



European
Commission

Operational Guidance for the EU's international cooperation on cyber capacity building

European Commission
Instrument contributing to Stability and Peace
Service Contract IFS/2017/385099

print ISBN 978-92-9198-755-9
QN-02-18-917-EN-C
DOI:10.2815/38445

online ISBN 978-92-9198-756-6
QN-02-18-917-EN-N
DOI:10.2815/05153

Printed in Luxembourg by Imprimerie Centrale.
Luxembourg: Publications Office of the European Union, 2018.

© European Union, 2018.

PRINTED ON RECYCLED PAPER

This study was commissioned by the European Commission's Directorate-General for International Cooperation and Development, Unit "Security, Nuclear Safety" and it was implemented by the European Union Institute for Security Studies (EUISS).



The study was authored by Dr Patryk Pawlak with the support of the EUISS Task Force for Cyber Capacity Building. Visuals were created by Christian Dietrich. The study was edited for the European Commission by Panagiota-Nayia Barmaliou, Policy Officer/ Project Manager.

This publication has been produced with the assistance of the European Commission. The contents of this publication do not necessarily reflect the position or opinion of the European Commission.

CONTENTS

- Acknowledgements 6
- List of acronyms 7

- ABOUT THIS OPERATIONAL GUIDANCE 10**
 - Context and objectives..... 10
 - Why is the operational guidance needed?..... 10
 - What is the aim of the operational guidance?..... 10
 - How to use this guidance..... 11
 - Methodology 11

- A GUIDE TO CYBER-RELATED CONCEPTS AND POLICY DEVELOPMENT 14**
 - 1. Cyber concepts and communities..... 14**
 - 1.1. Cyberspace as a development venue..... 15
 - 1.2. Cyberspace as a security domain 16
 - 1.3. Cyberspace as an area of justice and a crime scene..... 18
 - 1.4. Cyberspace as a diplomatic arena..... 18
 - 1.5. Cyberspace as a battlefield 20
 - 1.6. Cyberspace as a capacity-building site 21
 - 2. The EU approach to building resilience in cyberspace..... 22**
 - 2.1. Cybersecurity..... 27**
 - NIS Directive..... 28
 - Cybersecurity products and services 29
 - Industry, research and technology base 31
 - Crisis management cooperation..... 31
 - 2.2. Cybercrime and criminal justice in cyberspace..... 31**
 - Harmonisation and approximation of legislation 32
 - Cooperation amongst key stakeholders 34
 - 2.3. International cooperation in cyberspace 35**
 - Application of existing international law and norms of responsible state behaviour 36
 - Confidence-Building Measures..... 36
 - Human rights online..... 37
 - Cyber capacity building..... 37
 - Internet governance..... 38
 - 2.4. Defence in cyberspace..... 40**
 - 3. Policy dilemmas..... 41**
 - 3.1. Security and human rights 41**
 - 3.2. Sovereignty and governance 43**
 - 3.3. Accountability and transparency in cyberspace 44**
 - 3.4. Innovation, growth and security 45**

- A FRAMEWORK FOR THE EU’S EXTERNAL CYBER CAPACITY BUILDING 47**
 - 1. What is capacity building? 49**
 - 2. What is cyber capacity building (CCB)?..... 50**
 - 3. Elements of an EU approach to external cyber capacity building 51**
 - 3.1. Strategic scope of cyber capacity building..... 52**
 - 3.2. Policy stages: capacity to do what?..... 53**
 - 3.3. Pillars of the EU approach: capacity in what?..... 54**
 - National strategic framework..... 54
 - Criminal justice in cyberspace 55
 - Incident and crisis management system 57
 - Cyber hygiene and awareness..... 57
 - 3.4. Levels of capacity: capacity of who and/or what? 58**
 - Individual capacity..... 58

Organisational capacity.....	58
Enabling environment.....	58
3.5. Layers of capacity: what type of capacity?	59
Vision and policies.....	59
Laws and regulations.....	59
Institutions and resources.....	60
Cooperation and partnerships.....	60
3.6. Comparison to other approaches	61
4. An operational framework for CCB cooperation	62
5. Preparatory stage: decisions about an engagement	65
5.1. Mitigating risks	65
5.2. V-I-P approach to cyber capacity building	66
Values-based dimension.....	66
Interests-based dimension.....	66
Principles-based dimension.....	67
5.3. Rights-Based Approach	68
6. Step one – Problem and context analysis	70
6.1. Stakeholder analysis and engagement	70
6.2. Vulnerability and threat environment	77
6.3. Policy analysis and assessment	78
6.4. Policy dialogue and engagement	80
7. Step two – Capacity assessment and needs analysis	81
7.1. Assessing the existing capacities	81
7.2. Determining desired capacities	84
8. Step three – Formulating a logic of intervention	86
8.1. Possible actions	88
8.2. Result chain and indicators	89
8.3. Lessons learned	90
8.4. Complementarity and synergy with other actions	92
8.5. Cross-cutting issues	94
Gender.....	94
Environment and climate change.....	94
8.6. Cyber resilience as a cross-cutting issue: mainstreaming	94
9. Step four – Implementation, including monitoring and reporting	98
9.1. Performance and results monitoring	98
The EU Results Framework (EURF).....	98
Result Oriented Monitoring (ROM).....	99
Challenges linked to result monitoring and reporting.....	100
9.2. Project risk management	101
9.3. Closing	101
10. Step five – Evaluation of the Provided Support	103

APPLICATIONS OF THE OPERATIONAL GUIDANCE TO SPECIFIC PILLARS _____ **105**

1. National strategic framework	105
1.1. Policy analysis	105
1.2. Engagement	106
1.3. Risk mapping	106
1.4. Key stakeholders	106
1.5. Capacity assessment and needs analysis	107
1.6. Building an intervention logic	108
2. Criminal justice in cyberspace	112
2.1. Policy analysis	112
2.2. Engagement	113
2.3. Risk mapping	114
2.4. Key stakeholders	114
2.5. Capacity assessment and needs analysis	114

2.6.	Building an intervention logic	116
3.	Incident and crisis management system	120
3.1.	Policy analysis.....	120
3.2.	Engagement	121
3.3.	Risk mapping	122
3.4.	Key stakeholders	122
3.5.	Capacity assessment and needs analysis.....	123
3.6.	Building an intervention logic	125
4.	Cyber hygiene and awareness	129
4.1.	Policy analysis.....	130
4.2.	Engagement	131
4.3.	Risk mapping	131
4.4.	Key stakeholders	131
4.5.	Capacity assessment and needs analysis.....	132
4.6.	Building an intervention logic	133

REFERENCES	138
-------------------------	------------

Acknowledgements

This study benefited from the contributions, comments and suggestions by members of the EUISS Task Force for Cyber Capacity Building established for the purpose of this project: Dr. Andrea Calderaro (University of Cardiff), Alejandro Pinto (Ministry of Interior, Spain), Dr. Maria Grazia Porcedda (University of Leeds), Cristina Schulman (Ministry of Justice, Romania) and Dr. Thorsten Wetzling (Stiftung Neue Verantwortung). Tommaso Da Zan, James Galland-Jones and Eva Nagyfejeo provided research assistance.

The EU Institute for Security Studies would also like to thank experts, EU and government officials who provided feedback on earlier drafts of this study: Jacopo Bellasio, Katharina-Irene Bointner, Robert Collett, Stephanie Horel, Panagiotis Leventis, Elaine Miller, Konstantinos Missirilis, Emmanouil Ntanos, Jakub Otce-nasek, Eleonora Sconci, Alexander Seger, Roberto Segundo Navarro, Szilvia Tóth, Ben Wagner, and Carolin Weisser. Our thanks go to Ambassador Tomasz Kozlowski and Jorge Gallego-Lizon from the EU Delegation to India and Bhutan who kindly hosted one of the expert meetings at the premises of the Delegation. We are also indebted to numerous officials and experts who participated in the project activities and provided their feedback.

Last but not least, the author would like to thank Nayia Barmpalou, Policy Officer and Project Manager at the European Commission's Directorate-General for International Cooperation and Development, for her support and input into this document.

