measures are consistent with the data protection principles contained in the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union and the relevant European Union data protection legislation. They can be found in policy documents such as the Standard Operating Procedures (SOP) and the Guidelines on Data Protection, and they establish rules for the collection, handling and retention of personal data and include safeguards to protect the personal data of staff members and third parties. In fact, data protection measures relevant for CSDP missions and operations reflect the general data protection principles enshrined in the most modern legal instrument on data protection applicable for EU Member States – the GDPR.

Implementation

CSDP missions and operations need to collect, process and retain personal data – such as names, addresses, other identification details, location data or even sensitive information – of both staff and third parties on a daily basis. The protection of the right to privacy and consequently the protection of personal data are guaranteed by complying with the abovementioned data protection principles and basic requirements.

The overview table⁴ on data protection requirements provides a summary of the principles forming the backbone of data protection which are incorporated in the data protection legal framework, as described in guidance documents published by the European Data Protection Supervisor (EDPS). These requirements reflect the principles of Article 5 of the GDPR and are presented here with reference to point 4.1 of the EDPS guidelines on the protection of personal data in IT governance and IT management of EU institutions.

Lawfulness, legal grounds and data quality principles

Following these principles, and in the spirit of accountability, data controllers – i.e. entities that process personal data, such as missions and operations – must process personal data fairly and lawfully in accordance with one of the legal grounds, in particular where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the mission and operation. Other legal bases for processing may include its being necessary for compliance with a legal obligation, for the performance of a contract with the data subject or for protecting the vital interest of the data subject or another individual. The data subject can also consent to data processing.

A number of mission activities involve the collection and processing of personal data, e.g. recruitment, the payment of salaries or reimbursements, contractual arrangements with suppliers or the organisation of events. Accordingly, anyone processing personal data should verify whether the personal data is:

- fairly and lawfully processed for limited and explicit purposes
- adequate, relevant and not excessive
- accurate and kept up-to-date
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure and not transferred to third parties without adequate precautions.

Documenting personal data processes and providing information to data subjects

In order to demonstrate compliance and keep track of activities that involve personal data, all entities, including missions, need to record the processing of personal data. These records are simply descriptions of the activity. They are also important for fulfilling the obligation of informing data subjects. Providing information to the individuals

4 See table on page 69-page 70.

whose data is processed – whether mission staff or third parties – is compulsory, and it is done through ‘privacy statements’ or ‘data protection notices’.

Both the records and the privacy statements contain information on:

- the purpose of the processing
- who the data controller, the processor and the data protection focal point are
- the type of data being processed
- to whom data is disclosed, including recipients in third countries
- the legal basis on which data is processed
- how long the data is stored for
- what rights and recourse possibilities exist.

The records document and the privacy statement are compliance tools that help the controller, i.e. the mission, to demonstrate compliance according to the accountability principle.

Disclosure of data including third-country transfers

Personal data must not be disclosed to any unauthorised third party, whether orally or in writing, deliberately or accidentally. Unauthorised disclosure may be treated as a disciplinary matter. Accidental, unauthorised and unlawful disclosure must be reported immediately. When transferring personal data to entities in third countries, the controller should ensure that an adequate level of protection is provided.

Data security: confidentiality and integrity

The data controller ensures that there are adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of the individuals concerned. When transferring data, the controller needs to make sure that the recipient processes personal data solely for the purposes required in accordance with the relevant data security principles, in particular those on confidentiality and integrity.



The data controller ensures that technical and organisational measures are in place in order to:

- prevent any unauthorised person from gaining access to computer systems processing personal data and from using data-processing systems and transferring data, as well as to prevent any unauthorised reading, copying, alteration or removal of storage media, and any unauthorised disclosure, alteration or erasure of stored data;
- record which personal data have been communicated, when and to whom;
- ensure that authorised users of a data-processing system cannot access any personal data other than those for which they have access rights, that it is possible to check which personal data have been processed, when and by whom, and that personal data can only be processed on behalf of third parties upon the instruction of the controller;
- design the organisational structure in such a way that it meets the special requirements of data protection.

Rights of the data subject in addition to the right of information



In addition to the obligation to provide information to data subjects about the processing of personal data, the mission, as data controller, must also respect other data subject rights, such as the right to access, rectification, erasure and restriction of processing and the right to object to processing, in particular with regard to automated decision-making.

For the purpose of protecting the personal data of individuals in a CSDP mission, the mission – represented by the head of mission – is the data controller responsible for respecting data subject rights and for the management, integrity and confidentiality of personal data processed.

Conclusion

Cybersecurity, with a special emphasis on securing and safeguarding virtual personal data, is critical. We do not leave the house door open – we lock it to keep away any danger. The same applies to data processed in cyberspace. Data is not only personal but also vulnerable, and cyber-attacks are far from only being an issue for enterprises, governments and authorities. Individuals, both independently and as part of their organisations, can be the target of cyber-attacks. That is why preventive measures should be put in place, including for the protection of personal data. There are basic and well-known methods to protect data, such as changing passwords often, not opening

email attachments from unknown addresses, and having up-to-date antivirus, firewall and anti-malware systems. At the same time, it is an illusion to assume that zero risk can exist in cyberspace. Applying a precautionary approach to protecting personal data is therefore paramount, without limiting the opportunities offered by the web. These measures will reduce the risks, even if the only way to eliminate risk completely would be to go back to using typewriters. A guiding principle for data protection, as a user, is to treat other data subjects' rights and personal data with the same respect as we would like to see given to our own data.

Overview table on data protection principles and requirements based on Article 5 of GDPR (Ref. 4.1 of EDPS guidelines on IT governance and IT management of 23 March 2018, https://edps.europa.eu/data-protection/our-work/publications/guidelines/it-governance-and-it-management_en)

PRINCIPLE	REQUIREMENT
1. Lawfulness, fairness and transparency	<ul style="list-style-type: none"> Keeping transparency in mind when processing the personal data of data subjects (individuals whose data is being handled) Informing data subjects about the processing (purpose, identity of the controller, data processed, who has access (including third-country transfers), how long data is stored, the legal basis, and rights and recourse options) Making sure that a clear legal basis exists for the processing of personal data Respecting the rights of individuals to access and rectify their data, and developing procedures that clearly explain how data subjects can exercise their rights at each stage of data processing Informing data subjects if IT systems will handle their data manually or by automated means, and implementing functions in IT systems to respond to access, modification or blocking requests and to objections
2. Purpose limitation	<ul style="list-style-type: none"> Processing personal data only for specified explicit, legitimate and limited purposes Limiting the processing of data to its originally specified purpose Ensuring purpose limitation if different kinds of data are collected and processed for different purposes Adopting internal rules for the assessment of compatibility needs on a case-by-case basis to allow a change of purpose Communicating clearly to data subjects any change in the originally specified purpose of processing their personal data

PRINCIPLE	REQUIREMENT
3. Data minimisation	<ul style="list-style-type: none"> Ensuring that personal data is adequate, relevant and not excessive for the purpose Limiting categories of personal data chosen for processing to data collection that is directly relevant for the originally specified purposes Applying, if feasible, special privacy-enhancing technologies that allow excessive use of personal data to be avoided or enable the use of pseudonymised data
4. Accuracy	<ul style="list-style-type: none"> Ensuring that personal data is accurate and up-to-date Implementing processes to ensure and maintain the accuracy of processed data by checking the quality of information uploaded to the system before processing
5. Storage limitation	<ul style="list-style-type: none"> Keeping personal data for no longer than necessary for the originally specified purpose Determining retention time for data kept in a form which permits identification Ensuring that required retention periods are proportionate to the purposes of data collection and are limited in time. Separately assigning and managing retention times related to data collected for different purposes Designing IT system features to manage the retention time and perform the necessary subsequent actions: deletion or anonymisation
6. Integrity and confidentiality	<ul style="list-style-type: none"> Ensuring that personal data is secure Performing a security risk assessment and planning for mitigation measures Designing and implementing organisational and technical measures – based on risk assessment – to mitigate risks to a level that is acceptable, avoid processing operations for which mitigation would not be effective, and ensure that a clear decision is made by the responsible management on which risks are accepted and why. As data protection risks are related to the fundamental rights of others, externalisation of risks (insurance) is a less viable option than in other risk domains
7. Accountability	<ul style="list-style-type: none"> Making sure that compliance with the principles above can be demonstrated

Further reading

- EDPS
https://edps.europa.eu/data-protection_en
- DG JUST
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#relatedlinks
- GDPR
<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679>
- Regulation (EC) No 45/2001
<https://publications.europa.eu/en/publication-detail/-/publication/0177e751-7cb7-404b-98d8-79a564ddc629/language-en>
- Handbook on European Data Protection Law, European Union Agency for Fundamental Rights / Council of Europe, 2018
<http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>

2

Stakeholders

2.1 European Commission: the role of the European Commission in cyberspace

The European Commission helps to shape the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget. It also plays a significant role in supporting international development and delivering aid.

The European Commission develops and implements EU policies¹ by:

- proposing laws to the European Parliament and the Council of the European Union;
- helping EU countries implement EU legislation;
- managing the EU's budget and allocating funding;
- ensuring, together with the Court of Justice, that EU law is complied with;
- representing the EU outside Europe, together with the EU's diplomatic service, the European External Action Service.

Strategy and policy development²

European societies are increasingly dependent on electronic networks and information systems. In recent years, digital technology has become the backbone of our economy and a critical resource all economic sectors rely on. It now underpins the complex systems which keep our economies running in domains such as finance, health, energy and transport. Many business models are built on the uninterrupted availability of the internet and the smooth functioning of information systems.

Cybersecurity incidents, be they intentional or accidental, could disrupt the supply of essential services we take for granted, such as water or electricity. Threats can have different origins – from criminal, terrorist or state-sponsored attacks to natural disasters and accidents.

1 https://ec.europa.eu/info/about-european-commission/what-european-commission-does_en
2 For details, see Comprehensive assessment of EU security policy, SWD (2017) 278 final.

'Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.'

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017



The EU is already working on many of these issues. In 2013, the EU set out a Cybersecurity Strategy launching a series of key workstreams to improve cyber resilience³. Its main goals and principles – to foster a reliable, safe and open cyber ecosystem – remain valid.

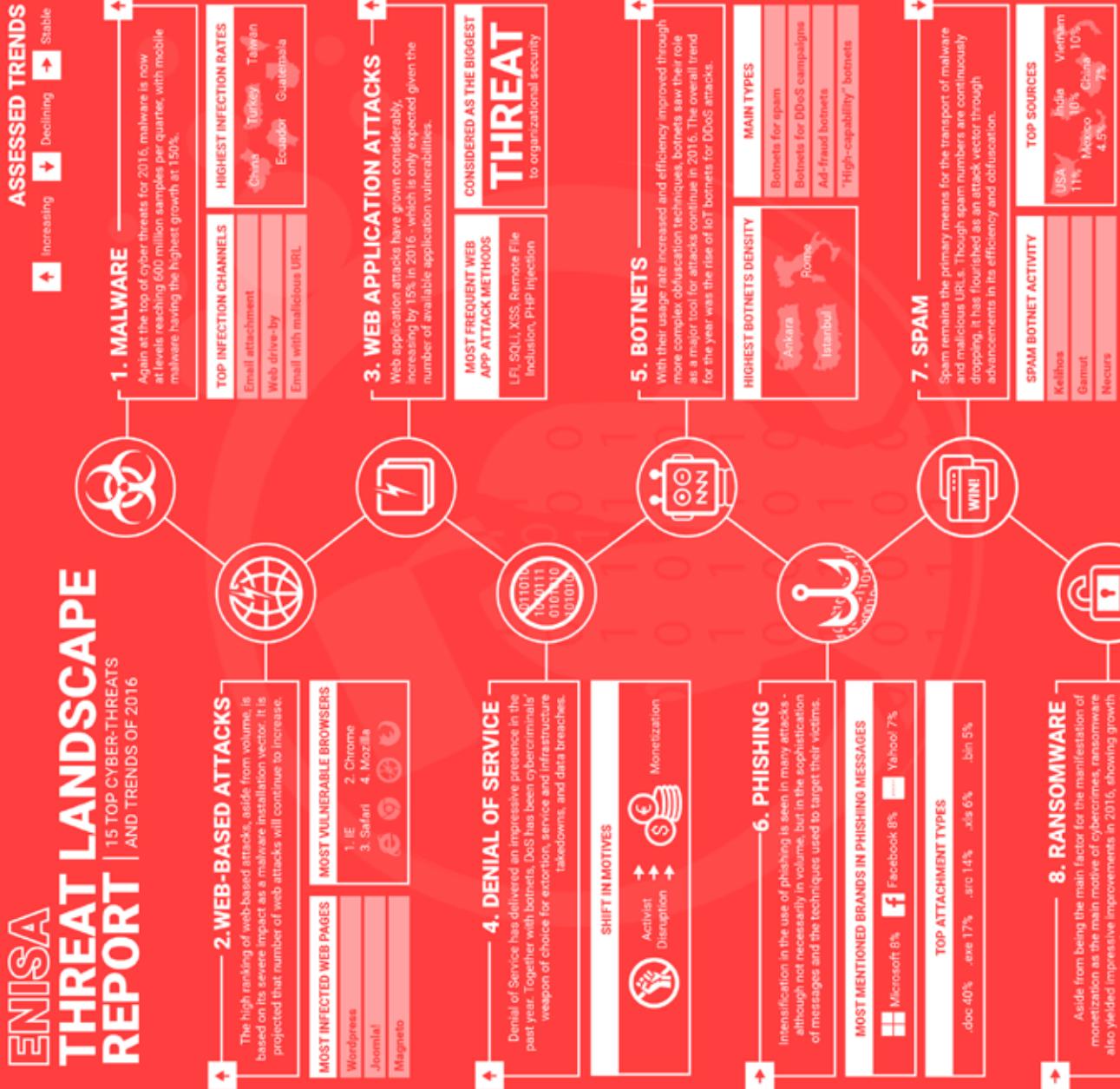
Since 2013, however, the technological and security landscape of the European Union has changed at a very fast pace. With digital technology now an integral part of our daily life, the Internet of Things revolution has become a reality, with tens of billions of devices expected to be connected to the internet by 2020. Unfortunately, the number and diversity of cyber threats is growing at the same time.

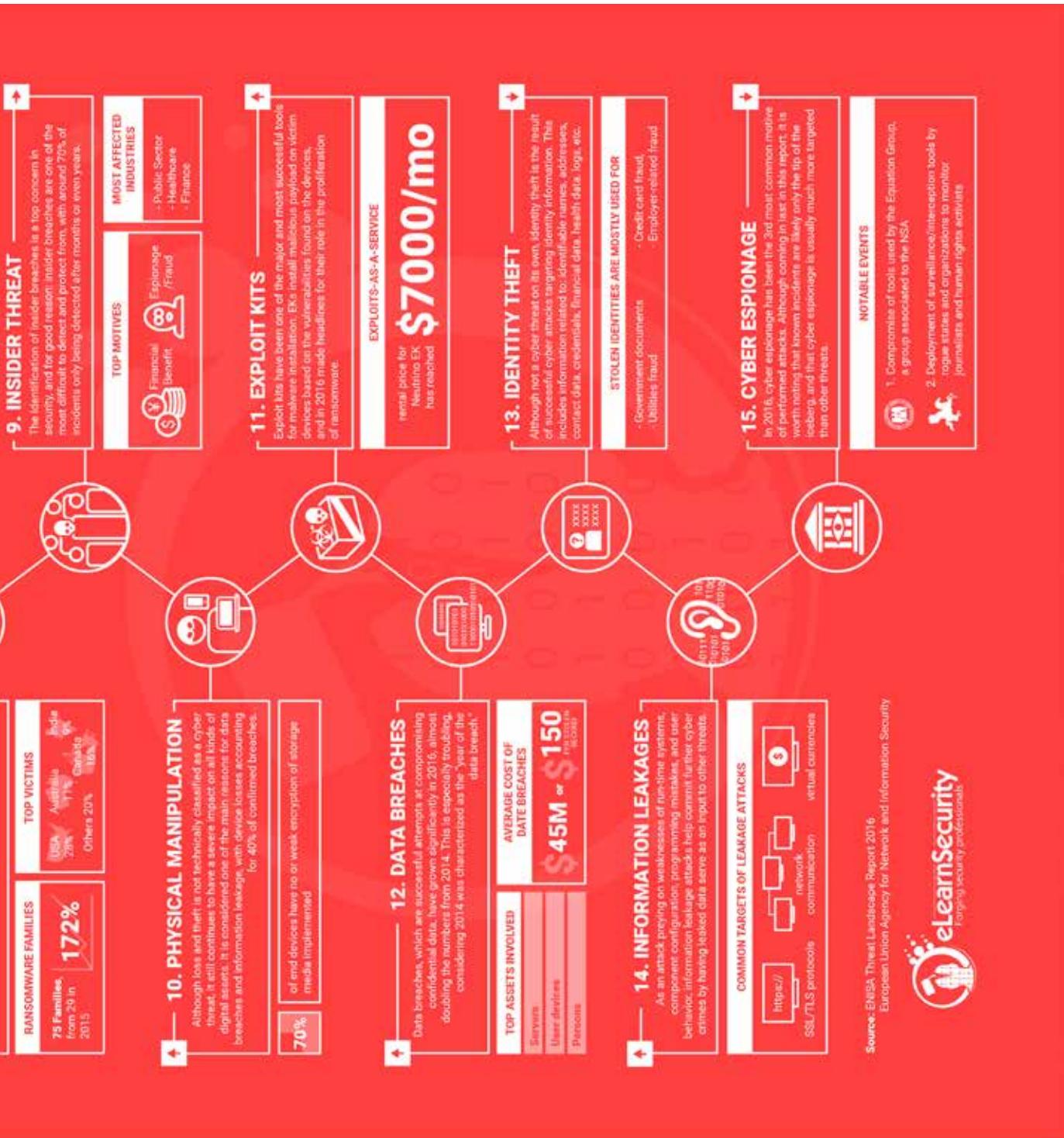
In the face of the recent ransomware attacks, a dramatic rise in cybercriminal activity, state actors increasingly using cyber tools to meet their geopolitical goals and the diversification of cybersecurity incidents, the EU needs to be more resilient to cyber-attacks and create effective cyber deterrence, including through criminal law, to better protect Europe's citizens, businesses and public institutions.

³ JOIN(2013) 1 final. An assessment of this strategy is available in SWD (2017) 295.

ENISA THREAT LANDSCAPE REPORT

15 TOP CYBER-THREATS
AND TRENDS OF 2016





Faced with these new challenges, and building on the approaches of the digital single market, the Global Strategy, the European Security Agenda⁴, the Joint Framework on countering hybrid threats⁵ and the Communication on Launching the European Defence Fund⁶, in September 2017, the Commission and the High Representative proposed a wide-ranging package of cybersecurity proposals based around three pillars:

- building EU resilience to cyber-attacks and stepping up the EU's cybersecurity capacity;
- creating an effective criminal law response;
- strengthening global stability through international cooperation.

The package included proposals to:

- establish a stronger European Union Cybersecurity Agency built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks;
- create an EU-wide cybersecurity certification scheme that will increase the cybersecurity of products and services in the digital world;
- develop a blueprint for how to respond quickly and in unison when a large-scale cyber-attack occurs;
- set up a network of competence centres in the Member States and a European Cybersecurity Research and Competence Centre that will help develop and roll out the tools and technology needed to keep up with ever-changing threat possibilities and make sure our defence is as strong as possible;
- adopt the new Directive on combating fraud and counterfeiting of non-cash means of payment to provide for a more efficient criminal law response to cybercrime;
- use the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and other measures to strengthen international cooperation on cybersecurity, including by deepening the cooperation between the EU and NATO;
- drive high-end skills development for civilian and military professionals by providing solutions and templates for digital training at national level and setting up a cyber-defence training and education platform.

⁴ COM(2015) 185 final.

⁵ JOIN(2016) 18 final.

⁶ COM(2017) 295.

⁷ 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).

 <p>A European Union Cybersecurity Agency to assist Member States in dealing with cyber-attacks.</p>	 <p>An EU-wide certification framework to ensure that products and services are cyber secure.</p>
 <p>A Blueprint for how to respond quickly, operationally and in unison when a large scale cyber-attack strikes.</p>	 <p>A network of competence centres in the Member States and a European Cybersecurity Research and Competence Centre to help develop and roll out the tools and technology needed to keep up with an ever-changing threat.</p>
 <p>A new Directive to combat fraud and counterfeiting of non-cash means of payment.</p>	 <p>Measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO.</p>

EU resilience to cyber-attacks.

Graphic: European Commission

Since September 2017, a number of other legislative proposals have been adopted by the Commission.

To further support the deterrence objective of the EU cybersecurity strategy, in April 2018, the Commission proposed new rules to make it easier and faster for police and judicial authorities to obtain the **electronic evidence** (such as emails or documents located in the cloud) that they need to investigate, prosecute and convict criminals and terrorists. The new rules will allow law enforcement authorities in EU Member States to track down leads online and across borders more effectively, while providing sufficient safeguards for the rights and freedoms of all concerned.

Most recently, in September 2018, building on the ambitious cybersecurity initiatives announced in 2017, the European Commission proposed the creation of a **Network of Cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence Centre** to invest in stronger and pioneering cybersecurity in the EU.



STATE OF THE UNION | 2018

Building a strong cybersecurity in Europe: A European Cybersecurity Competence Network & Centre



Ensure long-term strategic cooperation between Industries, research communities and governments



Pool, share and ensure access to existing expertise



Co-Invest and share costly infrastructure



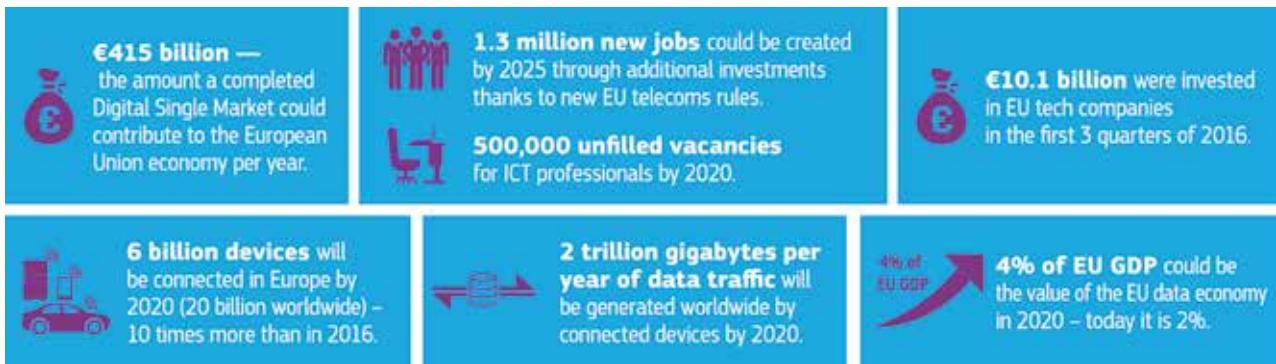
Help deploy EU cybersecurity products and solutions

#SOTEU



Graphic: European Commission

The mission of this proposal is to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to keep its digital single market secure. This goes hand in hand with the key objective of increasing the competitiveness of the EU's cybersecurity industry and turning cybersecurity into a competitive advantage of other European industries.

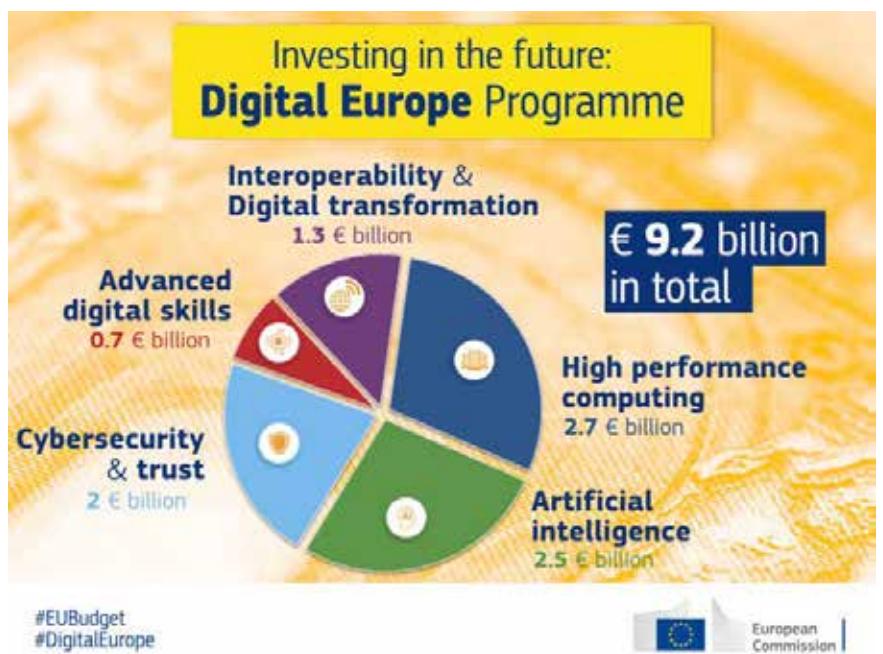


Graphic: European Commission

Benefits of the digital single market.

By managing cybersecurity funds under the next multiannual financial framework (2021-2027), this initiative will help to create a cybersecurity industrial and research ecosystem that is interconnected and Europe-wide. It should encourage better

cooperation between relevant stakeholders (including between civilian and defence cybersecurity sectors) to make the best use of existing cybersecurity resources and expertise throughout Europe – including those of the more than 660 cybersecurity expertise centres across all the Member States that responded to a recent survey conducted by the European Commission.

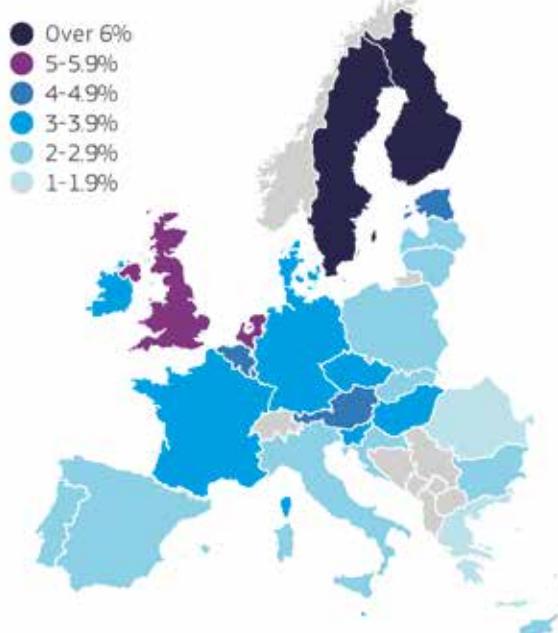


New Digital Europe
Programme brings
EUR 9.2 billion investment
between 2021-2027.

The initiative should also help the EU and Member States take a proactive, longer-term and strategic approach to cybersecurity industrial policy that goes beyond research and development. This approach should not only help stakeholders to come up with breakthrough solutions to the cybersecurity challenges faced by the private and public sectors, but also support the effective deployment of these solutions.

Furthermore, the Commission's proposal will allow relevant research and industrial communities, as well as public authorities, to gain access to key services such as testing and experimentation facilities, which are often beyond the reach of individual Member States due to insufficient financial and human resources. It will also contribute to closing the skills gap and to avoiding brain drain, by ensuring that those individuals with the most talent have access to large-scale European cybersecurity research and innovation projects, thereby providing interesting professional challenges.

ICT specialists in the workforce



The untapped potential



Today, **40%** of companies have difficulties finding ICT specialists



There will be **500,000 unfilled vacancies** for ICT professionals **by 2020**

Graphic: European Commission

Support for implementation of EU legislation

The Commission is already helping to reinforce the EU's deterrence of and resilience and response to cyber-attacks, including by supporting the effective implementation of the first EU cybersecurity law: the **Directive on Security of Network and Information Systems (NIS Directive)**.

Over the past few years, the European Commission has adopted a series of measures to raise Europe's preparedness to ward off cyber incidents. The adoption of the NIS Directive was a key step towards building European-level cybersecurity resilience. The Directive was adopted in July 2016; Member States had until May 2018 to transpose it into their national laws and six months more to identify operators of essential services. Its objective is to ensure that network and information systems within the EU have a high common level of security.

The four cornerstones of the NIS Directive are:

- *Improving national cybersecurity capabilities* – Member States will be required to adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures to be implemented in relation to cybersecurity. Member States will also be required to designate both a national competent authority for the implementation and enforcement of the Directive, and one or

more computer security incident response teams (CSIRTs) responsible for handling incidents and risks.

- *Improving cooperation* – The Directive creates a ‘Cooperation Group’, composed of representatives of the Member States, the Commission and the EU Agency for Network and Information Security (ENISA), to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence. The Commission provides the secretariat for the Cooperation Group. Similarly, the CSIRTs from the various Member States together form the CSIRTs Network, whose task is to promote swift and effective operational cooperation on specific cybersecurity incidents and share information about risks. ENISA provides the secretariat for the CSIRTs network.
- *Security and notification requirements for operators of essential services* – Businesses with an important role in society and the economy, referred to in the Directive as ‘operators of essential services’, will have to take appropriate security measures and report serious incidents to the relevant national authority⁸.
- *Security and notification requirements for digital service providers* – Important digital businesses, referred to in the Directive as ‘digital service providers’ (DSPs), will also be required to take appropriate security measures and report serious incidents to the competent authority. The Directive will cover the providers of the following services: online marketplaces, cloud computing services, and search engines.

In the field of deterrence, the Commission is also working to ensure full implementation of **Directive 2013/40/EU on attacks against information systems**⁹. The objectives of this Directive are to subject attacks on information systems in all Member States to effective, proportionate and dissuasive criminal penalties, and to improve and encourage cooperation between judicial and other competent authorities. For that purpose, the Directive establishes minimum rules concerning the definition of criminal offences and the relevant sanctions, and obliges Member States to establish a network of national operational points of contact.

8 The NIS Directive covers the following sectors: energy – electricity, oil and gas; transport – air, rail, water and road; banking – credit institutions; financial market infrastructures – trading venues and central counterparties; health – healthcare providers; water – drinking water supply and distribution; digital infrastructure – internet exchange points (which enable interconnection between the internet’s individual networks), domain name system service providers and top-level domain name registries.

9 Replacing Council Framework Decision 2005/222/JHA.

EU funding¹⁰

EU financial support in the field of cybersecurity focuses on three main strands: research and innovation, infrastructure, and capacity building in third countries.

Research and innovation

Between 2014 and 2016, the EU invested **EUR 160 million** (in cybersecurity research and innovation projects) under the **Horizon 2020 Research and Innovation Framework Programme**.

The EU will also invest up to **EUR 450 million** of Horizon 2020 funding in cybersecurity research and innovation under the **contractual Public Private Partnership on Cyber-security** for the period 2017-2020. This partnership was signed in July 2016 by the Commission and the European Cyber Security Organisation (ECSO)¹¹, as one of the 16 initiatives put forward in the Commission's Digital Single Market Strategy. Its goal is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, by building trust between Member States and industrial actors, and by helping align supply and demand for cybersecurity products



10 For details, see Comprehensive assessment of EU security policy, SWD (2017) 278 final.

11 The ECSO is a fully self-financed not-for-profit association (ASBL) under Belgian law. It was launched on 13 June 2016 in Brussels and became a legal counterpart for the contractual PPP in July 2016. Since its launch, more than 190 members have joined the organisation, including large European and global companies, SMEs and start-ups, research centres, universities, clusters and associations, and local, regional and national administrations.

and solutions. It aims to gather industrial and public resources to deliver excellence in research and innovation and maximise the use of available funds through greater coordination with Member States and regions. Cybersecurity market players are expected to invest three times the amount already invested in the partnership by the EU, bringing the total investment to EUR 1.8 billion.

Cybersecurity and privacy form part of two strands of the Horizon 2020 programme. Under the societal challenge '**Secure societies – Protecting freedom and security of Europe and its citizens**', the two relevant strands are the **Digital Security** strand and the **Fighting Crime and Terrorism** strand.

The **Digital Security** strand focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, and supporting the creation of lead markets and market incentives in Europe. Security is also a 'digital focus area' under other Challenges (privacy and security in e-health; energy; transport; innovative security solutions for public administrations). The aim is to ensure the integration of digital security into these application domains.

The **Fighting Crime and Terrorism** strand focuses on increasing knowledge of the cybercrime phenomenon: its specific characteristics, the cybercrime economy (including unlawful markets and use of virtual currencies) and the ways in which law-enforcement authorities can fight it more efficiently and prosecute offenders with more solid evidence from specialised forensic activities.

Projects on dedicated digital security building blocks (such as the 2014 calls for proposals on cryptography and security-by-design) are funded under the **Leadership in Enabling and Industrial Technologies** strand. Security is also integrated as a functional requirement in specific technologies, such as the Internet of Things, 5G, the cloud, etc.

Infrastructure

EU funding is also available for infrastructure projects. For the 2014-2020 period, the **European Structural and Investment (ESI)** funds provide for a contribution of up to **EUR 400 million** for investments in trust and cybersecurity. The ESI funds can finance security and data protection investments to enhance interoperability and interconnection of digital infrastructures, electronic identification, and privacy and trust services.

Cybersecurity is one of the areas supported under the Digital Service Infrastructures (DSIs) stream within the **Connecting Europe Facility (CEF)**. The funded projects deploy trans-European digital services based on solutions such as e-identification and interoperable health services. One of the aims is to achieve cross-border cooperation

in cybersecurity, enhancing security and thus also trust in cross-border electronic communication, and thereby contributing to the creation of the digital single market.

In 2014-2016, the EU invested about EUR 20 million in such projects; an additional investment of EUR 12 million is earmarked for a call for proposals due to open in May 2017.

Cybercrime projects

The Commission supports the fight against cybercrime by funding cybercrime projects through tools such as the Internal Security Fund (ISF), the successor to the Specific Programme 'Prevention of and Fight against Crime' (ISEC), for the period 2014-2020. This fund has a total budget of just over EUR 1 billion available for funding actions under its Police instrument, including the fight against cybercrime. Concrete actions to be funded through this instrument include setting up and running IT systems, acquiring operational equipment, promoting and developing training schemes, and ensuring administrative and operational coordination and cooperation.



Graphic: European Commission

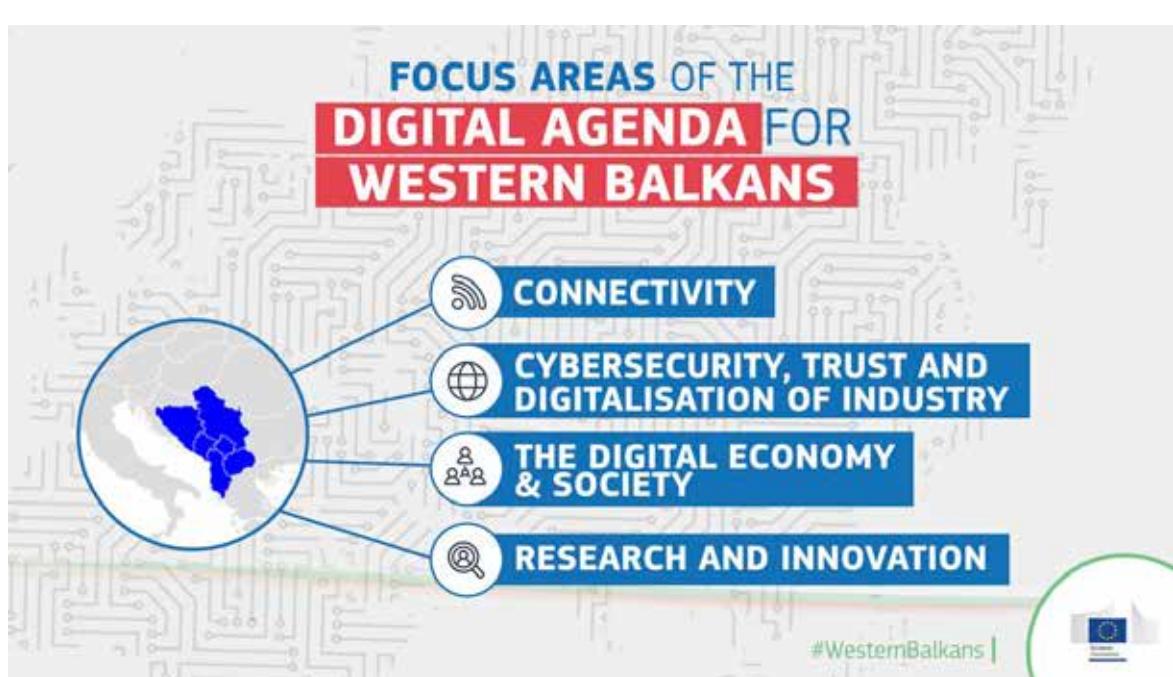
Capacity building in third countries

The Commission has also launched capacity building initiatives in third countries, recognising the strong link between increased cyber resilience and sustainable development. The objectives of these initiatives are to increase third countries' technical capabilities and preparedness and establish effective legal frameworks to address cyber-crime and cybersecurity problems, while at the same time enhancing their capacity for effective international cooperation in these areas. The Commission has partnered with the Council of Europe and EU Member States for the implementation of these actions.

At a global and trans-regional level, these initiatives are financed by the **Instrument contributing to Stability and Peace (IcSP)**. Cybersecurity and combating cybercrime have been identified as areas of priority for this instrument since 2013, with an allocation of EUR 4.5 million for 2013, and an indicative allocation of EUR 21.5 million over the period 2014-2017. This includes EUR 9 million for the GLACY+ project run by the Council of Europe (in partnership with INTERPOL) between 1 March 2016 and 27 February 2020,

which aims to strengthen the capacities of states worldwide to apply legislation on cybercrime and electronic evidence and enhance their ability to engage in effective international cooperation in this area.

The Commission has also used other instruments to support specific regions. For example, it has used the **European Neighbourhood Instrument (ENI)** to help Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) to set out strategic priorities related to the fight against cybercrime. The Instrument for Pre-accession Assistance (IPA) will provide EUR 5 million for the CyberProceeds@IPA project run by the Council of Europe between 15 December 2015 and 14 June 2019, which aims to strengthen the capacity of authorities in south-eastern Europe and Turkey to search, seize and confiscate cybercrime proceeds and prevent money laundering on the internet. More actions are set to be rolled out in these areas in the coming years, some of them through other financing instruments¹².



Graphic: European Commission

International cooperation

Coordinated EU action at international level in the field of cybersecurity is ensured by the European External Action Service (EEAS) and Commission services, together with the Member States. Through this action, they seek to uphold EU core values and

12 For details, see Comprehensive assessment of EU security policy, SWD (2017) 278 final, p. 7.

promote the peaceful, open and transparent use of cyber technologies. The HR, the Commission and the Member States engage in policy dialogue with international partners and with international organisations such as the Council of Europe, the Organisation for Economic Cooperation and Development (OECD), the Organisation for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organisation (NATO) and the United Nations (UN).

The EEAS and Commission services, in close cooperation with the Member States, also establish links and dialogues on international cyber policy, security of information and communication technologies with key strategic partners such as Brazil, China, India, Japan, the Republic of Korea and the United States.