List of acronyms

AI	Artificial Intelligence
ANSSI	French National Agency for the Security of Information Systems
APCERT	Asia-Pacific Computer Emergency Response Team
APWG	Anti-Phishing Working Group
ASEAN	Association of Southeast Asian Nations
BSA	Software Alliance
CaaS	Crime-as-a-Service
CBMs	Confidence-Building Measures
CCB	Cyber Capacity Building
CCBF	Cyber Capacity Building Framework
CCPCJ	UN Congress on Crime Prevention and Criminal Justice
ccTLD	Country Code Top-Level Domains
CDPF	Cyber Defence Policy Framework
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CERT	Computer Emergency Response Team
CERT-EU	EU Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CMM	Cybersecurity Capability Maturity Model
CoE	Council of Europe
cPPP	Contractual Public-Private Partnership
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSOC	Cyber Security Operations Centre
D4D	Digital for Development
DAC	Development Assistance Committee
DDP	Digital Development Partnership
DG DEVCO	Directorate-General for International Cooperation and Development
DG NEAR	Directorate-General for Neighbourhood and Enlargement Negotiations
DSM	Digital Single Market
EC3	European Cybercrime Centre
ECSO	European Cyber Security Organisation
ECTEG	European Cybercrime Training and Education Group
EDA	European Defence Agency
EEAS	European External Action Service
eIDAS	Electronic Identification, Authentication and Trust Services
EMERG	European Mediterranean Regulators Group
ENCYSEC	Enhancing Cyber Security Project
ENISA	European Union Agency for Network and Information Society
ESDC	European Security and Defence College
ETEE	Education, Training, Evaluation and Exercise

EU SatCen	European Union Satellite Centre
EUGS	European Union Global Strategy on Foreign and Security Policy
EUISS	EU Institute for Security Studies
EURF	EU Result Framework
Eurojust	European Union's Judicial Cooperation Unit
FIRST	Forum of Incident Response and Security Teams
GCCS	Global Conference on Cyberspace
GCI	Global Cybersecurity Index
GCSC	Global Commission on the Stability of Cyberspace
GDPR	General Data Protection Regulation
GFCE	Global Forum on Cyber Expertise
gTLD	Generic Top-Level Domains
HIPSSA	Support for Harmonisation of ICT Policies in Sub-Saharan Africa
HRVP	High Representative for Foreign Affairs and Security Policy / Vice President of the Commission
ICANN	Internet Corporation for Assigned Names and Numbers
ICO	Initial Coin Offerings
ICS	Industrial Control Systems
IcSP	Instrument contributing to Stability and Peace
ICTs	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IEG	Intergovernmental Expert Group on Cybercrime
IGF	Internet Governance Forum
IL	Intervention Logic
IMF	International Monetary Fund
IOT	Internet of Things
IPA	Instrument for Pre-accession Assistance
ISO	International Standardisation Organisation
ISP	Internet Service Providers
ITU	International Telecommunications Union
ITU-D	International Telecommunication Union Development Sector
LE	Law enforcement
LEAs/IC	Law enforcement agencies / Intelligence community
LFA	Logical Framework Approach
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organisation
NCIRC	NATO's Computer Incident Response Capability
NCSA	National Cyber Security Alliance
NCSI	National Cyber Security Index
NCSS	National Cyber Security Strategy
NGO	Non-Governmental Organisation
NIS	Network and Information Security
NRI	Networked Readiness Index
OAS	Organization of American States
OCSIA	Office of Cyber Security and Information Assurance
ODA	Official Development Assistance
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Security Cooperation in Europe

PESCO	Permanent Structured Cooperation
PI	Partnership Instrument
PIMS	Partnership Instrument Monitoring System
PoC	Point of Contact
PPMC	Project and Programme Management Cycle
PSIRT	Product Security Incident Response Team
R&D	Research and Development
RBA	Rights-Based Approach
RIA	Information System Authority of the Republic of Estonia
RIR	Regional Internet Registries
ROM	Result-Oriented Monitoring
SCADA	Supervisory Control and Data Acquisition
SCO	Shanghai Cooperation Organisation
SDGs	Sustainable Development Goals
T-CY	Cybercrime Convention Committee
TI	Trusted Introducer
ToC	Theory of Change
UN	United Nations
UN GGE	United Nations Group of Governmental Experts
UN IEG	United Nations Open-ended Intergovernmental Expert Group on Cybercrime
UNDP	United Nations Development Programme
UNODC	United Nations Office on Drugs and Crime
WEF	World Economic Forum
WSIS+10	World Summit on Information Society

ABOUT THIS OPERATIONAL GUIDANCE

Context and objectives

Ever-evolving **Information and Communications Technologies** (ICTs) have revolutionised how we work over the past 20 years, resulting in their contribution to various policy areas. However, risks and challenges associated with improved access to ICTs and the growing level of internet penetration are often underestimated. Consequently, cyber capacity building is crucial to promote cybersecurity across the globe.

In broad terms, capacity building in the cyber domain aims to build functioning and accountable institutions to respond effectively to cybercrime and to strengthen a country's cyber resilience. This is an integral component of international cooperation that can foster international solidarity with the EU's vision for a free, open, peaceful, secure, interoperable cyberspace for everyone, while ensuring compliance with human rights and the rule of law. Questions of how to structure the capacity-building efforts, what methods to use and how to measure their effectiveness are central in this process.

Since the adoption of its **Cybersecurity Strategy in June 2013**, the EU has been leading on international cyber capacity building and systematically linking these efforts with its development cooperation funds. Such actions are based on promoting a rights-based and whole-of-government approach that integrates lessons the EU has learnt from the development effectiveness agenda. Moreover, in 2017 there was a clear recognition at the EU level that cybersecurity should be considered a transversal issue in development cooperation that can contribute to the realisation of **the 2030 Agenda for Sustainable Development**, as stipulated in the **EU's Digital4Development** policy framework. The significance of efforts to build national resilience in third countries as a means of increasing the level of cybersecurity globally, with positive consequences for the EU, was also recognised in the 2017 **Joint Communication on 'Resilience, deterrence and defence: Building strong cybersecurity for the EU'**.

Why is the operational guidance needed?

Due to the highly sensitive aspects of cybersecurity and potential flow-on risks to key EU values and policies (e.g. the rights-based approach, freedom of expression online/offline, a multi-stakeholder internet governance model and the application of international law in cyberspace), vigilance is necessary to ensure coherence between EU policy and programmes. In light of increased financing for cyber capacity building, a concerted effort is necessary to **consolidate the lessons learned from the EU's experience** – particularly in bridging the development and technical communities – and to **articulate a systematic methodology** that combines the dimensions of cyber policy with development cooperation principles.

What is the aim of the operational guidance?

This **Operational Guidance** is intended to provide a comprehensive practical framework when designing and implementing the EU's external actions against cybercrime and for promoting cybersecurity and cyber resilience. It aims to:

- Provide a consolidated overview of key aspects of cyber policy;
- Assist in the design of appropriate, context-specific project interventions for cyber capacity building in third countries, drawing from development best practices and lessons learned;
- Propose metrics and indicators for measuring the results of cyber programmes.

The Operational Guidance is meant to serve as a resource for EU staff in headquarters and delegations as well as Member State services and implementing partners involved in cyber capacity building. It addresses programmes that have cyber-specific focus, but it is also intended to provide guidance on actions that have cyber-relevant dimensions in order to promote a holistic and consistent approach. External capacity-building programmes that touch on justice and security, in particular on fighting terrorism and organised crime, often address aspects of electronic evidence and cyber-enabled systems, infrastructure and services.

The **methods and frameworks** proposed in this document should be used to:

- Ensure the consistent pursuit of EU interests, values and principles in cyber capacity-building projects;
- Guide cyber capacity needs assessments and identify potential capacity constraints;
- Promote local ownership and comprehensive engagement;
- Ensure that programmes and projects include clear indicators that allow for monitoring progress and making any necessary adaptations;
- Assess the results of concrete initiatives.

How to use this guidance

This document is organised into three main parts:

- Part I, '**A guide to cyber-related concepts and policy developments**', aims to provide an overview of the evolution of cyber-related policies and concepts internationally and in the European Union. Understanding them is essential in designing interventions and partnerships that are grounded in EU values, interests and principles;
- Part II, '**A framework for the EU's external cyber capacity building**', gives an overview of the approach and concrete steps that together form a framework for cyber capacity building. This framework emerges from the current practices and methods employed by the European Commission in its international cooperation with partner countries; and
- Part III, '**Practical application of the guidance to specific pillars**', illustrates how the proposed framework can be employed in four specific areas (independently or in combination): national strategic frameworks, incident and crisis management systems, criminal justice in cyberspace and cyber hygiene and awareness.

The Operational Guidance is accompanied by a **Playbook** - an actionable summary that provides a quick overview of the main steps to follow and key challenges to take into consideration when designing and implementing cyber capacity-building interventions.

This document should be read in conjunction with existing documents, in particular the 'Operational Human Rights Guidance for EU External Cooperation Actions Addressing Terrorism, Organised Crime and Cybersecurity: Integrating the Rights-Based Approach (RBA)'¹, the 'Toolkit for Capacity Development'², and the 'the Project and Programme Cycle Management Guidance' (currently under revision).

For additional information about the EU's approach to project and programme cycle management and a more-broadly defined capacity building, readers are encouraged to use the EU's knowledge-sharing platform for development cooperation – **Capacity4dev** – where they can learn from and interact with other stakeholders, including EU staff, development professionals from EU Member States, partner governments, civil society, academia and the private sector.

Methodology

This Operational Guidance is a result of months of research, including desk research, research missions, interviews and focus groups with experts and policy makers. Between June 2017 and June 2018, the EUISS also organised six expert workshops to discuss different aspects of the study, feeding into the final version. The drafting process was supported by a dedicated EUISS Task Force for Cyber Capacity Building.

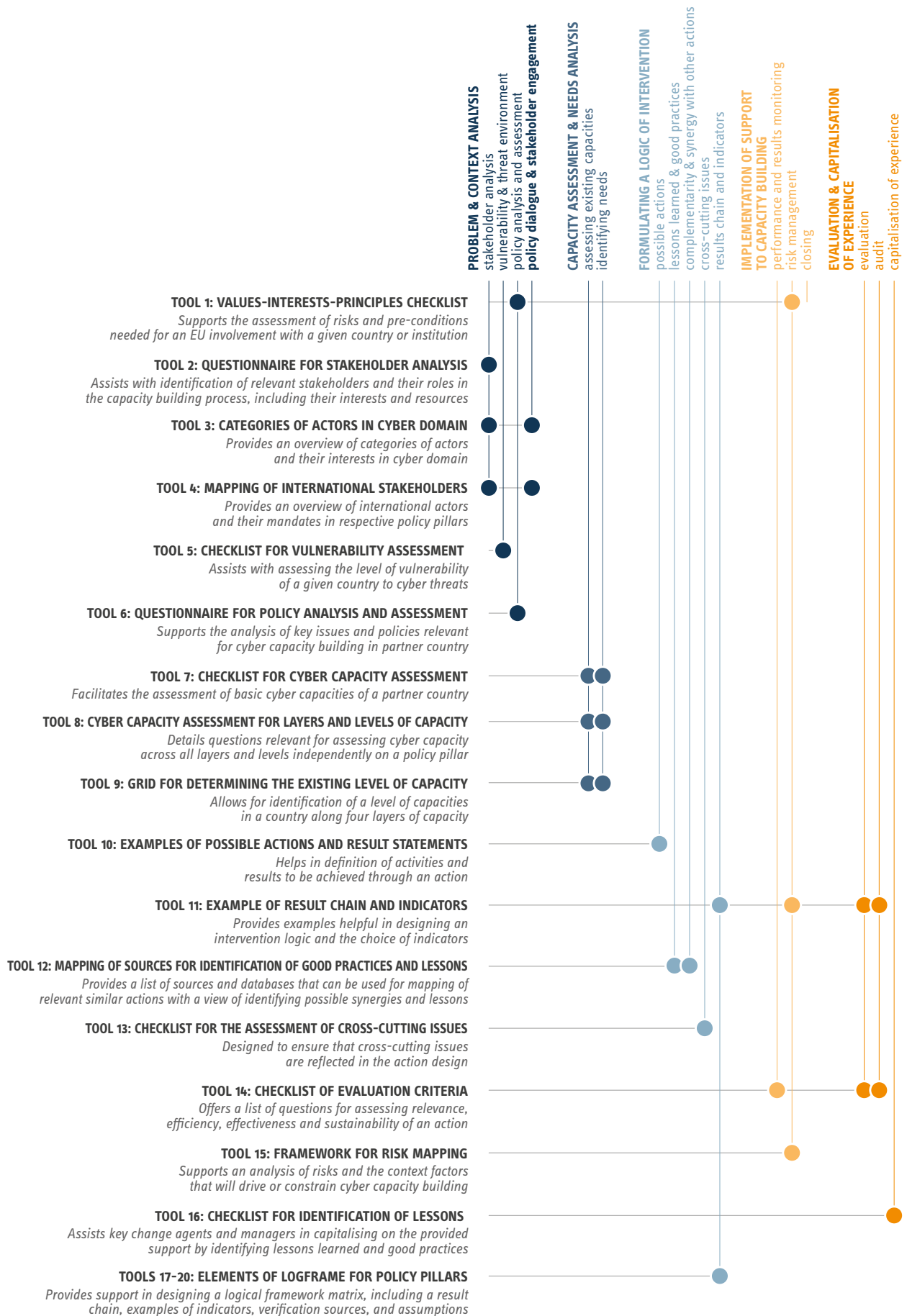
¹ See the European Commission website for [English version](#) and [French version](#).

² European Commission, "[Toolkit for Capacity Development 2010](#)", *Tools and Methods Series*, Reference Document no 6, September 2010.

FIGURE 1: Overview of the Operational Guidance for the EU's international cooperation on CCB



FIGURE 2: List of tools for cyber capacity building proposed in the Operational Guidance



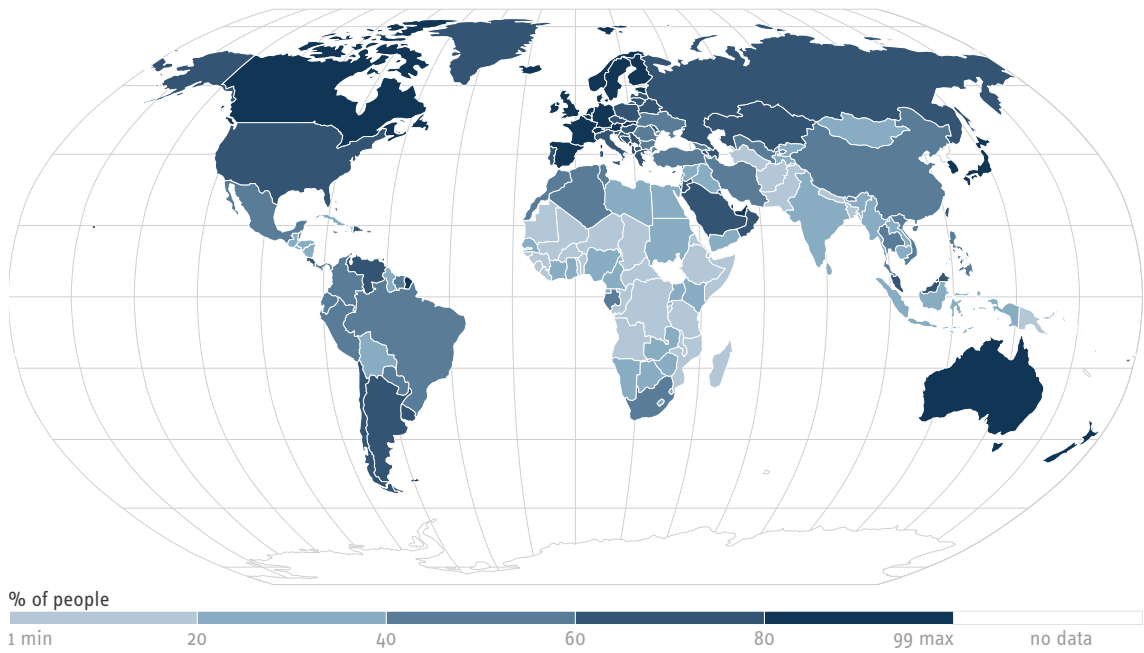
PART I

A GUIDE TO CYBER-RELATED CONCEPTS AND POLICY DEVELOPMENT

1. Cyber concepts and communities

‘Cyber’ today can refer to almost anything. From watches to washing machines to complex energy grids, more and more objects in daily life rely on internet-based platforms. The number of people using the internet has also grown exponentially, with the online population in developing countries, at 2.5 billion, easily surpassing the 1 billion ‘netizens’ in the developed world.³ At the same time, the digital divide remains: almost 78 per cent of people in Africa and 56 per cent in the Asia-Pacific region are still offline compared with 20 per cent of Europeans.⁴

FIGURE 3: The use of the internet globally



Data: ITU, 2017.

The online population trends have been accompanied by the growing importance of emerging or mid-income economies in generating internet-linked wealth. While Facebook and Google are globally recognised brands, companies like the China-based e-commerce giant Alibaba or South Africa-based Naspers are also among the 20 biggest internet firms. An analysis of start-up ecosystems shows the increasing competitiveness of IT hubs like Beijing, Singapore, São Paulo, Moscow and Bangalore. The language profile of the internet is evolving too. While English is still dominant, the percentage of content in other languages is growing fast. Technology and the ways in which societies rely on the internet evolve at an incredible pace too. Digital platforms

³ International Telecommunications Union, *ICT Facts and Figures*, 2017.
⁴ Ibid.

are no longer only about access to information or faster communication but have become essential for the delivery of services such as energy, transportation and finance. With the advancement of the Internet of Things, the number of internet-connected devices and actors responsible for their operations is growing.

This rapidly evolving environment determines the concepts and vocabulary used to describe the unfolding digital change. Naturally, the terminology is conditioned by the phenomena it aims to depict. On one hand, the **concepts of 'digital' and 'digitalisation'** entered the policy vocabulary to describe processes such as digital development, digital dividends or digital empowerment that highlight the positive contribution the internet has brought to our societies, for example by boosting economic growth, improving the delivery of services and promoting governance accountability.

On the other hand, **cyber-related concepts** are used to highlight that digital growth cannot be attained without a safe and secure underlying digital environment. In this light, cybersecurity is used in relation to the integrity and security of networks; cybercrime for criminal activities committed online or with the use of the internet; or cyber defence to describe aspects necessary to protect military assets.

Each of these has led to the emergence of distinct, area-specific sets of vocabulary, objectives and communities, which to an extent are characterised by a silo mentality among policymakers and stakeholders involved. Nevertheless, 'digital' and 'cyber' concepts are intertwined as no progress in the digital domain can be achieved without addressing risks and vulnerabilities in cyberspace.

This section will elaborate on the different dimensions of cyberspace in an attempt to introduce and help navigate the multi-layer discourses that relate to it across policy communities.

BOX 1: CYBER-RELATED DEFINITIONS (I)

Cyberspace is a 'man made global strategic domain (...) consisting of the interdependent network of information technology infrastructure and resident data, including the internet, telecommunications network, computer systems, and embedded processors and controllers for the production and use of information by individuals and organisations' (Fiddner, 2015).

Cybersecurity 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. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

Cybercrime commonly refers to a broad range of 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).

Cybersecurity capacity building: all types of activities (e.g. human resources development, institutional reform or organisational adaptations) that safeguard and promote the safe, secure and open use of cyberspace (Pawlak, 2014).

1.1. Cyberspace as a development venue

Cyberspace provides the underlying platform for the development and spread of transformative digital technologies, with profound global implications and many human, economic and social benefits. The **New European Consensus on Development** of 2017 acknowledges that digitalisation is an essential driver for achieving the **2030 Agenda on Sustainable Development** and reiterates that digital technologies and services are powerful enablers of inclusive growth and sustainable development. The **2016 World Development Report on Digital Dividends** points out that the internet has been instrumental in promoting socioeconomic development: *'By reducing information costs, digital technologies greatly lower the cost of economic and social transactions for firms, individuals, and the public sector. They promote innovation*

when transaction costs fall to essentially zero. They boost efficiency as existing activities and services become cheaper, quicker, or more convenient. And they increase inclusion as people get access to services that previously were out of reach’.