Operational cooperation and capabilities

Many EU organisations have started to include a cybersecurity perspective in their policies and/or operations. The European Commission itself has no operational capabilities¹³, but the EU has specialised agencies and capabilities at its disposal to support its action on cybersecurity, including ENISA, the European Cyber Crime Centre (EC3) at Europol and the Computer Emergency Response Team (CERT-EU), which will be presented later.

A number of instruments have already been put in place to mainstream cybersecurity issues at EU level, covering:

- horizontal legislation
- sectoral policy initiatives (e.g. in the energy and transport field)
- international relations
- research and innovation
- EU agencies and bodies.

The most important of these have been presented above.

As a consequence, many organisations in the EU ecosystem are involved in cybersecurity and some are gaining expertise in this area. Within the European Commission, two main directorates-general are tasked with addressing cybersecurity and cybercrime

13 This overview is based on open sources and SWD(2017) 500 final, part 1/6, Impact Assessment, accompanying the proposal for a Regulation on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), pp. 35-38.

(DG CONNECT and DG HOME), while at least eight have launched initiatives at sectoral level. The EEAS, which manages the EU's diplomatic relations with countries outside the EU and conducts the Common Foreign and Security Policy, handles cyber defence insofar as it relates to state activities and multinational or multilateral organisations (UN, NATO, OECD, etc.).

Below are some of the Commission departments involved in cybersecurity:

The Directorate-General for Communications Networks, Content and Technology (DG CONNECT) is the Commission department responsible for developing a digital single market to generate smart, sustainable and inclusive growth in Europe. It manages policy, regulation and research in the area of information and communication technology, and specifically cybersecurity (with a focus on cybersecurity resilience). It also supports the transposition and implementation of the NIS Directive and the implementation of funding under Horizon 2020 and the Connecting Europe Facility (see EU funding section above for details).

The Directorate-General for Migration and Home Affairs (DG HOME) aims to build an open and safer Europe, so that all activities necessary and beneficial to the economic, cultural and social growth of the EU can develop in a stable, lawful and secure environment. In particular, in the field of cybersecurity, DG HOME focuses on:

- developing and implementing policies against cybercrime, including aspects of criminal law;
- reducing vulnerabilities;
- dealing with (criminal) threat alerts;
- raising awareness;
- providing ransomware-prevention advice;
- dealing with issues related to deterring and investigating cybercrime, as well as the judicial follow-up.

The Directorate-General for Energy (DG ENER)¹⁴ focuses on developing and implementing policies that deliver secure, sustainable and competitive energy for Europe.

The Joint Research Centre (JRC) provides independent scientific evidence, advice and support throughout the whole EU policy cycle. DG JRC's activities also cover the energy and cybersecurity sectors.

14 <https://ec.europa.eu/energy>

The **Directorate-General for Mobility and Transport (DG MOVE)**¹⁵ works together with Member States and stakeholders to address a vast array of transport policies. Cybersecurity and cyber resilience with regard to different modes of transport – air, land (rail and road) and maritime – are emerging issues in this field.

The **Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA)**¹⁶ is in charge of initiating and implementing EU policy in the area of financial services, including banking and finance. As such, DG FISMA is also tasked with presenting sector-specific legislative initiatives, some of which address cybersecurity. Specifically, DG FISMA works on payment security and on the implementation of the financial acquis, which also covers other cybersecurity aspects strictly related to financial services.

The **Directorate-General for the Internal Market, Industry, Entrepreneurship and SMEs (DG GROW)** is responsible for completing the internal market for goods and services and helping turn the EU into a smart, sustainable, and inclusive economy by implementing the industrial and sectoral policies of the flagship Europe 2020 initiative. It also aims to foster entrepreneurship and growth by reducing the administrative burden on small businesses, facilitating access to funding for small and medium-sized enterprises (SMEs) and supporting access to global markets for EU companies.

As far as EU agencies and bodies are concerned, four main actors deal with cybersecurity, cybercrime and cyber defence: ENISA, CERT-EU, the European Defence Agency (EDA) and EC3. These bodies will be presented in detail in the following chapters. There are also at least a further four that are gaining experience in cybersecurity in sectors like energy, transport and finance¹⁷.

Increased cooperation and a more coordinated approach between the EU institutions, agencies and bodies is needed to unite their efforts and increase the effectiveness and efficiency of their contribution to the EU's overall cyber resilience.

15 http://ec.europa.eu/transport/index_en.htm

16 <http://ec.europa.eu/dgs/finance/>

17 European Agency for the Cooperation of Energy Regulators (ACER), European Aviation Safety Agency (EASA), European Union Agency for Railways (ERA), European Banking Authority (EBA), European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA), For more details, see Annex 9 (mentioned above).

SINCE MAY



Since **2015**, new VAT rules in force to clarify and simplify **VAT collection on e-services sold online**.



Cross-border sales of e-services has become easier for small businesses.



2015, EU DECISION-MAKERS HAVE ACHIEVED THE FOLLOWING



As of **May 2015**, a new single set of EU rules on the protection of personal data will apply, ensuring that personal data can flow freely across Europe while being protected by the highest standards.

First vouchers will be granted to the local communities already in few months' time. By 2020, at least 6000 to 8000 local communities will be able to benefit from the funding.



The action plan seeks to simplify the life of citizens and businesses by ensuring public registers are connected and by accelerating the transition to e-procurement and e-signatures.



Thanks to the new rules, EU citizens will know and control which personal data are published and there will be clear limits to the use of these data. Through a complaint and sanction mechanism, citizens will be better protected whenever their data is hacked or disclosed. Businesses will benefit from more legal certainty and a single set of rules: one single supervisory authority or one authorisation procedure. This makes things simpler and cheaper so that the data economy can flourish.



As of **2020**, EU Member States will for the first time coordinate their use of the **high-quality band 700 MHz**.



This will enable **5G** networks and bring new services such as connected cars, remote health care, smart cities or video streaming on the move and across borders.

As of **May 2018**, the EU will be equipped with its first ever **common cybersecurity law (the Network Information Security Directive)** to help keep network and information systems safe in all Member States.



As of **early 2018**, citizens will be able to enjoy their **online films, sports broadcasts, music, video games, and e-book subscriptions** when travelling in the EU.



On **15 June 2017**, mobile roaming charges were finally abolished in the EU.



After 15 June 2017, twice as many travellers used their mobile data or made voice calls abroad as often as at home than during the months before 31% vs. 15% for data, 24% versus 11% for calls.

2.2 European Defence Agency: cyber defence capability development

by Jorge Domecq



Set up in 2004 as an agency of the Council of the European Union, the European Defence Agency (EDA) supports its 27 Member States - all EU countries except Denmark - in improving their defence capabilities through European cooperation. The EDA has become the hub for European defence cooperation with expertise and networks allowing it to cover the whole spectrum: from harmonising requirements to delivering operational capabilities;

from research and innovation to developing technology demonstrators; from training and exercises to maintenance and support for CSDP operations. It also works towards strengthening the European defence industry and acts as a facilitator and interface between Member States' military stakeholders and wider EU policies with an impact on defence.

EDA's annual conference in 2017 dealt with 'Security in the digital age: the added value of European cooperation'. In the picture: EDA's Chief Executive Jorge Domecq opening the conference.



Photo: European Defence Agency

The mission

In May 2017, Member States agreed to further reinforce the agency's mission as:

- the **main intergovernmental prioritisation instrument** at EU level in support of defence capability development;
- the **preferred cooperation forum and management support structure** at EU level for participating Member States to engage in technology and capability development activities;
- the **interface** coordinating military views in wider EU policies to the benefit of the defence community and a **central operator** with regard to EU-funded defence-related activities.

The mandate

In 2013 the European Council approved the EU **Cybersecurity Strategy: An Open, Safe and Secure Cyberspace**. Among other things, it called for an assessment of operational EU cyber-defence requirements and the development of EU cyber-defence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability. The strategy led to the EU **Cyber Defence Policy Framework**. The Council conclusions on the development and implementation of the strategy proposed 43 different work strands and the EDA was given responsibilities in:

- supporting the development of Member States' cyber-defence capabilities related to the Common Security and Defence Policy;
- promoting civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector;
- raising awareness through improved training, education and exercise opportunities for the Member States;
- cooperating with relevant international partners, notably with NATO, as appropriate.

The strategy identifies the EU Military Staff (EUMS) and the European Security and Defence College (ESDC) as coordination partners, and it also encourages closer coordination and cooperation between the Agency and the European Network and Information Security Agency (ENISA), Computer Emergency Response Team (CERT EU) and the European Cyber Crime Centre (EC3). The EDA also works in close cooperation with the European External Action Service (EEAS), the European Commission and the relevant EU agencies and bodies, as well as liaising closely with NATO and its Cooperative Cyber Defence Centre of Excellence (CCDCOE).

The Capability Development Plan

The EDA's and Member States' main prioritisation tool is the Capability Development Plan (CDP), which is updated regularly (last revision: June 2018) and serves as a key reference for cooperative projects and programmes funded by the EU and Member States. In the cyber-defence domain, the CDP puts the focus on:

- supporting Member States in building a skilled military cyber-defence workforce;
- ensuring the availability of proactive and reactive cyber-defence technology;
- enabling cross-cutting activities in other domains and with other organisations.

The Agency works with Member States on these priorities by:

- agreeing on a strategic context case that outlines the capability landscape, and by detailing the programme to be conducted by the Cyber Defence Project Team and the Ad Hoc Working Group (AHWG) for Cyber Defence Research and Technology;
- engaging with other stakeholders at EU and extra-EU level (for instance NATO, within the remit of the 2016 EU/NATO Joint Declaration);
- promoting collaboration between Member States either by using internal project management vehicles or by supporting the definition of permanent structured cooperation (PESCO) projects;
- using its own operational budget to promote coordination and research studies in support of Member States' capability development.

The capability projects

Capability projects are initiated and conducted under the direction and guidance of Member States within the EDA's Cyber Defence Project Team. Examples:

Cyber Ranges Federation

Increased mutual availability of virtual cyber defence training and exercise ranges (Cyber Ranges) for national cyber defence specialists' training is an emerging need for many Member States. These ranges are multi-purpose environments supporting three primary processes: knowledge development, assurance and dissemination.



2018 EU CAPABILITY DEVELOPMENT PRIORITIES

Based on the identified trends and information gathered from Member States and the EU Military Committee, a set of EU Capability Development Priorities was proposed by EDA and approved by Member States. On the one hand, they address main capability shortfalls for deployed operations (land, maritime and air capabilities as well as logistic and medical support) with a reinforced focus on high-end warfare. On the other hand, they also cover other focus areas of Member States, such as the adaptation of military capabilities required for territorial defence and security or cyber defence, as required by the EU Global Strategy published in 2016.



Enabling capabilities for cyber responsive operation

- » Cyber cooperation and synergies;
- » Cyber R&T;
- » Systems engineering framework for cyber operations;
- » Cyber education and training;
- » Specific cyber defence challenges in the air, space, maritime and land domain.



Space-based information and communication services

- » Earth observation;
- » Positioning, navigation and timing;
- » Space situational awareness;
- » Satellite communication.



Information superiority

- » Radio spectrum management;
- » Tactical CIS;
- » Information management;
- » Intelligence, Surveillance and Reconnaissance (ISR) capabilities.



Ground combat capabilities

- » Upgrade, modernise and develop land platforms (manned/unmanned vehicles, precision strike);
- » Enhance protection of forces. (CBRN, CIED, individual soldier equipment).



Enhanced logistic and medical supporting capabilities

- » Military mobility;
- » Enhanced logistics;
- » Medical support.



Naval manoeuvrability

- » Maritime situational awareness;
- » Surface superiority;
- » Power projection.



Underwater control contributing to resilience at sea

- » Mine warfare;
- » Anti-submarine warfare;
- » Harbour protection.



Air superiority

- » Air combat capability;
- » Air ISR platforms;
- » Anti-Access Area Denial (A2/AD) capability;
- » Air-to-air refuelling;
- » Ballistic Missile Defence (BMD).



Air mobility

- » Strategic air transport;
- » Tactical air transport including air medical evacuation.



Integration of military air capabilities in a changing aviation sector

- » Military access to airspace;
- » Ability to protect confidentiality of mission critical information;
- » Coordination with civilian aviation authorities;
- » Adaptation of military air/space C2 capability.



Cross-domain capabilities contributing to achieve EU's level of ambition

- » Innovative technologies for enhanced future military capabilities;
- » Autonomous EU capacity to test and to qualify EU developed capabilities;
- » Enabling capabilities to operate autonomously within EU's LoA.

Last update: 28 June 2018

The Cyber Ranges Federation project aims **to create a federation of ranges**, with the intention of leveraging three complementary functionality packages: Cyber Training & Exercise Range, Cyber Research Range as well as Cyber Simulation & Test Range functionalities.

Training & exercises

Following a structured cyber-defence training need analysis, **the EDA develops, pilots and delivers a variety of cybersecurity courses** from basic awareness to expert level.

The Cyber Defence Training & Exercises Coordination Platform (CD TEXP) is a project intended to facilitate the pooling and sharing of training and exercises at European level, building on an EDA-developed collaborative platform.

The Senior Decision Maker's Course was developed and consolidated in 2017. Its objective is to enhance senior decision makers' knowledge and understanding with respect to their roles and responsibilities in the cybersecurity and defence domains, in order to equip them with what is needed to assume their responsibilities with regard to cyber defence aspects in the context of EU Common Security and Defence Policy (CSDP) military crisis management operations (CMOs).

Based on an EDA feasibility study, a Cyber Education, Training and Exercise Platform has been established within the framework of the European Security and Defence College (ESDC). This platform will act as a virtual coordination platform linking and coordinating existing and emerging cyber training facilities in EU Member States.

The research and technology projects

Research and technology (R&T) projects are initiated and conducted by Member States within an EDA Ad Hoc Working Group and include the following:

Cyber Defence Strategic Research Agenda (CSRA)

Cybersecurity technologies are relevant to both the civil and the military domain ('dual-use'). Considering ongoing and future civil research, for example within the EU research framework programmes, and the high resilience required in defence, it will be crucial to precisely target R&T efforts on specific military aspects.

Cyber situation awareness

The aim of the deployable Cyber Situation Awareness Package (CySAP) for the headquarters project is to integrate information originating from various sources and to provide a common and standardised cyber-defence planning and management platform, that allows commanders and their staff to perform cyber-defence-related tasks in their day-to-day business.

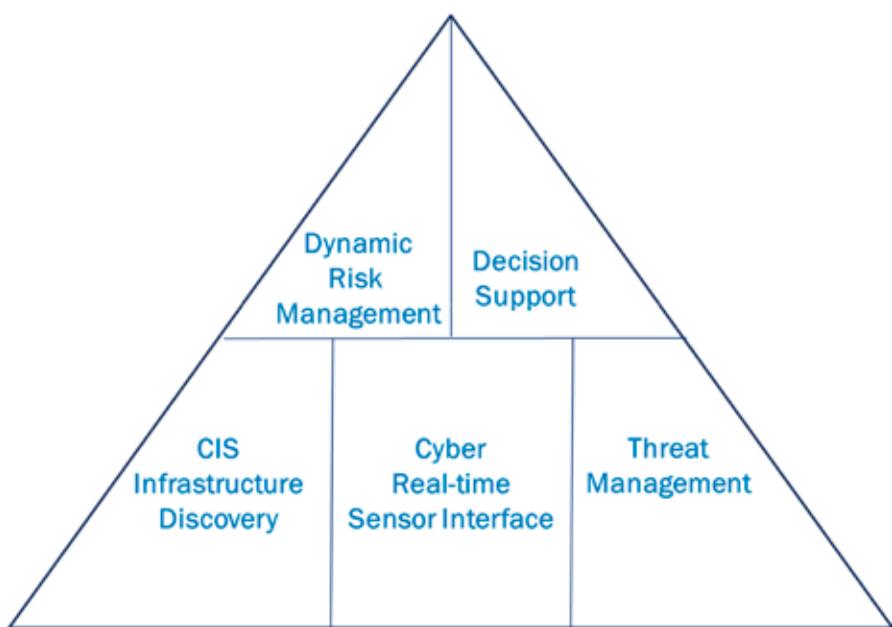


Figure 1: Intended features of the CySAP prototype

Advanced persistent threats (APTs)

An advanced persistent threat (APT) is a prolonged, focused cyber-attack on a specific target intended to compromise that target's system and gain information from or about the target. The target can be a person, an organisation or a business. Traditional cybersecurity measures such as defence-in-depth, firewalls and antivirus cannot protect against an APT attack, and leave organisations vulnerable to data breaches.

Governments and their institutions are among the most prominent targets for APT malware, mostly aimed at cyber espionage. Intrusions are either discovered too late or not at all. Early detection is crucial to properly manage the risk imposed by APTs. After a very successful feasibility demonstrator, the EDA is leading a follow-on project with a group of interested Member States to develop an even more capable solution as an operational prototype.

Digital forensics for military use

The collection and evaluation of digital evidence in a military context is becoming more and more important in order to learn lessons from previous attacks, to attribute attacks to perpetrators, to harden military information infrastructures and to improve online analysis capabilities. In order to address these issues, the EDA launched a Deployable Cyber Evidence Collection and Evaluation Capacity (DCEC2) project aimed at developing a **technical demonstrator for a digital forensics capability** for the military, based on specific requirements of deployed military operations, such as force protection, agility and rapidity.



Figure 2: DCEC2 forensics domains

The future

Cybersecurity is evolving at an unprecedented pace: new threats are identified almost every day, new tools are developed, new approaches to secure assets and networks are tested and proposed.

As threat actors improve their strategies and introduce new technologies, defenders will need a more structured approach and a better consolidation of their efforts. The asymmetric nature of the cyber domain will play an even more important role: as attackers can produce disruptive effects with investments sometimes 100 or even 1 000 times lower than those of the defenders, there is a strong need for improved

cooperation between organisations in areas such as information sharing, burden sharing, and technical integration.

In such a dynamic and challenging environment, the EDA will continue to support Member States in their efforts to build efficient and effective capabilities. In this respect, the Cyber Defence Project Team and the Cyber Research and Technology Ad Hoc Working Group constitute an excellent platform allowing experts to coordinate their efforts. Due to the increased use of information and communication technologies, the importance of addressing cyber-defence aspects in many other domains will become ever more urgent.

Summary of seven overall future military capability requirement trends.



2.3 EUROPOL: the role of Europol in cyberspace

by Catherine de Bolle¹, Jelmer Brouwer² and Nicole van der Meulen³

Coordinating the European law enforcement response to cybercrime

With technology and the internet increasingly facilitating the organisation and coordination of criminal activities, the nature of organised crime has fundamentally changed. The use of new technologies by organised crime groups (OCGs) has not only altered the modi operandi of traditional forms of crime, it has also resulted in the emergence of a whole new set of cyber-dependent crimes. These developments pose significant challenges for law enforcement agencies both in Europe and worldwide.

The borderless nature of the internet allows for criminal activities that are transnational and therefore require responses that transcend national boundaries. As the European Union Agency for Law Enforcement Cooperation, Europol is particularly well placed to play a leading role in the fight against the many forms of cybercrime threatening the safety of European citizens. It does so by offering operational and analytical support and coordination for Member States' cross-border investigations, as well as through prevention and awareness measures.

Europol: the European Union Agency for Law Enforcement Cooperation



Europol is the EU's law enforcement agency, assisting the Member States in their fight against serious international crime and terrorism. Founded as an inter-governmental organisation in 1999, it has been an EU agency since 2010, making it ultimately accountable to the Justice and Home Affairs (JHA) Council and the European Parliament. Europol is not a European police force and it does not have executive powers. Instead, it provides coordination and support to the law enforcement agencies of EU

¹ Executive Director, Europol.

² Research Officer, Strategic Analysis Team, Europol.

³ Senior Strategic Analyst, EC3, Europol.

Member States. All EU Member States have liaison officers seconded to the Europol headquarters in The Hague, where police officers share information with each other and with Europol crime analysts.

Europol serves as a support centre for law enforcement operations, a hub for information exchange and a centre for law enforcement expertise. It achieves this by offering operational coordination and support, a platform for the fast and secure exchange of operational and strategic crime-related information, and a range of analytical products. Each year Europol provides operational support and expertise to over 60 000 international investigations by law enforcement agencies. Meanwhile, strategic analysis products – such as the EU Serious and Organised Crime Threat Assessment (SOCTA), Internet Organised Crime Threat Assessment (IOCTA) and EU Terrorism Situation and Trend Report (TE-SAT) – not only provide Europe's law enforcement community with a detailed account of current and emerging threats, but they also play a key role in informing decision makers at EU level in setting the priorities in the fight against crime.

In recent years, Europol has set up several dedicated centres that focus on specific threats facing the EU. The European Serious Organised Crime Centre (ESOCC) focuses on a range of threat areas related to economic and property crimes and illicit commodities. The European Migrant Smuggling Centre (EMSC), covering crimes related to migrant smuggling and trafficking in human beings, is part of the ESOCC. The other centres are the European Cybercrime Centre (EC3) and the European Counter Terrorism Centre (ECTC). Although EC3 is the main centre with regard to cybercrime, various teams in the other centres also play an important role in securing cyberspace and protecting European citizens from cyber-related criminal threats.

EC3: fighting the multifaceted cybercrime threat



Based on a feasibility study commissioned by the European Commission and carried out by RAND Europe, Europol established the European Cybercrime Centre (EC3) in 2013. Since its inception, EC3 has evolved into a fully-fledged centre, playing a leading role in fighting cybercrime. To ensure cybercrime is approached from a holistic perspective, EC3 comprises three different units: Operations, Strategy and Forensic Expertise.

Head of EC3



Within the Operations Unit, there are five different teams, including three analysis projects (APs). The first team (AP Cyborg) focuses on cyber-dependent crime, which is any form of crime that cannot be carried out in the absence of the internet. The second team (AP Terminal) focuses on payment fraud, including card-present and card-not-present fraud. The third team (AP Twins) focuses on online Child Sexual Abuse (CSA). The fourth and fifth teams are the Cyber Intelligence Team and the Dark Web Team. Both cut across the different operational teams and support them.

The main focus of the operational teams is to support the Member States in their investigations. A good example of this is the arrest of the leader of the OCG behind the Carbanak and Cobalt malware attacks. The OCG used malware attacks targeting financial institutions in more than 40 countries, cashing out over one billion euro. Its leader was arrested by the Spanish police in March 2018, after a complex international investigation coordinated by Europol and involving various law enforcement agencies from around the world, the European Banking Federation and private cybersecurity companies.

The operational teams lead and coordinate a number of recurring actions. Prime examples of these are the European Money Mule Action (EMMA) and the Global Airline Action Days (GAAD). Another good example is the Victim Identification Taskforce (VIDTF) initiative, where experts gather at Europol's headquarters to identify victims of CSA. Supported by specialised Europol staff, they use advanced techniques and software and their knowledge and expertise to find vital clues in the enormous amount of CSA material

online. During the 2017 edition, 25 experts from 16 countries and 21 law enforcement organisations located 10 offenders and victims in 9 different countries. Since the first edition in 2014, more than 50 victims from 14 different countries have been identified and saved.

MALWARE: COMMON SOURCES OF INFECTION

 EMAIL: Opening suspicious or unsolicited attachments or clicking on links from spam/phishing emails and unknown senders	 WEBSITES: Clicking on links to unknown websites or just by visiting them (e.g. websites featuring adult content)	 POP-UP WINDOWS: Clicking on them to download software or to view compromised advertisements
 OPEN WI-FI: Cybercriminals use these networks to harvest your personal data and access your electronic systems	 SOFTWARE: Downloading pirated or free software (games, screen savers, etc.) or downloading files via peer-to-peer networks	 REMOVABLE STORAGE DEVICES: Malware can spread by copying itself from any removable device connected to a computer system
 Cybercriminals will use social engineering and phishing techniques to trick you into performing any of the described actions and obtain your personal information		

EUROPOL EC3 European Cybercrime Centre

Created by Europol

The investigation of cybercrime also requires capabilities in the area of forensics. Within EC3's Forensic Expertise Unit, various specialists therefore assist Member States with digital forensics as well as document forensics, with a focus on operational support and research and development.

The third unit of EC3, the Strategy Unit, focuses on the strategic elements of fighting cybercrime. Tackling cybercrime requires a comprehensive approach that combines intelligence from both public and private parties; therefore the unit's Outreach & Stakeholder Management Team is concerned with establishing partnerships. Through the establishment of partnerships, the team helps to combine efforts by various stakeholders.

**FAKE ANTI-VIRUS
ROGUE ANTI-VIRUS
SCAREWARE**

WHAT IS IT?

A fake application that pretends to scan and find malware/security threats on a user's device, misleading them into paying for the simulated removal

WHAT DOES IT DO?

Besides the standard payload (50-100 EUR) to remove the malware, they normally contain a Trojan. If the user pays, the credit card details will probably be stolen

HOW DOES IT SPREAD?

Various tactics to convince the user: spam email, social media messages with the software installer attached or compromised websites displaying fake security warnings

EUROPOL
EC3 European Cybercrime Centre

Created by Europol

The Strategy & Development Team, on the other hand, focuses on strategic analysis of cybercrime threats. The team uses horizon scanning to determine how innovative technological developments can introduce new opportunities for cybercrime and how law enforcement can respond to this. Another crucial element of the Strategy & Development Team is its prevention and awareness stream, which aims to ensure a coordinated approach to campaigns across the EU. The Strategy & Development Team also focuses on enhancing the knowledge and skills of law enforcement officials by coordinating relevant training courses. Finally, both teams within the Strategy Unit ensure that the law enforcement voice is heard regarding policy and legislative developments, as they communicate the challenges faced by law enforcement to relevant policymakers.

To ensure there is coordination across the different agencies within the EU dealing with cybercrime and cybersecurity, EC3 has a Programme Board. This provides EC3 with direction on how to achieve its goals and fulfil its officially assigned tasks, building

TROJAN

WHAT IS IT?

A legitimate or useful-looking computer programme (or embedded within one) but with malicious intentions

WHAT DOES IT DO?

It depends on the attacker's motivation: spying, stealing data, deleting files, expanding a botnet, performing DDoS attacks, etc.

HOW DOES IT SPREAD?

It requires user interaction, normally by opening an email attachment or downloading/running a file from a website; social engineering is common

EUROPOL
EC3 European Cybercrime Centre

Created by Europol

on partnerships, shared responsibility and cooperation with all Board members. The Programme Board is the main platform where the activities of the various actors in the domain of strengthening cybersecurity and fighting cybercrime can be aligned. Members comprise different EU institutions, agencies and bodies, as well as international organisations like Interpol.

Working alongside EC3 is the Joint Cybercrime Action Taskforce (J-CAT), established in 2014 and working on the most important international cybercrime cases that affect EU Member States. Based at Europol's headquarters, J-CAT consists of a standing operational team of cyber liaison officers from several EU Member States and non-EU partners, complemented by EC3 staff. The objective of J-CAT is to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation and initiation of cross-border investigations and operations by its partners.



One of Europol's most successful recent operations was coordinating the takedown in July 2017 of two of the largest criminal dark web markets, AlphaBay and Hansa, by the Federal Bureau of Investigation (FBI), the US Drug Enforcement Agency (DEA) and the Dutch National Police. The operations took months of preparation and coordination and were among the most sophisticated takedown operations ever carried out. Following the arrest of two administrators of Hansa, Europol supported the Dutch National Police in taking over the marketplace and covertly monitoring all criminal activities taking place. During the same period, AlphaBay was shut down and many of its users moved to Hansa. Europol played a coordinating and de-conflicting role in both investigations, providing technical and forensic support, as well as hosting coordination meetings and secure communication channels for the exchange of information during the operations. The double takedown severely disrupted criminal enterprises around the world, led to the arrest of key figures involved in online criminal activity and yielded large amounts of intelligence leading to further investigations.

Although EC3 is the main Europol centre for all issues related to cybercrime, other centres also deal with cyber-related criminal activities. Two of the main threats that are tackled by teams outside EC3 are online intellectual property crime and the use of the internet by terrorist organisations.

IPC3: countering intellectual property crimes on the internet

Intellectual property (IP) crime is a widespread phenomenon in the EU, as cheap fake copies of popular goods remain highly popular with consumers. Counterfeit and pirated products are estimated to constitute 5 % of all imports to the EU. Poly-criminal OCGs are increasingly involved in IP crimes, producing a wide range of counterfeit and sub-standard goods that are distributed on EU markets. This creates risks for consumers' health and safety and affects legitimate economies as a result of unpaid taxes, reduced revenues, decreased sales volumes and job losses.



Graphic: <http://www.arena-international.com/Journals/2017/10/16/k/f/v/Chris-Vansteenkiste---Europol.pdf>

IP crime increasingly takes place online. Nowadays online marketplaces are the main distribution channel for counterfeit goods, with products usually sent directly to customers via postal and express freight services. Infringements of digital content are nowadays also mostly disseminated online, through BitTorrent networks which facilitate illegal downloads or streaming of IPR-protected content without the consent of the rights holder. Another common infringement method involves the illegal distribution of television channels using internet protocol television (IPTV) technology. Over the last few years Europol has coordinated a number of operations against criminal networks illegally distributing pay-TV channels across the EU, shutting down servers and arresting suspects.

What is Intellectual Property Crime?

Intellectual Property Rights (IPR)



Industrial property

- inventions (patents)
- trademarks
- industrial designs
- geographical indications of origin
- plant variety rights

Intellectual Property Crime

is any breach of intellectual property rights



Counterfeiting

The manufacture, importation, distribution and sale of goods which falsely carry the trade mark of a genuine brand without permission and for gain or loss to another



Copyright

- literary and artistic works
- performing artists in their performances
- producers of phonograms in their recordings
- broadcasters in their radio and television programmes



Piracy

An unauthorised copying, use, reproduction, distribution of materials protected by intellectual property rights

Graphic EUROPOL

In July 2016 Europol and the European Union Intellectual Property Office (EUIPO) launched the Intellectual Property Crime Coordinated Coalition (IPC3), hosted within Europol's ESOCC. The coalition provides operational and technical support to law enforcement agencies and other partners in a number of ways. It facilitates and coordinates cross-border investigations, monitors and reports online crime trends and emerging modi operandi, and raises awareness of IP crime among the public and law enforcement authorities.

One of Europol's main operations in the area of IP crime is the annual Operation In Our Sites (IOS), launched in 2012 to target the sale of counterfeit goods on the internet and online piracy. Coordinated by IPC3, the operation has resulted in a total of 7 776 websites being seized to date. In 2017, through increased cooperation with anti-counterfeiting associations and brand owner representatives, joint investigations by IPC3, the US National Intellectual Property Rights Coordination Center, Interpol, 27 EU Member States and third parties resulted in the seizure of over 20 520 domain names offering counterfeit goods and online piracy on e-commerce platforms and social networks.

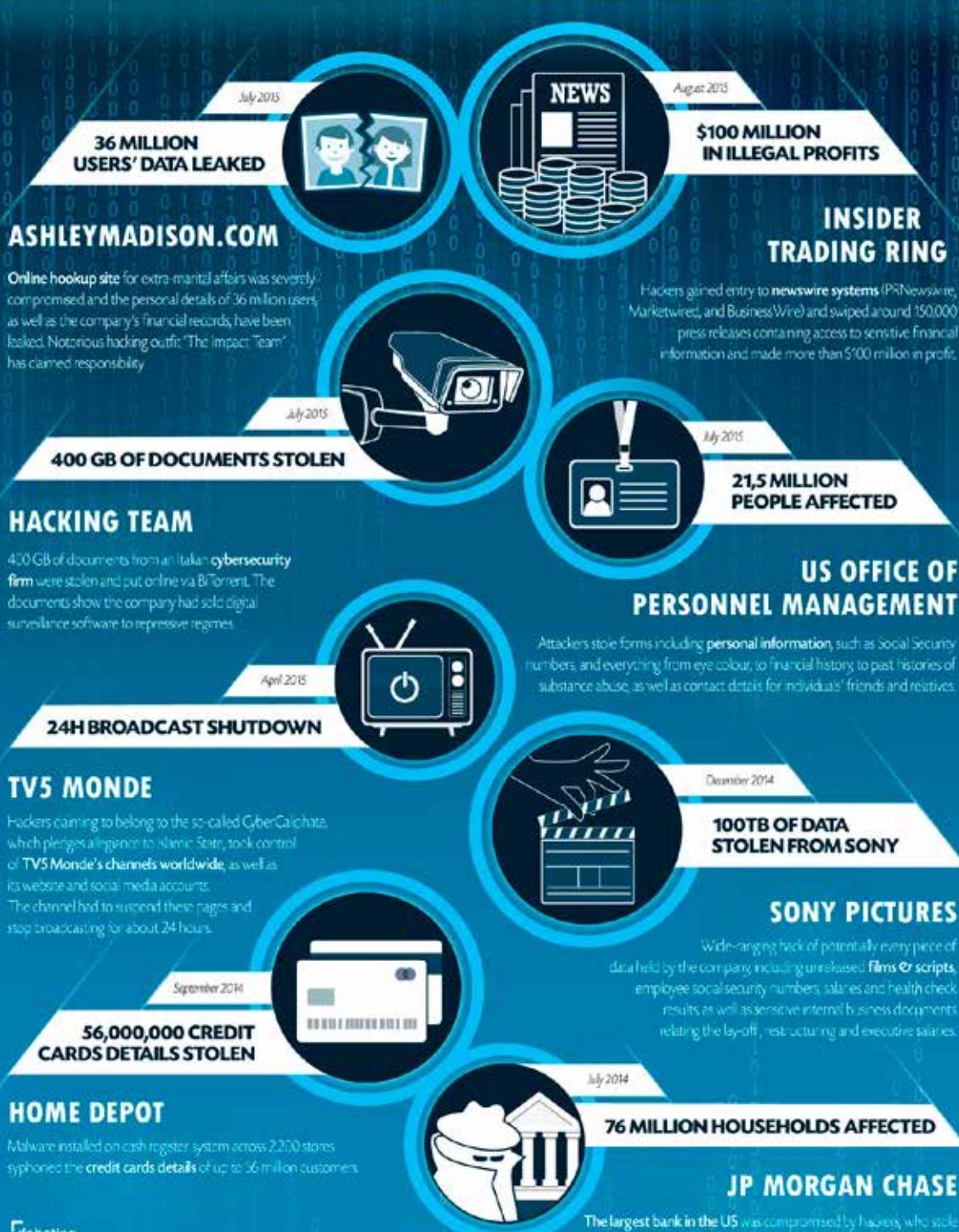
EU IRU: tackling terrorist and violent extremist content online

In recent years terrorist organisations have increasingly turned to the internet and social media to share knowledge, raise money, recruit followers and propagate and glorify acts of terrorism and violent extremism. In particular, al-Qaeda and Da'esh have managed to share their propaganda with a wide variety of audiences both through encrypted communication applications and on public social media networks. Da'esh has also developed a sophisticated communications strategy on social media, although recent territorial losses have caused a decline in the release of new propaganda material. Nonetheless, the organisation still employs a robust network of core supporters who are responsible for maintaining an uninterrupted online presence for the terrorist organisation.

To tackle this phenomenon, EU Justice and Home Affairs ministers mandated Europol to establish a European Union Internet Referral Unit (EU IRU) within the ECTC. Created in 2015, one of the aims of the EU IRU is to flag terrorist and violent extremist content online and refer it to online service providers in order for it to be removed if it breaches their terms of service. The unit focuses on referring content in Arabic, Russian and Turkish issued by al-Qaeda or Da'esh. It also supports competent authorities in the Member States with strategic and operational analysis. Since its creation, the EU IRU has expanded its activities by providing internet investigation support to high-profile terrorism investigations in Member States.

On 25 April 2018, the EU IRU coordinated a joint action against the Da'esh propaganda machine, carried out by law enforcement authorities of six EU Member States, Canada and the US. The action resulted in the takedown of major Da'esh media outlets, including Amaq News Agency, the main mouthpiece of the terrorist organisation. The action followed previous takedowns in 2016 and 2017 and severely compromised the ability of Da'esh to distribute terrorist material. It also resulted in the seizure of digital evidence that is expected to help identify the administrators behind IS media outlets and potentially radicalised individuals.

CYBERSPACE UNDER ATTACK



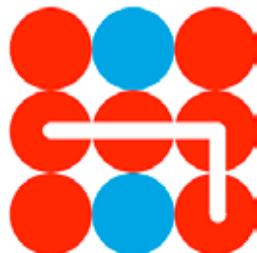
Sources: SEC, The Verge, The Guardian, Reuters, EUobserver, BuzzFeed, Krebs on Security, The New York Times, September 2015

Conclusion

Although cybercrime and the criminal abuse of cyberspace continue to take place, the law enforcement response can claim some success. Thanks in part to the support and coordination of Europol, law enforcement agencies across the EU and beyond have demonstrated that a coordinated, intelligence-led and adaptive approach, involving multiple sectors and partners, can result in significant success in fighting cybercrime. As these threats are unlikely to diminish in the near future, Europol will continue to play a leading role in the fight against cybercrime and work towards making Europe a safer place for its citizens.

2.4 European Centre of Excellence for Countering Hybrid Threats: cyber in the realm of hybrid threats

by Matti Saarelainen and Hanna Smith



In September 2017 the European Centre of Excellence for Countering Hybrid Threats (HybridCoE) started its first capability year in Helsinki, Finland. The HybridCoE's vision is to be the leading facilitator and enabler building participants' capabilities and enhancing EU-NATO cooperation in countering hybrid threats.

At the official inauguration ceremony, the four speakers were first to sign the centre's guest book.