Opportunities for human development are also at the heart of the digital revolution. For example, the European Commission’s **2017 Digital4Development** Staff Working Document explores the significant influence digitalisation can have towards increased productivity, sustainable growth, job creation and the empowerment of women. From the perspective of personal freedoms, the internet provides significantly greater possibilities for individuals to express themselves and to access information, while the roll-out of eGovernment initiatives has improved the transparency and accountability of public institutions. For this reason, access to an open, free, stable and secure cyberspace along with unhindered, uncensored and non-discriminatory use of ICTs, are rightfully considered essential components in fostering open societies and enabling economic growth and social development globally.

1.2. Cyberspace as a security domain

The focus on cybersecurity can be broadly understood in terms of policies, laws and institutions with the primary objective to protect citizens and infrastructure from threats resulting from an ever-changing relationship between humans and technology. The ‘founding fathers’ of the internet designed it as a means to facilitate communication and exchange information. However, as the ways of using the internet evolved and our society became more dependent on computer systems and networks, wireless protocols and internet-enabled ‘smart’ devices, so has the focus on potential vulnerabilities grown. Cybersecurity lapses or flaws generate a significant cost for global economy and undermine trust in the digital society. As control over cyberspace becomes further diffuse, the responsibility for cybersecurity also becomes fragmented and dispersed among governmental and non-governmental actors.

While generally regarded by the public as a mystifying technical issue best left to ICT security specialists and network managers, the complexity of cybersecurity and the cross-cutting nature of the involved policy challenges increasingly call for attention from other communities, including law enforcement, behavioural experts and the development community. In this vein, the Organisation for Economic Cooperation and Development (OECD) in its 2015 digital risk management framework suggested approaching digital risks not as a technical problem but as an economic risk that should form an integral part of an overall risk management process.⁵

The most common goals associated with cybersecurity are securing the network and information systems. However, there is no single definition of cybersecurity. The OECD, for instance, avoids references to cybersecurity and instead talks of ‘digital security risk management’, which it describes as a set of coordinated actions that will minimise risk and maximise opportunities in the digital environment.⁶ The United Nations framed cybersecurity as challenges relating to ICTs, and steers most definitions and understandings through its specialised agency, the International Telecommunications Union (ITU). The International Standardisation Organisation (ISO) primarily refers to cybersecurity as internet security and is concerned primarily with the preservation of confidentiality, integrity and availability of information in cyberspace.⁷

In recent years, broad definitions of cybersecurity have become relatively harmonised, with the common goal being to inhibit the disruption of cyberspace or its users and their assets. Cybersecurity has been gradually included in strategic planning in an attempt to streamline the approach across different policy strands and address challenges comprehensively. It currently covers issues linked not only to network and information security but also has clear overlaps with other policy areas including research and development, industry, education, diplomacy and in certain cases defence.

5 OECD, “Digital Security Risk Management for Economic and Social Prosperity”, Paris, 2015.












6 Ibid.

7 ISO/IEC27032, “Information technology – Security techniques – Guidelines for cybersecurity”, 2012.

FIGURE 4: Layers of governance in cyberspace

Economic & societal layer

KEY GOVERNANCE ACTORS: IGF, technical organizations (ISOC, W3C, ...), NETmundial, World Economic Forum, national governments, civil society, intergovernmental organizations (OECD, UNESCO, ...), law enforcement agencies

 LAWS, POLICIES AND REGULATIONS Governing bodies in local, national, regional and international spheres are engaged with their citizens and with other bodies to develop and apply laws, policies, and/or regulations. The transnational nature of the Internet must be synchronized with the established International system of governance and laws.	 INDUSTRY AND TRADE Manufacturing, retail, supply chain/logistics, healthcare, finance, etc.	 NEWS AND INFORMATION Newspapers, broadcast, personal & professional blogs, social media.	 APPLICATIONS Worldwide web, email, cloud, VoIP, mobile apps
 CIVIC AND HUMAN RIGHTS Privacy, identity, access to content, freedom of expression, consumer protection, cultural diversity	 SOCIAL MEDIA Sharing photos, videos, ideas and information	 USERS There are over 3.5 billion users worldwide. Most users connect to the Internet through their mobile phone.	 MOBILE Smart phones, tablets, cars. There are now more mobile devices on the planet than people.
		 SECURITY Cybersecurity, cyber warfare, cyber espionage, cybercrime.	 EDUCATION Online universities, research, tutorials, classroom engagement
			 ENTERTAINMENT Music, movies, television, games

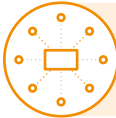





Logical layer

KEY GOVERNANCE ACTORS: ETSI, ICANN / IANA, EITF, ISO, ITEE, NRO, TLD Operators, W3C

ROOT SERVICES 12 organizations from 4 countries administering 13 different root servers that provide top-level DNS services via hundreds of machines in dozens of countries	THE ROOT ZONE == NAMES + NUMBERS + INTERNET PROTOCOLS = IDENTIFIERS' PUBLIC REGISTERS	DOMAIN NAMES 250+ Country Code Top-Level Domains (ccTLDs) such as .fr, .br, .us, ... 1,200+ Generic Top-Level Domains (gTLDs) such as .com, .biz, .realtor, ... ~1500+ Domain Name Registrars such as GoDaddy, Network Solutions, Register ...	IP ADDRESSES IPv4: More than 4 billion addresses. IPv6: 340 undecillion (trillion, trillion) addresses. 5 Regional Internet Registries (RIRs) that coordinate policy related to Internet address resources.	PROTOCOL PARAMETERS Protocol parameters are the commands and identifiers that are used inside protocols, the structured communications used for the web, email, etc., to transfer the information <i>These parameters are used in standards defined by the IETF in coordination with other standard organizations such as the W3C. e.g. TCP/IP, VoIP, HTTP, HTTPS.</i>
---	--	--	---	---

Infrastructure layer

KEY GOVERNANCE ACTORS: GSMA, IEEE, IETF, ITU, National ICT Ministries, Network Operator Groups

 THE INTERNET BACKBONE (IP NETWORKS) 90% is privately owned by global companies like: Level 3 Communications, TeliaSonera International Carrier, CenturyLink, Vodafone, Verizon, Sprint, AT&T	 INTERNET EXCHANGE POINTS (IXP) ~550 points worldwide.	 TERRESTRIAL CABLES	 UNDERSEA CABLES ~300 cables that transmit 99% of all international Internet data.	 SATELLITES ~2,000 communications satellites in use, many used now for Internet data.	 WIRELESS SYSTEMS ~824,000 wireless towers worldwide.
--	--	--	--	--	---

Data: ICANN, 2015.

1.3. Cyberspace as an area of justice and a crime scene

The internet has made life easier not only for those using it to communicate, learn or do business, but also for criminals seeking wealth or to promote an ideology. The increased number of users has also led to a rapid uptake in online criminality including identity theft, fraud, unauthorised retention of payment or credit card information and child pornography. That negative dimension and the threat to the safety and well-being of citizens pushed the issue out of the hands of IT experts alone and to the top of policy discussions.

The initial reaction to cybercrime had a mainly economic flavour. The 1992 OECD guidelines were among the first to underline the importance of information security from the perspective of preventing criminal acts from being committed online.⁸

In 1996 a comprehensive review began at the Council of Europe with a focus on how to keep criminal law abreast of technological developments that create openings for misusing cyberspace or damaging legitimate interests.⁹ This launched a negotiation process that culminated in the **2001 Convention on Cybercrime (known as the Budapest Convention)** which remains the most relevant legally binding global instrument to address cybercrime and electronic evidence.¹⁰ It is meant to provide a framework for criminalising offences against and by means of computers in domestic law, for specifying procedural powers to secure electronic evidence in relation to any crime while establishing rule of law safeguards to limit such powers, and for effective international cooperation.

Different actors picked up on the issue from a law-enforcement perspective, with the Group of 8 endorsing in 1998 an action plan on combatting high-tech crime that expanded the focus towards new ways in which technology was being used for illicit ends – notably in organised crime and the illegal drugs trade.¹¹

Cybercrime was first put on the agenda of the 8th United Nations Congress on Crime Prevention and Criminal Justice in 1990 and then more specifically at the 11th Congress of 2005, with subsequent discussions at the 2010 UN Crime Congress and the setting up of an Intergovernmental Expert Group on Cybercrime in 2011. These meetings helped achieve broad agreement at the UN level on capacity building as an effective way to enable societies to address the challenges of cybercrime and electronic evidence.

As the nature of crime in the digital space takes new forms (e.g. with the use of cryptocurrencies or Malware-as-a-Service) and crime groups seek to exploit cybercrime ‘safe havens’, policy responses need to encompass such areas as privacy and data protection, content-related offences, economic crimes and unauthorised access and intellectual property violations. Internet use by terrorist organisations has given a new flavour as well as urgency to the discussions. The increased focus on countering radicalisation online has also resulted in the emergence of the term ‘**cyber terrorism**’ as an alleged novel form of crime that requires a new international treaty. However, existing international instruments, notably the Budapest Convention, have substantive provisions that are applicable to the ‘**terrorist use of ICT**’. The existing procedural and international mutual legal assistance tools are also available to investigations and prosecutions on terrorist-related crimes. Finally, the ‘cyber terrorism’ term is often used vaguely, opening the door for human rights abuses.