From left to right:
Mr Sauli Niinistö, President of Finland;
Mr Jens Stoltenberg, Secretary General of NATO;
Ms Federica Mogherini, EU's High Representative and Mr Juha Sipilä, Prime Minister of Finland

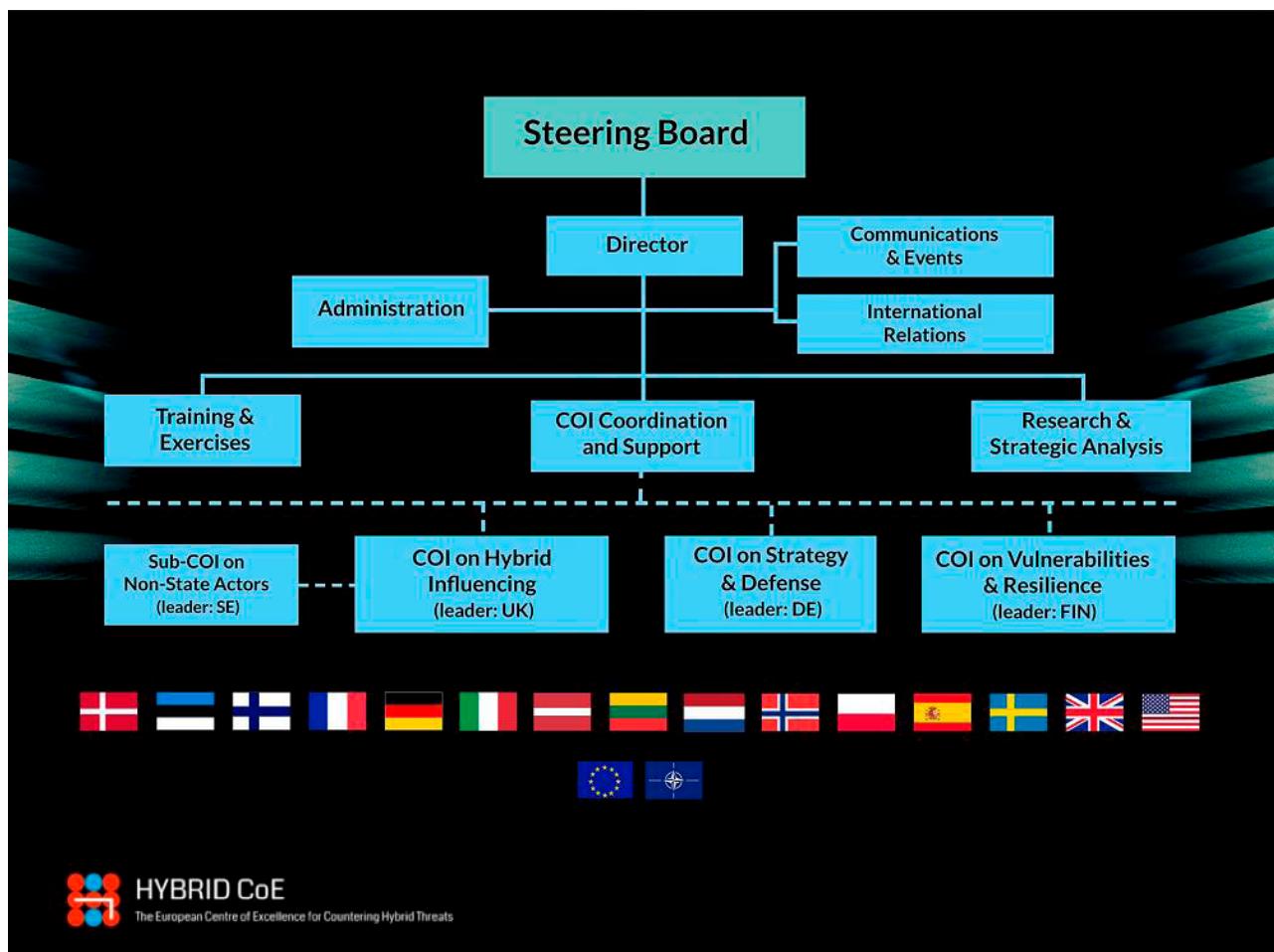


Photo: HybridCoE 2017

The tasks of the new centre of excellence include bringing clarity into security debates and finding solutions as to how countries can improve their civil-military capabilities; enhancing resilience against forces that try to polarise societies in ways that undermine democracy and democratic countries' decision-making, improving preparedness for attacks that seek to weaken different alliances and states; finding better ways to build solidarity among nations and share best practices and expertise; as well as seeking to improve coordinated responses. This is just one development among many promoted by both the EU and NATO, as well as their individual Member States, in response to the

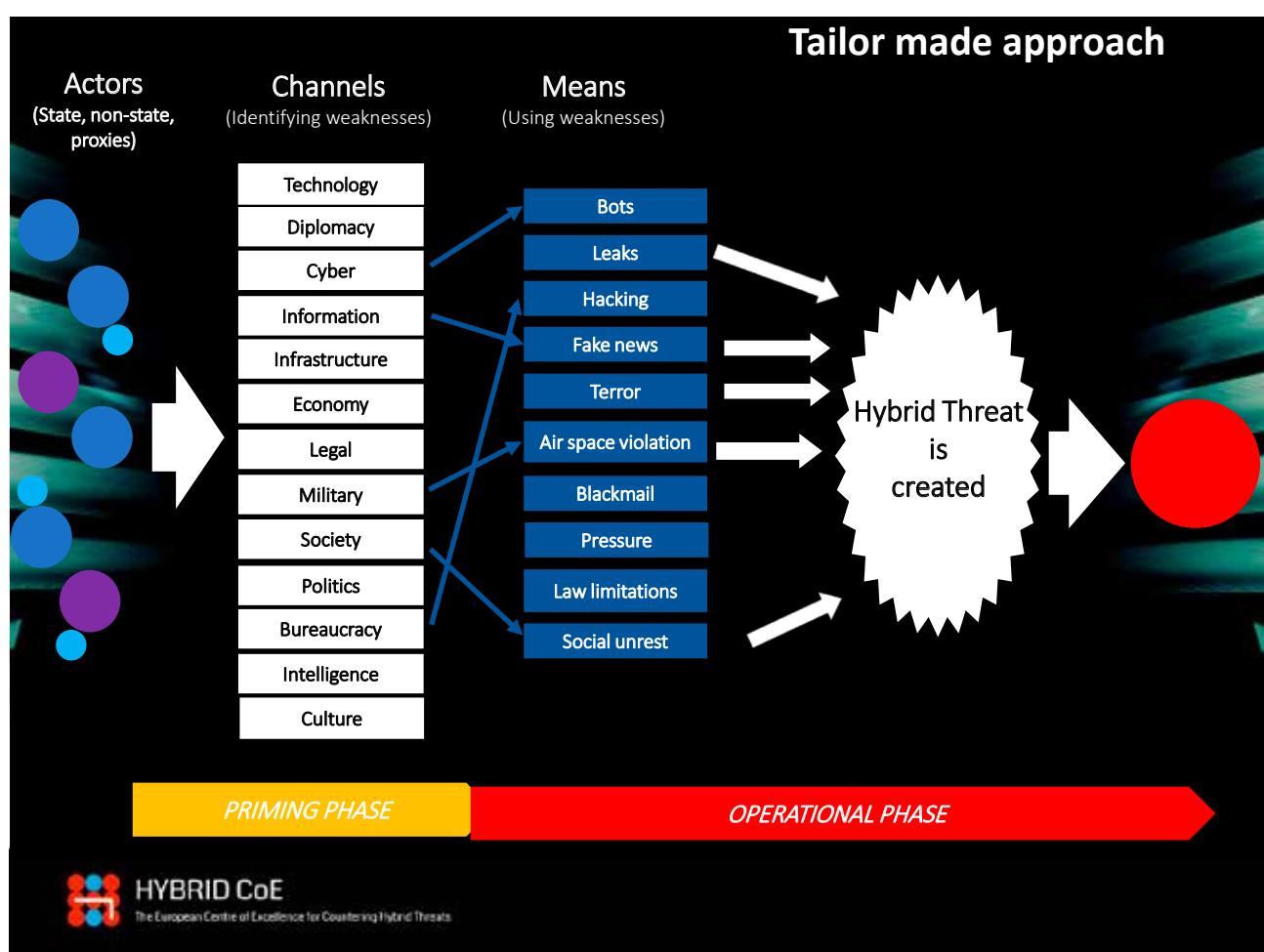
changing security environment. These measures are an indication that there is indeed a need to reassess, inspect and review existing methods for countering security threats. The functions of HybridCoE include the following:

- investigate and examine hybrid influencing targeted at Western democracies by state and non-state actors, map participants' vulnerabilities and improve their resilience and response;
- conduct tailored training and arrange scenario-based exercises for practitioners aimed at enhancing the Member States' individual capabilities, as well as interoperability between and among Member States, the EU and NATO for countering hybrid threats;
- conduct research and analysis into hybrid threats and methods to counter such threats;
- engage with and invite dialogue with governmental and non-governmental experts and practitioners from a wide range of professional sectors and disciplines with the aim of improving situational awareness of hybrid threats.



What characterises hybrid threats?

Changes occurring in the security environment are among the causes of an increased feeling of insecurity and reasons why 'hybrid threat' has become a household concept to indicate today's threats to democratic states. HybridCoE characterises hybrid threats as coordinated and synchronised action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means. Activities exploit the thresholds of detection and attribution as well as the border between war and peace. The aim is to influence different forms of decision-making at local (regional), state or institutional level to favour and/or achieve the agent's strategic goals while undermining and/or hurting the target.



A major part of the changes in the ways influence can be achieved comes from the revolutions in fast-developing technologies, giving rise to new domains such as cyberspace where national and international rules of the game have to be thought out. One enabler for using synchronised and coordinated action with multiple means (hybrid

threats) is cyberspace. In the realm of hybrid threats, cyber is one of the channels that can be used for hostile influencing and illegal activity.

Humans have always tried to influence thinking, but the means and areas in which influence is exerted are changing fast. Cyberspace and virtual worlds are products of our time and thus something new. This has major implications for security thinking. Cyber-security covers many domains such as infrastructure protection, new media landscape elements, effects of digitalisation, cyberspace intelligence as well as network-based action, the dark side of globalisation, which favours weaker states and non-state actors. But as Mariarosaria Taddeo, Research Fellow at the Oxford Internet Institute, University of Oxford, and the Deputy Director of the Digital Ethics Lab and Faculty Fellow at the Alan Turing Institute, has pointed out, *'Cyber-attacks are escalating in frequency, impact and sophistication. State actors play an increasingly large role in this escalating dynamics, as they use cyber-attacks both offensively and defensively'*. It can therefore be stated that cyberspace is now used by all actors and activity is increasing.

Digitalisation provides opportunities and threats

It is important to bear in mind that while cybersecurity provides many opportunities, for example to European companies, and opens up new possibilities for developing technologies, it is at the same time one of the greatest challenges of the future due to threats relating to it. The unique nature of cyberspace makes it an ideal domain for cyber-attacks and influence activities for all kinds of actor - state and non-state actors, politically- or profit-motivated groups or individual hackers.

Furthermore, cyberspace has compressed geography and timelines. This change, along with other factors, has highlighted the need to understand different political and strategic cultures as well as the need for better preparedness and foresight. Information produced in one country can be interpreted in another country in very different ways. The internet has become a new battlefield where rules are still being formulated. These elements are one of the best ways of proving that, in today's security environment, internal and external security aspects are more closely intertwined with each other than they have been in recent decades.

For example, information-influencing operations by hostile actors in democratic states have been conducted by using the '*vilify and amplify*' approach. Here, different parts of the hostile actor's systems generate, gather and amplify material which is designed to undermine the target, while maintaining a degree of plausible deniability. This method has already been used for decades. However, cyberspace, deniable websites and social media have made the use of this technique - in several different ways - much easier to deploy today. At the same time, in cyberspace the attribution aspect has become very

problematic, if not impossible. Cyber-attacks are often launched in different stages and involve globally distributed networks of machines, as well as pieces of code that combine different elements provided (or stolen) by a number of actors. The tactics and nature of cyberspace makes deterrence against cyber threats extremely complicated.

Another worrying trend is that terrorists have adopted the use of cyberspace to further their objectives. Online activities have been used to boost their agenda, distribute propaganda, collect intelligence information, recruit new members, raise funds and radicalise potential supporters. Cyberspace has also been used for the purposes of communication and planning of attacks. This emphasises the fact that network-based action is one of those security challenges that should be considered most seriously.

What is the nature and intensity of cyber-attacks?

It should be noted that the nature and intensity of cyber-attacks vary from low- to high-end attacks, as do the cyber capabilities used. So far, terrorist groups have only been able to conduct low-end cyber-attacks with low-end cyber capabilities by defacing websites and breaking into social media accounts. The vast majority of state activities in cyberspace have also remained below the level of high-end cyber-attacks. But Piret Pernik, research fellow at the International Centre for Defence and Security (ICDS) in Tallinn, has noted that '*long-term low-level cyber-attacks can cumulatively produce large-scale damage*'. It is noteworthy that state actors do have the high-end cyber capabilities to launch, for example, a large-scale destructive cyber-attack against critical infrastructure, but so far the majority of state-actor activity has also remained below the high-end capabilities.

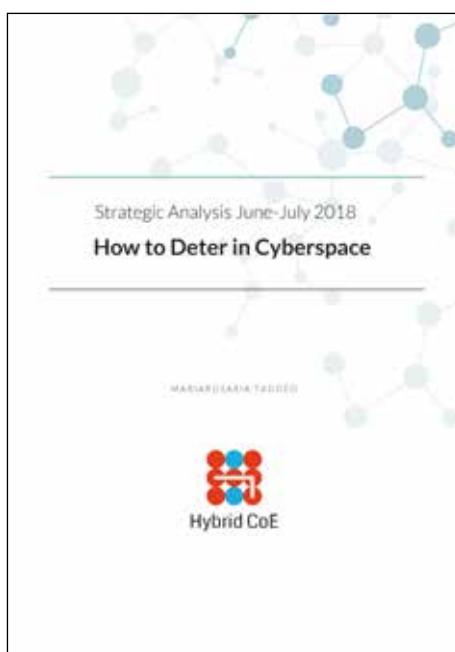
During the last couple of years, advanced persistent threats (APTs) have gained a lot of attention. These long-term cyber operations, the purpose of which is to stay below detection, are carefully targeted and multiple techniques are combined in order to obtain the desired end-result. The operations are expensive, complex and require a lot of resources, which is why they have so far rarely been used by non-state actors. However, state-sponsored freelance groups and organised criminals, that collect valuable information/intelligence, steal intellectual property, pilfer sensitive financial data and even transfer cash in attacks aimed at banks have also been detected. APT actors have made the attribution aspect relating to cyber threats even more complex, if not impossible.

How to counter these challenges in the cyber domain?

To begin with, it should be kept in mind that different kinds of cyber-attack require different kinds of protection measure. Disinformation influencing can be countered

by improving resilience - for example, by improving media literacy ability, providing education, and by paying attention to the regulation of journalistic standards, and regular fact-checking in order to reveal false narratives and sources of fakes. Exposing influence attempts is also an effective countermeasure. In turn, the detection of advanced persistent threats, for example, requires highly specialised expertise and investment in technology. Therefore, the countermeasures also need to be combined and viewed from different angles.

Deterring cyber threats cannot be done by traditional means of deterrence. Traditional deterrence does not address the global reach, anonymity, or the distributed and interconnected nature of the cyber domain. However, if deterrence is considered in a creative way and adapted to new domains such as cyber and the changing security environment, there is still a lot that can be done. In cyberspace as in all influencing channels belonging to the realm of hybrid threats, active countering strategies need to be developed which include better detection, retaliation, and demonstration capabilities, resilience building including legal frameworks - both international and national, collaboration and network-building among the like-minded and alliances, as well as recovery strategy. Furthermore, as Jarno Limnell, professor of cybersecurity in Finland's Aalto University, has pointed out, inter-agency cooperation such as civil-military, public-private, etc. needs to be enhanced further. A culture of shared responsibility will strengthen the democratic states. It can become a powerful tool to counter hybrid threats.



See also the Strategic Analysis Papers of the Hybrid CoE. One of the most recent editions deals with cyber deterrence and can be downloaded from:

<https://www.hybridcoe.fi/wp-content/uploads/2018/06/Strategic-Analysis-2018-6and7-Taddeo.pdf>

2.5 The European Security and Defence College: Cyber Education, Training, Evaluation and Exercise platform

by Dirk Dubois



The European Security and Defence College, led by the 28 EU Member States, is a network college consisting of 140 partners within and outside the European Union. During a special meeting on 6 February 2018, the 28 Member States represented in the Steering Committee of the European Security and Defence College (ESDC) decided to create a Cyber Exercise, Training, Exercise and Evaluation (ETEE) Platform. Where does this platform come from and what exactly is it supposed to do? What about all those other actors that are already active in this field? What is the added value of this new area for the ESDC? Won't it distract the focus of the ESDC from its core tasks?

The origins of the Cyber ETEE platform

Looking back at the origins of this initiative leads to a more or less random choice: which is the first document to mention? For the purposes of this article, we go back to the EU Cyber Defence Policy Framework adopted by the Council on 18 November 2014. Paragraph 4 of this document relates to improving training, education and exercise opportunities for the Common Security and Defence Policy (CSDP)¹ and gives specific roles and tasks to the EEAS, together with the EDA and the ESDC. However, we could also have started in 2013, with the Cybersecurity Strategy of the European Union². The overall aim of the strategy was to create additional education and training opportunities related to the EU CSDP for different audiences. At the same time, synergies needed to be created with different stakeholders such as ENISA, EUROPOL, ECTEG and CEPOL. Closer cooperation between the ESDC and NATO was also promoted in this field.

1 Council of the European Union, Doc ST15585/14 of 18 November 2014, p.11.

2 Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, document JOIN(2013) 1 of February 2013, and the related General Affairs Council conclusions of 25 June 2013.



Graphic: Jochen Rehrl

The Joint Communication on Resilience, Deterrence and Defence³ talks about the creation of a cybersecurity competence network with a European Cybersecurity Research and Competence Centre. This centre, to be established in 2018, would play a significant role in training and would initially be set up by the Commission as a Horizon 2020 project with a budget of EUR 50 million. By February 2018, no concrete steps had been taken to create such a network and the understanding in the ESDC Steering Committee was that the ESDC would create the network. However, the legal basis⁴ of the ESDC doesn't allow the use of Commission funds other than from the CFSP budget.



The Joint Communication can be found on:
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450>

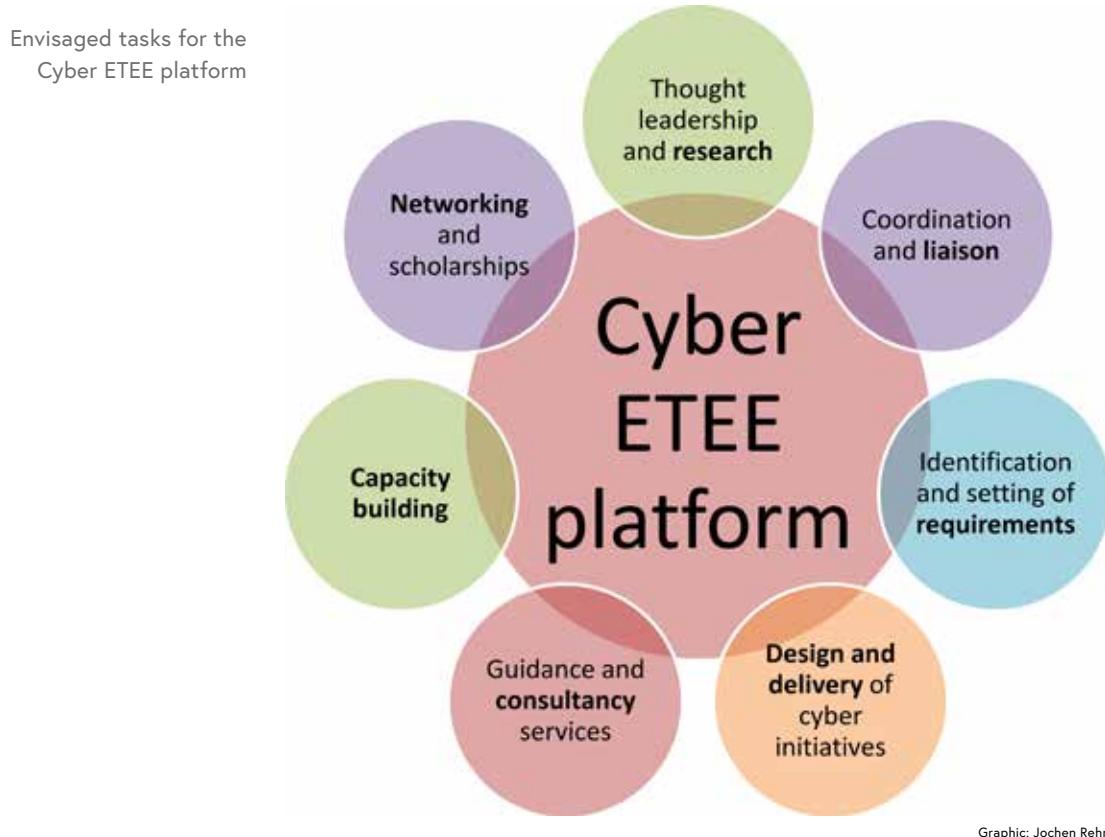
³ Joint Communication on Resilience, Deterrence and Defence: building strong Cybersecurity for the EU, (JOIN(2017) 450 final) of 13 September 2017.

⁴ Council Decision (CFSP) 2016/2382 of 21 December 2016.

A third source for the creation of the Cyber ETEE platform can be found in a study on the EU Cyber Defence Centre for the CSDP, performed by Rand Europe at the request of the European Defence Agency⁵ and the subsequent Collegiate View of the EU Military Committee⁶. This study, based on input from the Member States and from the EDA itself, identifies seven core functions of Cyber ETEE for the CSDP, namely:

1. Thought leadership and research
2. Coordination and liaison
3. Identification and setting of requirements
4. Design and delivery of the CD ETEE initiatives and programmes for CSDP
5. Guidance and consultancy services
6. CD ETEE field development and capacity building
7. Networking and scholarships

These functional clusters are further split into 24 core tasks.



5 RandEurope: Update Study on the EU Cyber Defence Centre for CSDP. Final Project Report. October 2017.

6 EUMC Collegiate View, Document EEAS (2017) 1371 Rev 3 of November 2017.

During consultations in the summer of 2017 between the Rand project team and the ESDC staff, it became clear that most of these tasks could be covered using existing ESDC structures and procedures. Some tasks would, however, require more time to implement and certain aspects, such as research, would have to be completely reliant on resources made available through the ESDC network.

The main concern of the Member States during the discussions leading up to the decision on 6 February was to make certain that there would be no duplication/competition between the efforts of the Cyber ETEE platform and the work done by the European Commission.



Photo: European Security and Defence College/Michael Chia

The inauguration ceremony of the platform was held on 20 and 21 November 2018 in the Museums of Fine Arts in Brussels.

(in the picture:
Mr. Dirk Dubois/ESDC,
Mr. Jorge Domecq/EDA,
Mr. Gustav Lindstrom/EU ISS
and Mr. Jochen Rehrl/ESDC)

The aim of the Cyber ETEE platform

Taking into account the different elements mentioned above, the Member States agreed on the final aim of the Cyber EYEE platform as follows:

'To address cyber security and defence training among the civilian and military personnel, including for the CSDP requirements for all CSDP training levels as identified by the EU Military and Civilian Training Groups, and upscaling the training opportunities for the Member States. The detailed tasks and functions for this platform have been identified in Ref 2, 3 and 6.'

At a later stage and depending on the further development of such a concept, the Cyber ETEE platform could advance ETEE opportunities for wider cyber defence workforce (so-called Cyber Reserve).¹

Although the CSDP remains in the text, it is clear that the role of the platform is not limited to the CSDP alone. Also, it is clear that the platform needs to address a generalist public, and should not be limited to high-ranking officials. On the contrary, the aim is to address the training requirements of all levels - from working level to senior decision makers - with courses ranging from awareness level through to technical courses and specialised courses. In the field of cyber security as in normal life, we should avoid exacerbating the differences between civilian and military cyber security. The challenges and risks for both are similar and this is even more the case for our critical infrastructure. It therefore makes sense that we educate, train and exercise together, as has always been the case for ESDC activities.

This ambitious aim should be addressed in a cost-effective way, without creating duplication of effort with other organisations. In spring 2018, the Member States agreed to increase the staff of the ESDC Secretariat gradually by six people spread over two years. The initial intent was to work with Seconded National Experts, in line with ESDC tradition. However, if these Experts cannot be made available, it will be possible to recruit contract staff so that the strict deadline of having an initial capability by the end of 2018 can be met.

At the same time, the necessary funds were made available to start work on the project. Here lies the main advantage of working in the way the ESDC does: the whole project would represent a cost to the EU budget of around EUR 500 000 per year, or approximately 1 % of what the Commission was originally willing to contribute in the Joint Declaration of 2017. In other words, the Member States have committed themselves to offering the necessary courses to the ESDC by pooling and sharing their resources and foregoing the additional funding by the Commission, which could then be used in other ways. At the same time, the Commission committed to investigating ways to support the efforts of the Cyber ETEE platform.

Coordination and cooperation

Now that the resources have been identified, it is time to identify the different stakeholders and their expectations for the platform. The ESDC Secretariat sent out a questionnaire to the Member States with a view to identifying the specialised institutes

¹ Document ESDC 2018/013 Rev 1 - Cyber ETEE Platform.

they would like to have join the ESDC network. An initial meeting was held in June 2018 to establish a working program for the coming years. The elements of the work programme are derived not only from the documents mentioned above, but also from the input of the so-called 'discipline leader' on cyber defence training identified by the EU Military Training Group. As soon as it is set up, the civilian training group will also be invited to provide its input. The work programme also covers the challenges and expectations identified by the Member States.

Although the ESDC already had a limited offer of cyber courses in its portfolio, and some highly qualified training providers in this field in its network, other actors are far more dedicated to the cyber field. From the very beginning of setting up the platform, the ESDC team contacted these entities one by one. Reactions from partners such as the EDA were predictable, as they had been extremely supportive of the ESDC completing this task from the beginning. Others, such as EUROPOL and CEPOL, had already been cooperating with the ESDC over the course of many years. Other entities with fewer links with the ESDC immediately reacted in a positive way to this initiative. On the EU side, initial meetings were held with representatives from the European Cybercrime Training and Education Group (ECTEG) and from the European Union Agency for Network and Information Security (ENISA). All agreed that they were willing to share their experience and expertise - to the extent permitted by their own legal basis – with the new platform. In particular, ENISA saw huge added value in the experience of the ESDC in organising training activities. In addition to their experience in the field of cyber security and defence, they were immediately willing to share the taxonomy they had developed over the years. This would in principle allow them to speak the same 'language' when talking about cyber incidents. Talks with EU CERT and other stakeholders are going to take place in the immediate future and in any case before the declaration of the Initial Operating Capability of the platform.

Mirroring the initial task contained in the EU Cyber Defence Policy Framework of 2014, Member States also requested that the ESDC coordinate its efforts with the relevant NATO services and certified Centres of Excellence. So far, informal contacts have been established with both the NATO Communications and Information Agency (NCIA) and the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn. These contacts will need to be deepened and broadened in order to enable their respective training activities to be reinforced.

The Joint Declaration of September 2017 cites a potential figure of 350 000 people who will need to be trained for the private sector alone. It is clear that even the ESDC's large network, with over 150 training providers, would not be able to train all of those people in addition to the requirement for training EU and Member States' officials.

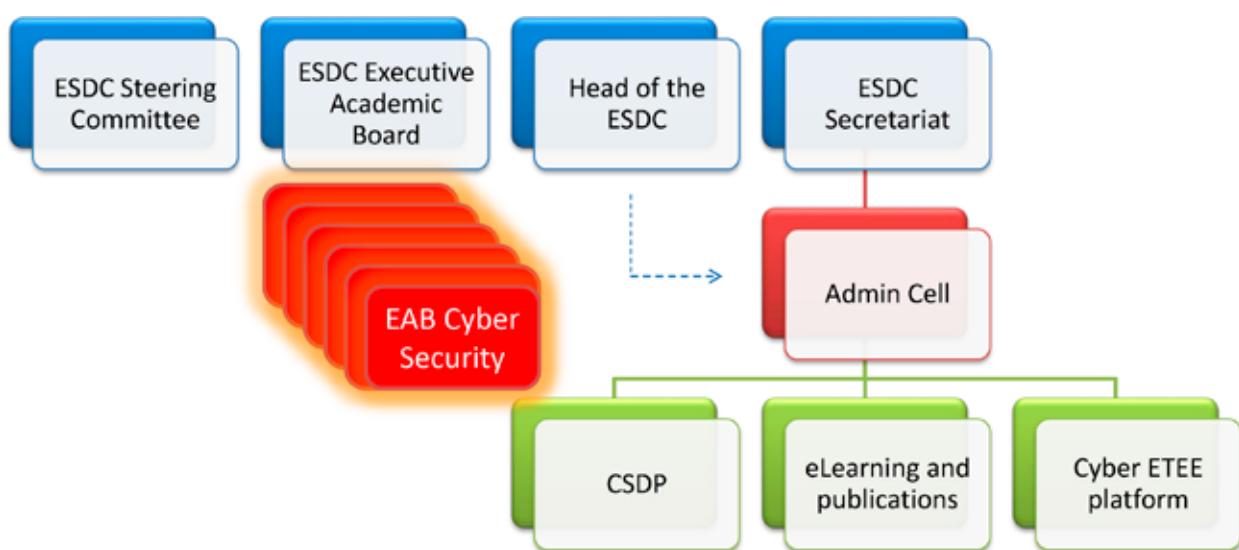
When, in future, the concept of a so-called 'cyber reserve' is agreed, a large number of additional people will need to be trained just to meet the needs of the Member States.

Together with the various stakeholders, we remain committed to setting standards in training in a very flexible way, whilst focusing on what really counts at the end of the day: being certain that, at the end of an education or training activity, the participant is a knowledgeable, skilled, autonomous and responsible person. Making certain that the Member States and the EU institutions can count on the outcome of training is the key condition for success for the cyber platform, creating economies of scale and exchange opportunities for all.

Will the ESDC change?

A final question remains: will this new task endanger the 'normal' functioning of the ESDC? The question is of course linked to the large influx of new people with varied backgrounds into the ESDC Secretariat. However, the training institutes of the network and the core team at the Secretariat, covering the traditional ESDC activities, are very experienced and have long-standing best practices. The stability of the personnel will ensure that the core functions of the College are maintained for the foreseeable future. It is also my personal opinion and conviction that we can easily mitigate this risk and that the Member States will keep us on track should we deviate from this path.

Structure of the ESDC including its Cyber ETEE platform



Graphic: Jochen Rehrl

2.6 ENISA – the European Union Agency for Network and Information Security

by Udo Helmbrecht



Hosted by Greece, the ENISA has its seat on the island of Crete, and the majority of its staff work in the operations office located in the northern suburbs of Athens. As a centre of excellence that supports the experts in the Member States, ENISA was set up in 2004 to work on a wide range of cybersecurity topics and to fill the gaps that neither public nor private sector bodies could fill.



ENISA has its seat on the island of Crete.

Photo: ENISA

ENISA specialises in EU policy implementation. In this regard, the Agency strongly supports the EU Commission and the Member States by giving guidance on the technicalities of network and information security, thus contributing to the proper functioning of the internal market.

The structure

ENISA's Management Board defines the Agency's general orientation. It is a structure composed of representatives of the Member States and the Commission which, among other tasks, appoints the Executive Director, establishes the budget and approves the work programme. The Agency also has an Executive Board, tasked with preparing decisions for adoption by the Management Board on administrative and budgetary matters.

An Executive Director, appointed by the Management Board, manages the Agency. Two heads of department – the Core Operations Department and the Resources Department – assist the ED in his daily work.

The Core Operations Department deals mainly with aspects related to secure infrastructures and services, information security and data protection, operational security, support and analysis, relations with security incident response teams, public affairs and policy.

The Resources Department is responsible for facilities management, finance and accounting, human resources, information technology, safety and security, and relations with the host Member State.

The ENISA Permanent Stakeholders Group is an advisory body composed of 33 members appointed from all over Europe. The group advises the Executive Director on the development of the Agency's work programme, and on communication with the relevant stakeholders.

In addition, the Executive Director may, in consultation with the Permanent Stakeholders Group, establish ad hoc working groups composed of various experts. The ad hoc working groups address specific technical and scientific matters.

Our vision

ENISA's priorities at the moment include critical information infrastructure protection, the NIS Directive, capacity-building activities such as the cybersecurity exercises, standardisation and certification, provision of consolidated threat information to its stakeholder community, identification and dissemination of best practices on how to mitigate threats associated with new technologies, and supporting EU legislation such as GDPR, eIDAS, and PSD2.

Over the last decade, society has made a tremendous leap into the evolving age of technology. Today we enjoy endless benefits and countless opportunities in all sectors of our economy. However, this brings about risks and challenges for EU citizens and businesses: data protection issues, cybercrime, and online disinformation to name a few.

Fortunately, cybersecurity remains high on the agendas of the EU and its Member States, and increasingly high budgets are allocated to boosting cyber resilience and supporting the European community.

The strategic objectives of the Agency derive from its regulation. The feedback from the Member States – both public and private sector – complements these objectives:

- Knowledge and information: stay up-to-date on developments in the EU digital environment and use the NIS knowledge of the staff to collate the information collected, in order to anticipate emerging challenges and better prepare the EU to face them;
- Policy development and implementation: support the institutions of the European Union and the EU Member States in developing, implementing and reviewing EU cybersecurity legislation;
- Capacity building: assist the institutions of the European Union and the EU Member States in building up and strengthening their NIS capabilities and expertise, thus supporting Europe as a whole in sustaining NIS capacities of the highest standards;
- Community: encourage the development of the European NIS community, which is becoming more and more prominent, by promoting and strengthening the cooperation between EU Member States, EU institutions, NIS stakeholders and the private sector;
- Enabler: bolster the impact of the Agency by improving the management of its resources and the engagement with its stakeholders at both European and international level.

NIS in education as part of the Austrian Cyber Security Strategy

National ICT Security Strategy Austria

In 2011 the Federal Chancellery of Austria (Österreichisches Bundeskanzleramt, BKA) initiated the development of Austria's National ICT Security Strategy (Nationale ICT-Sicherheitsstrategie Österreich). The aim was to assess the current situation and to develop a proactive concept to protect cyberspace and human beings in this virtual space by taking into account their fundamental rights and freedoms.



Starting with a kick-off-meeting in November 2011

The results of the five working groups
'Stakeholders and Structures'
'Critical Infrastructure'
'Risk Management and Situation Assessment'
'Education and Research' and 'Awareness'
were integrated into an overall strategy and presented in June 2012.

130 experts
from industry, science and public administration participated in the development of this strategy.

5 working groups
were established to deal in-depth with the various aspects of cybersecurity – from awareness raising to specific counter-actions against security incidents.

The Austrian National ICT Security Strategy identifies 23 strategic aims and 55 measures to ensure and enhance security in cyberspace. The results are to be integrated with the Austrian Strategies on Cyber Defence and Cyber Crime in 2013.

The Working Group on Education and Research

Discussions in the working group showed a strong need for NIS in education even for the youngest groups – children in primary and secondary schools, not forgetting teachers and parents.

The working group identified in total **seven** strategic aims, **three** of them dealing specifically with NIS in education.

These three aims were as follows:

While it is evident that a national security strategy deals with the protection of critical infrastructures, risk management or stakeholders, it is interesting to note that education and research formed a significant part of the overall strategy. The fact that there was a specific working group dedicated to these topics indicates the importance of having a sound basis of knowledge and skills in information security and cyber-security, both on the expert level and at the broad level of citizens and users of all ages.

The working group dealt with **3 main items:**

- network and information security (NIS) in primary and secondary education;
- study and training programmes – offered as specialisation of general ICT studies as well as specific ICT security studies – with a focus on security at tertiary level;
- Strengthening research in ICT and information security.

Next steps:

As next steps specific measures and concrete actions will be derived from the strategic aims identified in the National ICT Security Strategy. The discussions in the working group showed that there is much material available and many highly interesting activities are going on. Yet, those activities are usually restricted to specific types of education or specific schools, often based on the personal involvement of dedicated teachers. It will be necessary to define an agreed level of minimum knowledge to be reached in the various stages of education. In the next steps it will be important to involve all relevant stakeholders to integrate NIS education in schools and also to make it part of a lifelong learning process.

As a first step relevant material concerning NIS in education will be integrated into an ICT security platform that will be set up in Austria during the coming months. In this platform specific information will be provided for target groups, comprising children, parents, teachers, people of 60+, but also institutions such as companies, the research and technology sector and public administration. This platform will serve as a means to exchange and spread information among all stakeholders. ENISA's material on NIS in education will be integrated as a valuable part of this information.

Education in ICT; ICT security and media competence in early school grades:

- Attacks on ICT infrastructures through inadequately protected private systems as well as the individual's loss of privacy may be prevented on a long-term basis only if citizens have a wider understanding of ICT security and adequate skills in using the new media. This understanding needs to be developed at school as early as possible.
- ICT and ICT-security must be incorporated to a greater extent into school curriculums and daily teaching practice from primary school level onwards. It is a medium-term goal that each individual's familiarity with the use of modern media can be taken for granted – this is not only in the interest of the citizens but also the basis for protecting national infrastructures.
- Dealing with new technologies in a competent and secure way has to become an integral part of education in all types of schools. As children interact with new media at a very young age this issue must be addressed even at primary-school level and reinforced in secondary schools. Educational standards should be defined to ensure adequate level of competence in all school types.

Education in ICT and ICT security for all teachers:

- Schools will not succeed in reaching a creative, safe and critical approach to ICT and new media unless teachers receive adequate training.
- Providing children with the skills for the constructive and secure handling of ICT and new social media requires teachers to be familiar with the subject and the new developments and to have profound and up-to-date knowledge on the subject. ICT and ICT-security should become an integral part of the training of all future teachers during their university studies, regardless of their main subject. Continuing education and training has to be provided for teachers already in the field.

Special programs for parents:

- Parents often hesitate to discuss the use of modern technologies with their children, believing that young people have more skills in this area. Yet it is important that parents are able to question critically the way their children handle new media and to help them understand the opportunities and risks of the modern technologies. Special programmes have to be developed for parents within the school system which will help them to become a knowledgeable source of advice for their children and to examine their use of new media and media skills.



European Network
of Information
and Security Agency

Our projects

Every year, based on the needs of the stakeholders, ENISA produces deliverables covering different areas, with the aim of supporting the EU's NIS policy. A deliverable could be a report, a position paper, a risk assessment or a briefing. ENISA deliverables are comprehensive documents that outline key information and provide practical recommendations.



Most deliverables cover areas such as the CSIRT community, cybersecurity, privacy, critical information infrastructure protection, resilience, the Internet of Things, threat intelligence, cloud computing, risk management and many others. When preparing a deliverable, ENISA is supported by experts in that field, including members of academia, industry and governmental organisations.

CSIRTs Network

The CSIRTs Network provides a forum where Computer Security Incident Response Teams from the Member States can cooperate, exchange information, and build trust. National CSIRTs work on improving the handling of cross-border incidents and look for ways to respond to specific cybersecurity incidents in a coordinated manner. ENISA provides the secretariat for the CSIRTs Network. With its strong expertise in this field, the agency regularly supports the meetings and tasks of the Network.



CSIRTs by country - interactive map

Cyber Europe

As a simulation of large-scale cybersecurity incidents that escalate into EU-wide cyber crises, the pan-European exercise *Cyber Europe* is a sophisticated crisis management exercise that ENISA organises for the public and private sectors in EU and EFTA Member States. The exercises offer opportunities to analyse advanced cybersecurity incidents, and to deal with complex business continuity and crisis management situations. Over 600 organisations across Europe participate in this exercise every two years. In 2018, ENISA organised the fifth edition of the exercise.





European Cyber Security Month road map to the future...

EUROPEAN
CYBER
SECURITY
MONTH

Enhanced content of ECSM:

- Continue the development of repository of materials
- Keep encouraging private-public common activities
- Introduce a best practice section on the website



YOU

Further develop a stable model of coordination at European level and MS level:

Plan in advance all steps and communicate them

Improve interactivity

Improve content and participation

28

European Union Member States
+ more partner countries

INTERNATIONAL COOPERATION

Develop an International training kit for NIS activities

Exploring common webinars and e-learning solutions

Advance planning



'Online security requires your participation'
find out more at
www.cybersecuritymonth.eu

enisa.europa.eu
#cybersemonth #OctoberNIS

European Cybersecurity Month

The *European Cybersecurity Month (ECSM)* is a specific month dedicated to activities on cybersecurity and security/privacy awareness. The European Cyber Security Month is the EU's annual awareness campaign, which runs for the entire month of October. ENISA and DG CONNECT support the ECSM alongside many partners from all over Europe. ECSM aims to raise awareness of cybersecurity threats, promote cybersecurity among citizens and provide up-to-date security information through education and sharing of good practices.