1.4. Cyberspace as a diplomatic arena

The expanding role of the internet in modern society and the malicious use of ICTs by one state against another pushed cybersecurity into the diplomatic realm. Russia put it on the UN agenda in 1998 when it introduced a draft resolution on ‘Developments in the field of information and telecommunications in the context of international security’ in the First Committee of the UN General Assembly. However, the debate about the need for a ‘cyber stability regime’ remained a niche subject until the UN General Assembly in 2003 adopted Resolution 58/32 requesting the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them. The resolution also called for the establishment of a UN Group of Governmental Experts (UN GGE)¹² which convened in 2004. Since then,

8 OECD, “OECD Guidelines for the Security of Information Systems”, Paris, 1992.

9 Council of Europe, “Explanatory Report to the Convention on Cybercrime (CETS 185)”, 23 November 2001, Budapest.

10 Council of Europe, “Convention on Cybercrime, Budapest”, 23 November 2001, Budapest.

11 G8 Summit, “Drugs and International Crime”, Birmingham Summit, 15–17 May 1998.

12 For additional information about the UNGGE process, please see the UNODA website.

UN GGEs have become the main vehicle for the discussion about international security and stability in cyberspace based on three main pillars:

- **The application of existing international law in cyberspace:** Despite the consensus presented in the 2013 UN GGE report 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’,¹³ there is still an on-going debate about what that means in practice.
- **Norms, rules and principles of responsible state behaviour in cyberspace:** Norms reflect the expectations of states and the international community in their relations. However, the voluntary and non-binding nature of norms does not limit or prohibit actions that are otherwise consistent with international law. The compliance with norms allows states to assess their intentions, prevent conflict and contribute to social and economic development.¹⁴ The 2013 UN GGE report included 11 recommended norms and principles for responsible behaviour in cyberspace for the purposes of international security.
- **Confidence-Building Measures (CBMs) in cyberspace:** These practical steps aim to increase transparency, predictability and thereby stability as a form of preventive diplomacy to restrain the use of force¹⁵ and limit the causes of mistrust, misunderstanding and miscalculation between states. The UN GGE has developed a list of voluntary CBMs for cyberspace, recognising them as a key mechanism for ‘*reducing the risks of conflict stemming from the use of ICTs*’. They were further taken up at regional settings, most notably at the Organisation for Security and Cooperation in Europe as well as the ASEAN Regional Forum and, most recently, the Organisation of American States. The OSCE adopted two sets of CBMs in 2013 and 2016,¹⁶ with the focus now being on their meaningful implementation. One example is having a national point of contact ‘*to facilitate pertinent communications and dialogue on security of and in the use of ICTs*’.

The most significant breakthrough in this field came with the 2013 UN GGE report (A/70/174), wherein members for the first time recognised that the existing International Law applies to the use of ICTs. The 2015 report advanced these conclusions, including further defining norms applicable to cyberspace. The most recent UN GGE, with a growing membership of non-Western states, concluded its work in July 2017 without publishing a report due to a lack of consensus, in particular over how international law applies to states’ responses and countermeasures to cyber incidents.

BOX 2: PLATFORMS FOR CYBER DIPLOMACY DEBATES

The discussions in the UN have been accompanied by work conducted elsewhere. With regard to international law, the **Tallinn Manual process** coordinated by the NATO Cooperative Cyber Defence Centre of Excellence resulted in two volumes addressing the applicability of existing international law to cyber conflict and in situations that do not meet the threshold of an armed conflict. The Tallinn Manual was produced by leading international law scholars but remains an academic exercise and is not an official position of NATO. Two parallel tracks emerged regarding norms of responsible state behaviour: a series of bilateral agreements between governments and a more inclusive, expert-driven process under the auspices of the **Global Commission on Stability in Cyberspace**. The most progress on CBMs so far has been made in the framework of the OSCE, which has adopted a set of 16 voluntary measures.* Concerning cyber capacity building, a group of states, international organisations and private sector established in 2015 the **Global Forum on Cyber Expertise**, which aims to identify successful policies, best practices and ideas and multiply them on a global level.

* OSCE, Decision No. 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies, Vienna, 10 March 2016.

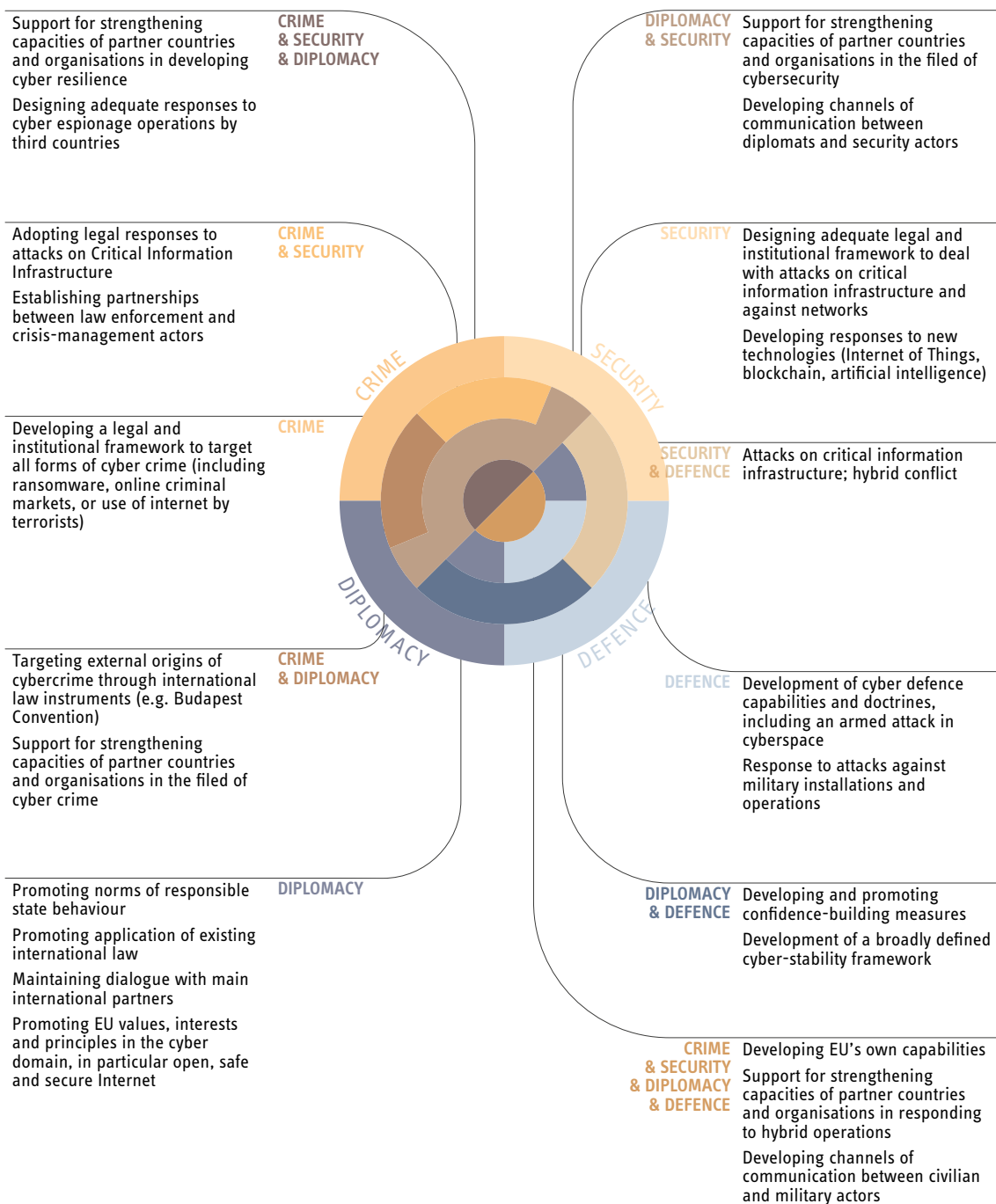
13 United Nations, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security”, New York, 24 June 2013.

14 United Nations, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security”, New York, 22 July 2015.

15 P. Pawlak, “Confidence-Building Measures in Cyberspace: Current Debates and Trends” in A-M Osula, & internet. Rõigas (Eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO Cooperative Cyber Defence Centre of Excellence Publications, Tallinn, 2016, pp.129-153.

16 See OSCE Ministerial Decisions [5/2016](#) and [5/2017](#).

FIGURE 5: Complexity of cyber-related concepts



1.5. Cyberspace as a battlefield

The increasing use of the internet and internet-enabled platforms in hybrid operations against states and non-state actors puts cyberspace at risk of becoming another domain for inter-state conflict. Cybersecurity has become an existential challenge for national security, giving the discussion a significant military dimension. NATO has already recognised cyberspace as **'fifth domain of warfare'**, in addition to land, sea, air and space. Consequently, numerous countries have moved to develop and adopt national cyber defence strategies covering the concepts, approaches and tools that they have or intend to develop for use in case of a cyberattack. However, despite the tendency to use cyber defence as a 'catch-all' expression to describe any efforts to strengthen preparedness and respond to cyber incidents, public or private, it is important to note that this concept is strictly linked to the protection of military assets and a state's territorial integrity exclusively through military means. In reality, this distinction is more complicated to make. Given that military infrastructure often relies on off-the-shelf solutions from the private sector and civilian networks (e.g.

energy, transportation, telecommunication), the nature of civil-military relations in cyberspace needs to be clarified. More analysis is needed concerning a state's right to store vulnerabilities (also referred to as 'cyber weapons') that could be used against other states or non-state actors and the obligations that would result from any damage caused. Beyond the question of capabilities, the discussion about cyber defence is closely linked to that of stability in cyberspace, in particular with regard to the rights and obligations of states stemming from the UN Charter. Those include the right to self-defence in case of an armed attack (Article 51) and the obligation to refrain in international relations from the threat or use of force against the territorial integrity or political independence of any state (Article 2).

1.6. Cyberspace as a capacity-building site

The intrusion of the digital continuum in all areas of human activity has made it impossible to treat cyber-security as a distinct policy area. Instead cyberspace has emerged as a cross-cutting, multifaceted policy issue. At the same time there is a realisation that no country or organisation is 'cyber ready'.¹⁷ Increasing the capacities of all stakeholders to fully benefit from digital technologies and address the accompanying challenges has become a common thread.

Capacity building is therefore an overarching concept applicable to all the above-mentioned cyber fields. It pertains to efforts to *'invent, develop and maintain institutions and organisations that are capable of learning and bringing about their continuing transformation, so that they can better play a dynamic role to sustain national development processes'*.¹⁸

Interestingly, given the multi-natured and multi-actor dimension of capacity building, the definition and implementation of cyber capacity-building measures are underpinned by distinct logics that most often are complementary. The following policy prerogatives are the most notable drivers for capacity-building efforts in the field of cyberspace:

- **Development and Resilience**, aimed at building functioning and accountable institutions essential for effectively responding to and recovering from cyber threats, while ensuring compliance with human rights and the rule of law;
- **Diplomacy**, whereby CCB constitutes one strategic building block of evolving cyber diplomacy efforts for upholding a global, open, free, stable and secure cyberspace;
- **Access and Connectivity**, as powerful enablers of inclusive growth and sustainable development, including for achieving Sustainable Development Goals. In this framework, the promotion of cybersecurity in the roll-out of digital infrastructure and solutions ('secure-by design') is an essential component of actions focused on improving open and affordable access to broadband connectivity.
- **Market**, whereby the deployment of digital services, the support to national regulatory frameworks, and promotion of trans-border digital trade, is seen as a means to ensuring open market access, an improved business environment, enhanced transparency and more private investment. Cybersecurity capacity building is considered essential to keep the online economy running and to ensure prosperity.
- **Defence**, in which defining cyber defence strategies, the adoption of measures for the protection of military networks and assets and related training and exercises are designed to enhance the resilience of defence institutions and bodies against cyber and hybrid attacks. Even though such capacity building is in principle outside the realm of development cooperation, one should bear in mind that during the development of national cybersecurity strategic frameworks, defence actors (e.g. ministries, academies) are important stakeholders as part of a whole-of-government approach.

As the concept of capacity building originates in development policy and practice, there are well-established and streamlined methodologies for result-orientation, in particular with regard to tools for programming, implementation and evaluation. However, their use in the field of capacity building for promoting cyber

17 M. Hathaway, "Cyber Readiness Index 2.0", Potomac Institute, 2015.

18 United Nations, "United Nations System Support for Capacity-Building", E/2002/58, 14 May 2002.

resilience and fighting cybercrime has been limited as some actors, primarily in the security community, argue that cyber capacity building requires ‘reinventing the wheel’.

However, there has been a growing convergence among different communities in recent years, fostered particularly by cases where cyber capacity building has been systematically linked with development co-operation funds and structural reform, as has been the EU approach. These tools and methodologies are therefore progressively applied, but there is a clear need for more learning and sharing of good practices across disciplines. This is particularly important to promote data- and evidence-driven policymaking and streamlined implementation that is results-oriented and accompanied by the requisite metrics and methods for measuring results.

2. The EU approach to building resilience in cyberspace

The EU’s approach to cyber-related issues has evolved from addressing policy-specific challenges – such as high-tech crime or network and information security – towards a more comprehensive and dynamic concept of resilience. That means moving away from crisis containment to a more structural and long-term approach to vulnerabilities, with an emphasis on anticipation, prevention and preparedness. The **Communication on the EU Strategic Approach to Resilience** defines resilience as ‘*the ability of an individual, a household, a community, a country or a region to withstand, adapt and quickly recover from stress and shocks*’.¹⁹ The concept of resilience is particularly helpful also in allowing for a stronger link with development policy, which is driven by the need to address global challenges and risks in the long-term such as security, economic growth, innovation, etc.

In light of the significant reliance of states and societies on internet-enabled technologies, the potential for conflict in the absence of clear norms of responsible state behaviour is real. But there is only a fragile consensus regarding the application of the existing international law in cyberspace. Thus, the EU’s approach to building cyber resilience has focused on both internal and external policy frameworks. This section explores the key relevant policy and legal frameworks the EU has put forward.

The adoption of the **EU Cybersecurity Strategy** was a defining moment for strengthening the EU’s role in shaping cybersecurity policies – both among the Member States and globally. The framework document brings together several objectives that constitute pillars of the EU’s cybersecurity policy:

- Increasing cyber resilience
- Reducing cybercrime
- Developing EU cyber defence policy and capabilities related to Common Security and Defence Policy (CSDP)
- Developing the industrial and technical resources for cybersecurity
- Establishing a coherent international cyberspace policy for the EU and promoting core EU values

Welcoming the adoption of the Strategy, the Council of the European Union recognised that cybersecurity constitutes ‘*one of the most important present and future challenges*’, and noted the important role of the EU ‘*in supporting and maintaining an open, secure and resilient cyberspace based on the core values of the EU such as democracy, human rights and the rule of law*’.²⁰

The adoption of the **Digital Single Market Strategy for Europe** in 2015 created a broad framework for enhancing the EU’s position as a world leader in the digital economy. It aims at strengthening the EU’s role in digital technologies, including through reinforcing trust and security aspects of digital goods and services. Consequently, addressing potential vulnerabilities that could be exploited illicitly resulting in financial losses, breaches of personal data or the subversion of democratic processes became one of the key components of the strategy.²¹

19 European Commission, “Communication from the Commission to the European Parliament and the Council - The EU approach to resilience: Learning from food security crises”, COM(2012) 586 final, Brussels, 3 October 2012.

20 Council of the European Union, “Council Conclusions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, 22 July 2013 (doc. 12109/13).

21 See: European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the Implementation of the Digital Single Market Strategy: A connected digital single market for all”, COM(2017) 228 final, Brussels, 10 May 2017.

The **Network and Information Security (NIS) Directive** is the first comprehensive, EU-wide cybersecurity legislation. It was proposed by the European Commission in 2013 and adopted by the European Parliament in July 2016. The NIS Directive sets benchmarks for what constitutes a desirable level of institutional, policy and regulatory capacity to minimise the impact of cyber threats. In addition, provisions concerning the prevention of cyber risks and the mitigation of cybersecurity breaches have been inserted in sector-specific laws such as the Electronic Communications Regulatory Framework, which has been under review by the co-legislators since 2016; the Payment Services Directive 2,²² the eIDAS Regulation²³ and the General Data Protection Regulation.²⁴

At the same time, the EU continued to work on strengthening the response to malicious and illegal activities in cyberspace. The **European Agenda on Security** of 2015 provided the impulse for strengthening those aspects of EU policies that addressed the security component specifically, prioritising terrorism, organised crime and cybercrime as interlinked threats with a strong cross-border dimension. The Agenda has the fight against cybercrime as a key priority that is translated in several cyber-related elements, such as:

- Renewed emphasis on implementation of existing policies on cybersecurity, attacks against information systems and combating child sexual exploitation;
- Reviewing and possibly extending legislation on combatting fraud and counterfeiting of non-cash means of payments;
- Reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules of access to evidence and information;
- Enhancing cyber capacity-building actions under external assistance instruments.

The Commission's **Communication on Security Union**, presented in April 2016, further enhanced the focus on cybercrime, which now constitutes a permanent component in regular implementation reports of the Security Union.

Reflecting the fast-evolving environment, the European Commission presented in July 2016 the **Communication on Strengthening Europe's Cyber Resilience System**, which aims to improve the EU's cybersecurity and incident-response capacity as well as making Europe a leading player in the cybersecurity industry. The Commission is calling for stepped-up cooperation to enhance preparedness and deal with cyber incidents, address challenges related to Europe's Single Market and nurture industrial capabilities in the cybersecurity field.

22 Council of the European Union, "Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337", Brussels, November 2015.

23 Regulation 910/2014/EU of the European Parliament and Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L257.

24 Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.