European Cybersecurity Challenge

The *European Cybersecurity Challenge (ECSC)* is an integrated element of the ECSM. Every year, cyber-talents from participating countries meet to network, collaborate, and finally compete against each other to determine which country has the best cyber-talents. The challenge consists of security-related tasks – from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics – that the participants have to complete. The team with the most points at the end of the challenge wins the competition. The challenge also hosts expert talks and a job fair, which have attracted a lot of interest from some of the best cybersecurity talents and hundreds of visitors from across Europe.



Training material

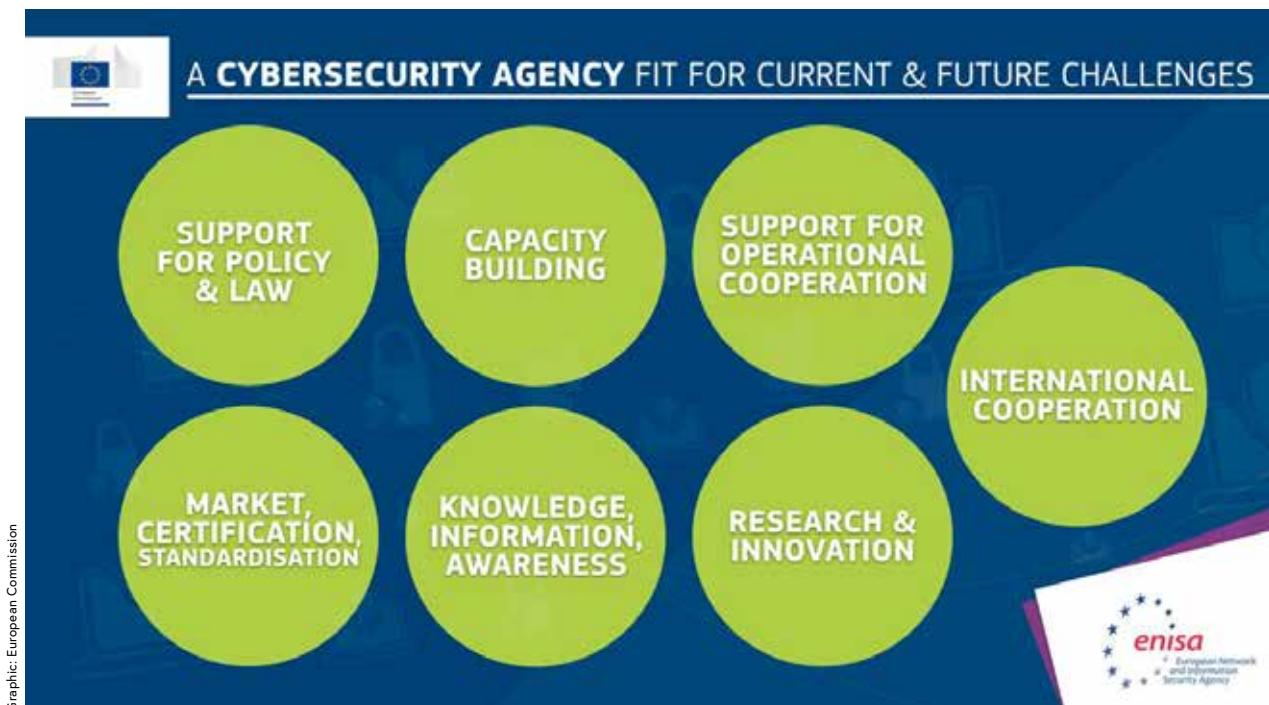
For over a decade, ENISA has been producing cybersecurity training material, containing essential material for developing skills in the community of incident responders and in the field of operational security. Apart from providing training material, ENISA organises courses and trains over 200 cyber specialists every year.



The future

Recent developments have increased the European Commission's determination to scale up the Union's response to cyber attacks, improve cyber resilience and increase trust in the EU Digital Single Market

Therefore, building on the current Agency, a proposal was put forward to establish a European Union Cybersecurity Agency – with a strong mandate, permanent status and adequate resources – and to set up an EU cybersecurity certification framework – that will, amongst other things, ensure the trustworthiness of billions of 'Internet of Things' devices.



The most important task that the Commission envisages for ENISA is undoubtedly the production of 'candidate schemas' that will serve as the basis for the certification of products and services that are crucial for the Digital Single Market. ENISA is expected to work together with the Commission and the Member States to assist them in implementing this new proposed certification framework, thereby making it easier for businesses to trade across borders and for buyers to understand the security features of the product or service.

Equally, this boost foresees the addition of response-oriented tasks, which will enable ENISA to play a more active role in supporting Member States in the event of cyber-attacks. This includes the possibility for the Agency to carry out post-incident analysis when requested by the Member States.

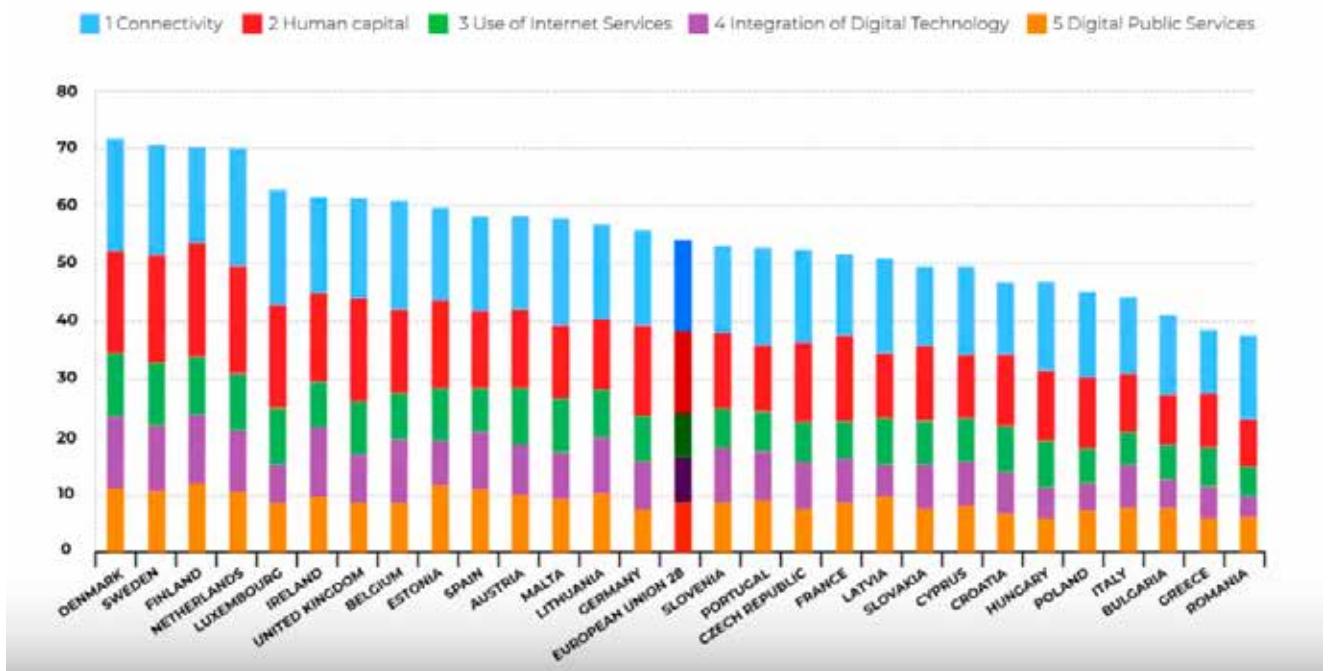
2.7 CERT-EU: European CERT cooperation

by Georgios Psykakos and Arthur de Liedekerke



Digital technologies underpin the complex systems which keep our economies running. The latest 2018 Digital Economy and Society Index (DESI)¹, published by the European Commission, reveals that almost half of Europeans (46 %) use the internet to make calls while more and more businesses send electronic invoices (18 % compared with 10 % in 2013) and use social media to engage with customers and partners.

Digital Economy and Society Index 2018



Graphic: http://europa.eu/rapid/press-release_MEMO-18-3737_en.htm

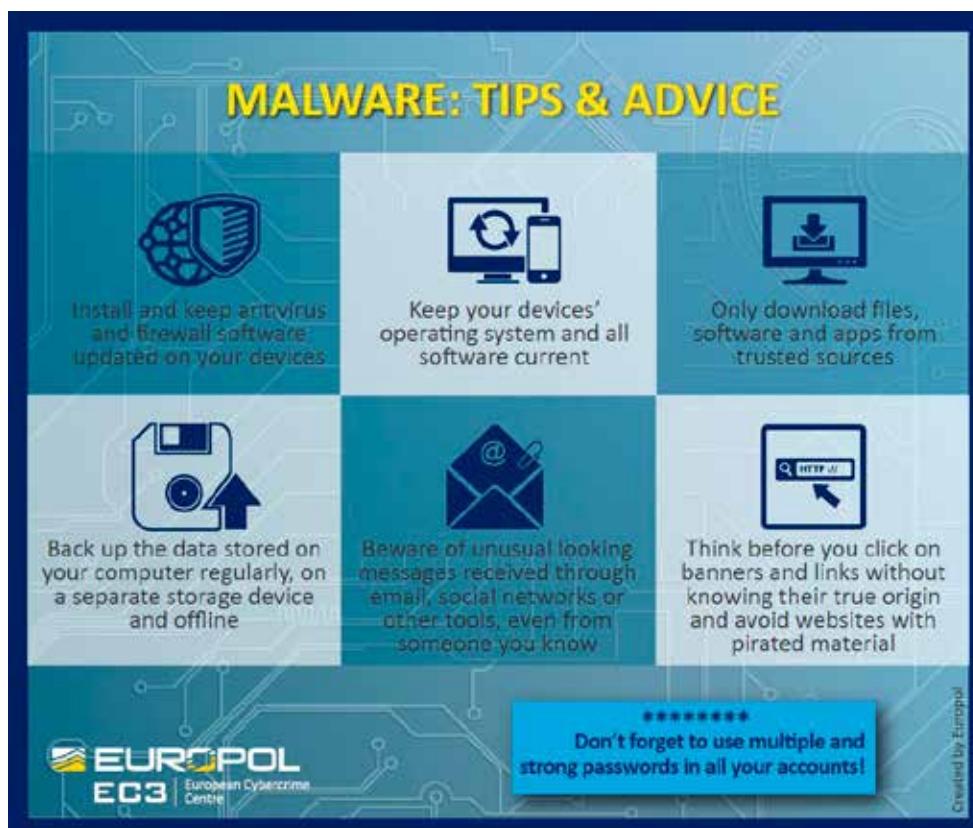
The Digital Economy and Society Index (DESI) is a composite index published every year by the European Commission since 2014, measuring the progress of EU countries towards a digital economy and society.

1 European Commission Fact Sheet on Results of DESI 2018.
Accessible at: http://europa.eu/rapid/press-release_MEMO-18-3737_en.htm

The new digital reality in Europe

Increasing dependence on information technology and the growing interconnectedness of our lives have brought about a paradox – a situation where digitisation simultaneously offers significant opportunities but exposes our societies to new risks. WannaCry, NotPetya, the Mirai botnet... These are some of the infamous examples that have highlighted the large-scale impact that malicious cyber activities can have on essential sectors such as energy, transport and health.

Our vulnerability to cyber-attacks is a daily reality: it is estimated that, in 2017, Europe faced up to 4 000 ransomware attacks per day². In light of the potential consequences of these incidents, strengthening the security and resilience of cyberspace has become a priority on the global political agenda.



² Remarks of former Director of Europol, Rob Wainwright, during the Web Summit in Lisbon, Portugal on 8 November 2017. Accessible at: <https://www.reuters.com/article/us-portugal-websummit-europol/fast-growing-cyber-crime-threatens-financial-sector-europol-idUSKBN1D82QS>

Origins and role of CERTs/CSIRTs

The name Computer Emergency Response Team (CERT) is the historic designation given to the first such team at Carnegie Mellon University in 1988. The CERT designation is now a registered trademark, leading many organisations to adopt the more generic Computer Security Incident Response Team (CSIRTs) in their title (although minor differences in taxonomy exist, both terms will be used in this article synonymously).

Composed of cyber experts, they are key actors in the prevention of and effective response to information security incidents and cyber-attacks. CERTs handle computer security incidents, identify vulnerabilities, mitigate threats and promote information exchange among the wider cybersecurity community. Today a wide variety of CERTs exist, differing in their missions, the constituencies they serve and their authority, organisational setup and funding – from governmental and non-governmental entities to commercial, military or academic structures.



This article intends to focus mainly on the cooperation between national and/or governmental (n/g) CSIRTs and the EU's cyber bodies as well as to provide a concise overview of the developments and challenges currently characterising the sphere of cybersecurity in Europe.

An ever-evolving cyber threat landscape

Cyberspace is an environment which knows no overarching authority nor stringently observed rules and norms. It is widely acknowledged to be the 21st century's new battlefield.

Attacks, which are increasingly sophisticated, can stem from various sources, using multiple vectors and taking different forms. Understanding who is behind them, identifying the methods being used and having a sound assessment of the nature of these threats is essential to mitigate their impact and improve one's cybersecurity posture. The threat landscape snapshot provided below is based on disclosable information collected and analysed by CERT-EU's Cyber Threat Intelligence team and trusted partners.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	↔	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	↔	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	↔	8. Botnets	↑	↓
9. Insider threat	↔	9. Insider threat	↔	→
10. Physical manipulation/damage/theft/loss	↑	10. Physical manipulation/damage/theft/loss	↔	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends:  Declining,  Stable,  Increasing
 Ranking:  Going up,  Same,  Going down

Graphic: ENISA Threat Landscape Report 2017, p.9.

Threat actors

Threat actors can be broadly divided into the following categories:

- state or state-affiliated groups: these tend to possess advanced capabilities and significant resources as well as objectives aligned with the agenda of their sponsor;
- organised crime: often engage in targeted attacks, driven by profits;
- hacktivists: attackers with ideological motivations, seeking to raise awareness or benefit their cause through their cyber militancy;
- opportunistic: largely amateur criminals or, sometimes, legitimate security researchers, looking to expose flaws and exploits.

Tactics, Techniques and Procedures (TTPs)

The level of sophistication witnessed in the attack landscape is unprecedented. Attackers, and the tools they use, are increasingly difficult to detect.

Of major concern are Advanced Persistent Threats (APTs). Typically these involve the stealthy penetration of an organisation's network, with the hackers operating methodically and sometimes over lengthy periods of time to obtain data that can be exploited.

Additionally, the uptake of Internet of Things (IoT) technologies, cloud services and other innovations have considerably expanded the attack surface and offer plenty of new vulnerabilities to malicious actors. Despite all the technological advances, human action and error are often at the root of cybersecurity issues. Phishing attacks and email-based social engineering (collecting personal information which is then used for identity fraud) tactics are routinely used by attackers to circumvent advanced cybersecurity systems.

Motivations

The motives behind attacks vary widely. Foreign nations may resort to cyber warfare or espionage to obtain sensitive information; hacktivists like the Anonymous group can target and disrupt particular websites through Distributed Denial of Service (DDoS) operations; cybercriminals will often seek to steal data and blackmail individuals or businesses.

Geopolitical tensions are a growing factor in cyber risk. The successful shutdown of Ukraine's power grid in 2016 is considered by many sources to be an example of political frictions. Cyber warfare has very real advantages: the difficulty of attribution provides plausible deniability.

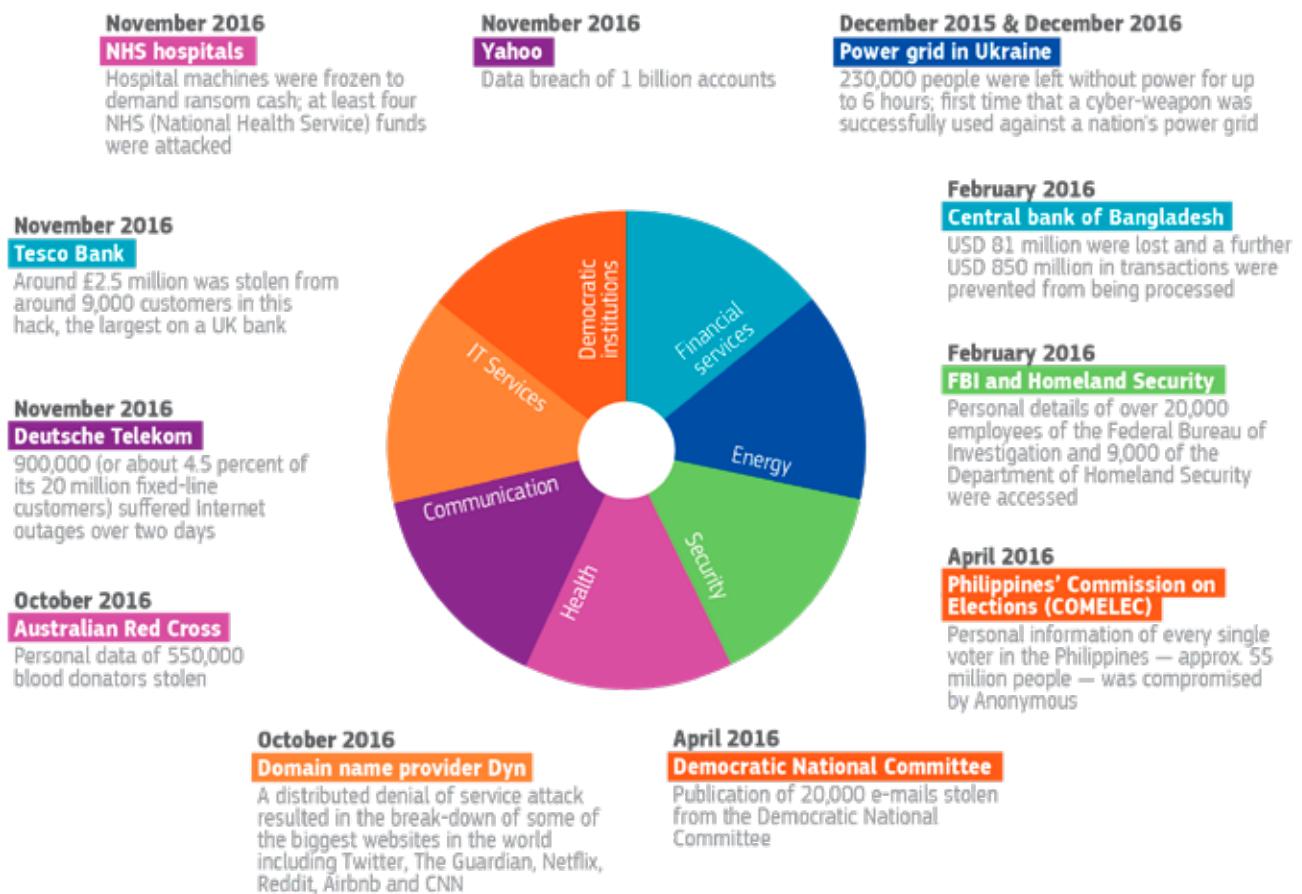
In terms of cyber criminality, the surge in popularity and value of cryptocurrencies for instance has seen cryptomining (malware taking advantage of someone else's computational power to generate cryptocurrency) soar as a popular form of cyber-crime. Ransomware, too, remains extremely profitable, with the preferred method of distribution being spam email campaigns.

However, other intrusions seemingly have no other intention but to have a destructive effect and obliterate data, as demonstrated by the 2017 Nyetya wiper malware.

Targets

All industries are targets. Nevertheless, some sectors with activities of a more sensitive nature, such as critical infrastructure, healthcare institutions and financial entities, are particularly under attack.

While the notorious 2018 examples of attacks against Singapore's government health database and the cyberheist in Mexico, which saw thieves siphon more than USD 15 million out of several banks, have made headlines around the world, many more go unnoticed or unreported for fear of reputational damage.



Graphic: European Political Strategy Centre (EPSC)

The state of play of EU cybersecurity cooperation

The cybersecurity challenges we face do not respect or recognise borders – they are common problems in any interconnected society. The transnational character of these security threats has led to calls for better cybersecurity governance and more robust defences through enhanced cooperation between national, European and international actors.

Avoiding duplicative structures, striking a balance between Member State sovereignty and EU competences, respect for principles such as that of subsidiarity these are some of the many elements that have to be factored into the collective and wide-ranging approaches being developed. Today, although the main tools to combat cybersecurity challenges remain largely in the hands of Member States, a growing number of initiatives are being taken to address them at EU level.

Ramping up EU-level collaboration

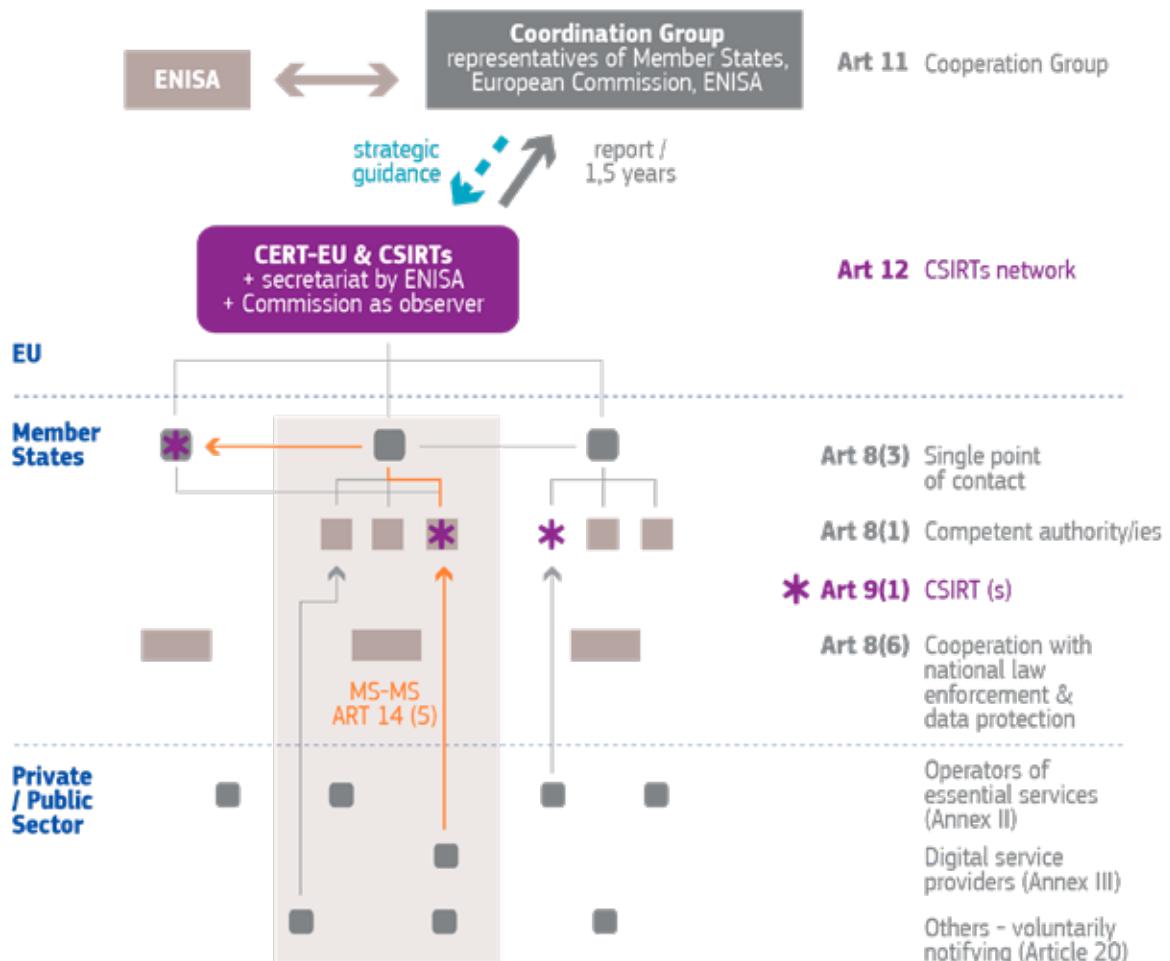
The NIS Directive and the CSIRT Network

Improving collaboration and coherence of cooperation on IT security between Member States and the EU institutions was precisely the rationale behind the European Union's 2016 Network and Information Security (NIS) Directive³, the first EU-wide legislation on cybersecurity.

Among other rules, it creates an NIS Cooperation Group involving the European Commission, EU Member States and ENISA (the European Union Agency for Network and Information Security) to facilitate coordination on information security; it requires the EU Member States to adopt a national strategy on the security of network and information systems; and it stipulates that a single point of contact per country be nominated in order to liaise and ensure cross-border cooperation with other Member States.

3 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. Accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN>

Of particular interest is Article 12, which establishes the CSIRTs Network, comprising 28 national CSIRTs, one per Member State, and CERT-EU, the body responsible for protecting the EU institutions, bodies and agencies against cyber-attacks. ENISA provides secretarial and support functions to this group.



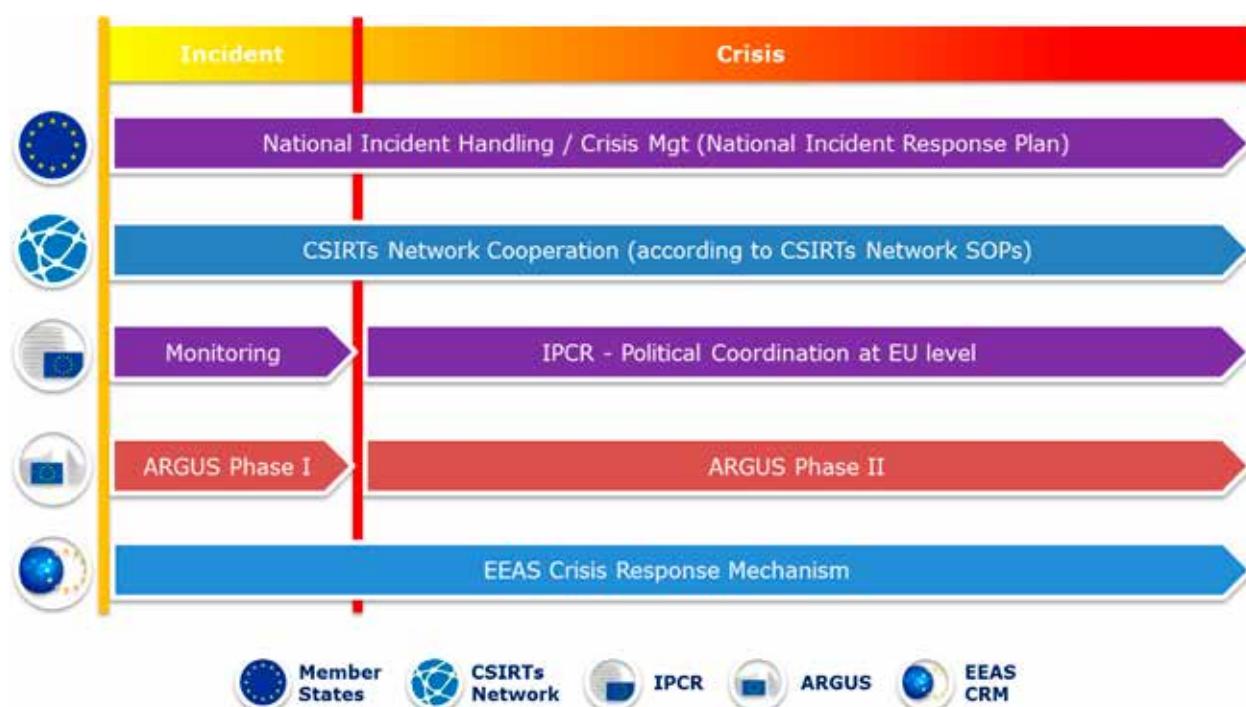
Graphic: European Political Strategy Centre (EPSC)

The CSIRTs Network role is to foster operational cooperation, notably in terms of information exchange, provide a forum where members can discuss the handling of cross-border incidents and build trust. Now in its second year of existence, the Network is fully functional and has been tested both during cyber exercises and routine business, supported by tools and infrastructure (i.e. the MeliCERTes platform) developed with funding from the Connecting Europe Facility (CEF) programme.

The blueprint

In September 2017, the European Commission presented a ‘Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises’⁴ calling for the creation of an EU Cybersecurity Crisis Response Framework to ‘identify the relevant actors, EU institutions and Member State authorities, at all necessary levels – technical, operational, strategic/political’ in order to develop an adequate, coordinated response to highly disruptive cybersecurity incidents.

Cybersecurity Incident/Crisis Response at EU level



Graphic: ANNEX to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises. C(2017) 6100 final, p 10.

Although not a legally binding policy document, it lays down suggestions for Member States and EU actors in terms of joint incident handling and analysis, shared situational awareness and timely decision-making. It also offers insights into how existing crisis management mechanisms could be made more coherent to improve responsiveness in

⁴ Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. Accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H1584&from=EN>

the case of EU-wide cyber-attacks. The CSIRTs Network, the national CSIRTs of individual Member States and relevant EU cyber agencies and bodies – such as CERT-EU, ENISA and Europol’s EC3 to name but a few – are identified prominently throughout the text with a view to emphasising the need for collaborative interaction between them.

Fostering international partnerships

The need to expand collaboration beyond the Member States of the EU and engage in cyber dialogues with third countries was recognised as early as 2013 with the Cyber-security Strategy⁵ and was later reaffirmed in the Council conclusions on cyber diplomacy in 2015. Platforms for dialogue and cooperation on cybersecurity have therefore been set up with major actors, states and international organisations alike.

The European Government CERTs Group

The European Government CERTs group (EGC) is an informal association of government CERTs in Europe, with a largely technical focus. It comprises a number of representatives of EU Member States, CERT-EU and members from non-EU countries such as Switzerland (SWITCH CERT) and Norway (NorCERT). With a restrictive membership process based on mutual trust, similarities in constituencies and demanding criteria in terms of maturity, this group exchanges sensitive information relating to IT security incidents and malicious code threats and vulnerabilities.

NATO-EU cooperation

In the face of common challenges and with 22 EU Member States also being NATO allies, a Joint Declaration was signed in July 2018, listing hybrid threats and cybersecurity as areas of enhanced cooperation and interoperability. In the current strategic environment, CERT-EU, along with entities in the European External Action Service (such as the Intelligence Centre, the Hybrid Fusion Cell, etc.), the European Defence Agency (EDA) and the EU Military Staff (EUMS), hold regular staff-to-staff meetings and discussions on policy alignment and exchange best practices.

⁵ Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013

Signing ceremony of the
2nd EU-NATO Joint
Declaration on
July 10, 2018.

From left to right:
Mr Donald TUSK, President
of the European Council;
Mr Jens STOLTENBERG,
Secretary General of NATO;
Mr Jean-Claude JUNCKER,
President of the European
Commission.

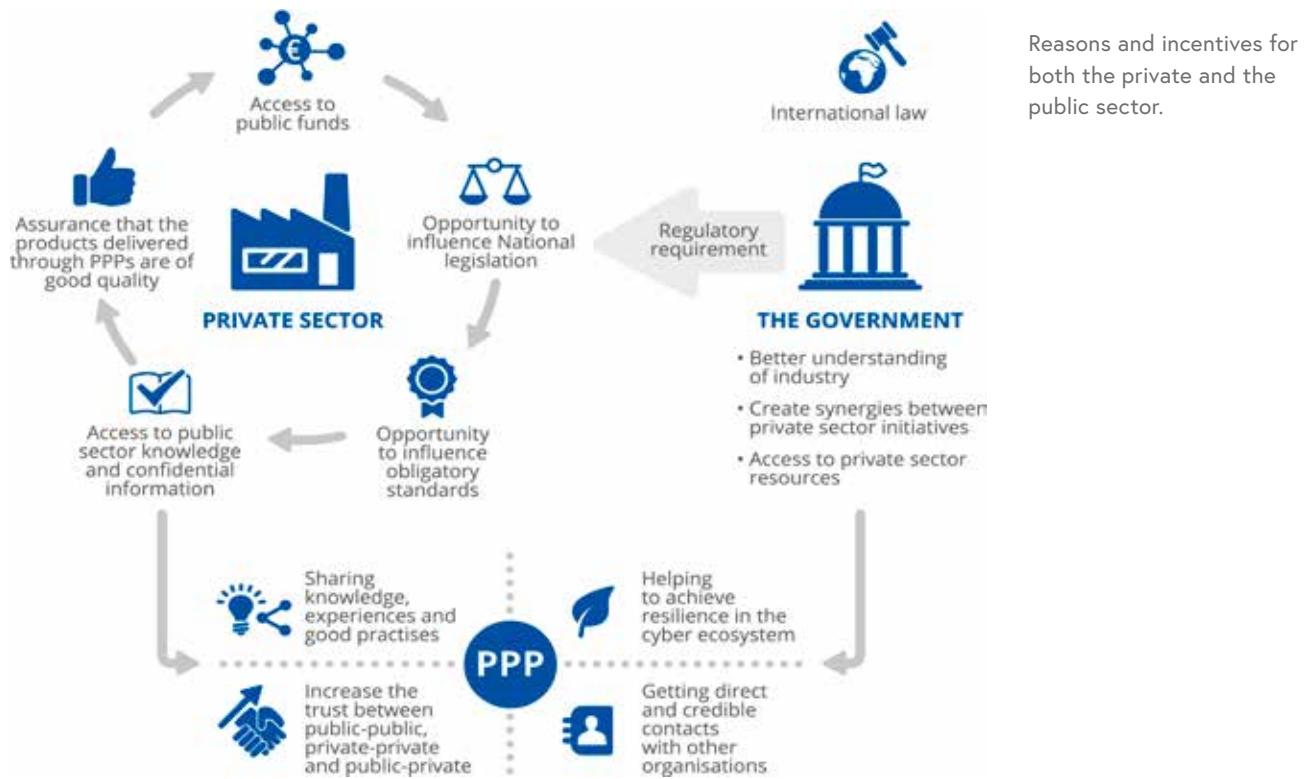


Since 2016, CERT-EU has enjoyed a particularly close relationship with its counterpart at NATO, the Computer Incident Response Capability (NCIRC). A Technical Arrangement, signed in 2016, facilitates technical information sharing between these two bodies. Routine exchanges of threat indicators and threat alerts, mutual briefings and participation in joint exercises (LockedShields, PACE) are among the key features of their cooperation.

Working with the private sector

The targets of cyber-attacks are often companies, and their consequences frequently affect critical infrastructure or essential businesses in the hands of the private sector; many of today's cybersecurity products are the result of commercial endeavours and research. Involving private sector CSIRTs in cybersecurity governance is therefore crucial: not only do they possess considerable, industry-specific knowledge and participate in general awareness-raising efforts concerning cyber hygiene but they are also often able to deploy resources and capabilities at a greater scale than many countries.

Although some barriers to information sharing exist, notably due to legal rules and issues of trust, fruitful cooperation between the private and public communities does happen. Two main multilateral forums enable EU bodies and n/g CSIRTs to engage with the private sector: at the regional level, the Task-Force - Computer Security Incident Response (TF-CSIRT) and, at the global level, the Forum for Incident Response and Security Teams (FIRST).



Graphic: ENISA: Public Private Partnerships (PPP). Cooperative models. p 10.

TF-CSIRT

TF-CSIRT is a regional forum which has been promoting collaboration and coordination between CSIRTs in Europe and neighbouring regions since 2000. It enables sharing of statistical data about incidents in order to observe common trends, provides education and training and assists new teams in developing their organisational and technical capabilities.

FIRST

FIRST, formed in 1990, is an international confederation of CSIRTs from the government, commercial, and academic sectors with the goal of establishing better communication and coordination between incident response teams. Today, FIRST consists of about 300 teams spread across more than 60 countries that develop and share technical information, tools, methodologies, processes and best practices.

A comprehensive approach to cybersecurity

Hybrid threats and the diversity and intensity of attacks which we face today have blurred the boundaries between the realms of civilian and military matters, and of cyber criminality and traditional crime. This has created the need for a comprehensive, holistic approach to the digital domain.

Sharing a common, high-level goal – the security of our societies – the cybersecurity community, law enforcement, the military and intelligence services increasingly work together on cyber matters. Only by involving all relevant stakeholders can the EU hope to achieve a safer cyberspace.

This is precisely the spirit of the 2017 ‘Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’ Joint Communication⁶, which states that ‘cybersecurity is a common societal challenge, so that multiple layers of government, economy and society should be involved’ and calls for ‘a more comprehensive, cross-policy approach to building cyber-resilience and strategic autonomy’.

The Memorandum of Understanding was signed by Udo Helmbrecht, ENISA's Executive Director, Jorge Domecq, Chief Executive of the EDA, Steven Wilson, Head of EC3 and Ken Ducatel, CERT-EU's Acting Head. HR/VP Federica Mogherini and Commissioner for Digital Economy and Society, Mariya Gabriel supervised the ceremony.



The Memorandum of Understanding signed between the EDA, ENISA, Europol's EC3 and CERT-EU in May 2018 marks a tangible milestone in these cooperation efforts. It foresees exchanges of staff, mutual participation in joint exercises, information sharing and involvement in cross-sectoral policy work.

⁶ JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU – JOIN2017/0450. Accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=EN>

Looking to the future

The World Economic Forum's Global Risks Perception Survey of 2017-2018 shows that large-scale cyber-attacks are now seen as the third most likely global risk for the world. This is telling of the heightened concern with which our societies view cyber.

Top 10 risks in terms of Likelihood

- 1 Extreme weather events
- 2 Natural disasters
- 3 Cyberattacks
- 4 Data fraud or theft
- 5 Failure of climate-change mitigation and adaptation
- 6 Large-scale involuntary migration
- 7 Man-made environmental disasters
- 8 Terrorist attacks
- 9 Illicit trade
- 10 Asset bubbles in a major economy

Top 10 risks in terms of Impact

- 1 Weapons of mass destruction
- 2 Extreme weather events
- 3 Natural disasters
- 4 Failure of climate-change mitigation and adaptation
- 5 Water crises
- 6 Cyberattacks
- 7 Food crises
- 8 Biodiversity loss and ecosystem collapse
- 9 Large-scale involuntary migration
- 10 Spread of infectious diseases

Graphic: World Economic Forum Global Risks Perception Survey 2017-2018

A slew of challenges for Europe's cybersecurity community lie ahead. First among them, a projected gap of 350 000 skilled security personnel by 2022⁷. Significant investments in areas such as high performance computing are also needed in order to develop the EU's capabilities and enhance its cyber maturity. Moreover, cooperation efforts sometimes appear too fragmented or hampered by a lack of trust among stakeholders.

However, there are many encouraging signs indicating that awareness of this challenge and the resources dedicated to addressing it are increasing. The EU's proposal for the next 2021-2027 Multiannual Financial Framework has earmarked EUR 9.2 billion in investments

⁷ The Global Information Security Workforce Study, produced by the Center for Cyber Safety and Education (Center) and (ISC)². Accessible at: <https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf>

for key strategic digital capacities, such as artificial intelligence, high-performance computing and cybersecurity. As part of the proposed ‘EU Cybersecurity Act’, discussions are also ongoing to give ENISA a permanent mandate and significantly bolster its resources.

Lastly, in July 2018, in the framework of a permanent structured cooperation (PESCO) project, seven Member States signed a Declaration of Intent to set up an EU Cyber Rapid Response Force, pooling experts from the participating countries to reinforce neutralisation and investigation efforts in the event of a significant cyber incident.