FIGURE 6: Selected legal and strategic documents adopted by the EU (1999-2018)



These objectives were further developed in the 2017 **Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'**, which provides an overarching framework for the EU's cyber policies. The revised approach is based on three main pillars:

- **Building EU resilience to cyber attacks** based on a 'collective, wide-ranging approach' which requires a more comprehensive, cross-policy approach and strategic autonomy. Concrete steps to that effect will include: strengthening the mandate of ENISA and turning it into a permanent Cybersecurity Agency; creating a Single Cybersecurity Market through a certification framework covering security in critical or high-risk applications, widely deployed digital products and the use of 'security by design' in interconnected mass consumer devices; full implementation of the NIS Directive; developing a 'Blueprint' for crisis management; establishing a Cybersecurity Emergency Response Fund and European Cybersecurity Research and Competence Centre; building the EU cyber skillbase; promoting cyber hygiene and awareness.
- **Creating effective cyber deterrence** involves putting in place credible measures to dissuade criminals and attackers – both state and non-state. This includes effective law enforcement and political and diplomatic responses. Concrete measures foreseen in the Communication include enabling cross-border access to electronic evidence and working towards common forensic standards. It also covers the role of encryption in criminal investigations. The implementation of the **Cyber Diplomacy Toolbox** adopted in June 2017, which sets out a range of EU joint diplomatic measures in response to cyber attacks, including sanctions, is another key aspect in improving deterrence. Recognising the need for synergies between civilian and military efforts, the **Permanent Structured Cooperation (PESCO)** and the **Cyber Defence Policy Framework** further contribute to the deterrence goal.
- **Strengthening international cooperation on cybersecurity** to promote global cyber stability as well as contribute to Europe's strategic autonomy in cyberspace. This involves promoting existing international law and developing voluntary norms, rules and principles of responsible state behaviour. The most relevant part of the new Communication concerns cybersecurity capacity building, including the creation of a dedicated EU Cyber Capacity Building Network that would bring together the Commission services, the EEAS, Member States' cyber authorities as well as other EU bodies and agencies.

The EU has also **mainstreamed cyber issues into its foreign and security policy**, in particular through official dialogues with key partners (e.g. Brazil, China, India, Japan, South Korea and the United States) on issues such as norms, the application of existing international law in cyberspace, Confidence Building Measures and capacity-building initiatives in third countries. The **EU's Cyber Defence Policy Framework** and the **Council Conclusions on Cyber Diplomacy** adopted in November 2014 and February 2015 respectively guide the EU's international engagements in the cyber domain. The 2016 **Joint Framework on countering hybrid threats** recognises the need to improve the resilience of Europe's critical infrastructure and address the broad array of cybersecurity risks to essential service providers in the fields of energy, transport, finance or health.

The **European Union's Global Strategy on foreign and security policy** (EUGS) presented in June 2016 also recognises the growing importance of cybersecurity. In many aspects, the EUGS reiterates earlier commitments, including increasing the focus on cybersecurity by '*equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace*', and stressing the need to develop the EU's strategic autonomy in cyberspace. The EUGS also gives an indication of the EU's external priorities in this regard, including the commitment to make the EU a '*forward-looking cyber player*'.

BOX 3: EU AGENCIES AND BODIES WITH CYBER-RELATED TASKS

European Network and Information Security Agency (ENISA) is a centre of expertise for Member States regarding building cyber resilience. The revision of the ENISA's mandate foresees establishing it as a permanent EU Cybersecurity Agency with responsibility, among others, for support to policy development in ICT standardisation.

European Cybercrime Centre (EC3) at Europol provides operational support to national authorities in Member States in the fight against cybercrime, including by serving as the hub for criminal information and intelligence and support in cybercrime cases.

European Union's Judicial Cooperation Unit (Eurojust) assists national cybercrime investigations and prosecutions to speed up information-sharing on legal matters. Other tasks include support to the **European Judicial Cybercrime Network** (EJCN).

European Union Agency for Law Enforcement Training (CEPOL) is dedicated to developing, implementing and coordinating training for law enforcement officials, including in line with the Cybercrime Training Competency Framework developed by CEPOL together with Europol and the European Cybercrime Training and Education Group (ECTEG).

Computer Emergency Response Team EU (CERT-EU) monitors and responds to concrete information-security incidents and threats to EU institutions, agencies and bodies.

European Defence Agency (EDA) supports cyber capabilities development in Member States and closer cooperation at the European Union level. EDA is involved in training and exercises, Advanced Persistent Threats Detection, digital forensics for military use and the Cyber Defence Strategic Research Agenda.

EU Institute for Security Studies (EUISS) conducts analyses of foreign, security and defence policy issues. As part of its mandate, the EUISS conducts research and implements projects linked to broadly defined cyber capacity building, cyber diplomacy and cyber resilience.

European Security and Defence College (ESDC) provides strategic-level education and training in the Common Security and Defence Policy. It is responsible for managing the education, training, evaluation and exercise (ETEE) platform in the cybersecurity/defence field.

FIGURE 7: Key actors in cyberspace



2.1. Cybersecurity

Since the late 1990s, the EU’s efforts to ensure the proper functioning of network and information systems and to strengthen their resilience against any form of interruption or damage were driven by a recognition that the capabilities of Member States varied, a situation that could harm the smooth functioning of the internal market as well as the development of the Digital Single Market. The first piece of EU legislation aimed at ensuring a common level of comprehensive cybersecurity in the EU was the NIS Directive, complemented by measures for the creation of a European cybersecurity marketplace; cybersecurity public-private partnerships; and a Blueprint for crisis management.

BOX 4: CYBER-RELATED DEFINITIONS (II)

Network and information system

- an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services;*
- any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or
- digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

Cyber incident: Any occurrence that has impact on any of the components of cyberspace or on the functioning of cyberspace, independent of whether it was natural or human made; malicious or non-malicious in intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions, is called a cyber incident. A cyber incident is also any incident generated by any cyberspace component even if the damage/disruption/dysfunctionality is caused outside the cyberspace.

Cyber accident: To support a 'grading' of cyber incidents, cyber accidents are defined as any occurrence associated with cyberspace causing significant damage to cyberspace or any other asset (has performance impact, requires repairs, replacement) or causing personal injury.

* Which reads: '(a) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.'

Source: Network and Information Security (NIS) Directive.

NIS Directive

The NIS Directive is structured along three main pillars: (1) establishing foundations for building cyber resilience; (2) strengthening cooperation among stakeholders; and (3) building a culture of security across critical sectors reliant on ICTs.

In an effort to harmonise the level of preparedness and the capacities for response across the Union, the NIS Directive requires each Member State to adopt a national strategy on the security of network and information systems that outlines objectives and measures to ensure a high level of security in sectors such as energy, transport, banking, financial-market infrastructure, healthcare, drinking-water supply and distribution and digital infrastructure, e.g. IXPs, DNS service providers and TLD name registries. National NIS strategies should also include a governance framework, an indication of the education and training programmes relating to a given strategy, potential research and development plans, a list of actors involved in implementing the strategy and a risk assessment plan.

To monitor the implementation of the Directive, each Member State is to designate and provide adequate resources for one or more national authority and a single point of contact to ensure cross-border cooperation. In addition, at least one Computer Security Incident Response Team (CSIRT) will be designated as responsible for risk and incident handling, including monitoring at a national level, providing early warning, responding to incidents and participating in the CSIRT network.

The NIS Directive also puts forward measures aimed at improving strategic and operational cooperation among EU stakeholders. For instance, the new NIS Cooperation Group supports strategic cooperation and exchange of information among Member States. Representatives from Member States, the Commission and ENISA provide strategic guidance for the CSIRTs and use the Group to exchange best practices on incident notification, capacity building, raising awareness, training and research and development. The CSIRT network composed of national CSIRTs and CERT-EU plays a particular role in building confidence and trust between Member States and in promoting effective operational cooperation.

Finally, the Directive requires Member States to ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of network and information systems, and that any incident that significantly affects the continuity of essential services is communicated to the competent authority or the CSIRT without undue delay. The information should be shared with other

affected Member States while preserving the security and commercial interests of the service operator. The Directive also includes provisions with regard to risk-management practices of digital-service providers such as online marketplaces, search engines and cloud-computing services.

Table 1: Pillars of the NIS Directive

Resilience	
National strategy on the security of network and information systems	<ul style="list-style-type: none"> • Strategic objectives, priorities and governance framework • Identification of measure on preparedness, response and recovery • Cooperation methods between public and private sectors • Awareness raising, training and education • Research and development plans related to NIS strategy • Risk assessment plan • List of actors involved in the strategy implementation
Designation of competent national authorities for the NIS Directive	<ul style="list-style-type: none"> • Designation of a single point of contact to ensure cross-border cooperation
Designation of one or more CSIRTs	<ul style="list-style-type: none"> • Monitoring incidents at national level • Providing early warning, alerts, announcements and other pertinent information to relevant stakeholders • Responding to incidents • Providing dynamic risk and incident analysis and situational awareness • Participating in the network of national CSIRTs
Cooperation	
Group to support and facilitate strategic implementation and information exchange among Member States, and to build trust and confidence	<ul style="list-style-type: none"> • In addition to planning and reporting activities, the Cooperation Group has two major roles: • Steering: Provide guidance for the CSIRT network, assist Member States in NIS capacity building, support Member States in identifying operators of essential services, discuss incident-notification practices, discuss standards, engage with relevant EU institutions and bodies, evaluate NIS strategies and CSIRTs • Sharing information and best practices on risks, incidents, awareness raising, training, R&D
Network of national CSIRTs to contribute to building trust among Member States and promote swift and effective operational cooperation	<ul style="list-style-type: none"> • Exchange of information, a coordinated response to a cyber incident, support cross-border incident handling, discuss lessons learned from NIS exercises, guidelines on operational cooperation
Culture	
Taking appropriate security measures and creating a notification system for serious incidents	<ul style="list-style-type: none"> • Security measures include technical and organisational steps to reduce risks, ensure the security of network and information systems and handle incidents to prevent and minimise the impact of incidents on IT systems used to provide services.

The Directive entered into force in August 2016 with Member States having to transpose it into their national laws by 9 May 2018 and to identify operators of essential services by 9 November 2018.