2.8 Other cyber stakeholders

compiled from internet sites

2.8.1 Security Policy Directorate within the EEAS (SECPOL)



The security policy directorate (SECPOL) of the European External Action Service (EEAS) includes a cyber sector responsible for the formulation, implementation and coordination of cyber security and defence issues under the Common Foreign and Security Policy (CFSP).

Among others, the cyber sector supports the establishment of a strategic framework for conflict prevention, cooperation and stability in cyberspace that is based on the application of existing international law, in particular the UN Charter in its entirety, for the development and implementation of universal norms of responsible state behaviour, and for regional confidence building-measures between states. It does so as part of its engagement within the UN, the OSCE and the ASEAN regional forum, and through bilateral dialogues organised yearly with Brazil, China, India, Japan, South Korea, and the US.

The cyber sector supports the implementation of the Framework for a joint EU diplomatic response to malicious cyber activities (the 'cyber diplomacy toolbox'). The framework is expected to encourage cooperation, facilitate mitigation of threats, and influence the behaviour of potential aggressors in the long term. The framework makes use of the CFSP measures, including restrictive measures, to respond to malicious cyber activities.

The cyber sector is also active on cyber defence issues, coordinates the implementation of the cyber defence policy framework and assists the EEAS cyber governance board. The latter was created in 2017, is chaired by the EEAS Secretary General and aims at improving the coordination, enhancing the protection and strengthening the resilience of the CSDP CIS and networks.

Other entities within the EEAS with cybersecurity related tasks include the EU Military Staff (EUMS), the Civilian Planning and Conduct Capability (CPCC), the Military Planning and Conduct Capability (MPCC), the Single Intelligence Analysis Capacity (SIAC) and the CERT-EU.

2.8.2 EU Institute for Security Studies (EUISS)



The European Union Institute for Security Studies (EUISS) is the Union's agency dealing with the analysis of foreign, security and defence policy issues. Its core mission is to assist the EU and its Member States in the implementation of the Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP) as well as other external action of the Union.

The Institute was set up in January 2002 as an autonomous agency under Council Joint Action 2001/554/CFSP [now regulated by Council Decision 2014/75/CFSP] to strengthen the EU's analysis, foresight, and networking capacity in external action. The Institute also acts as an interface between the Union institutions and external experts – including security actors – to develop the EU's strategic thinking. The EUISS is now an integral part of the structures that underpin the further development of the CFSP/CSDP.

The Institute is funded by the EU Member States according to a GNI-based formula. It is governed by a Board chaired by the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP). The Political and Security Committee (PSC) exercises political supervision – without prejudice to the intellectual independence and operational autonomy of the EUISS.

The Institute has a close working relationship with the European Security and Defence College. Besides contributing to ESDC training modules and related outputs such as the ESDC Handbooks, the Institute's directors were twice elected chairs of the College's Executive Academic Board (2005-2006 and 2016-2017).

In the area of cybersecurity, the EUISS is currently implementing the EU Cyber Direct project with two other partners in support of EU cyber diplomacy and cyber resilience. The Institute's three latest publications on cybersecurity include 'Building capacities for cyber defence', 'Hybrid threats and the EU - State of play and future progress' and 'The cybridisation of EU defence'. All publications can be downloaded via the EU ISS homepage www.iss.europa.eu.

2.8.3 European Cybercrime Training and Education Group (ECTEG)



The ECTEG is composed of European Union and European Economic Area Member States' law enforcement agencies, international bodies, academia, private industry and experts. In November 2016, the ECTEG became officially an international non-profit association with founder members from the law enforcement and academic world. When the group was established, CEPOL, Europol, Eurojust and Interpol were defined as permanent members.

Funded by the European Commission and working in close cooperation with Europol's EC3 and CEPOL, both members of the advisory group, the ECTEG's activities aim to:

- support international activities to harmonise cybercrime training across international borders;
- share knowledge and expertise and find training solutions;
- promote standardisation of methods and procedures for training programmes and cooperation with other international organisations;
- collaborate with academic partners to establish recognised academic qualifications in the field of cybercrime and work with universities that have already created such awards, making them available across international borders;
- collaborate with industry partners to establish frameworks whereby their existing and future efforts to support law enforcement by the delivery of training are harmonised into an effective programme that makes the best use of available resources;
- provide training and education material and reference trainers to international partners, supporting their efforts to train law enforcement on cybercrime issues globally.

2.8.4 The European Union Agency for Law Enforcement Training (CEPOL)



CEPOL is an agency of the European Union dedicated to developing, implementing and coordinating training for law enforcement officials. CEPOL's official name is the European Union Agency for Law Enforcement Training. Its headquarters are located in Budapest, Hungary.

CEPOL contributes to a safer Europe by facilitating cooperation and knowledge sharing among law enforcement officials of the EU Member States and, to some extent, of third countries, on issues stemming from EU priorities in the field of security; in particular, from the EU policy cycle on serious and organised crime.

CEPOL brings together a network of training institutes for law enforcement officials in EU Member States and supports them in providing frontline training on security priorities, law enforcement cooperation and information exchange. CEPOL also works with EU bodies, international organisations and third countries to ensure that the most serious security threats are tackled with a collective response.

The agency's annual work programme is built with input from this network and other stakeholders, resulting in topical and focused activities designed to meet the needs of Member States in the priority areas of the EU internal security strategy. Moreover, CEPOL assesses training needs to address EU security priorities.

CEPOL constantly strives to offer innovative and advanced training activities by integrating relevant developments in knowledge, research and technology, and by creating synergies through strengthened cooperation. CEPOL's current portfolio encompasses residential activities, online learning (i.e. webinars, online modules, online courses, etc.), exchange programmes, common curricula, research and science.

Several aspects of cybersecurity are covered in the annual work programme, such as 'cross cutting aspects of cyber investigations', 'first responders and cyber forensics' and 'cybercrime'. In 2017, CEPOL concluded a MoU with the European Security and Defence College.

3 Cyber challenges

3.1 Emerging cybersecurity challenges

by Gustav Lindstrom

To many observers, ensuring cybersecurity is an emerging security challenge. This view is probably reinforced by the media's growing coverage of malicious cyber incidents worldwide while policymakers raise concerns over hybrid threats – most of which include a cyber dimension.

Despite a growing awareness of cyber challenges, it is more accurate to view it as an already emerged challenge. In other words, cybersecurity challenges are not new. Malicious code such as computer viruses and worms existed already in the 1980s. Over time, they have become more sophisticated. For example, the computer worm Conficker – which affected millions of computers and still affects systems today – first appeared in 2008. Stuxnet, the first computer worm to knowingly affect industrial control systems, was discovered in 2010.

Thus, when we speak of cybersecurity challenges, we should consider it as an emerged or even re-emerging issue. Why re-emerging? One reason is that the cyber domain is continually evolving, bringing with it new risks and opportunities. These require new tools to be found or leveraged. This chapter highlights three evolving cybersecurity challenges, focusing on their potential security ramifications.

Why and how to improve EU cyber security

WHY?

The EU works to face cyber threats and challenges, but also to grasp opportunities

CHALLENGES
SOME OF THE
MOST CYBER
DEPENDENT
SECTORS

TRANSPORT

HEALTH

ENERGY

FINANCE



THREATS
FOR MEMBER STATES
AND INSTITUTIONS



4000
RANSOMWARE
ATTACKS PER DAY
IN 2016



50%
PERCENTAGE OF CYBER
CRIMES OUT OF TOTAL IN
SOME EU COUNTRIES

Graphic: European Union

OPPORTUNITIES

The transition to a digital single market can bring benefits such as 5G and connectivity



HOW ?

EU countries discuss measures such as:

A STRONGER EU CYBER AGENCY



AN EU-WIDE CYBER SECURITY CERTIFICATION SCHEME FOR PRODUCTS AND SERVICES



Source: European Commission



Council of the European Union
General Secretariat

© European Union, 2017.
Reproduction is authorised, provided the source is acknowledged

Graphic: European Union

Managing the path towards the Internet of Things (IoT)

The Internet of Things is still a relatively unknown concept. It refers to the increase in the number of objects connected to the internet. Currently, around 10 billion things are connected to the internet, ranging from computers to critical infrastructures to home appliances. According to projections, this number will increase substantially over the coming years. CISCO projects that at least 50 billion things may be connected to the internet by 2020. Further down the line, the number may be in the trillions. Given this trend, some also refer to IoT as the 'Internet of Everything', as there is an expectation that almost all new products in the future will offer embedded connectivity options. While the IoT will contribute to new applications and economic growth, it also raises important security considerations.

European Union figures:

- It is estimated that 50 billion devices and objects will be connected to the internet by 2020;
- The global smart cities market is estimated to be worth in the order of €1.5 trillion and growing by 17% each year, according to a recent Arup report;
- Over the next 10 years, cities will be the largest generators / users of IoT which will directly benefit citizens in their every day lives;
Some examples: connected and sustainable mobility, healthcare systems and assisted living of ageing population, environmental monitoring and management of water, energy and other resources, and cultural life.

Source: European Commission

First, since the majority of IoT devices do not include security features, they are vulnerable to outside tampering. The insecurity is mainly due to a combination of low computing power, complicating the introduction of authentication processes, and the need to facilitate customer use. Further exacerbating this vulnerability are challenges associated with regular patching or upgrading.

As a result, individuals or groups with malicious intent have a growing number of targets they can zero in on, many with little or no security. Vulnerable targets include items such as household appliances, cameras, printers, toys and DVR players. Once compromised, these can be 'herded' into a large botnet and used to execute a distributed denial of service (DDoS) attack. A telling example of this type of attack occurred in October 2016, when Dyn was compromised by an outside group. Since Dyn controls a substantial portion of the domain name system infrastructure, the impact was felt across the internet as well as by multiple companies worldwide. The DDoS attack was executed by corralling tens of thousands of insecure IoT devices and foreshadows future types of such cyber-attacks.



From **72%** of m2m short-range connections (Wi-Fi, Zigbee, in-building PLC,...) to **69% by 2024**

from **28.4**

billion devices connected in **2017**

to **30.7**

billion devices connected in **2020**

and **75.4**

billion devices connected in **2025**

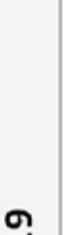
From **900** million dollars in **2015** to **3.7**

billion in market value in **2015**

32.6% CAGR from **120 billion dollars** in **2016 to 253 billion in 2021.**

Global spending on IoT technology-based products and services

from **120 billion dollars** in **2016 to 253 billion in 2021.**



Wearables market to grow

from **84** million units in **2015**

to **245** million units in **2019**

million units in **2019**

REFERENCIAS:

- 1 / Columbus, Lewis. 2013a. "Roundup of Analytics, Big Data & BI Forecasts And Market Estimates." [Http://www.forbes.com/sites/forbusicolumbus/2013/08/20/roundup-of-analytics-big-data-bi-forecasts-and-market-estimates-2016/](http://www.forbes.com/sites/forbusicolumbus/2013/08/20/roundup-of-analytics-big-data-bi-forecasts-and-market-estimates-2016/).
- 2 / "Roundup of Cloud Computing Forecasts And Market Estimates." 2016. "Forbes." Accessed March 14. [Http://www.forbes.com/sites/forbusicolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/](http://www.forbes.com/sites/forbusicolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/).
- 3 / "Roundup of Internet Of Things Forecasts And Market Estimates." 2016. "Forbes." Accessed March 14. [Http://www.forbes.com/sites/forbusicolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/](http://www.forbes.com/sites/forbusicolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/).
- 4 / "Global M2M Market to Grow to 27 Billion Devices, Generating USD 1.6 Trillion Revenue in 2024." 2017. Accessed March 14. [Https://machinerearch.com/news/global-m2m-market-to-grow-to-27-billion-devices-generating-usd-16-trillion-revenue-in-2024/](https://machinerearch.com/news/global-m2m-market-to-grow-to-27-billion-devices-generating-usd-16-trillion-revenue-in-2024/).
- 5 / M2M Global Forecast & Analysis. 2014-26. "2017. Accessed March 14. [Https://machinerearch.com/report/m2m-global-forecast-and-analysis-2014-24/](https://machinerearch.com/report/m2m-global-forecast-and-analysis-2014-24/).
- 6 / "IoT Number of Connected Devices Worldwide 2012-2020." Statista. Accessed March 14. [Https://www.statista.com/statistics/421264/iot-number-of-connected-devices-worldwide/](https://www.statista.com/statistics/421264/iot-number-of-connected-devices-worldwide/).
- 7 / "Wearables Market to Be Worth \$25 Billion by 2019." 2017. Accessed March 14. [Http://www.techinsight.com/press/company-news/2832-wearables-market-to-be-worth-25-billion-by-2019-reveals-cs-insight](http://www.techinsight.com/press/company-news/2832-wearables-market-to-be-worth-25-billion-by-2019-reveals-cs-insight).

Second, as the IoT takes hold, societies will increasingly gravitate towards so-called 'smart cities', 'smart grids', and 'smart healthcare systems'. IoT devices will play a key role in these environments, given their ability to monitor a situation and communicate rapidly with other devices. While these developments may help relieve issues such as urban congestion, or facilitate more efficient delivery of energy, they also open the door to new vulnerabilities. Again, the lack of embedded security systems in most of these sensors leads to the possibility of tampering and disruption. This may be particularly problematic for our critical infrastructures and services which are increasingly connected to the internet via commercial, off-the-shelf systems. Should one of these infrastructures – such as the energy grid – be compromised, it could result in effects that quickly 'cascade' to other critical systems. As a result, the move to 'smart' communities and services may in the future become an Achilles heel unless security systems are systematically introduced over the coming years.



Graphic: BEREC report 'Enabling the Internet of Things', p 8.

Thirdly, and related to the previous point, the IoT revolution results in greater machine-to-machine (M2M) communications. Already in 2012, a report by IDC Digital Universe estimated that 40 % of data worldwide may be machine-generated by 2020, a substantial increase from approximately 11 % in 2005. While growth in M2M does not pose a direct security challenge, this may not be the case should M2M exchanges be tampered with. By way of illustration, imagine a bridge fitted with multiple sensors to identify early signs of cracking in the structure. What would happen if someone triggered these sensors falsely? Besides creating disruptive false alarms, it could undermine trust in an IoT world.



Graphic: Commission staff working document: Advancing the Internet of Things in Europe. SWD(2016) 110 final.

Managing the security impact of new cyber developments

Reinforcing the 're-emerging' nature of cybersecurity challenges are developments in evolving fields such as big data, cloud computing and machine learning. As is the case of IoT, advances in these fields will result in multiple benefits to society, including economic growth and innovation (see Table 1 below). Unfortunately, they may also contribute to new vulnerabilities and challenges.

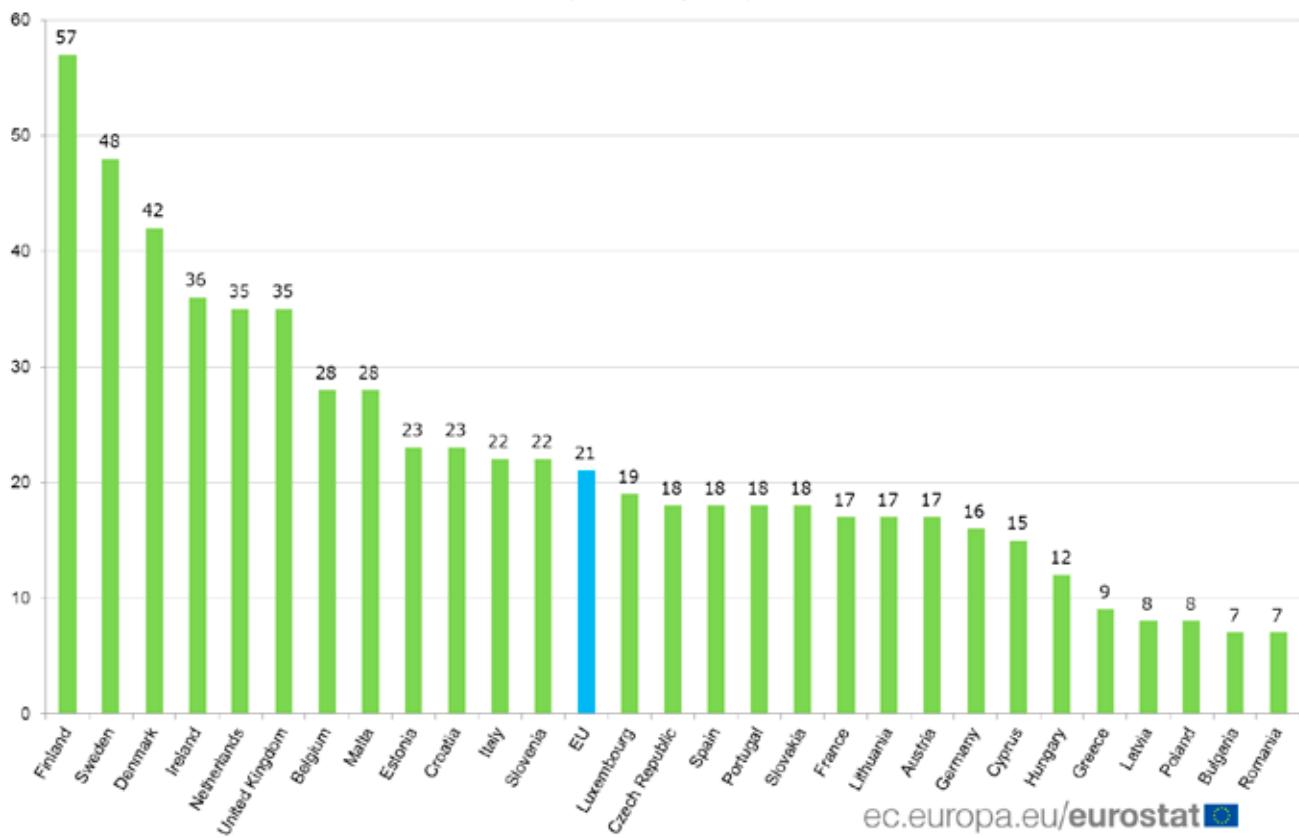
Table 1: Estimated Potential Economic Impact of Select Technologies in 2025

Technology	Lower Bound Estimate (\$billion)	Upper Bound Estimate (\$billion)
The Internet of Things	2.7	6.2
Cloud technology	1.7	6.2
Autonomous and near-autonomous vehicles	0.2	1.9

Source: McKinsey Global Institute analysis, May 2013

Concerning cloud computing, the benefits are already well-known. Companies worldwide have experienced efficiency savings through less spending on IT infrastructure – especially on the software side – while facilitating employee mobility. Less well-known are some of the drawbacks of cloud services.

Use of cloud computing services by enterprises in the EU Member States, 2016
(% of enterprises)



To illustrate, cloud service providers increasingly attract attention from individuals and groups with malicious intent. They are interested in leveraging the cloud to hide their tracks or stage their attacks. Others seek to target the clouds themselves to gain access to the companies relying on their services. Yet other groups are discovering the economic value of almost any kind of data, viewing it as a potential source of revenue. According to a recent Tech2 report citing an IBM study, cloud-related cyber-attacks increased by over 400 % in 2017 in comparison with 2016. In the future, as more activities are routed through cloud service providers, the greater is the likelihood that it will become a significant cybersecurity dilemma.

Within the field of big data, positive prospects range from more precise analytics to developments in areas such as artificial intelligence. A major challenge, however, is that big data poses an attractive target given the vast amount of data involved. Data breaches on big data sets can yield valuable information while undermining data protection efforts – indirectly affecting societal trust in such entities or structures. A little known but illustrative big data breach took place in June 2015. At that time, the US Office of Personnel Management discovered that millions of records from its

personnel files were compromised. These included 18 million Standard Form 86 (SF-86) questionnaires for federal security clearances.¹ The implications of such a breach are manifold and still being examined, from potentially revealing agents operating abroad to facilitating the blackmail of specific individuals.

Progress in machine learning – a cornerstone for artificial intelligence – is likely to impact society in multiple ways. Among the perceived positive benefits are driverless cars and autonomous platforms that can take on search and rescue operations in hazardous environments. On the more worrisome side are concerns over possible lethal autonomous weapons (LAWs), especially if these can be tampered with in any way. While the debate is still in the early phase – examined mainly under the auspices of the Convention on Certain Conventional Weapons – the diverging positions are maturing. Among many key issues of concern is whether autonomous weapons systems can be compromised or sabotaged via cyber means; and if so, to what types of unintended consequence might follow.

Managing the relationship between cyber defence and cyber offence

A third emerging cybersecurity challenge concerns the balance between defensive and offensive cyber capabilities. The debate is not new but the boundaries between the two postures have become increasingly blurred. In a January 2017 Joint Statement to the Senate Armed Services Committee concerning cyber threats to the United States, senior US officials noted that over 30 countries are developing offensive cyber-attack capabilities. This is consistent with a 2011 UNIDIR report stating that 33 states include cyberwarfare in their military planning and organisation, with another close to 40 States having the ability to move in that direction quickly if needed.²

Looking to the future, it seems that interest in cyber offensive capabilities is likely to increase among states. Several already openly admit that they are pursuing such capabilities, providing also some indication as to the circumstances under which they might be used. This trend is likely to yield new cybersecurity challenges. One challenge is the risk of stolen state-created ‘cyber-weapons’. There is already one precedent. In the summer of 2016, a group known as the Shadow Brokers stole sophisticated malicious code from the US National Security Agency. Some of this code eventually

1 For more information, see Brendan Koerner, ‘Inside the Cyberattack that Shocked the US Government’, *Wired Magazine*, October 2016 (available at <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>)

2 James A. Lewis, Katrina Timlin, ‘Cybersecurity and Cyberwarfare’, UNIDIR Resources 2011 (available at <http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>)

made its way into well-known cyber-attacks such as the WannaCry ransomware attack from 2017 – affecting hundreds of thousands of computers worldwide. The risk of this happening again would multiply should more countries move towards the stocking of offensive cyber code.

Efforts to acquire offensive cyber capabilities may likewise lower the bar for usage. Early signs of such a trend are gradually becoming visible, with countries exploring how cyber means can be applied to advance security policy agendas without having to rely on kinetic means. Challenges associated with assigning attribution make it an appealing option for exercising influence without attracting undue attention. Should this trend eventually grow, it could fuel a cyber arms race, opening the door to new forms of hybrid threat – testing the resilience of society in unprecedented ways.

Graphic: RandEurope 2018 / EDA: Exploring Europe's capabilities requirements for 2035 and beyond, p31



Key technologies that may facilitate future military capabilities in 2035+.

3.2 Cyber reservists: a flexible solution to address peaks in malicious cyber activities

by François Rivasseau and Elois Divol

Cyber threats to the European Union and its Member States are growing exponentially. As recalled in the Council conclusions of April 2018 on malicious cyber activities, the EU is concerned about the increased ability and willingness of third states and non-state actors to pursue their objectives by undertaking malicious cyber activities. The EU stresses that the use of information and communication technologies (ICTs) for malicious purposes is unacceptable as it undermines stability, security and the benefits provided by the internet and the use of ICTs.

In September 2017, the EU complemented its cybersecurity strategy with a Joint Communication of the EEAS and the Commission on building strong cybersecurity for the EU. The Joint Communication includes measures to boost our resilience to cyber threats, measures to increase our capabilities to catch cybercriminals and measures to strengthen international cooperation. It also stresses the need to build a strong EU cyber skills base, as skilled professionals are indeed central in implementing the new objectives.

The transposition of the Directive on security of network and information systems (the 'NIS Directive') also played an important role in ensuring Member States' preparedness, notably with regard to protecting the essential services which are vital for our economy and society, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. The Directive requires Member States to be appropriately equipped, including via the establishment of a government Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.

NEW SECURITY THREATS FOR EUROPE

debating
europe

AT THE START OF 2016, THE WORLD ECONOMIC FORUM PUBLISHED A TOP 10 OF SECURITY THREATS:

1 2
3 4
5 6
7 8
9 10

- LARGE-SCALE INVOLUNTARY MIGRATION
- EXTREME WEATHER EVENTS
- FAILURE OF CLIMATE-CHANGE MITIGATION
- INTERSTATE CONFLICT
- NATURAL CATASTROPHE
- FAILURE OF NATIONAL GOVERNANCE
- UNEMPLOYMENT OR UNDEREMPLOYMENT
- DATA FRAUD OR THEFT
- WATER CRISIS
- ILICIT TRADE

FOUR POTENTIAL DANGERS OF TECHNOLOGY:

I
II
III
IV

ADVERSE CONSEQUENCES OF TECHNOLOGICAL ADVANCES

- LIKE ARTIFICIAL INTELLIGENCE, GEO-ENGINEERING, SYNTHETIC BIOLOGY CAUSING HUMAN, ENVIRONMENTAL AND ECONOMIC DAMAGE

BREAKDOWN OF CRITICAL INFORMATION INFRASTRUCTURE AND NETWORKS

- LIKE ATTACKS ON INTERNET NETWORKS, SATELLITES, ETC. CAUSING DISRUPTION

LARGE-SCALE CYBER ATTACKS

- CAUSING LARGE ECONOMIC DAMAGE, GEOPOLITICAL TENSION OR LOSS OF TRUST IN THE INTERNET

MASSIVE INCIDENT OF DATA FRAUD/THEFT

- OF PRIVATE OR OFFICIAL DATA ON A LARGE SCALE

EXAMPLE:

UKRAINE'S POWER PLANT HACK

WHAT IS...

"THE INTERNET OF THINGS" (IOT)

NETWORK OF PHYSICAL OBJECTS THAT ARE CONNECTED VIA INTERNET, SENSORS, SOFTWARE AND ELECTRONICS, ALLOWING THESE OBJECTS TO EXCHANGE AND COLLECT INFORMATION.

IN 2015, HACKERS BROUGHT DOWN THE POWER SUPPLY TO HUNDREDS OF THOUSANDS OF HOMES IN UKRAINE
(MORE THAN 800,000 PEOPLE)

INFRASTRUCTURES VULNERABLE TO CYBERATTACKS:



*THEY HAVE LITTLE OR NO CYBER PROTECTION.

CYBERSECURITY & TERRORISM...



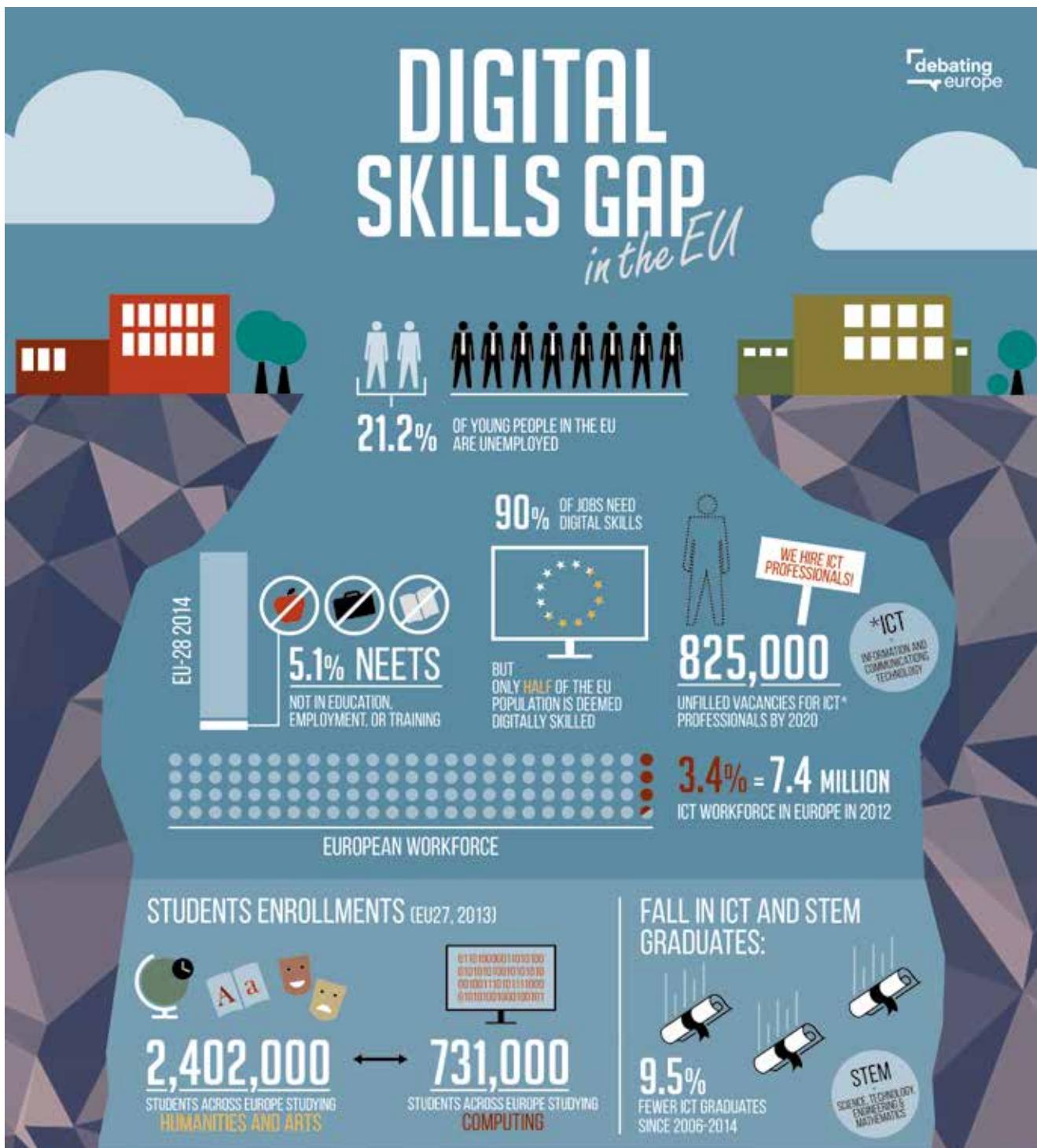
A TERRORIST CYBERATTACK ON THESE INDUSTRIES COULD CAUSE ENVIRONMENTAL DISASTERS, ECONOMIC CASUALTIES AND LOSS OF PROPERTY AND/OR LOSS OF LIFE



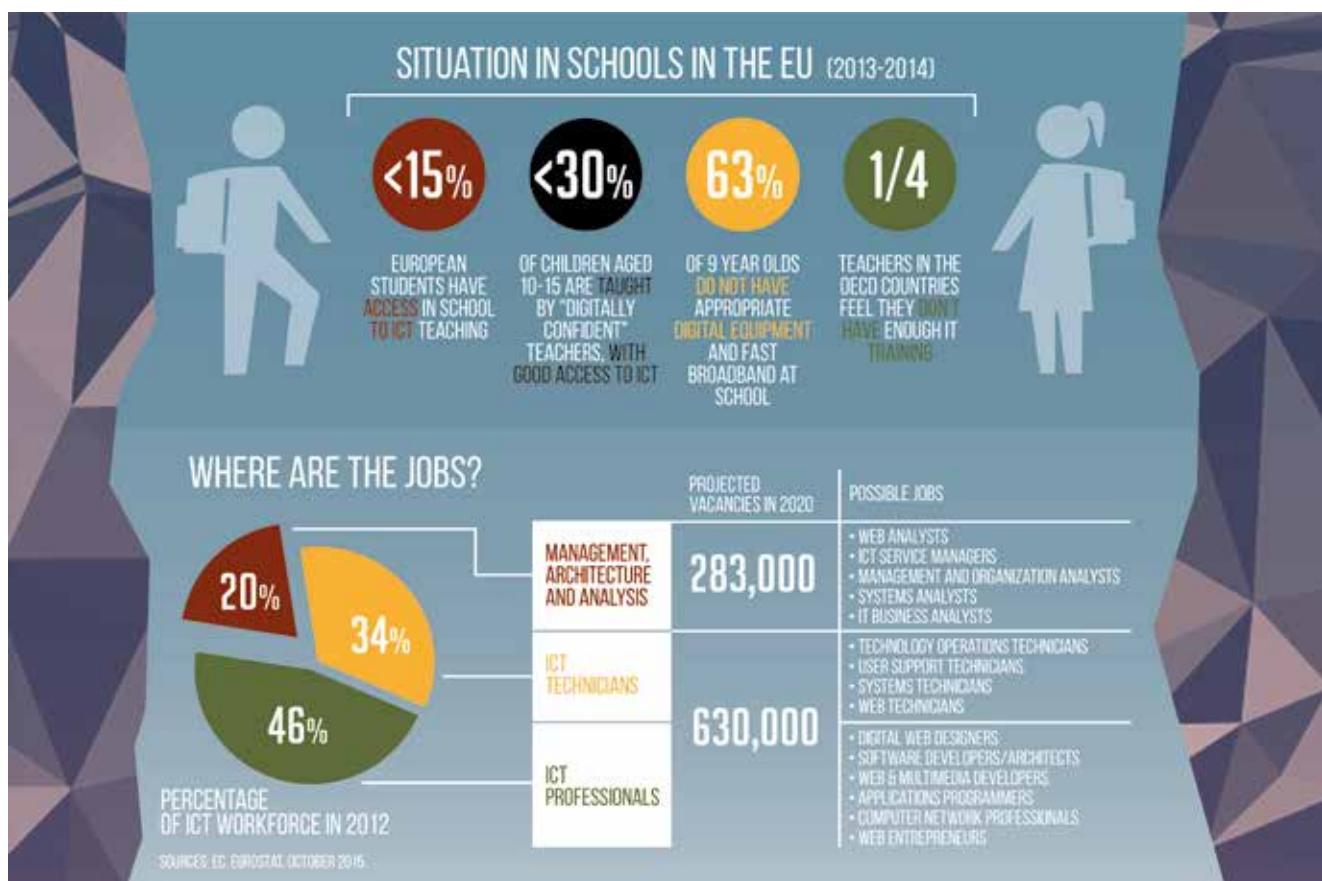
WHICH COUNTRIES ARE MOST WORRIED ABOUT CYBERATTACKS?

ESTONIA	THE NETHERLANDS
GERMANY	SINGAPORE
JAPAN	SWITZERLAND
MALAYSIA	UNITED STATES

Sources: European Commission, World Economic Forum, February 2016.



Graphic: Debating Europe, www.debatingeurope.eu



Protecting critical infrastructures and essential services

The CSIRT and the competent national NIS authority form the basis for efficiently protecting critical infrastructures and essential services against malicious cyber activities. They should be appropriately staffed so as to be able to handle the day-to-day work with operators of essential services and support the response to several successful cyber-attacks in parallel when such events occur.

However, such national structures cannot mitigate all possible risks at one and the same time. In the unlikely, but still possible, event of a significant number of critical infrastructures and essential services being affected simultaneously, they would require additional human resources.

Cybersecurity

Why do we need to reinforce cybersecurity?

Because **incidents undermine trust** in the digital society:

Theft of commercial trade secrets,
business information & personal data



Disruption of essential services &
of critical infrastructure



Losses of hundred of billions of euro each year



ec.europa.eu/digital-single-market/en/cybersecurity
#DigitalSingleMarket #cybersecurity #PPP #NIS

Cooperation and solidarity among Member States forms part of the answer. The CSIRT Network, which connects all the CSIRT of EU Member States and the CERT-EU, promotes swift and effective operational cooperation on specific cybersecurity incidents and sharing of information about risks. Under the framework of the PESCO, some Member States will create Cyber Rapid Response Teams to provide mutual assistance among participating Member States.

This would be effective if several critical infrastructures and essential services of one Member State were affected by malicious cyber activities, but would have limitations if several Member States were affected simultaneously.

In the latter case, the government agencies responsible for the protection of critical infrastructures and essential services should be able to draw on a workforce normally assigned to other tasks, such as cyber security in the private sector. Such a workforce would by definition be a '**reserve**'. It would offer the required flexibility of being able to rapidly mobilise a large additional number of cyber defence specialists in the event of a major cyber-attack putting national critical infrastructures and essential services at risk.

Cyber reserves in practice, and the EU's added value

Some of the most forward-thinking Member States on cybersecurity and cyber defence, such as France, Germany, the Netherlands and Estonia, have started to structure part of their forces into such cyber reserves. It is worth noting that outside of the EU, other major cyber players (including the US, China and Russia) are developing such a capability

as well. NATO also promotes reserves, stating that specialised reservists are crucial, including in the cyber domain.

As every national context is different, a reserve can be managed by either military or civil chains of command. Reservists should be managed by their country of citizenship, in accordance with their respective reserves procedures. We can identify three phases: attracting and selecting good candidates, training them, and managing them.



The EU's added value lies in the training, as the attraction and management of reserves is largely dependent on the national context. A certain degree of harmonisation of the training requirements would contribute to the development of a common strategic culture and would ensure complementarity between the reserves (internal operational mobility of resources) and the cooperative and solidarity initiatives (operational mobility of resources between Member States).

To that end, the EU could leverage the cyber training and education platform, which was established under the ESDC in February 2018, following the commitment made in the update of the EU cybersecurity strategy that 'the Commission [would] work in close cooperation with Member States, the High Representative and other relevant EU bodies to establish a cyber training and education platform to address the current skills gap in cybersecurity and cyber defence by 2018'.

The main goal of the platform would therefore be to provide all EU Member States with the option of developing a cyber-defence reserve capability. The platform would in practice bring together all providers of cyber-defence training in a network, and actual training would be carried out by Member States' national universities, academies, colleges and institutes certified as platform members. The certified institutions would receive funding for each trainee, with trainees being citizens of any Member State of

the European Union selected through the standard procedure of each institution. Direct funding should be provided by appropriate Commission funds to echo its commitment under the European Defence Action Plan and the Joint Communication, and should be at a level in line with our ambitions.

Potential to make a big difference

Such a platform has the potential to make a huge difference and confirm the unique added value of the EU in this field. Building as much as possible on training opportunities offered throughout the EU, the platform would finance the training of reservists and encourage exchanges between Member States. Among the numerous programmes implemented or planned by Member States to increase training and education – and which could be scaled up by the platform – we can cite the establishment of a cyber defence specialisation route under the Master's in international security in Germany's University of the Armed Forces in Munich, the postgraduate programme on cybersecurity for military staff in Portugal, and the creation of the *Pôle d'excellence* cyber in France.



Graphic: Ecole nationale de la statistique et de l'analyse (ENSAI)

Additionally, the platform could benefit from and strengthen EU-NATO cooperation, as the common set of proposals for the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary-General of the North Atlantic Treaty Organisation in Warsaw on 8 July 2016 includes proposals in the cyber domain, including on the harmonisation of training requirements, where applicable, and the opening of respective training courses for mutual staff participation.

It should also be noted that when there is no peak of malicious cyber activities for a long period of time, the cyber reservists could also be regularly mobilised for other missions leveraging their skills, such as promoting cyber awareness or strengthening the defence culture of citizens.

3.3 Gender and cyberspace

by Charlotte Isaksson

When I mentioned that I had been asked to write a chapter on Gender and Cyberspace for this handbook, the immediate response from a colleague was to ask: what on earth does gender have to do with cyberspace?

Well, let's start by looking at the European Commission and the High Representative's 2013 Cybersecurity Strategy. This was the first comprehensive EU policy document in the area, and it can provide us with some answers. The EU Cybersecurity Strategy clearly sets the priorities for EU international cyberspace policy:

1. freedom and openness: the strategy outlines the vision and principles for applying core EU values and fundamental rights in cyberspace;
2. ensuring that the EU's laws, norms and core values apply as much in cyberspace as in the physical world: responsibility for a more secure cyberspace lies with all players in the global information society, from citizens to governments;
3. developing cybersecurity capacity building: the EU should engage with international partners and organisations, the private sector and civil society to support global capacity building in third countries, including by improving access to information and an open internet and by preventing cyber threats;
4. fostering international cooperation in cyberspace: preserving open, free and secure cyberspace is a global challenge which the EU is addressing together with relevant international partners and organisations, the private sector and civil society.



'Gender Equality is one of the fundamental values of the EU' emphasises Ms. Helga Schmidt, Secretary General of the External Action Service (second from right).

Photo: European Union

Cyberspace and gender-based violence

With the increased availability of internet access and the expansion of social media, violence against women and girls (VAWG) in cyberspace has become a growing phenomenon. Evidence shows that 10 % of women aged 15 or older have experienced some form of cyber violence, and that men and women experience the resulting harm differently, highlighting the problem with taking a gender-blind approach to cyber violence. Other available research suggests that women are disproportionately targeted by certain forms of cyber violence, compared with men. In a recent survey of more than 9 000 German internet users aged 10 to 50, women were found to be victims of online cyber stalking and sexual harassment¹ significantly more frequently than men.

The expanding internet and the wide diffusion of social media present new opportunities for women to make their voices heard and raise awareness on several pressing issues – take, for example, the recent #metoo campaign. Moreover, the annual 16 Days of Activism campaign against violence against women uses the internet and social media as an instrument and asset to spread the message globally. While the internet may offer connectivity, empowerment and access to services, it can also cement and normalise gender roles and cultural customs. The online world, or cyberspace, is not just a mirror image of the real world, but a ‘hall of mirrors’ reflecting and amplifying both the positive and the negative. For women and girls, these reflections are all too often reflections of a culture of misogyny, marginalisation and violence. With 450 million new women expected online over the next three years, more and more women are relying on the internet for educational and professional resources. Cyberspace undoubtedly offers multitudes of possibilities and opportunities for women’s empowerment and, in the long run, even

The campaign '#WeSeeEqual' was launched to advocate for gender equality ahead of International Women's Day.



Photo: European Union

¹ Staude-Müller, F., Hansen, B. and Voss, M., 'How stressful is online victimization? Effects of victim's personality and properties of the incident', European Journal of Developmental Psychology, Vol. 9(2), 2012. Available at: <http://www.tandfonline.com/doi/abs/10.1080/17405629.2011.643170>

gender equality, but there are two sides to the coin. The gender-based violence and discrimination present in our society is equally present online, if not more so.

Blurred border between online and offline violence

We need to understand that we must not try to address cyber violence separately from real-world manifestations of violence, since it is an inherent part of the continuum of sexual and gender-based violence (SGBV): VAWG, domestic violence, femicide, trafficking and female genital mutilation. It also targets men and boys, and it can take many forms. Research has shown that online abuse against women shares several features with offline abuse, so when someone suffers offline, they are likely to suffer online too.

Women and girls who have been victims of stalking, sexual harassment or violence offline by an intimate partner are also often victims of online violence by the same perpetrator. As with all types of violence, cyber violence deeply affects the lives of victims. Yet, most cyber VAWG goes unreported and law enforcement agencies are failing to take appropriate action² against cyber VAWG in 74 % of the 86 countries surveyed. One in five female internet users live in countries where online abuse and harassment are unlikely to be punished.



² WWW Foundation

However, cyber-related gender-based violence is not fully conceptualised or legislated against at EU level, while in the EU Member States where it is, the available data is not disaggregated by the gender of the victim and perpetrator and the relationship between them. This makes it impossible to conduct a gendered analysis of cyber violence and to compare online and offline VAWG. A recent and growing form of cyber VAWG is that linked to an intimate partner, e.g. stalking, harassment and non-consensual pornography. Research shows that up to 90 % of non-consensual pornography victims are women. Many women in these studies have experienced multiple types of abuse as a routine part of their online lives, meaning abuse is experienced as a course of behaviour rather than a set of individual acts. Indeed, women are often frustrated when law enforcement authorities treat each individual, harassing communication 'as a discrete act, rather than grasping the harm caused by the accumulation of abuse'³.

We can therefore see that gender-related crimes and assaults in cyberspace impact, and are impacted by, the world outside. This means that cyberspace must be sufficiently factored in to any gender analysis and/or assessments if we want to be comprehensive in our approach.

Gendered cyber violence as a limitation of democracy

Fear of being targeted in cyberspace can reduce the likelihood of women's rights activists and human rights defenders taking an active part in society, politics, democratic activities or actions promoting women's rights. We know that the space for women's rights activists and women's human rights defenders is shrinking in many places around the globe. In this regard, violence and threats against them in cyberspace represent not only an individual problem but also a democratic problem limiting their freedom of movement and speech.

In Colombia, a woman journalist was given a warning message saying that she should take care of her children so that nothing would happen to them and that she should not be surprised if she was raped on her way home. Providing detailed information about the victim's children and the location of their home is a common modus operandi when the victim is a woman, not when the victim is male.

Furthermore, the space for online activism is decreasing due to repression and intimidation through blackmail, slander, harassment and stalking – by both state and non-state

3 Lewis, R., Rowe, M. and Wiper, C., 'Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls', *The British Journal of Criminology*, Vol. 57, No 6, 2017, pp. 1462-1481.

actors. In a report from 2015⁴, human rights defenders were asked about harassment and attacks in an online survey. 'More than half (55 %) of the respondents said that they had faced threats on the internet'⁵.



See: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf

Da'esh, recruitment and gendered roles

A recent article argues that suspension is an integral part of the online lives of Da'esh supporters, a fact which is reproduced in online identities, and that Da'esh considers cyberspace to be the new frontline. The highly gendered roles of Da'esh males and females are 'enforcing norms that benefit the group: the shaming of men into battle and policing of women into modesty'⁶. While women have long participated in violent extremist groups around the world, the proportion joining Da'esh from abroad is particularly high. Of the Da'esh members who have joined from Europe, approximately 20% are women. Da'esh messages targeted specifically at women and girls are not simply about the nobility of becoming a 'jihadi bride'⁷. Instead, the recruiters – often women themselves – use the narrative that Western societies do not respect Muslim women and assert that Muslim women are looked upon in the West solely as victims, oppressed or ridiculed by their own communities.

4 Femdefenders report (2015) <http://thekvinnatillkvinnafoundation.org/en/files/qbank/f16ba6f00bce15507c766cd5e8057728.pdf>

5 <https://kvinnatillkvenna.se/wp-content/uploads/2018/03/kvinna-till-kvinna-suffocating-the-movement-report-eng-2018.pdf>

6 Pearson, E., 'Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media', *Studies in Conflict & Terrorism*, 2017, DOI: 10.1080/1057610X.2017.1352280

7 Heather Hurlburt and Jacqueline O'Neill (2017) <https://www.vox.com/the-big-idea/2017/6/1/15722746/terrorism-gender-women-manchester-isis-counterterrorism>

A different version of these gendered narratives is related to men. Mercy Corps⁸ found that the most common justification offered by Jordanian fighters as to why they had joined the war in Syria was not poverty or compensation, but protecting Sunni women and children, particularly from rape.

Da'esh promises a future where women will hold a highly valued place of honour, playing a foundational role in building their caliphate, including as informants and enforcers of their rules. Lately, European observers have even noticed a slight increase in female Da'esh recruits using the language of women's rights – dignity and autonomy – to talk about their role in carrying out terrorist plots. All of this amounts to highly gendered narratives entering cyberspace, with both direct and indirect consequences for EU security.

Cyberspace as a positive area for change

Not everything about cyberspace is negative in terms of gender. There are also examples of technology and social networking working as allies against gender-based violence. The most well-known by now is probably the #metoo campaign from autumn 2017, but there are many other similar examples. In Argentina, the hashtag #NiUnaMenos (or 'not one less') was established recently to reject femicides, which continue to go unpunished, and has become an ongoing slogan for cyber activism against domestic violence. In Pakistan, #Bytes for All (or 'aware girls') has been promoted as an effective campaign to combat gender-based violence. It uses storytelling to engage teenage girls and teach them about their rights. In the Democratic Republic of the Congo, the Medicap app is being introduced, giving users the possibility to collect, share and preserve forensic evidence of sexual violence.

There are several good examples of technology and social networking working as allies against gender-based violence.



Photo: European Union, 2015 / EC - Audiovisual Service / Johanna Leguere

8 A humanitarian organisation

A similar project exists in Nicaragua using video blogs, while 'Take back the tech!' was launched in 2006 by a group of young women in South-East Asia in response to the increasing use of mobile phones and geo-location software as means to physically violent ends.

Conclusion

To conclude, the importance of women's access to technological empowerment as one of the core indicators for progress towards gender equality cannot be emphasised enough. However, to achieve this goal, we must make sure that the internet is a safe and secure place that allows all women and girls to fulfil their potential as equal members of society and live a life free from all forms of violence. Therefore, oversight and enforcement of laws and rules prohibiting cyber VAWG are of critical importance if the internet is to become a safe, respectful and empowering space for women and girls, as well as for men and boys.

There is still much to be done to address gendered aspects of cyberspace, including dealing with the shrinking space for actors working for women's rights and gender equality. Social attitudes and norms must change if we are to shift the way online abuse is understood and address the lack of seriousness with which it is treated. There is a need for public education as well as education of enforcement agency staff, such as police. Policy responses should be formulated in recognition of the fact that gendered violence in cyberspace is a form of VAWG and needs to be addressed in the same way as any other form of sexual or gender-based violence. This highlights the need to engage not only with policymakers and institutions but also, increasingly, with internet actors and tech companies as they have a very big role to play, as does anyone working with issues related to gender equality, women's empowerment and the implementation of the Women, Peace and Security agenda. We must all factor in what is happening in cyberspace in our decision-making processes and activities.

3.4 The EU as a partner in cyber diplomacy and defence

by Thomas Renard and Andre Barrinha

The European institutions became involved in cyber-related issues in the 1990s. However, cyberspace only came to be conceived as a security space a decade later. As late as 2003, cyber issues were not even mentioned in the European Security Strategy (ESS). That was to be progressively rectified with a number of non-binding communications from the European Commission, focusing mostly on the security of the EU's cyberspace.

More recently, the EU's cyber agenda has broadened considerably to embrace more systematically the international dimension of cyber issues. In 2013 it adopted its first cybersecurity strategy, which included international priorities. It also adopted European Council conclusions specifically on 'cyber diplomacy' in 2015, marking the beginning of a more proactive role for the EU in international cyberspace policy-making. In 2017, the Council agreed to develop a full cyber-diplomacy 'toolbox', with the potential for approving retaliatory measures against cyber-attacks conducted or sponsored by other states.



The development of the EU's global cyber agenda sits at the juncture of three key trends. First, the growing importance of cyber issues, which have progressively become core themes in Member States' agendas. Second, beyond domestic priorities, cyber

issues have climbed the international agenda as well, becoming increasingly 'politicised'. Indeed, cyberspace has become an immensely contested area, confronting distinct national interests and visions for the digital age. Cyber issues were treated first as purely technical issues, then as external aspects of domestic policies, before being recognised as a major foreign policy topic. Third, the EU's own internal evolution, gradually developing itself as a diplomatic and security actor with global ambitions, is naturally leading to the development of global cyber ambitions and tools. This short contribution seeks to highlight key elements of that evolution.

The EU as a cybersecurity actor

The EU became interested in cybersecurity in the late 1990s, with a clear focus on cybercrime and its potential negative impact on the single market. Since the early 2000s, it has progressively expanded its interest and role in this domain, internally at first and subsequently externally. At the domestic level, the European Commission and the Council adopted a series of non-binding documents throughout the 2000s related to computer security, critical (information) infrastructure protection and even cyberterrorism. It was only at the turn of the first decade of the 21st century that cyberspace became a paramount political and strategic concern, leading the EU to agree on a number of key documents and legislation, such as:

- the 2005 Council Framework Decision on Attacks Against Information Systems;
- the 2010 EU Internal Security Strategy, which identified cybersecurity as one of its five strategic objectives;
- the 2013 EU Cybersecurity Strategy, which identified five strategic priorities: building resilience; fighting cybercrime; developing cyber defence policy; fostering industrial and technological resources; and embedding EU values in cyberspace;
- the 2015 Agenda on European Security, which defines cybercrime as one of its three priorities (together with serious organised crime and terrorism);
- the 2016 Network Information Security (NIS) Directive, which is the first EU-wide legislation on cybersecurity. It makes it mandatory for EU Member States: to be prepared and equipped to respond to cyber incidents (e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority); to cooperate swiftly and effectively among themselves in case of incidents, notably by sharing information; and to develop a 'cybersecurity culture' among critical sectors and businesses, with the obligation to notify security breaches.
- a revised EU Cybersecurity Strategy was adopted in September 2017, together with a package of new proposals. It focuses on the creation of new technological capabilities via research, innovation and skills development and on the improvement of cooperation at EU level.

At the external level, the EU's activity is more recent and to some extent more modest. The 2003 European Security Strategy, a key document that listed the main security challenges to the EU, did not even mention cyberspace. It was only the 2008 *Report on the Implementation of the European Security Strategy* that mentioned cyber as a potential challenge with an external dimension. High-scale cyber-attacks in the preceding months in both Estonia (2007) and Georgia (2008) certainly contributed to the progressive prioritisation of cyber issues on the security agenda. Four EU documents are particularly relevant and illustrative of the EU's growing focus on international aspects of cyber issues:

- the above-mentioned 2013 EU Cybersecurity Strategy called for a more active EU engagement at international level, notably by deepening the dialogue with third countries and international organisations and by stepping up capacity-building programmes in third countries;
- the 2015 Council conclusions on cyber diplomacy promote a number of objectives and principles related to the EU's global cyber engagement: the promotion and protection of human rights in cyberspace; norms of behaviour and application of existing international law in the field of international security; internet governance; enhancing competitiveness and prosperity; capacity building and development; and strategic engagement with key partners and international organisations;
- the 2016 EU Global Strategy, the main guiding document for the EU's foreign policy, considers 'cyber' as one of the key constituents of Europe's security but also as a significant element in the EU's foreign policy (e.g. to build cyber resilience in the neighbourhood or to shape the global cyberspace);
- the 2017 Council conclusions on a 'cyber-diplomacy toolbox' affirm the EU's willingness to put to use the entire scope of CFSP measures, including restrictive ones (such as sanctions), in order to respond in a proportionate manner to cyber malicious activities by third parties, to protect the Union and to attain its foreign policy objectives.

In its pursuit of domestic and foreign cyber policies, the EU relies on a growing number of agencies that are particularly relevant. They include:

- the European Union Agency for Network and Information Security (ENISA), established in 2004, which strengthens EU Member States' cyber resilience through advice and capacity building;
- the EU Computer Emergency Response Team (CERT-EU), set up in 2012, which is in charge of the response to cyber incidents within EU institutions;
- Europol's European Cybercrime Centre (EC3), established in 2013 to strengthen the law enforcement response to cybercrime, notably through operational support;

- the European Defence Agency (EDA), which considers 'cyber' as one of its priorities and works on the cyber-defence capability development of its member states;
- the European Security and Defence College (ESDC), which has been in charge of education, training, evaluation and exercise in the field of cybersecurity and defence (cyber ETEE platform) since 2018 and is therefore tasked with providing cyber-related training to civilian, police and military staff, in line with CSDP requirements.

Cyber diplomacy and cyber partnerships

Cooperation in cyberspace is a choice, not a given. In 2011, Barack Obama wrote in the introduction to the US *International Strategy for Cyberspace* that '*by itself, the internet will not usher in a new era of international cooperation. That work is up to us.*' Indeed, cyberspace is a disputed domain. More than 30 countries worldwide are said to have developed offensive cyber capabilities, and that number is growing. Countries are also promoting very distinct models for internet governance. On the one hand, some countries, including most EU Member States, are promoting a vision of a free and open internet, whereas on the other hand, countries such as Russia and China seek to assert more government control over the internet.

In this context, and with a view 'to promot[ing] openness and freedom of the internet' and '*to encourag[ing] efforts to develop norms of behaviour and apply existing international laws in cyberspace*', as stated in the 2013 Cybersecurity Strategy, the EU has deepened its engagement with a number of strategic partners.



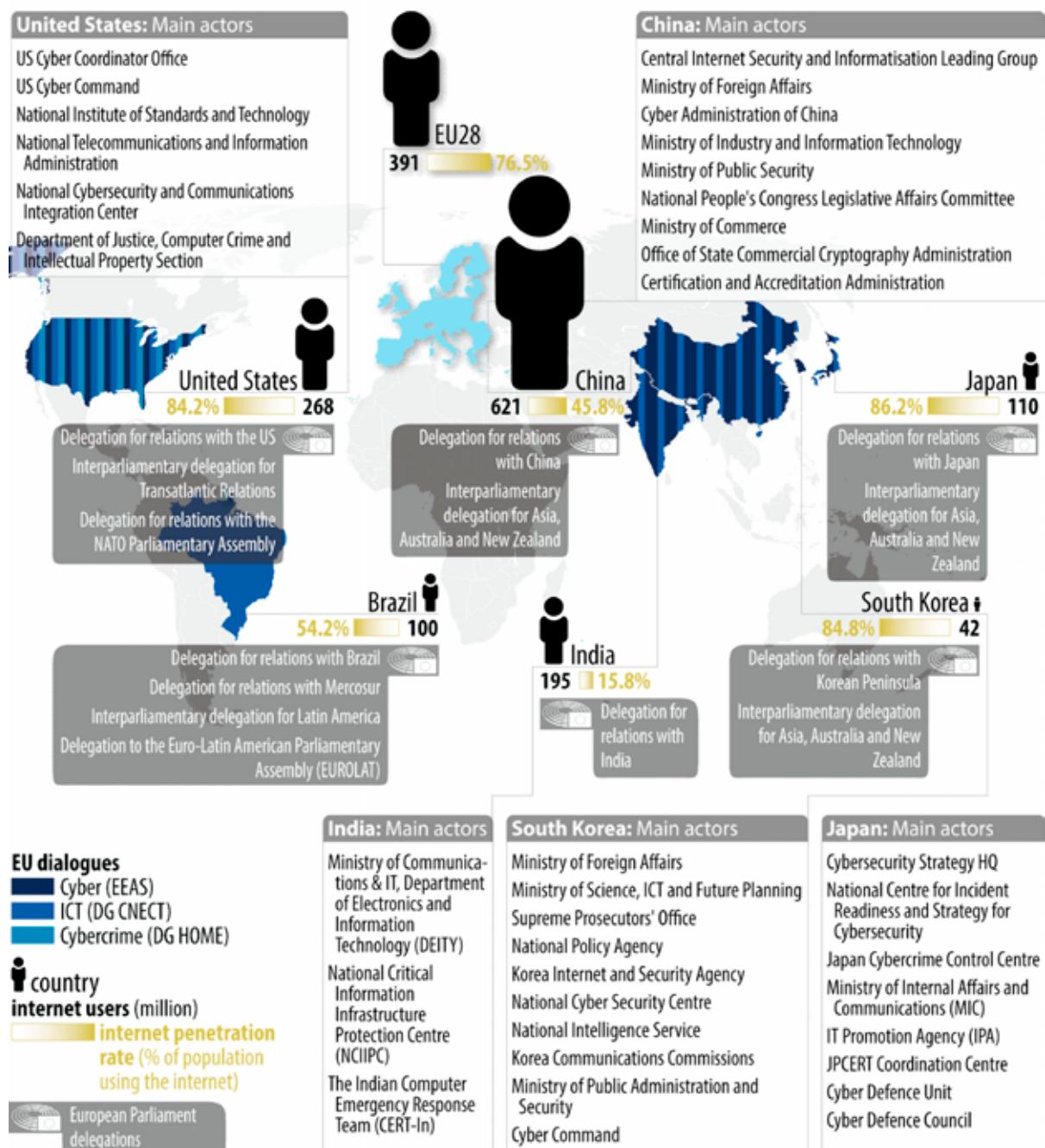
The EU has deepened its engagement in cyberspace with a number of strategic partners.

Photo: European Union, 2018 / EC - Audiovisual Service / Lukasz Kubus

It has formalised a number of partnerships with third countries by establishing regular policy dialogues on cyber issues and by adding a cyber chapter to the joint cooperation agenda, when there is one (such as the EU-China 2020 Strategic Agenda for Cooperation). Not all partnerships deliver equally, however. The EU-US cyber partnership is by far the oldest and most developed, with several annual dialogues covering various aspects of cyber policies. It is also the only partnership singled out in the EU Cybersecurity Strategy as well as in the EU Global Strategy. The partnerships with Japan and, to a lesser extent, Canada are less ambitious but still productive in a 'like-minded' context, as also illustrated by the 2017 G7 Lucca declaration on responsible state behaviour in cyberspace. Conversely, cyber partnerships with China and Russia are less straightforward. These two countries are perceived as major sources of cyber-attacks and cyber-espionage in Europe. As mutual trust is lacking, cooperation focuses mostly on confidence-building measures. This is one of the key aims of the EU-China cyber taskforce, as well as of the track 1.5 Sino-European Cyber Dialogue (SECD). Cooperation with other 'strategic partners', such as India or Brazil, remains largely under-delivering.

Such an observation would fundamentally challenge the notion of cyber partnership, were it not for the distinction between results-oriented and process-oriented partnerships. Whereas the transatlantic partnership aims for tangible deliverables, such as increasing cybersecurity in the transatlantic space and beyond, the partnerships with China and Russia mostly seek to keep the dialogue open on contentious issues, and possibly aim to build mutual confidence. Having said this, most cyber partnerships ultimately operate a balance between results and process. Even the EU-US partnership seeks to strike this balance, as it is still hampered by a serious trust deficit.

Map 1 – EU's cyber-related dialogues with third countries



Cyber defence and CSDP

When it comes to cyber defence, the EU's evolution in the field is both more recent and also more limited, due to NATO's activities and the greater reticence of Member States to cooperate in a field in which stakes are considerably higher. The first relevant incursion of the EU into the field came in late 2012 with the approval of the Concept for Cyber Defence for EU-led CSDP operations. This was followed soon afterwards by the EU defence ministers' agreement to put cyber defence on the Pooling & Sharing agenda. The European Defence Agency (EDA) has had a leading role in this field, facilitating and supporting Members States' related activities.

In greater depth, and in line with the above-mentioned 2013 Cybersecurity Strategy, the Council approved the Cyber Defence Policy Framework in November 2014, defining the general guidelines for the EU's activities in its external dimension, including CSDP, protection of the EEAS networks and relations with other partners, such as NATO.

In 2016, the EU and NATO reached an agreement on the issue – the Cyber Defence Pledge. This document focuses on areas of common interest such as fostering joint training exercises and deepening cooperation between states and between the two organisations. The European Commission also included cyber defence as a top priority in its European Defence Action Plan (November 2016). That has also been reflected in two separate projects within the permanent structured cooperation (PESCO): one on the creation of a European Cyber Information Sharing Platform and another on the development of European Cyber Rapid Response Teams.

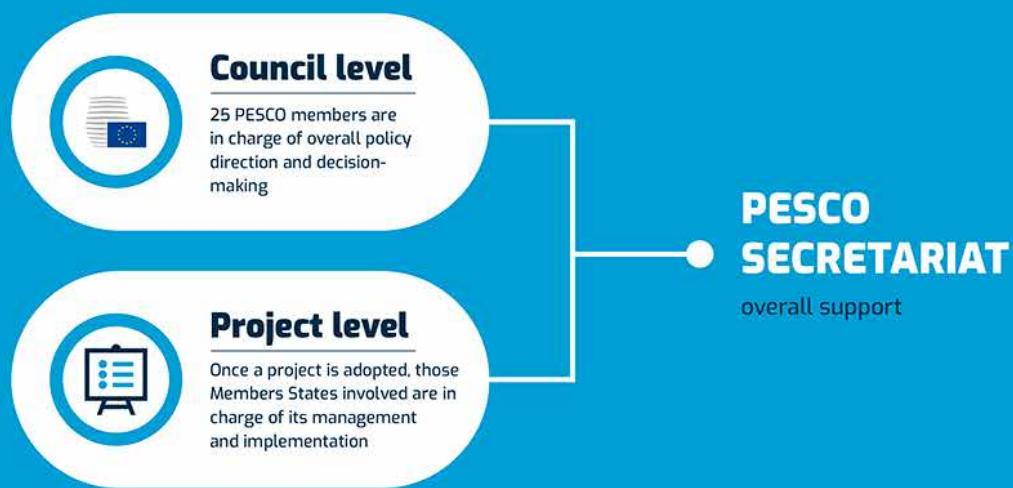
Despite the EU's recent emphasis on resilience and deterrence – made clear by the 2017 Joint Communication by the European Commission and the High Representative for Foreign Affairs and Security Policy – its own role in terms of cyber resilience and cyber deterrence remains limited.



PESCO - WHAT IS IT?

Permanent Structured Cooperation, treaty-based framework and process to deepen defence cooperation among participating Member States to develop capabilities and increase their operational availability.

HOW DOES IT WORK?



PESCO SECRETARIAT - WHAT IS IT AND WHAT DOES IT DO?

- ▶ Run by EEAS (Crisis Management and Planning Directorate and EU Military Staff) and European Defence Agency
- ▶ Supporting identification and implementation of new projects
- ▶ Project assessment and support for new PESCO projects
- ▶ Supporting PESCO participating Member States

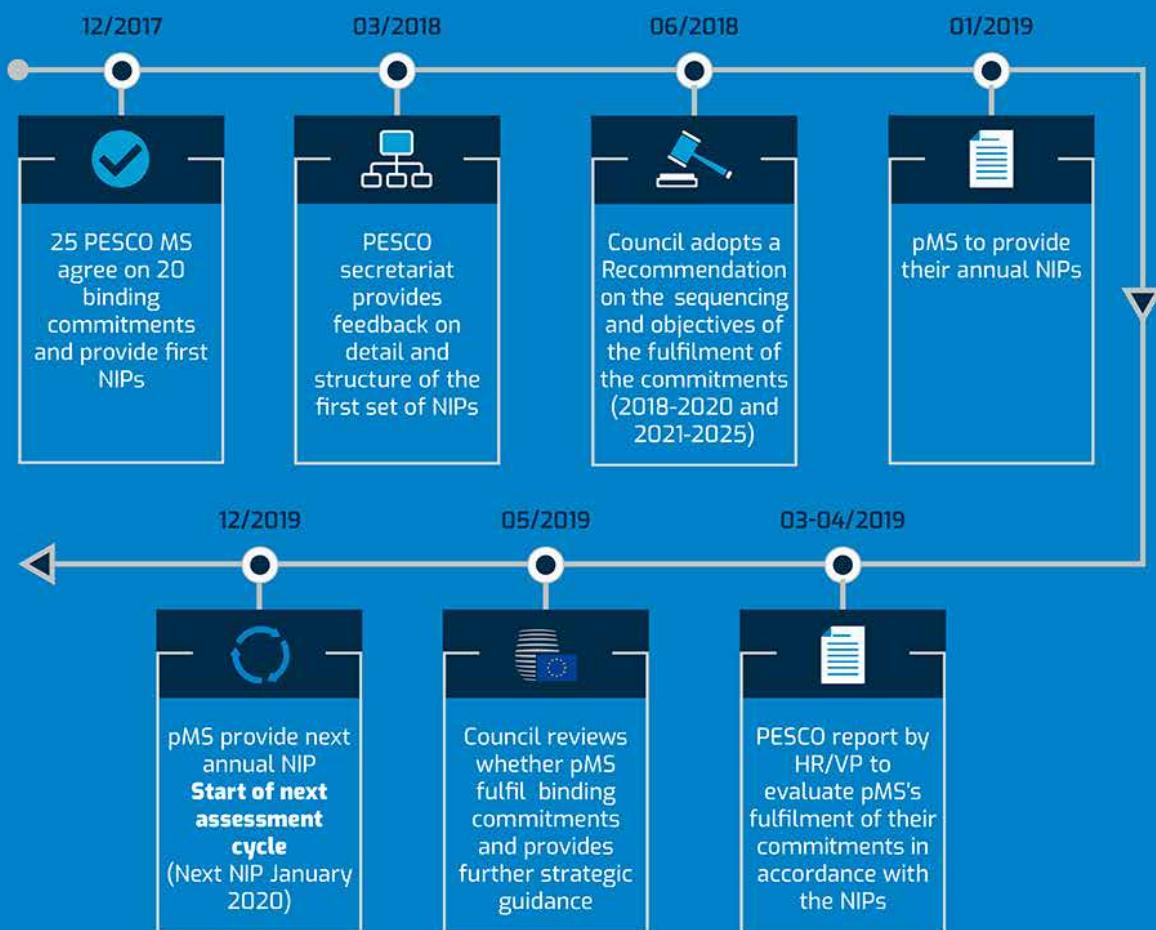
**17 PROJECTS
ADOPTED**


AS OF 06/03/2018



PESCO ASSESSMENT PROCESS 12/2017 – 12/2019

HOW DOES IT WORK?



PESCO = Permanent Structured Cooperation

MS = EU Member States

pMS = participating PESCO Member States

HR/VP = High Representative of the Union for Foreign Affairs and Security Policy / Vice-President of the Commission

EEAS = European External Action Service

EDA = European Defence Agency

NIP = National Implementation Plan

Council Recommendation = a non-binding legal act agreed on by the Council

Council Decision = binding legal acts agreed on by the Council

Conclusion

The EU cannot be considered a major cybersecurity actor yet, but it has considerably raised its interest and role in cyberspace over the past two decades, establishing itself as a focal point and facilitator for its Members States and, to a lesser extent, as a partner for third countries. The EU's future actorness in this field will be partly shaped by the more general developments of the EU as a diplomatic and security actor. However, in light of the strategic importance of the issue, it is unlikely that there will be a waning of interest or ambition in this domain.

3.5 The human layer of cybersecurity – the art of social engineering

by Elisa Norvanto

When it comes to cyber security, any successful organisation must focus on people, processes and technology. Technology provides automated safeguards and processes to determine the series of actions to be taken to achieve a particular end. However, even organisations with strong security practices are vulnerable to human error.¹ To ensure the strength of the human aspects in any information security plan, an organisation must first recognise and address the human aspect's biggest threat, namely social engineering.

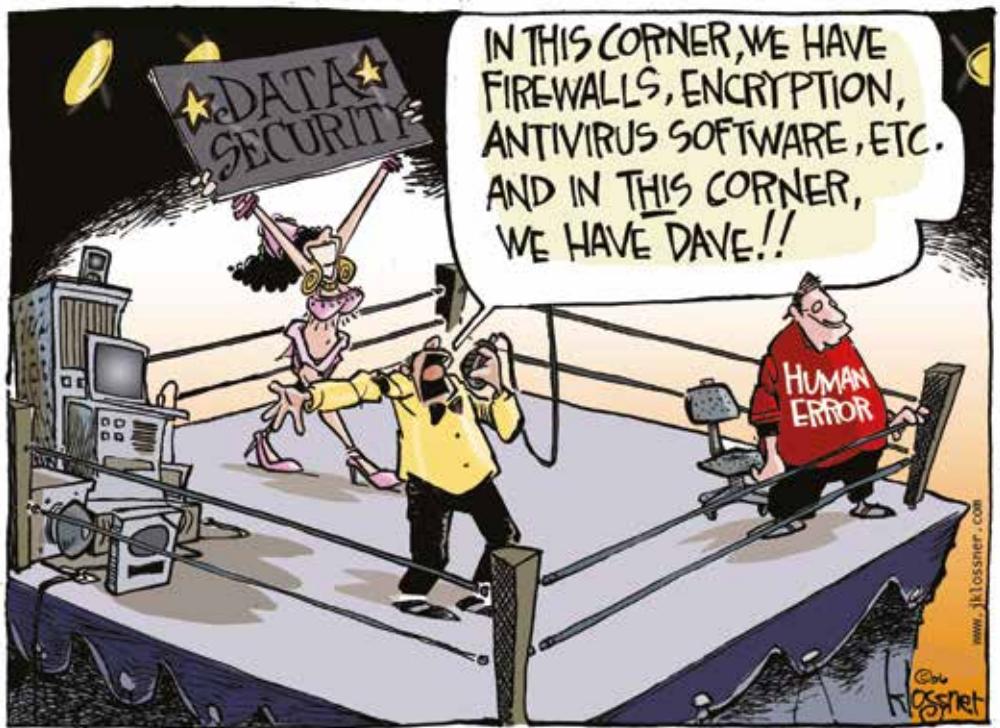
Cybersecurity has become a part of everyone's life, and it can affect anyone using and anything related to the Internet. As the digital era develops, cyber security evolves and software vulnerabilities diminish. However, people, as individuals, are more exposed today than ever before. Cyber security is vitally important to public and private organisations. Effective information security comprises multiple layers of defence which work together to protect information, access to networks and information systems. The premise is that if one layer fails, other layers will fail too. Technical layers such as firewalls, software patches, intrusion detection systems, anti-virus programmes, and encryption are often the only areas that are considered in cyber security. However, effective penetration attacks are often social rather than technical and they account for the majority of cyber attacks. Indeed, **the most significant vulnerability in information security relates to human error**. If, as a result, an individual with malicious intent is able to bypass a system, that individual can bypass all of the other defensive layers designed to ensure information security.²

According to IBM's Cyber Security Intelligence index³, 95% of all information security incidents involve human error. Many of these entail successful attacks by external

1 Fran Howarth, 'The Role of Human Error in Successful Security Attacks', *SecurityIntelligence.com*, 2.9.2014. Retrieved on: <https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/>

2 Ugo Emekauwa, 'The Human Layer of Information Security Defense', 19.10.2007. Retrieved from <http://securitynewswire.com/block/index.html>.

3 Fran Howarth, 'The Role of Human Error in Successful Security Attacks', *SecurityIntelligence.com*, 2.9.2014. Retrieved on: <https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/>



attackers who exploit human vulnerabilities in order to trick insiders within organisations into unwittingly providing access to sensitive information. These mistakes can be costly since they involve privileged insiders, such as government employees, who often have access to the most sensitive information. The greatest impact of successful security attacks concerns disclosure of sensitive data, the introduction of malware, or the theft of intellectual property. While cyberattacks are generally considered to be technical, successful ransomware operations employ **social engineering tactics** to help identify, target and exploit vulnerabilities.

Social engineering

Cyber criminals use social engineering tactics in order to convince people to open email attachments infected with malware, persuade unsuspecting individuals to divulge sensitive information, or even scare people into installing and running malware.⁴

⁴ Andy Mc, 'Do your employees know they are being targeted?', *Security*, 18.11.2017.
Retrieved on: <https://www.insta.digital/do-your-employees-know-they-are-being-targetted/>.

Social engineering is the art of exploiting human flaws to achieve a malicious objective.⁵ They can be human-based and technology-based. ‘Human-based’ involves a person-to-person interaction to obtain the desired action. ‘Technology-based’ involves a digital interface that attempts to achieve the desired outcome, such as pop-up windows and email attachments.⁶ In both cases, social engineering uses **human interaction to psychologically manipulate targets** through deception and persuasion in order to influence the target’s actions. Cyber threat actors use social engineering techniques to deceive, persuade, and influence targets to disclose information. It often involves tricking people into breaking standard security practices or giving away information, most often over the telephone or via email, but also through direct observation and unauthorised physical access. When successful, many social engineering attacks enable attackers to gain authorised access to confidential information. Social engineering attacks differ from traditional hacking in the sense that social engineering attacks can be non-technical and do not necessarily involve the compromise or exploitation of software or systems.⁷

5 Mitnick, K. D. and Simon, W. L. ‘The art of deception: Controlling the human element of security.’ (Indianapolis, IN: Wiley, 2002).

6 Thomas R. Peltier. ‘Social Engineering: Concepts and Solutions’, last modified 20.6.2018. Retrieved on: http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm#WY-RU6YUk7M.

7 Nate Lord, ‘What is Social Engineering? Defining and Avoiding Common Social Engineering Threats’, *Digital Guardian*, 27.7.2017. Retrieved on: <https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats>.

FRAUD SCAMS TARGETING EMPLOYEES HOW TO PROTECT YOURSELF ?



KEY TARGETS
Mid-level employees in financial or procurement services



HIGHLY ATTRACTIVE CRIME
large profits and low risk of detection



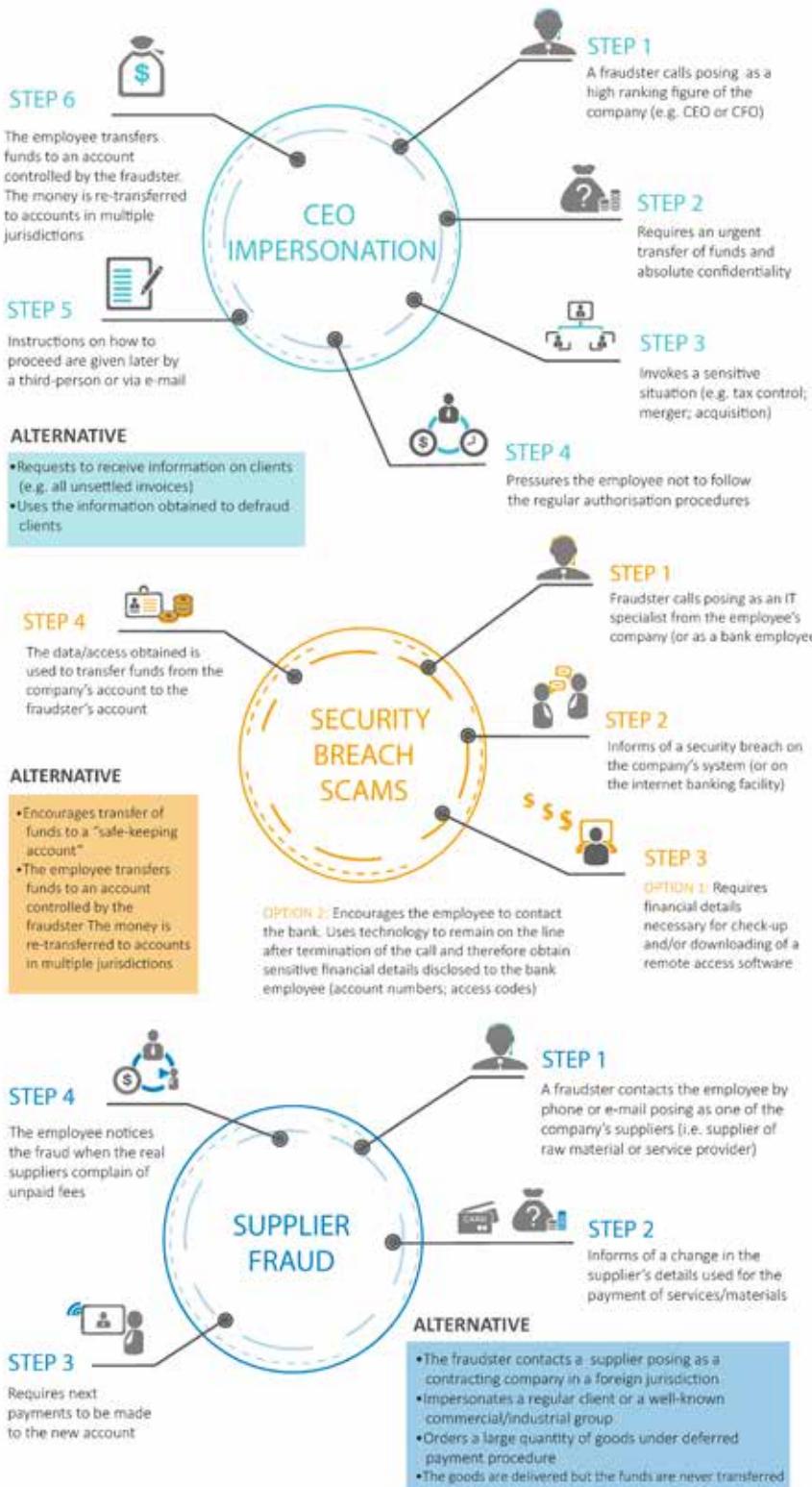
High financial impact for targeted companies:
LOSSES UP TO SEVERAL MILLION EUROS



DIRECT HUMAN COSTS
shame; sanctions; loss of employment



KNOW THE SCAMS

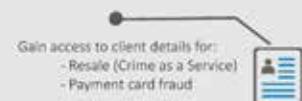
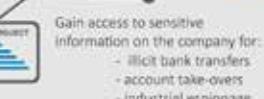
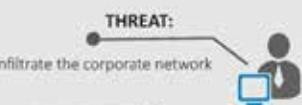


HOW DO FRAUDSTERS CONCEAL THEIR IDENTITY?

- Use forged documents with legitimate company logo/signatures obtained online
- Use copycat e-mail addresses
- Disguise the origin of the call through applications faking the caller's identity (display the number of the service/individual they impersonate)
- Use VOIP and proxy servers to lower the risks of detection
- Use the services of illicit call centres based outside the EU



MALWARE



GAIN ACCESS THROUGH:





KNOW THE SIGNS

 **EUROPOL**

- Unsolicited call/e-mail requesting information on internal procedures for payment or procurement
 - Unsolicited call/e-mail requesting financial information (account numbers, access codes)
 - Feeling of emergency
 - Pressure



CEO IMPERSONATION

- Direct contact by a senior official you are normally not in contact with
- Unusual request in contradiction with internal procedures
- Request for absolute confidentiality
- Threats or unusual flattery/promises of reward



SECURITY BREACH SCAM

- Use of particularly alarming tone by an IT/security officer
- Request to download external software (e.g. remote access software)
- Offer of a safe-keeping account



SUPPLIER FRAUD

- Sudden change in contact/payment details of an international supplier (would normally be announced a few weeks/months in advance)
- Change occurring shortly after a significant order was passed or shortly before a deadline for payment



MALWARE

- Unsolicited e-mails with generic greetings
- Unsolicited e-mail containing suspicious links/URLs



KNOW HOW TO REACT

 **EUROPOL**

- Be AWARE of the risks and spread the information within your company.
- Be careful when using social media: by sharing information on your workplace and responsibilities you increase the risks of becoming a target.
- Avoid sharing sensitive information on the company's hierarchy, security or procedures.
- Never open suspicious links or attachments received by e-mail. Be particularly careful when checking your personal mail boxes on the company's computers.
- If you receive a suspicious e-mail or call, always inform your IT department; they are the ones in charge of such issues. They can check the content of suspicious mail and block the sender if necessary.
- Always carefully check e-mail addresses when dealing with sensitive information/money transfers. Fraudsters often use copycat e-mails where only one character differs from the original.
- If you receive a call/email alerting you of a security breach, do not provide information right away or proceed with a transfer. Always start by calling the person back using a phone number found in your own records or on the official website of the company; do not use the number provided to you in the mail or by the caller. If you were contacted by phone, call back using another phone (fraudsters use technology to remain online after you hang up).
- In case of doubt on a transfer order, always consult a colleague even if you were asked to use discretion.
- Consider assigning responsibility to an employee whom others can consult in case of doubt.
- If a supplier informs you of a change in payment details, always contact him to confirm the new information. Keep in mind that the e-mail/phone number provided on the invoice might have been modified.
- Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

Social engineering attacks

Social engineering is recognised as one of the greatest security threats facing organisations. Targeting employees of an organisation through social engineering tactics allows hackers to bypass advanced defences and technologies. Social engineering attacks that target companies or individuals are most easily and successfully launched through **email**. But malicious emails require two triggers to be effective. The first is a cleverly worded subject line that will engage the recipient's curiosity and encourage them to open the email. Once the recipient opens an email, the message has to be compelling enough to encourage the recipient to click on a link or open an attached file in order to initiate or deliver the attack.

The success of a social engineering attack depends on how well the attacker can persuade the victim to perform some action on their behalf, and they may employ a number of influencing techniques (see text box 1). Cyber criminals can seek to provoke emotions such as fear, greed, hope and curiosity to make their attacks more effective. Social engineers use several avenues and techniques for attack. Here are examples of some of the common techniques.

Box 1. Influencing techniques

The psychologist and author Robert Cialdini defines a number of influencing techniques through which social engineers can affect their targets:

- 1. Reciprocation:** Manipulating somebody to feel grateful and thus obligated to the social engineer. This often results in the victim feeling that they owe the social engineer a favour.
- 2. Scarcity:** Many social engineering attacks invoke scarcity of a resource such as time or money to influence their targets.
- 3. Consistency:** Human nature means that people generally try to stick to promises, so as not to appear untrustworthy.
- 4. Liking:** People are more likely to comply with someone they like.
- 5. Authority:** People comply when a request comes from a figure of authority.
- 6. Social Proof:** People comply if and when others are doing the same thing.

(Cialdini, R. B. *Influence: Science and practice* (5th ed.).
(Boston: Allyn & Bacon, 2008).

Social engineering comes in several forms such as:

- Phishing
- Pretexting
- Baiting
- Quid Pro Quo
- Typosquatting

Phishing

Phishing attacks are the most prevalent way of obtaining information or access to a network. The most effective technique is sending an email with a **phishing link**. Attackers usually send well-crafted emails with seemingly legitimate attachments and an individual will open the email, and either click on a link that leads to a malicious site or download an attachment which contains malicious code, thereby compromising the system.

Pretexting

Another common method is a technique called '**pretexting**', where an invented scenario, or pretext, is established for the target to perform an action for the attacker. These attacks often involve scammers who pretend that they need certain information from their target in order to confirm the latter's identity⁸. Subject lines are carefully chosen to inspire a response and emotional reactions can often be enough to make an employee forget about basic security measures. Pretexting attacks rely on building a false sense of trust. This requires the attacker to create a credible story that leaves little room for doubt in their target's mind.⁹

A classical scenario in pretexting is that someone calls a company claiming to represent a phone company, an IT help desk, an internet provider, and starts asking questions. They claim to have a simple problem or know about a problem that can be fixed quickly but they just need a piece of information. It could be as innocuous as asking for a username

8 David Bisson, 'Social Engineering Attacks to Watch Out For', *Tripwire*, 23.3.2015. Retrieved on: <https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>.

9 Nachaat AbdElatif Mohamed, Aman Jantan and Oludare Isaac Abiodun, 'An Improved Behaviour Specification to Stop Advanced Persistent Threat on Governments and Organizations Network', *Proceedings of the International Multi Conference of Engineers and Computer Scientists* Vol I. IMECS 2018, (March 2018), Hong Kong.

or someone's schedule or as blatant as asking for a password. Once the attacker has this information, they call someone else in the organisation and use the information obtained to refine their attack. They may even combine this with information publicly available on the company's website. After a few calls, they can often pass themselves off as an employee, working for instance in IT support or as the assistant of someone in the organisation's hierarchy, and request access to information or more detailed information *immediately*. The unsuspecting employee, not wanting to annoy anyone in the hierarchy, then bypasses security protocols and complies with the request before they have had time to think¹⁰.

Baiting and Quid Pro Quo

In *baiting* the hacker deceives the victim by enticing the latter with the promise of a reward or good. There are two classic scenarios where baiting is used. In the first scenario, the attacker uses a malicious file disguised as a software update or as generic software. Baiters may also offer users free music or movie downloads if they surrender their login credentials to a certain site. In the second scenario the attacker leaves infected USB sticks on a table or even in a parking lot of a target organisation in the hope that staff will insert these devices into the organisation's computers. This tactic takes advantage of an individual's curiosity. The USB device might be labelled 'confidential', 'salary information' or indicate the name of a person in the organisation's hierarchy. The devices carry malicious software, resulting in the victim's machine being compromised.

A *quid pro quo* technique differs from baiting. Instead of baiting a target with the promise of a good, this technique promises a service or a benefit based on the execution of a specific action. A quid pro quo attack occurs when an attacker requests private information from someone in exchange for something desirable or some type of compensation. For instance, an attacker requests login credentials in exchange for a free gift.

Typosquatting

Typosquatting is when the attacker sets up a website with a similar domain name to a legitimate site. For example, instead of www.e-visa-usa.com, the attacker may register www.e-visa-usa.org. The fake site will match the look and feel of the original. The

10 Keith Casey, 'What is Social Engineering? Defining and Avoiding Common Social Engineering Threats', interview by Nate Lord, *Digital Guardian*, 27.7.2017. Retrieved on: <https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats>.



Keep control

what and with whom you share your private information online?



Keep your private stuff private

Don't share your personal information - phone number, address or school - with someone you have only met online. What do they need it for?

Always set the privacy settings of your social media accounts to protect your private data.



How do i look? Be aware of your online presence

Abusers look for young people who use a sexualised username, post sexualised pictures or talk about sex online. Think about how your online profile makes you appear to others.



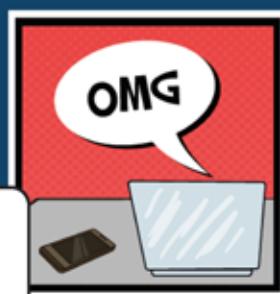
Want to meet up? Always put your safety first

It is a bad idea to share your location or meet up with someone you have only met online. But if you do so, stay safe: meet in a public place and take a trusted adult with you.



A 'friend of a friend'? To be sure, ask your friend

It's easy for anyone to post fake photos and stream a fake video over a webcam. If they claim to be a 'friend of a friend', ask your friend if they have met them in person. Anyone can learn about you and your friends from information that they find online.



Finally... Just between us? Make sure you don't expose yourself (or your privacy)

idea is to trap users who mistype a URL in their web browser. They will often be prompted to enter information, such as passport information, which is then captured by the attacker. The victim is then forwarded to the legitimate site and logged in, but without realising that they were redirected and that their information is now compromised¹¹.

How to combat social engineering?

The threat of social engineering is very real. This very profitable industry seeks unauthorised access to information or unlawfully extracts information for its customers. Social engineering is the hardest form of attack to defend against because it cannot be countered using hardware or software alone. Technology can be used, but not in isolation. A successful defence will require an effective information security architecture, starting with policies and standards and following through with vulnerability assessment processes. Technology provides automated safeguards and processes determine the series of actions to be taken to achieve a particular end. However, even organisations with strong security practices are still vulnerable to human error. Consequently, there are three categories that are considered to mitigate the risk of social engineering; people, processes and technology.



¹¹ Curtis Peterson, '23 Social Engineering Attacks You Need To Shut Down: Device Left Behind', *Smartfile.com*, 16.3.2016. Retrieved from: <https://www.smartfile.com/blog/social-engineering-attacks/>.

Traditional IT security activities such as patch management and system hardening are essential to prevent cyberattacks. However, **awareness** is crucial to the reduction of human error in information security. If users are made aware of the threats and risks they face, they can make decisions that are more informed and they will be less vulnerable to falling for well-known ruses. Therefore, the most important advice for organisations is to **train their employees in cyber security**. As a rule, organisations should put in place a security culture that comprises ongoing training which consistently informs employees about the latest security threats. Behavioural change is more effective than technological defence in countering attacks on the human mind. If employees learn how to protect their data and the organisation's confidential data, they will be better able to identify an instance of social engineering and avoid its damaging consequences. They will then be more vigilant and so play a much-needed role in ensuring security.¹²

Cybersecurity training must start at a very early stage in order to reduce the human error in information security.



12 Lily Teplow, 'Breaking Down the Dangers of Social Engineering', *Continuum IT management platform*, 24.3.2017, Retrieved from: <https://www.continuum.net/blog/breaking-down-the-dangers-of-social-engineering>.

3.6 Social media: manipulating people

by Jochen Rehrl

In former days, newspapers published articles and commentaries, the vast majority of which were based on the principles of journalism – the obligation to the truth, verification of information and loyalty to citizens, among others. The newspapers, which actually provided 'old' news from the previous day, were read and discussed, at least by those parts of society who had the possibility of buying a paper. When something happened around the world, readers only learned about it in the days following the event.

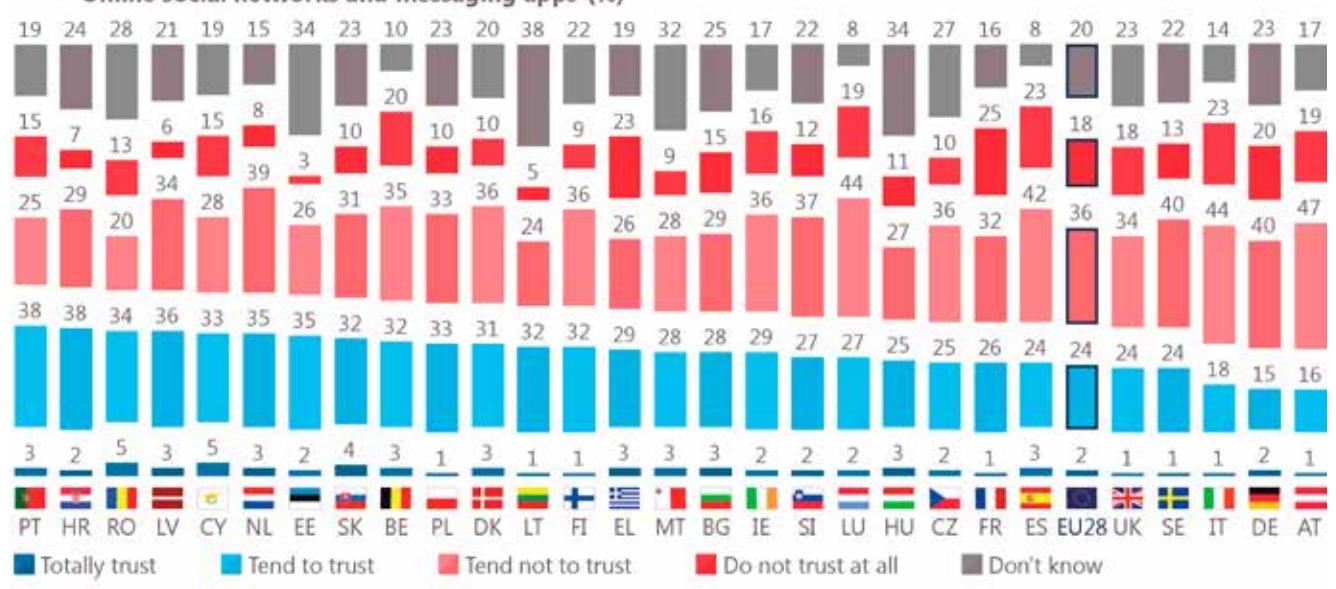
The internet has changed society

Since the dawn of the internet, this picture has changed dramatically. More people read the 'news', more people get engaged (with likes, dislikes and emojis), more people are informed about everything happening on our globe – albeit with varying degrees of expertise. People can easily be influenced or even manipulated by incoming true/half-true/false information. Nowadays, anyone can be a journalist, without any specific education or training and without being bound by the principles of journalism. Everybody can share their thoughts, everybody else can read them in real time, and everything is for free. The time for reflection is short, tending to zero.

Q1.3 How much do you trust or not the news and information you access through...

Online social networks and messaging apps (%)

Graphic: Flash Eurobarometer 464/2018, Fake News and Disinformation online, p.9.

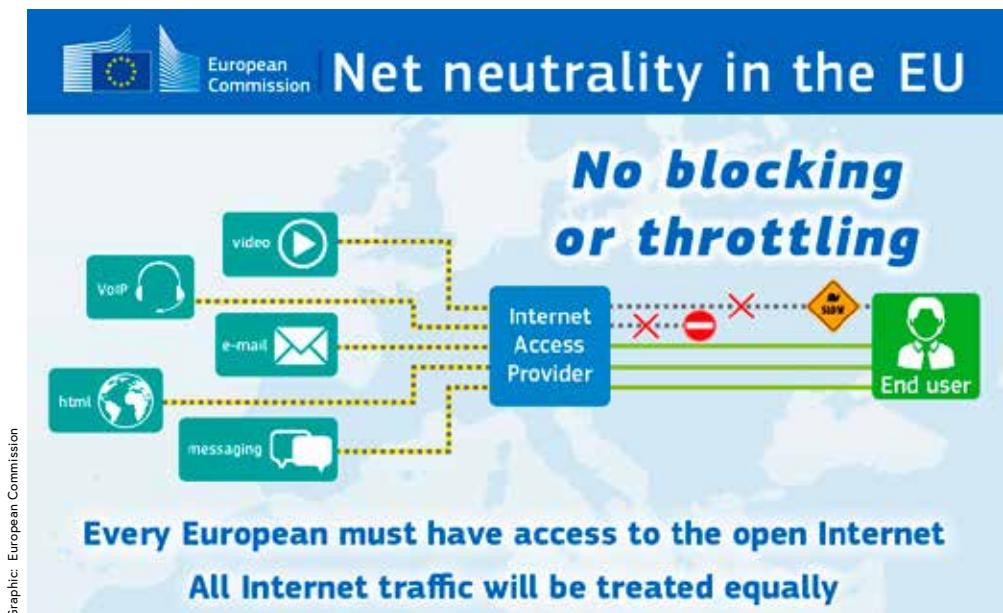


Base: All Respondents (N=26,576)

Social media is the name of the game, be it Facebook, Twitter, YouTube, LinkedIn or others. All media outlets are accessible online 24/7, they have an outreach which no single newspaper has ever obtained and they are cost-free with a few minor exceptions. They can therefore reach, influence and manipulate the hearts and minds of their audience, which currently includes about 85 % of the European population (51 % worldwide). Being able to get people to change their minds is a valuable skill. The vast majority have good intentions and genuinely want to influence people, not manipulate them.

We know you better than you do

The recognition factors of the various media outlets are that they are cost-free and accessible 24/7, their content is provided by 'members' and the media outlet seldom interferes. The content from members ranges from private to public, personal to political. Pictures and short videos are widely used and longer texts and commentaries often remain unread. All the information provided is stored on servers around the world forever. What goes on the net stays on the net, whether you like it or not.



The internet provides a variety of tools for influencing people. In the past couple of years, we have experienced two models: one uses 'big data' in order to microtarget people to get their support; the other tries to manipulate people's behaviour by publishing fake news, commenting on blogs and providing advice to people under false identities.

Model 1: Cambridge Analytica

The data on the net represent a valuable tool for some companies specialised in analysing big data. Big data means the full volume of data available on the internet. Information on the net can be structured, semi-structured or unstructured. 95 % of the information belongs to the latter category, i.e. 'unstructured'. Such data cannot be handled by a human being, so advanced analytic techniques do the work when it comes to very large, diverse data sets.

The results of these analyses can be used for good, but they can also be used by the 'dark side'. Christopher Wylie, a former research director at Cambridge Analytica, became a whistleblower and gave some insights on the work of the company. On its website you can read: 'Data drives all we do. Cambridge Analytica uses data to change audience behaviour.' The company came to the public's attention by using data from 50 million Facebook accounts, some say not necessarily in accordance with the law.



Christopher WYLIE, former employee at Cambridge Analytica, attended the hearing on the Facebook/Cambridge Analytica case in the European Parliament.

How does it work

Cambridge Analytica came into contact with Mr Aleksandr Kogan, a research fellow at the University of Cambridge, who had – via an application – access to a number of Facebook users. This access also included access to the 'friends' of those users and even to the 'friends' of their 'friends' (snowball effect). Cambridge Analytica used the app, paying USD 1 000 000 to about 170 000 users. Each user had an average of 300 'friends', which added up to around 50 million users' data. But there are also other ways of data mining/harvesting.

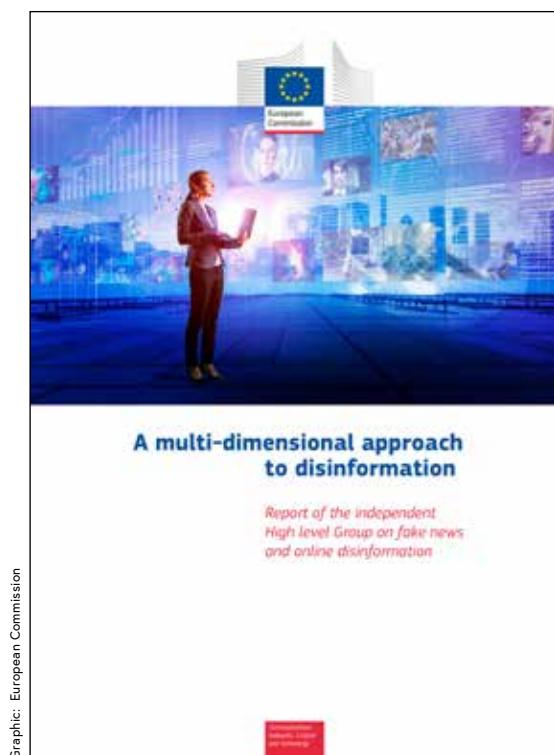
What is done with big data

Example 'Election Campaign': Big data is analysed and potential supporters of a party are identified. Psychographic analyses of individuals are drafted in order to manipulate them for election day by sending them individualised messages at the right time. 'We can get better than human-level accuracy in predicting your behaviour,' said Christopher Wylie in an interview with British newspaper *The Guardian*. If individual analysis shows that a Facebook user is more cautious and uses Facebook more at night, then Facebook will show that user an advertisement at the right time of the day adapted to their profile – this technique is precise, accurate and targeted, and is known as 'microtargeting'.

The manipulation of voters goes hand in hand with blackmailing, disinformation, conspiracies and staging scandals involving political opponents. 'I mean, it sounds a dreadful thing to say but these are things that don't necessarily need to be true as long as they're believed', said Alexander Nix, the former Chief Executive of Cambridge Analytica.

During the US presidential elections, Cambridge Analytica used the brand 'Defeat Crooked Hillary', which was distributed systematically via smaller platforms. Secrecy is one of the main factors for success; therefore self-destroying ProtonMail was used, which destroys each message after 24 hours. The slogan itself infiltrated the online community and expanded, but with no branding, making it unattributable, untraceable and unrecognisable as manipulation.

<https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>



There is nothing new in the fact that social media services such as Facebook provide data to third parties. There is nothing wrong with it, because the user agrees to these terms. The use of data from your friends and your friends' friends, however, is another matter. It should be noted that almost all political parties are now using big data to gain an advantage during election campaigns. However, stricter rules must be applied in order to avoid the erosion of democracy. Otherwise we will see politicians winning election campaigns not on the facts, but purely on emotions.

Model 2: the troll factory

Another model for manipulating people without using big data is the troll factory. Some of these are located in Russia, but there are other 'factories' around the world as well. The main task of the staff employed there, known as 'trolls', is to craft fake characters and then spread false information under their names.

Lyudmila Savchuk, a Russian journalist who went undercover at a troll factory for two months in 2015, reported in an interview with NBC News that at the troll factory, mostly young people in their twenties work. They receive around USD 700, which is much higher than an academic at a university or a doctor at a hospital. The trolls are divided in teams such as social media, media commentary, blogging and YouTube. People with foreign languages received the highest wages and worked on a separate floor.'

Being believably human

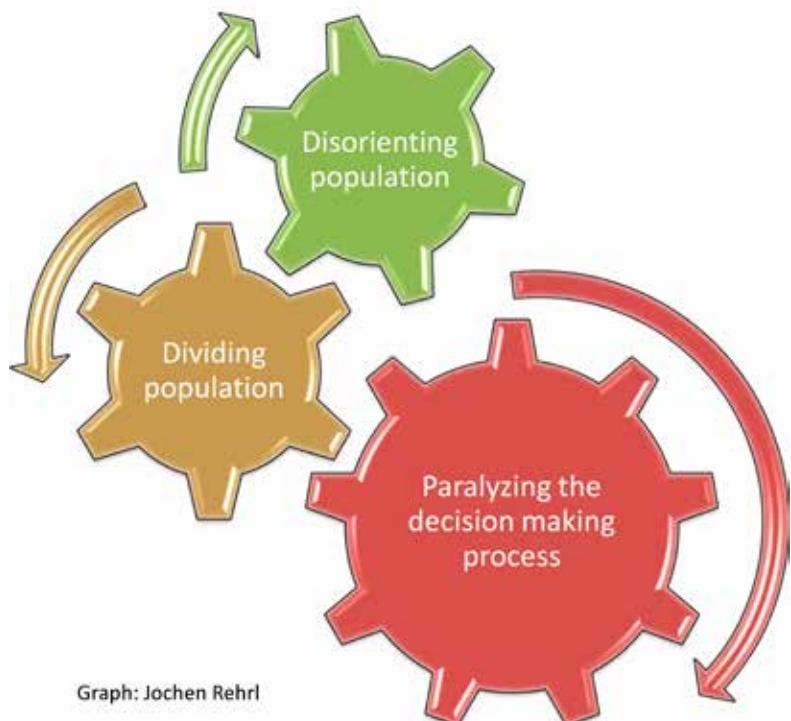
The goal of a troll is to be believably 'human'. Trolls do not write from a script, but rather are supposed to write like regular human beings, using their own words, just like the neighbour next door. Nevertheless, their message is similar to that of the leading political party, their employer or the parent organisation. There is not much news in troll-factory news – it is all propaganda. This propaganda is directed not only at foreign audiences, but also – even mainly – at the audience at home. The main goal is to reinforce readers' own beliefs or to cause discomfort to others.

How does it work

The techniques deployed include aggressively re-sharing content, pushing clickbait, trolling and intimidating political 'enemies', copying/pasting fake news, producing templated sites en masse, creating divisive material, assembling audiences via selective postings and engaging in adversarial flagging. As is usual online, the real identity behind

an account cannot be easily uncovered, and the person/organisation and their location cannot be easily traced.

Goals of disinformation campaigns



Besides troll factories, there are also other actors looking to manipulate the population in a similar way, such as commercially motivated individuals and foreign and domestic influence operators, as well as individual participants. Even in well-established political parties in Europe, and also in the NGO environment, you can find examples of troll factories 'liking' and 'disliking' content or commenting on fake or half-truth news with a single goal: to influence or manipulate human behaviour.

Falsehood spreads faster than the truth

Three researchers at the Massachusetts Institute of Technology (MIT) have concluded that fake news spreads significantly faster and more widely than news or information that is factually accurate. In their study, the researchers examined 4.5 million tweets sent between 2006 and 2017. In these, they found that 126,000 rumours were spread by approximately 3 million people and that fake news reached more people than news

that was factually correct. In order to differentiate between factually accurate and fake news, the researchers used six independent fact-checking organisations (snopes.com, politifact.com, factcheck.org, truthorfiction.com, hoax-slayer.com and urbanlegends.about.com). The results elicited from the fact-checking had a match rate of between 95 and 98 percent.



The 'EU versus Disinformation' campaign is run by the European External Action Service East Stratcom Task Force and aims to better forecast, address and respond to pro-Kremlin disinformation.

A Twitter-example: rumor cascade

'A rumor cascade begins on Twitter when a user makes an assertion about a topic in a tweet, which could include written text, photos, or links to articles online. Others then propagate the rumor by retweeting it. A rumor's diffusion process can be characterized as having one or more cascades, which we define as instances of a rumor-spreading pattern that exhibit an unbroken retweet chain with a common, singular origin.'¹

1 000 vs 100 000 users

News that is factually correct will be read by only 1 000 users, whereas fake news will spread rapidly to 100 000 users. The likelihood that fake news will be retweeted is 70 % higher than the rate for news that is factually correct. The speed at which fake news is disseminated is six times higher. Robots accelerated the spread of factually accurate and fake news at the same pace, which means that humans, and not robots, are to blame.

¹ Soroush Vosoughi, Deb Roy, Sinan Aral: 'The spread of true and false news online'. In: Science 09 March 2018. Vol. 359, Issue 6380, pp. 1146-1151.

Five steps to spot fake news

Social media and their personalisation tools have made it easier and faster to spread bogus stories. What can you do to spot and counter fake, lies and disinformation?

2 Check the author



Does this person even exist? A well-respected journalist always has a track record. If the author has made up his or her name, the rest is also likely to be fake.

4 Think before you share



The headline might be catchy to generate clicks. It could also be distortions of real or old events — or it could be satire. If an event is real, mainstream media will cover it. Compare and draw your own conclusions.

1 Check the media outlet



Do you know it? Check the 'about' section. If the language there is overly dramatic, be sceptical. Who is behind it? Who is funding it? Double-check what other (trustworthy) sources say.

3 Check the references



Does the author use reliable sources (for example, well-established and respected media outlets)? Are the quoted experts real specialists? If the story uses anonymous (or no) sources, it could be fake.

5 Join the myth-busters



Keep on top of the latest tricks used by those spreading fake news.* Report fake stories. Spread the word.

* For example follow @EUvsDisinfo, @StopFakeNews, or @DFRLab.

EPRS | European Parliamentary Research Service

Why do people prefer fake news?

There are a number of reasons for this:

- a. Fake news has a high degree of 'novelty'. People who retweet such information gain social status. By retweeting this information, they are seen by others as insiders.
- b. Fake news has a greater presence in the media than news that is factually accurate. As a result, fake news is often seen as being accurate, although it could easily be categorised as fake news (e.g. by doing some crosschecks).

- c. Human beings believe what they want to believe or whatever confirms a belief or bias they may have. If the information originates from a trusted source (e.g. family, a friend or a political party), this information will often be regarded as factually accurate or true.

Conclusion

The internet opens up a wealth of opportunities which can really bring about positive change for our whole society, and indeed for our whole globe. But we should not forget the other side of the coin. Manipulation of the population is just one aspect of that.

In my view, there are two ways forward. Firstly, politicians will have to create a legal system in which propaganda and manipulation are controlled, but which at the same time does not hinder the further development of an interconnected society. Secondly, education on internet behaviour must be strengthened. 'There is no need for your coffee machine to be online' and 'there is no need for everyone to know when you are on holidays' are just two examples which should remind people to apply their – sometimes forgotten – common sense in cyberspace.



copyright 2013 John Klossner, www.jklossner.com

Annexes



EUROPEAN
COMMISSION

HIGH REPRESENTATIVE OF THE
EUROPEAN UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

**JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,
THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE
COMMITTEE OF THE REGIONS**

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

**JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,
THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE
COMMITTEE OF THE REGIONS**

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

1. INTRODUCTION

1.1. Context

Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring.

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role.

Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

By completing the Digital Single Market, Europe could boost its GDP by almost €500 billion a year¹; an average of €1000 per person. For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication², citizens will need trust and confidence. Unfortunately, a 2012 Eurobarometer survey³ showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. An overwhelming majority also said they avoid disclosing personal information

¹ http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

² For example, plants embedded with sensors to communicate to the sprinkler system when it is time for them to be watered.

³ 2012 Special Eurobarometer 390 on Cybersecurity

online because of security concerns. Across the EU, more than one in ten Internet users has already become victim of online fraud.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity⁴ incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU economy is already affected by cybercrime⁵ activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cybersecurity strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

1.2. Principles for cybersecurity

The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent. This strategy clarifies the principles that should guide cybersecurity policy in the EU and internationally.

The EU's core values apply as much in the digital as in the physical world

The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain.

⁴ Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

⁵ Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

Protecting fundamental rights, freedom of expression, personal data and privacy

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.

Access for all

Limited or no access to the Internet and digital illiteracy constitute a disadvantage to citizens, given how much the digital world pervades activity within society. Everyone should be able to access the Internet and to an unhindered flow of information. The Internet's integrity and security must be guaranteed to allow safe access for all.

Democratic and efficient multi-stakeholder governance

The digital world is not controlled by a single entity. There are currently several stakeholders, of which many are commercial and non-governmental entities, involved in the day-to-day management of Internet resources, protocols and standards and in the future development of the Internet. The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach⁶.

A shared responsibility to ensure security

The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.

2. STRATEGIC PRIORITIES AND ACTIONS

The EU should safeguard an online environment providing the highest possible freedom and security for the benefit of everyone. While acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance. These actions are both short and long term, they include a variety of policy tools⁷ and involve different types of actors, be it the EU institutions, Member States or industry.

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above:

- Achieving cyber resilience
- Drastically reducing cybercrime

⁶ See also COM(2009) 277, Communication from the Commission to the European Parliament and the Council on "Internet Governance: the next steps"

⁷ The actions related to information sharing, when personal data is at stake, should be compliant with EU data protection law.

- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

2.1. Achieving cyber resilience

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. Building on the positive results achieved via the activities carried out to date⁸ further EU action can help in particular to counter cyber risks and threats having a cross-border dimension, and contribute to a coordinated response in emergency situations. This will strongly support the good functioning of the internal market and boost the internal security of the EU.

Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents. This is why the Commission has developed a policy on Network and Information Security (NIS)⁹. The **European Network and Information Security Agency ENISA** was established in 2004¹⁰ and a new Regulation to strengthen ENISA and modernise its mandate is being negotiated by Council and Parliament¹¹. In addition, the Framework Directive for electronic communications¹² requires providers of electronic communications to appropriately manage the risks to their networks and to report significant security breaches. Also, the EU data protection legislation¹³ requires data controllers to ensure data protection requirements and safeguards, including measures related to security, and in the field of publicly available e-communication services, data controllers have to notify incidents involving a breach of personal data to the competent national authorities.

Despite progress based on voluntary commitments, there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness. This strategy is accompanied by a proposal for **legislation** to notably:

- establish common minimum requirements for NIS at national level which would oblige Member States to: designate national competent authorities for NIS; set up a well-functioning CERT; and adopt a national NIS strategy and a national NIS cooperation plan. Capacity building and coordination also concern the EU institutions: a Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies ("CERT-EU") was permanently established in 2012.

⁸ See references in this Communication as well as in the Commission Staff Working Document Impact Assessment accompanying the Commission proposal for a Directive on network and information security, in particular sections 4.1.4, 5.2, Annex 2, Annex 6, Annex 8,

⁹ In 2001, the Commission adopted a Communication on "Network and Information Security: Proposal for A European Policy Approach" (COM(2001)298); in 2006, it adopted a Strategy for a Secure Information Society (COM(2006)251). Since 2009, the Commission has also adopted an Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP) (COM(2009)149, endorsed by Council Resolution 2009/C 321/01; and COM(2011)163, endorsed by Council Conclusions 10299/11).

¹⁰ Regulation (EC) No 460/2004

¹¹ COM(2010)521. The actions proposed in this Strategy do not entail amending the existing or future mandate of ENISA.

¹² Article 13a&b of Directive 2002/21/EC

¹³ Article 17 of Directive 95/46/EC; Article 4 of Directive 2002/58/EC

- set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities. National NIS competent authorities will be asked to ensure appropriate EU-wide cooperation, notably on the basis of a Union NIS cooperation plan, designed to respond to cyber incidents with cross-border dimension. This cooperation will also build upon the progress made in the context of the "European Forum for Member States (EFMS)"¹⁴, which has held productive discussions and exchanges on NIS public policy and can be integrated in the cooperation mechanism once in place.
- improve preparedness and engagement of the private sector. Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector.

However, private actors still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture or to invest in security solutions. The proposed legislation therefore aims at making sure that players in a number of key areas (namely energy, transport, banking, stock exchanges, and enablers of key Internet services, as well as public administrations) assess the cybersecurity risks they face, ensure networks and information systems are reliable and resilient via appropriate risk management, and share the identified information with the national NIS competent authorities. The take up of a cybersecurity culture could enhance business opportunities and competitiveness in the private sector, which could make cybersecurity a selling point.

Those entities would have to report, to the national NIS competent authorities, incidents with a significant impact on the continuity of core services and supply of goods relying on network and information systems.

National NIS competent authorities should collaborate and exchange information with other regulatory bodies, and in particular personal data protection authorities. NIS competent authorities should in turn report incidents of a suspected serious criminal nature to law enforcement authorities. The national competent authorities should also regularly publish on a dedicated website unclassified information about on-going early warnings on incidents and risks and on coordinated responses. Legal obligations should neither substitute, nor prevent, developing informal and voluntary cooperation, including between public and private sectors, to boost security levels and exchange information and best practices. In particular, the European Public-Private Partnership for Resilience (EP3R¹⁵) is a sound and valid platform at EU level and should be further developed.

¹⁴ The European Forum for Member States was launched via COM(2009) 149 as a platform to foster discussions among Member States public authorities regarding good policy practises on security and resilience of Critical Information Infrastructure

¹⁵ The European Public-Private Partnership for Resilience was launched via COM(2009) 149. This platform initiated work and fostered the cooperation between the public and the private sector on the identification of key assets, resources, functions and baseline requirements for resilience as well as cooperation needs and mechanisms to respond to large-scale disruptions affecting electronic communications.

The Connecting Europe Facility (CEF)¹⁶ would provide financial support for key infrastructure, linking up Member States' NIS capabilities and so making it easier to cooperate across the EU.

Finally, cyber incident exercises at EU level are essential to simulate cooperation among the Member States and the private sector. The first exercise involving the Member States was carried out in 2010 ("Cyber Europe 2010") and a second exercise, involving also the private sector, took place in October 2012 ("Cyber Europe 2012"). An EU-US table top exercise was carried out in November 2011 ("Cyber Atlantic 2011"). Further exercises are planned for the coming years, including with international partners.

The Commission will:

- Continue its activities, carried out by the Joint Research Centre in close coordination with Member States authorities and critical infrastructure owners and operators, on identifying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.
- Launch an EU-funded pilot project¹⁷ early in 2013 on **fighting botnets and malware**, to provide a framework for coordination and cooperation between EU Member States, private sector organisations such as Internet Service Providers, and international partners.

The Commission asks ENISA to:

- Assist the Member States in developing strong **national cyber resilience capabilities**, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure
- Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU.
- Continue supporting the Member States and the EU institutions in carrying out regular **pan-European cyber incident exercises** which will also constitute the operational basis for the EU participation in international cyber incident exercises.

The Commission invites the European Parliament and the Council to:

- Swiftly **adopt** the proposal for a Directive on a **common high level of Network and Information Security (NIS)** across the Union, addressing national capabilities and preparedness, EU-level cooperation, take up of risk management practices and information sharing on NIS.

The Commission asks industry to:

- Take leadership in **investing** in a high level of cybersecurity and develop best practices and information sharing at sector level and with public authorities with the view of ensuring a strong and effective protection of assets and individuals, in

¹⁶ <https://ec.europa.eu/digital-agenda/en/connecting-europe-facility>. CEF Budget line 09.03.02 – Telecommunications networks (to promote the interconnection and interoperability of national public services on-line as well as access to such networks).

¹⁷ CIP-ICT PSP-2012-6, 325188. It has an overall budget of 15 Million Euro, with EU funding amounting to 7.7 Million Euro.

¹⁸ <http://www.trustindigitallife.eu/>

particular through public-private partnerships like EP3R and Trust in Digital Life (TDL)¹⁸.

Raising awareness

Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.

Several initiatives have been developed in recent years and should be continued. In particular, ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities are also active in raising awareness. In October 2012, ENISA, with some Member States, piloted the "European Cybersecurity Month". Raising awareness is one of the areas the EU-US Working Group on Cybersecurity and Cybercrime¹⁹ is taking forward, and is also essential in the context of the Safer Internet Programme²⁰ (focused on the safety of children online).

The Commission asks ENISA to:

- Propose in 2013 a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators).

The Commission will:

- Organise, with the support of ENISA, a cybersecurity **championship** in 2014, where university students will compete in proposing NIS solutions.

The Commission invites the Member States²¹ to:

- Organise a yearly **cybersecurity month** with the support of ENISA and the involvement of the private sector from 2013 onwards, with the goal to raise awareness among end users. A synchronised EU-US cybersecurity month will be organised starting in 2014.
- **Step up national efforts on NIS education and training**, by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations.

The Commission invites industry to:

- Promote cybersecurity **awareness at all levels**, both in business practices and in

¹⁹ This Working Group, established at the EU-US Summit in November 2010 (MEMO/10/597) is tasked with developing collaborative approaches on a wide range of cybersecurity and cybercrime issues.

²⁰ The Safer Internet Programme funds a network of NGOs active in the field of child welfare online, a network of law enforcement bodies who exchange information and best practices related to criminal exploitation of the Internet in dissemination of child sexual abuse material and a network of researchers who gather information about uses, risks and consequences of online technologies for children's lives.

²¹ Also with the involvement of relevant national authorities, including NIS competent authorities and data protection authorities.

the interface with customers. In particular, industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity.

2.2. Drastically reducing cybercrime

The more we live in a digital world, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high-profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders - the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross-border approach to respond to this growing threat.

Strong and effective legislation

The EU and the Member States need strong and effective legislation to tackle cybercrime. The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, is a binding international treaty that provides an effective framework for the adoption of national legislation.

The EU has already adopted legislation on cybercrime including a Directive on combating the sexual exploitation of children online and child pornography²². The EU is also about to agree on a Directive on attacks against information systems, especially through the use of botnets.

The Commission will:

- Ensure swift transposition and implementation of the cybercrime related directives.
- Urge those Member States that have not yet ratified the **Council of Europe's Budapest Convention on Cybercrime** to ratify and implement its provisions as early as possible.

Enhanced operational capability to combat cybercrime

The evolution of cybercrime techniques has accelerated rapidly: law enforcement agencies cannot combat cybercrime with outdated operational tools. Currently, not all EU Member States have the operational capability they need to effectively respond to cybercrime. All Member States need effective national cybercrime units.

The Commission will:

- Through its funding programmes²³, support the Member States to **identify gaps and strengthen their capability** to investigate and combat cybercrime. The Commission will furthermore support bodies that make the link between

²² Directive 2011/93/EU replacing Council Framework decision 2004/68/JHA

²³ For 2013, under the Prevention and Fight against Crime Programme (ISEC). After 2013, under the Internal Security Fund (new Instrument under MFF).

research/academia, law enforcement practitioners and the private sector, similar to the on-going work carried out by the Commission-funded Cybercrime Centres of Excellence already set up in some Member States.

- Together with the Member States, coordinate efforts to identify best practices and best available techniques including with the support of JRC to fight cybercrime (e.g. with respect to the development and use of forensic tools or to threat analysis)
- Work closely with the recently launched **European Cybercrime Centre (EC3)**, **within Europol and with Eurojust** to align such policy approaches with best practices on the operational side.

Improved coordination at EU level

The EU can complement the work of Member States by facilitating a coordinated and collaborative approach, bringing together law enforcement and judicial authorities and public and private stakeholders from the EU and beyond.

The Commission will:

- Support the recently launched **European Cybercrime Centre (EC3)** as the European focal point in the fight against cybercrime. The EC3 will provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community²⁴.
- Support efforts to increase accountability of registrars of domain names and ensure accuracy of information on website ownership notably 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.
- Build on recent legislation to continue strengthening the EU's efforts to tackle child sexual abuse online. The Commission has adopted a European Strategy for a Better Internet for Children²⁵ and has, together with EU and non-EU countries, , launched a **Global Alliance against Child Sexual Abuse Online**²⁶. The Alliance is a vehicle for further actions from the Member States supported by the Commission and the EC3.

The Commission asks Europol (EC3) to:

- Initially focus its analytical and operational support to Member States' cybercrime investigations, to help dismantle and disrupt cybercrime networks primarily in the

²⁴ On 28 March 2012, the European Commission adopted a Communication "Tackling Crime in a Digital Age: Establishing a European Cybercrime Centre"

²⁵ COM(2012) 196 final

²⁶ Council Conclusions on a Global Alliance against Child Sexual Abuse Online (EU-US Joint Statement) of 7th and 8th June 2012 and Declaration on the launch of the Global Alliance against Child Sexual Abuse Online (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

- areas of child sexual abuse, payment fraud, botnets and intrusion.
 - On a regular basis produce strategic and operational reports on trends and emerging threats to identify priorities and target investigative action by cybercrime teams in the Member States.
- The Commission asks the European Police College (CEPOL) in cooperation with Europol to:**
- Coordinate the design and planning of training courses to equip law enforcement with the knowledge and expertise to effectively tackle cybercrime.
- The Commission asks Eurojust to:**
- Identify the main obstacles to judicial cooperation on cybercrime investigations and to coordination between Member States and with third countries and support the investigation and prosecution of cybercrime both at the operational and strategic level as well as training activities in the field.
- The Commission asks Eurojust and Europol (EC3) to:**
- Cooperate closely, *inter alia* through the exchange of information, in order to increase their effectiveness in combating cybercrime, in accordance with their respective mandates and competence.
 -

2.3. Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats

Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU. To avoid duplications, the EU will explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.

The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate:

- Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability;
- Develop the EU cyberdefence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis

- and information sharing. Improve Cyber Defence Training & Exercise Opportunities for the military in the European and multinational context including the integration of Cyber Defence elements in existing exercise catalogues;
- Promote dialogue and coordination between civilian and military actors in the EU – with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority
 - Ensure dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts.

2.4. Develop industrial and technological resources for cybersecurity

Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products and services are located outside the EU. There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.

Promoting a Single Market for cybersecurity products

A high level of security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority. It seems²⁷ however that many players still regard security as little more than an additional burden and there is limited demand for security solutions. There need to be appropriate cybersecurity performance requirements implemented across the whole value chain for ICT products used in Europe. The private sector needs incentives to ensure a high level of cybersecurity; for example, labels indicating adequate cybersecurity performance will enable companies with a good cybersecurity performance and track record to make it a selling point and get a competitive edge. Also, the obligations set out in the proposed NIS Directive would significantly contribute to step up business competitiveness in the sectors covered.

A Europe-wide market demand for highly secure products should also be stimulated. First, this strategy aims to increase cooperation and transparency about security in ICT products. It calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions. A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses.

Second, the Commission will support the development of security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing, while taking in due

²⁷ See the Commission Staff Working Document Impact Assessment accompanying the Commission proposal for a Directive on network and information security, Section 4.1.5.2

account the need to ensure data protection. Work should focus on the security of the supply chain, in particular in critical economic sectors (Industrial Control Systems, energy and transport infrastructure). Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI)²⁸, of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players.

The Commission will:

- Launch in 2013 a public-private **platform on NIS solutions** to develop incentives for the adoption of secure ICT solutions and the take-up of good cybersecurity performance to be applied to ICT products used in Europe.
- Propose in 2014 recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform
- Examine how major providers of ICT hardware and software could inform national competent authorities on detected vulnerabilities that could have significant security-implications.

The Commission asks ENISA to:

- Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, **technical guidelines and recommendations for the adoption of NIS standards and good practices** in the public and private sectors.

The Commission invites public and private stakeholders to:

- Stimulate the development and adoption of industry-led **security standards**, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers; new generations of software and hardware should be equipped with **stronger, embedded and user-friendly security** features.
- Develop industry-led standards for companies' performance on cybersecurity and improve the information available to the public by developing **security labels** or kite marks helping the consumer navigate the market.

Fostering R&D investments and innovation

R&D can support a strong industrial policy, promote a trustworthy European ICT industry, boost the internal market and reduce European dependence on foreign technologies. R&D should fill the technology gaps in ICT security, prepare for the next generation of security challenges, take into account the constant evolution of user needs and reap the benefits of dual use technologies. It should also continue supporting the development of cryptography. This has to be complemented by efforts to translate R&D results into commercial solutions by providing the necessary incentives and putting in place the appropriate policy conditions.

²⁸ Particularly under the Smart Grids Standard M/490 for the first set of standards for a smart grid and reference architecture.

The EU should make the best of the Horizon 2020²⁹ Framework Programme for Research and Innovation, to be launched in 2014. The Commission's proposal contains specific objectives for trustworthy ICT as well as for combating cyber-crime, which are in line with this strategy. Horizon 2020 will support security research related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address interoperability among network and information systems. Specific attention will be drawn at EU level to optimising and better coordinating various funding programmes (Horizon 2020, Internal Security Fund, EDA research including European Framework Cooperation).

The Commission will:

- Use Horizon 2020 to address a range of areas in ICT privacy and security, from R&D to innovation and deployment. Horizon 2020 will also develop tools and instruments to fight criminal and terrorist activities targeting the cyber environment.
- Establish mechanisms for better coordination of the research agendas of the European Union institutions and the Member States, and incentivise the Member States to invest more in R&D.

The Commission invites the Member States to:

- Develop, by the end of 2013, good practices to use the **purchasing power of public administrations** (such as via public procurement) to stimulate the development and deployment of security features in ICT products and services.
- Promote early involvement of industry and academia in developing and coordinating solutions. This should be done by making the most of Europe's Industrial Base and associated R&D technological innovations, and be coordinated between the research agendas of civilian and military organisations;

The Commission asks Europol and ENISA to:

- Identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies.

The Commission invites public and private stakeholders to:

- Develop, in cooperation with the insurance sector, **harmonised metrics for calculating risk premiums**, that would enable companies that have made investments in security to benefit from lower risk premiums.

2.5. Establish a coherent international cyberspace policy for the European Union and promote EU core values

Preserving open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society.

²⁹ Horizon2020 is the financial instrument implementing the [Innovation Union](#), a [Europe 2020](#) flagship initiative aimed at securing Europe's global competitiveness. Running from 2014 to 2020, the EU's new Framework Programme for research and innovation will be part of the drive to create new growth and jobs in Europe.

In its international cyberspace policy, the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cybersecurity capacity. The EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.

Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy

The Commission, the High Representative and the Member States should articulate a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector. EU consultations with international partners on cyber issues should be designed, coordinated and implemented to add value to existing bilateral dialogues between the EU's Member States and third countries. The EU will place a renewed emphasis on dialogue with third countries, with a special focus on like-minded partners that share EU values. It will promote achieving a high level of data protection, including for transfer to a third country of personal data. To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime.

One of the major elements of the EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance. The EU should promote corporate social responsibility³⁰, and launch international initiatives to improve global coordination in this field.

The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments. The EU supports the efforts to define norms of behaviour in cyberspace that all stakeholders should adhere to. Just as the EU expects citizens to respect civic duties, social responsibilities and laws online, so should states abide by norms and existing laws. On matters of international security, the EU encourages the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour.

The EU does not call for the creation of new international legal instruments for cyber issues.

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 should be also respected online. The EU will focus on how to ensure that these measures are enforced also in cyberspace.

To address cybercrime, the Budapest Convention is an instrument open for adoption by third countries. It provides a model for drafting national cybercrime legislation and a basis for international co-operation in this field.

³⁰

A renewed EU strategy 2011-14 for Corporate Social Responsibility; COM(2011) 681 final

If armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand. **Developing capacity building on cybersecurity and resilient information infrastructures in third countries**

The smooth functioning of the underlying infrastructures that provide and facilitate communication services will benefit from increased international cooperation. This includes exchanging best practices, sharing information, early warning joint incident management exercises, and so on. The EU will contribute towards this goal by intensifying the on-going international efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks involving governments and the private sector.

Not all parts of the world benefit from the positive effects of the Internet, due to a lack of open, secure, interoperable and reliable access. The European Union will therefore continue to support countries' efforts in their quest to develop the access and use of the Internet for their people, to ensure its integrity and security and to effectively fight cybercrime.

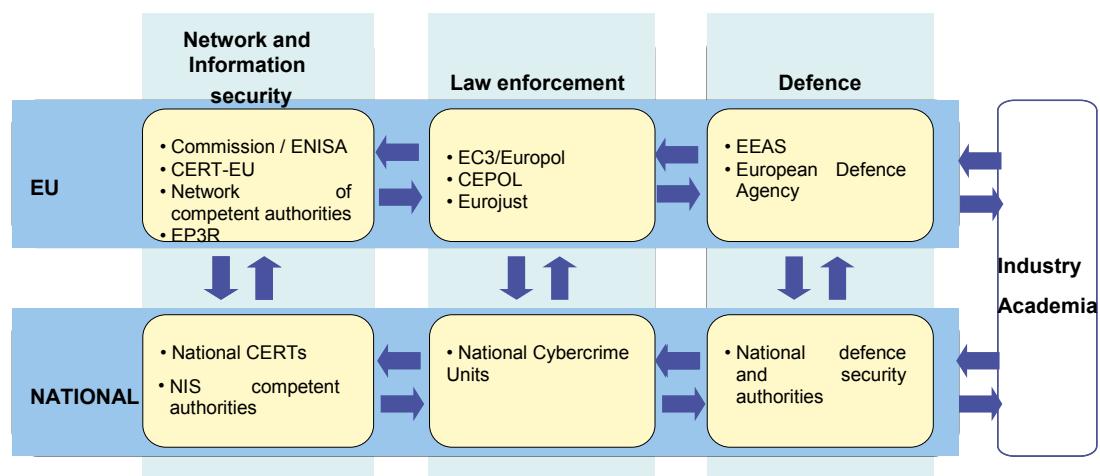
In cooperation with the Member States, the Commission and the High Representative will:

- Work towards a coherent EU International cyberspace policy to increase engagement with key international partners and organisations, to mainstream cyber issues into CFSP, and to improve coordination of global cyber issues;
- Support the development of norms of behaviour and confidence building measures in cybersecurity. Facilitate dialogues on how to apply existing international law in cyberspace and promote the Budapest Convention to address cybercrime;
- Support the promotion and protection of fundamental rights, including access to information and freedom of expression, focusing on: a) developing new public guidelines on freedom of expression online and offline; b) monitoring the export of products or services that might be used for censorship or mass surveillance online; c) developing measures and tools to expand Internet access, openness and resilience to address censorship or mass surveillance by communication technology; d) empowering stakeholders to use communication technology to promote fundamental rights;
- Engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries to improve access to information and to an open Internet, to prevent and counter cyber threats, including accidental events, cybercrime and cyber terrorism, and to develop donor coordination for steering capacity-building efforts;
- Utilise different EU aid instruments for cybersecurity capacity building, including assisting the training of law enforcement, judicial and technical personnel to address cyber threats; as well as supporting the creation of relevant national policies, strategies and institutions in third countries;
- Increase policy coordination and information sharing through the international Critical Information Infrastructure Protection networks such as the Meridian network, cooperation among NIS competent authorities and others.

3. ROLES AND RESPONSIBILITIES

Cyber incidents do not stop at borders in the interconnected digital economy and society. All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU-level and work together to strengthen cybersecurity. As different legal frameworks and jurisdictions may be involved, a key challenge for the EU is to clarify the roles and responsibilities of the many actors involved.

Given the complexity of the issue and the diverse range of actors involved, centralised, European supervision is not the answer. National governments are best placed to organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement. To address cybersecurity in a comprehensive fashion, activities should span across three key pillars—NIS, law enforcement, and defence—which also operate within different legal frameworks:



3.1. Coordination between NIS competent authorities/CERTs, law enforcement and defence

National level

Member States should have, either already today or as a result of this strategy, structures to deal with cyber resilience, cybercrime and defence; and they should reach the required level of capability to deal with cyber incidents. However, given that a number of entities may have operational responsibilities over different dimensions of cybersecurity, and given the importance of involving the private sector, coordination at national level should be optimised across ministries. Member States should set out in their national cybersecurity strategies the roles and responsibilities of their various national entities.

Information sharing between national entities and with the private sector should be encouraged, to enable the Member States and the private sector to maintain an overall view of different threats and get a better understanding of new trends and techniques used both to commit cyber-attacks and react to them more swiftly. By establishing national NIS cooperation plans to be activated in the case of cyber incidents, the Member States should be able to clearly allocate roles and responsibilities and optimise response actions.

EU level

Just as at national level, there are at EU level a number of actors dealing with cybersecurity. In particular, the ENISA, Europol/EC3 and the EDA are three agencies active from the perspective of NIS, law enforcement and defence respectively. These agencies have Management Boards where the Member States are represented, and offer platforms for coordination at EU level.

Coordination and collaboration will be encouraged among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field.

Informal channels for coordination and collaboration will be complemented by more structural links. EU military staff and the EDA cyber defence project team can be used as the vector for coordination in defence. The Programme Board of Europol/EC3 will bring together among others the EUROJUST, CEPOL, the Member States³¹, ENISA and the Commission, and offer the chance to share their distinct know-how and to make sure EC3's actions are carried out in partnership, recognising the added expertise and respecting the mandates of all stakeholders. The new mandate of ENISA should make it possible to increase its links with Europol and to reinforce links with industry stakeholders. Most importantly, the Commission's legislative proposal on NIS would establish a cooperation framework via a network of national NIS competent authorities and address information sharing between NIS and law enforcement authorities.

International

The Commission and the High Representative ensure, together with the Member States, coordinated international action in the field of cybersecurity. In so doing, the Commission and the High Representative will uphold EU core values and promote a peaceful, open and transparent use of cyber technologies. The Commission, the High Representative and the Member States engage in policy dialogue with international partners and with international organisations such as Council of Europe, OECD, OSCE, NATO and UN.

3.2. EU support in case of a major cyber incident or attack

Major cyber incidents or attacks are likely to have an impact on EU governments, business and individuals. As a result of this strategy, and in particular the proposed directive on NIS, the prevention, detection and response to cyber incidents should improve and Member States and the Commission should keep each other more closely informed about major cyber incidents or attacks. However, the response mechanisms will differ depending on the nature, magnitude and cross-border implications of the incident.

If the incident has a serious impact on the business continuity, the NIS directive proposes that national or Union NIS cooperation plans be triggered, depending on the cross-border nature of the incident. The network of NIS competent authorities would be used in that context to share

³¹ via representation within the EU Cybercrime Task Force, which is made up of the heads of the EU cybercrime Units of the Member States

information and support. This would enable preservation and/or restoration of affected networks and services.

If the incident seems to relate to a crime, Europol/EC3 should be informed so that they - together with the law enforcement authorities from the affected countries – can launch an investigation, preserve the evidence, identify the perpetrators and ultimately make sure they are prosecuted.

If the incident seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union).

If the incident seems having compromised personal data, the national Data Protection Authorities or the national regulatory authority pursuant to Directive 2002/58/EC should be involved.

Finally, the handling of cyber incidents and attacks will benefit from contact networks and support from international partners. This may include technical mitigation, criminal investigation, or activation of crisis management response mechanisms.

4. CONCLUSION AND FOLLOW-UP

This proposed cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, [to make the EU's online environment the safest in the world](#).³²

This vision can only be realised through a true partnership, between many actors, to take responsibility and meet the challenges ahead.

The Commission and the High Representative therefore invite the Council and the European Parliament to endorse the strategy and to help deliver the outlined actions. Strong support and commitment is also needed from the private sector and civil society, who are key actors to enhance our level of security and safeguard citizens' rights.

³² The financing of the Strategy will occur within the foreseen amounts for each of the relevant policy areas (CEF, Horizon 2020, Internal Security Fund, CFSP and External Cooperation, notably the Instrument for Stability) as set out in the Commission's proposal for the Multi-Annual Financial Framework 2014-2020 (subject to the approval of the Budget Authority and the final amounts of the adopted MFF for 2014-2020). With regard to the need to ensure overall compatibility with the number of posts available to decentralised agencies and the sub-ceiling for decentralised agencies in each expenditure heading in the next MFF, the agencies (CEPOL, EDA ENISA, EUROJUST and EUROPOL/EC3) which are requested by this Communication to take on new tasks will be encouraged to do so in so far as the actual capacity of the agency to absorb growing resources has been established and all possibilities for redeployment have been identified.

The time to act is now. The Commission and the High Representative are determined to work together with all actors to deliver the security needed for Europe. To ensure that the strategy is being implemented promptly and assessed in the face of possible developments, they will gather together all relevant parties in a high-level conference and assess progress in 12 months.



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 Council¹, 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 Ransomware⁴ has seen a particular increase, with the recent attacks⁵ 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 Defence⁷ 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 Agenda⁹, the Joint Framework on countering hybrid threats¹⁰ and the Communication on Launching the European Defence Fund.¹¹¹²

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 future¹⁴.

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 Systems¹⁶ (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 teams¹⁷, 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 applications²¹: 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 obligations²² – 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 disclosure²⁵ should be created across Member States, building on best practices²⁶ 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 services²⁸, energy, transport and health.²⁹

The Commission has already highlighted the specific issues concerning **liability** raised by new digital technologies³⁰ 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 Communication³³ 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 Council³⁷ and the EU's general rapid alert systems³⁸. 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 Recommendation⁴⁰ 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 bodies⁴¹ 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 exercises⁴² 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 Cybersecurity⁴³ 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 world⁴⁴ 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 cybersecurity⁴⁷; 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 challenges⁴⁹ 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 cybersecurity 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 Coalition⁵² 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' campaign⁵⁴, 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 consumers⁵⁷. 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 certification⁵⁸;
- 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 world⁶¹ 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 WHOIS⁶³ 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 explored⁶⁹, 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 fraud⁷³. 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 Units⁷⁵ 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 States⁷⁶ 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 incidents⁷⁹. Situational awareness necessary for the use of measures within the framework should be fused, analysed and shared by INTGEN⁸⁰ 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 Framework⁸², 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. STRENGTHENING 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 Experts⁸⁴; 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 dialogues⁸⁵ 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 proposal⁸⁷ 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 bodies⁹⁰. 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.

List of authors

André Barrinha is a Lecturer in International Security at the University of Bath. He also co-convenes the UACES CRN INTERSECT: Technology-Security-Society interplays in Europe and is a Researcher at the Centre for Social Studies, University of Coimbra. He has previously published on critical security studies, European security, Turkish foreign policy and international relations theory. He is currently working on the role of new technologies in the formation of security policies (mostly) in Europe, with a special focus on cybersecurity.

Jelmer Brouwer works as a research officer in the strategic analysis team at Europol. Before joining Europol, he worked for four years as a researcher and teacher at the Department of Criminology at Leiden University. He holds master's degrees in international criminology from VU University Amsterdam and in European human rights law from the European Inter-University Centre for Human Rights and Democratisation. He has published on issues of policing and migration and is in the process of finishing his doctoral thesis.

Catherine de Bolle is the Executive Director of Europol, the European Union's law enforcement agency supporting the EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. Prior to her appointment she worked as the General Commissioner of the Belgian Federal Police. Ms De Bolle graduated from the Royal Gendarmerie Academy and she holds a law degree from Ghent University.

Arthur de Liedekerke is currently working for CERT-EU, on policy and administrative matters. He previously worked in the European Parliament as an accredited assistant, on foreign affairs and security issues. He has also collaborated with a number of corporate and strategic intelligence companies, working from/based in ?? the US and Brussels. He holds two master's degrees – in geopolitics and international relations – from King's College London and the University of Maastricht.

Eloïs Divol is currently seconded by France to the European External Action Service (EEAS), where he is responsible for cyber security policies. Before joining the EEAS, he also dealt with multilateral issues, as a negotiator for the French Presidency of the COP21 on climate change. Eloïs Divol is a graduate of the Ecole Polytechnique.

Jorge Domecq is Chief Executive of the European Defence Agency. Prior to his appointment in February 2015, Domecq, a senior Spanish diplomat, served as Ambassador and Permanent Representative to the Organisation for Security and Cooperation in Europe (OSCE) and as Ambassador to the Republic of the Philippines. Since the start of his diplomatic career in 1985, Domecq has held several positions with the Spanish Ministry of Foreign Affairs. He was also Director of the Private Office of the NATO Secretary-General and Diplomatic Adviser to the Spanish Minister of Defence.

Dirk Dubois graduated from the Belgian Military Academy with a master's degree in social and military science in 1985. In the first part of his career he occupied several operational posts, including abroad, and positions as a staff officer. From 2007 to 2012 he was a training manager at the ESDC, before joining the Directorate-general for Education of the Belgian MoD. On 01 April 2015, he was appointed Head of the ESDC. In December 2017, the EU Member States decided to extend his mandate by consensus until 2022.

Angelina Gros-Tchorbadijska is a member of the Secretariat of the Task Force on Security in DG Migration and Home Affairs of the European Commission. As such she provides policy advice and coordinates the activities of the Task Force in the field of cybersecurity and cybercrime by linking and following the implementation of the various policy initiatives in those fields. She previously served as a member of the Legal Service of the European Parliament, advising on institutional and budgetary matters. From 2014 to 2016, she was a member of the Cabinet of the Vice-President for Budget and Human Resources. Before joining the European civil service in 2008, Angelina was a researcher concerned with the new eastern borders of the EU and the enlargement of Schengen at the Institute for European Law at K U Leuven, Belgium and associate research fellow at the European Institute in Sofia, Bulgaria. Angelina holds first law degree with a specialization in international law and international relations from University of Sofia, an LLM in European law and Ph.D. in law from K U Leuven, Belgium.

Udo Helmbrecht, Prof. Dr., took office as Executive Director of ENISA in October 2009. His 40 years of professional management experience in the IT sector were acquired through work in a variety of areas, including the energy, defence, and the space industries. He became the president of the German Federal Office for Information Security in 2003. He studied physics, mathematics and computer science at Ruhr University Bochum, and in 1984 he was awarded a PhD in theoretical physics. In 2010, he was appointed honorary professor at the University of Bundeswehr in Munich, Germany.

Enrico Introini is Cyber-Security Team Leader for Civilian CSDP Missions in the EEAS Civilian Planning and Conduct Capability (CPCC) Mission Support division. He is primarily responsible for cyber-defence capabilities enforcement and cyber-security coordination for the 10 different Civilian CSDP missions. He previously worked in the European Commission as project officer in the security team for Galileo and EGNOS European satellite programmes and in the EEAS Secure Communication Division in the team in charge of the security accreditation of classified networks. He started his career as ICT Officer in the Italian Ministry of Foreign Affairs and holds a Master's degree in Telecommunications Engineering from the University of Trento and Politecnico di Milano.

Charlotte Isaksson is currently working in the European External Action Service (EEAS) in Brussels as a senior expert with the Principal Advisor on Gender Equality, Women's Empowerment and WPS (Women, Peace and Security). She has worked primarily on gender and WPS-related issues in the domain of security and defence, including operations and missions, in national and international positions. She was Gender Advisor to SACEUR and functional manager for the integration of gender perspective within Allied Command Operations, NATO at SHAPE in Belgium 2011-2016. Ms Isaksson's main work has focused on gender equality and integration of gender perspectives, including UNSCR 1325 on Women, Peace and Security and related resolutions on Conflict-related Sexual Violence. She has a military background and in addition to her higher military education she holds two advanced degrees, in Sociology (Lund University) and in International Relations (Cambridge University).

Arnold H. Kammel is an Austrian lawyer and political scientist who currently serves in the Cabinet of the Federal Minister for the EU, Culture, Arts & Media in the Austrian Federal Chancellery. Prior to that, he directed the Austrian Institute for European and Security Policy (AIES). He holds a doctoral degree in law and master's degrees in political science and European studies. He graduated from the Universities of Graz and Vienna. His publications deal with European affairs as well as with international security and defence policy.

Gustav Lindstrom is the Director of the EU Institute for Security Studies (EUISS) – the European Union's agency dealing with the analysis of foreign, security and defence policy issues. Previously, Dr Lindstrom worked with the Geneva Centre for Security Policy (GCSP), the RAND Corporation, and the World Bank. His current areas of focus include the EU's Common Security and Defence Policy, cybersecurity, EU-NATO relations, and emerging security challenges.

Elisa Norvanto is currently working as a Senior R&D Communication and Project Adviser at Laurea UAS, responsible for developing and planning security-related education, training and R&D activities, with a substantial focus on crisis management, border security, cyber security, and ethics. She is also responsible for setting up Laurea's R&D communication function and advising the Laurea Management on strategic communications, media cooperation, and impactful stakeholder engagement. Alongside her duties at Laurea UAS, she also works as a part-time Research Fellow and Adviser at Finnish Defence Forces International Centre responsible for several research and training activities related to European Foreign and Security Policy, and UN-led peace operations. She holds a master's degree in political sciences and is currently doing her Ph.D. at the Finnish National Defence University. Her research interests relates to trust and international cooperation; cyber competencies; and implications of disruptive technologies for military leadership.

Neil Powell, Wing Commander, is an Action Officer on the EU Military Staff at the CIS Directorate and Head of the Cyber Defence Team. He is primarily responsible for concept development and implementation of cyber defence aspects in planning for the conduct of military operations and missions.

Georgios Psykakos joined the European Institutions in 2015 and is currently working for CERT-EU, leading its First Response group. He started his career in the banking sector as an IT security officer. Since 2009, he has been providing his country's national authorities with cyber-security expertise in the fields of incident handling, forensic investigation and policy making. He has extensive experience in security intelligence and counter-intelligence. He holds an MSc in computer security with a specialisation in intrusion detection systems.

Jochen Rehrl is an Austrian lawyer who is currently seconded as national expert to the European Security and Defence College. He previously worked in political advisor positions at ministerial level in both Vienna (Austria) and Brussels (Belgium). He holds a doctoral degree in law and three master's degrees in communications, international relations and economy. He graduated from the Universities of Salzburg and Vienna as well as from the Diplomatic Academy in Vienna. His publications deal with security and defence policy. Between 2014 and 2018, he was the Chairperson of the ESDC's Executive Academic Board configuration on 'Cyber Security'.

Thomas Renard is Senior Research Fellow at the Egmont Institute, a Brussels-based think tank, and an Adjunct Professor at the Vesalius College. He is also a member of the ESDC Executive Academic Board on Cyber Issues (EAB.Cyber). He works mainly on security challenges in Europe (terrorism and cyber). He has published widely for global think tanks and academic publishers, and appears regularly in worldwide media.

François Rivasseau currently serves as Special Envoy for Space and Head of Security Policy and Space, European External Action Service, Brussels. He previously served as minister counsellor and deputy chief of mission (DCM) of the Delegation of the European Union to the United States (2011–2015); minister counsellor, DCM, of the Embassy of France in Washington, D.C. (2007–2011); permanent representative of France to the Conference on Disarmament in Geneva (2003–2006); and assistant secretary for press and communication and spokesperson of the French Ministry of Foreign Affairs (2000–2003). Born in Bordeaux, France, Mr Rivasseau graduated from the Bordeaux Institute of Political Studies and holds a Ph.D. in law from the University of Bordeaux I. He is a graduate of the National School of Administration and also holds a degree of Romance languages from the University of Bordeaux III. He speaks fluent English, Spanish, and German and has a basic knowledge of Russian.

Matti Saarelainen began his career in the Finnish Security Intelligence Service (SUPO) in the 1980s, working in various fields within the organisation ever since. From 1998–2004 he worked as the Director at the Finnish Directorate of Immigration, and from 2005–2008 as the Situation Awareness Coordinator at the Prime Minister's Office. At present, he is the Director of the European Centre of Excellence for Countering Hybrid Threats.

Emese Savoia-Keleti has long-term experience in the field of data protection. She is in her 10th year dealing with privacy and processing personal data in EU institutions and bodies. She worked three years in the Directorate -General for Humanitarian Aid and Civil Protection as a Data Protection Coordinator and stayed in external relations by using her expertise in data protection to assist the EEAS with the launch of the Data Protection Office after its establishment. Ms. Savoia-Keleti gained her doctorate in Budapest, complementing it with a second master's in European Studies. She was a Fulbright scholar in New York for a year and acquired her Data Protection Officer certificate in the first EIPA programme for DPOs and other data protection professionals in Maastricht supported by the EDPS. Ms Savoia-Keleti speaks 5 languages and regularly gives presentations, trainings and workshops in the domain of data protection, including data and cyber security in the digital age.

Hanna Smith was research fellow at the University of Helsinki's Aleksanteri Institute and the Finnish Centre of Excellence in Russian Studies 2003-2017. In 2006 she was an analyst at the Finnish Ministry of Foreign Affairs Unit for Research and Policy Planning. She has degrees from University of Stockholm (BA), University of London (MA) and University of Helsinki (PhD). At present she is the director of strategic planning and responses at the European Centre of Excellence for Countering Hybrid Threats (September 2017)

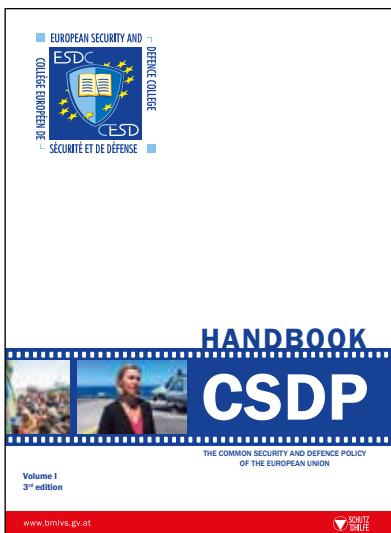
Heli Tiirmaa-Klaar is currently Head of Cyber Policy Coordination at the European External Action Service, where she steers EU cyber diplomacy and cyber defence efforts. She has been working on cyber security issues since 2007 when she led the development of the Estonian Cyber Security Strategy. In 2008-2010 she coordinated the implementation of the Estonian strategy, managed the National Cyber Security Council and led the re-organisation of country's cyber structures as well as public-private partnerships for cyber security. In 2011-2012, she was assigned to the NATO International Staff to develop the new NATO cyber defence policy. In her earlier career, she held various managerial positions at the Estonian Ministry of Defence and Tallinn University since 1995. She has academic background in political science, sociology and international Relations. She studied as a Fulbright Fellow at George Washington University in Washington D.C., obtained her M.A. degree from the Central European University and is enrolled in a PhD programme.

Nicole van der Meulen works as a Senior Strategic Analyst and Head of the Strategy & Development team at the European Cybercrime Centre (EC3) at Europol. She has previously held a variety of posts in the area of cybercrime and cybersecurity at the Dutch Banking Association, RAND Europe, VU University Amsterdam and the Dutch Ministry of Security & Justice. She holds a doctorate in law from Tilburg University and a master's degree in political science with specialisations in comparative politics and international relations from VU University Amsterdam. Her primary publications deal with digital identity theft and cybersecurity policy.

Liis Vihul is the Chief Executive Officer of Cyber Law International, a boutique international law firm that offers consultancy and training seminars regarding the international law applicable to cyber operations and cyber conflict. She is also Ambassador of the NATO Cooperative Cyber Defence Centre of Excellence and Deputy Chair of the Global Commission on the Stability of Cyberspace's Research Advisory Group. Previously, Ms. Vihul spent 9 years as a senior analyst in the Law and Policy Branch at the NATO CCD COE and was the managing editor of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. She holds master's degrees in law from the University of Tartu and in information security from the University of London.

Previously published handbooks

All handbooks focus on the Common Security and Defence Policy of the European Union within the wider framework of the Common Foreign and Security Policy. The authors of the articles are experts from diverse backgrounds: the bodies of the EU itself, academic institutions, and CSDP missions and operations. In these volumes all share their knowledge and experience and thereby contribute to a common European security culture.

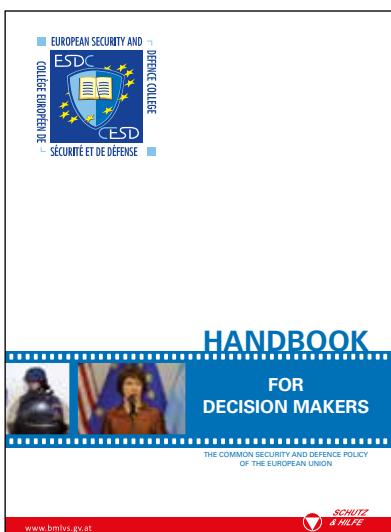


Handbook on CSDP

Volume I, 3rd edition, 2017

Published by the Austrian Ministry of Defence

This handbook gives a general overview of the various topics dealt with in the Common Security and Defence Policy of the European Union. It describes the various structures at EU level and summarises the procedural guidelines for establishing a CSDP mission and CSDP operations. This publication is the reference document for all those interested in the security and defence dimension of the EU.

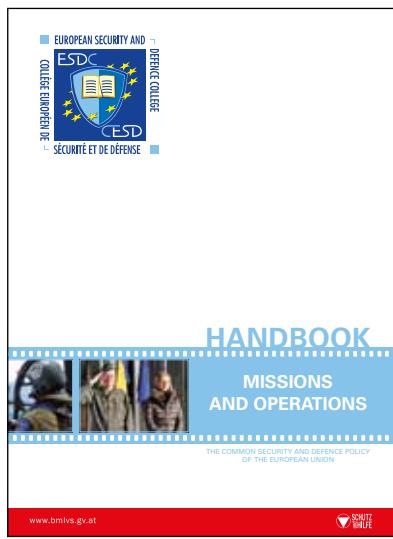


Handbook for decision makers

Volume II, 1st edition, 2014

Published by the Austrian Ministry of Defence

This handbook is designed for decision-makers working in national ministries or for EU bodies and dealing with CSDP missions and operations. It characterises the various dimensions of the Common Security and Defence Policy of the EU and will provide readers with guidance and help them develop the skills they need to make decisions and shape the decision-making process [in this field].

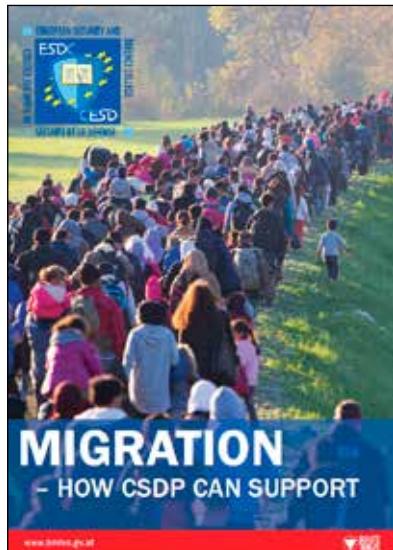


Handbook for missions and operations

Volume III, 1st edition, 2015

Published by the Austrian Ministry of Defence

This handbook is designed for practitioners working in the field of the Common Security and Defence Policy of the EU. It reflects the specific challenges and aspects of CSDP relevant to personnel deployed to CSDP missions and operations and gives clear guidance on how to cope with difficult situations. It also gives a comprehensive overview of legal, political, strategic and political dimensions of the CSDP, leading from vision to action.



Migration – How CSDP can support

Volume IV, 1st edition, 2016

Published by the Austrian Ministry of Defence

This handbook was the product of a conference on migration held in September 2016 in the Egmont Palace in Brussels. It includes articles by recognised experts on migration and a compendium of factsheets on migration from various EU institutions, such as the European Commission, the European Parliament, the European Council and the European External Action Service.

ISBN: 978-3-902275-48-6