Cybersecurity products and services

The rollout of the 'internet of things' and the proliferation of new technologies (robotics, artificial intelligence [AI], 3D-printing) bring additional challenges, especially regarding the security of connected systems, products and services.²⁵ The need for high-quality, affordable and interoperable cybersecurity products and solutions has been universally recognised across the EU. The supply of such solutions remains very fragmented

²⁵ European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the Implementation of the Digital Single Market Strategy: A connected digital single market for all", COM(2017) 228 final, Brussels, 10 May 2017.

due to differences in national demand, which results in a lack of interoperable solutions (technical standards) and practices (process standards).²⁶ In that context, ICT standardisation is a priority for the Digital Single Market.

Several efforts are underway. In 2014, the EU adopted a **Regulation on Electronic Identification and Trust Services** (eIDAS), which put in place an EU-wide set of rules on such services as electronic signatures, seals, time stamping, delivery services and website authorisation. The European Commission has also proposed new measures (like certification and labelling) aimed at increasing trust and security in products and services. The proposed **EU-wide certification framework**, put forward in September 2017 and under negotiation with the co-legislators, intends to create a comprehensive set of rules, technical requirements and procedures that address specific types of ICT-based products or services.²⁷ The voluntary schemes are not intended to replace current ones but rather refer to existing Union or international standards. Member States will likely be responsible for enforcement, with each appointing a national body to assess compliance, handle disputes, conduct investigations, audit certificate holders and impose penalties for non-compliance. In addition, the Commission proposal envisages a 'light' labelling scheme to help users understand what level of cybersecurity the products they buy have, and to increase the competitiveness of such products in the single market and globally.

BOX 5: REFORM OF EU DATA PROTECTION RULES

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC. It is designed to adapt the law to a rapidly evolving digital and data-driven environment by strengthening citizens' fundamental rights and by simplifying rules for companies in the Digital Single Market.

GDPR regulates the processing by an **individual, a company or an organisation** of **personal data** relating to **individuals** in the EU. The main innovations introduced by the GDPR concern:

- **Scope:** the GDPR applies to 1) a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or 2) a company established outside the EU offering goods/services (paid or for free) or monitoring the behaviour of individuals in the EU;
- **Consent:** A consent request needs to be presented in a **clear and concise** way, using language that is easy to understand, and be **clearly distinguishable** from other pieces of information such as terms and conditions. The request has to specify **what use will be made of your personal data** and include **contact details** of the company processing the data. Consent must be **freely given, specific, informed** and unambiguous;
- **Breach Notification:** becomes mandatory in all Member States where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of having first become aware of the breach. Notifications to customers and controllers have to be made 'without undue delay';
- **'Data protection by design'** and **'Data protection by default'**: Companies/organisations are encouraged to implement technical and organisational measures at the earliest stages of the design of the processing operations in such a way that safeguards privacy and data protection principles ('data protection by design'). By default, companies/organisations should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that personal data isn't made accessible to an indefinite number of persons ('data protection by default').

Sources: European Commission; European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", *Official Journal of the European Union*, L 119, 4 May 2016.

²⁶ European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", COM(2016) 410 final, Brussels, 5 July 2016.

²⁷ European Commission, "Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")", COM(2017) 477 final, Brussels, 13 September 2017.

Simultaneously, the EU contributes to building a culture of cybersecurity by further strengthening its data protection laws. The **General Data Protection Regulation** (GDPR) gives citizens additional security guarantees by reinforcing their control of their personal data. The GDPR also obligates companies and organisations to secure the integrity and confidentiality of personal data or face severe administrative fines, and to notify national supervisory authorities of any data breaches. That in turn will incentivise data controllers to take appropriate security measures and enable users to better protect their data.

Industry, research and technology base

Cybersecurity research and innovation cuts across several policy areas. However, market fragmentation has effectively prevented cooperation from picking up. This is mainly due to different policies across the EU, the dependence on public procurement and governmental purchase and the lack of well-functioning mechanisms of certification or labelling.

Development of industrial and technological resources for cybersecurity is listed as one of the priority areas of the EU Cybersecurity Strategy and is included in the framework of the Network and Information Security (NIS) Platform. The **2015 Cybersecurity Strategic Research Agenda** proposed a multidisciplinary approach to research that fosters collaboration between researchers, industry and policymakers.

In the framework of the Digital Single Market Strategy and the 2016 Communication on cyber resilience, the Commission signed in July 2016 a contractual public-private partnership (cPPP) with the **European Cyber Security Organisation (ECSO)** under the Horizon 2020 Programme.²⁸ Aiming to stimulate industrial competitiveness, the EU will invest €450 million to spark digital security research and innovation in Europe through joint agenda-setting, more efficient use of resources, streamlined objectives and better visibility for the European R&I cybersecurity industry. The partnership foresees that parties will collaborate to improve the cybersecurity market, creating jobs and wealth; to pilot and bring to market products to support the development of the Digital Single Market (DSM); to spread the use of trusted cybersecurity; to create an EU-wide technological base; and to mobilise private and public resources for EU cybersecurity policies. The cPPP is forecasted to trigger €1.8 billion of investment by 2020.

Crisis management cooperation

As businesses and services become increasingly dependent on ICTs, the risks of disruptions that negatively impact the EU's economy, democracy and society increase too. This requires an effective EU response and crisis management, building on the existing structures and instruments based on European solidarity and mutual assistance. Cooperation on cyber incidents can take several forms, including joint investigations into the technical causes of an incident (i.e. malware analysis) and operational cooperation, depending on the scope, as laid down in the **EU Cyber Diplomacy Toolbox** or the **EU protocol for countering hybrid threats**. Moreover, given the potential wide-ranging impact of cyber incidents and crises, the European Commission in 2017 adopted a set of complementary documents that form a Union cooperation framework in case of large-scale cybersecurity incidents and crises. The so-called **Blueprint** describes the objectives and modes of cooperation between the Member States and EU institutions, bodies, offices and agencies and how existing crisis-management mechanisms can make full use of the existing cybersecurity entities at the EU level. It is important to note that because cybersecurity incidents can be isolated or part of a broader crisis impacting several sectors, any appropriate response must be able to rely on both cyber and non-cyber mitigation measures.²⁹

2.2. Cybercrime and criminal justice in cyberspace

Cybercrime violates fundamental rights, causes financial losses and disrupts vital operations. To counter the new forms of criminal activity arising from the technological revolution, the EU over the years has put forward several legislative measures, coupled with operational cooperation mechanisms.

28 In relation to the H2020 priorities 'Leadership in Enabling and Industrial Technologies' and 'Societal challenge Secure Societies'.

29 Council of the European Union, "Council conclusions on EU coordinated response to large-scale cybersecurity incident and crises", 26 June 2018.

Harmonisation and approximation of legislation

The **Directive on attacks against information systems** adopted in 2013,³⁰ replacing the **2005 Council Framework Decision**, recognised the need for a common approach to defining criminal offences - illegal access to an information system, illegal system or data interference and illegal data interception - and the relevant sanctions. The Directive was adapted to avoid over-criminalisation through the introduction of minimum standards in the definitions and sanctions. It also obliges Member States to set up a network of national operational points of contact.

Furthermore, **the Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment** is considered to be the first instrument that aimed to criminalise such illicit activity and create effective, proportionate and dissuasive sanctions in all Member States. In 2017, the European Commission proposed an updated legal framework that would expand the scope of offences, including transactions through virtual currencies; introduce new online criminal offences; clarify the scope of jurisdiction; ensure the rights of cybercrime victims and improve EU-wide criminal justice cooperation.

Moreover, the Commission is currently assessing ways to remove obstacles to investigations of cyber and cyber-enabled crime and terrorism by facilitating cross-border access to evidence.

BOX 6: CYBERCRIME AND E-EVIDENCE

The EU Cybersecurity Strategy defines cybercrime as *'a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. It comprises of 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).'*

It is a borderless problem that can be classified in three broad definitions:

- Offences unique to computers and information systems, such as attacks against entire systems, denial of service, malware or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts);
- Online fraud and forgery, considering that large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code;
- Illegal online content, including child pornography, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

Meanwhile, almost any type of crime nowadays leaves digital traces that can serve as evidence in court proceedings; often it will be the only lead law enforcement authorities and prosecutors can collect. But such evidence is often stored on cloud servers in foreign jurisdictions. In fact, more than half of all criminal investigations today include a cross-border request to obtain electronic evidence held by service providers based in another Member State or outside the EU. To obtain such data, judicial cooperation and mutual legal assistance is needed, but the process at present is slow and cumbersome. Almost two-thirds of crimes where electronic evidence is held in another country cannot be properly investigated or prosecuted, mainly due to the time it takes to gather such evidence or due to fragmentation of the legal framework. To address this challenge, the European Commission in April 2018 proposed new rules to make it easier and faster for police and judicial authorities to obtain electronic evidence, such as e-mails or documents located 'in the cloud'.

Source: European Commission website

³⁰ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

BOX 7: EU POSITION ON THE BUDAPEST CONVENTION AND ON PROPOSALS OF NEW TREATIES

The Directives and Decisions developed within the EU seek to ensure that comprehensive cybercrime legislation is in place across all Member States. They are all based on the relevant provisions of the **2001 Council of Europe Convention on Cybercrime (Budapest Convention)** to ensure consistency with the international legal framework of reference.

The Budapest Convention is the first international criminal justice treaty on crimes committed via the internet and other computer networks and any country can join.

The Convention aims principally at:

- Harmonising substantive criminal law issues, i.e. conduct that constitutes a criminal offence (illegal access and interception, system and data interference, misuse of devices, child pornography, computer-related fraud and forgery, copyright infringements and others);
- Addressing procedural law issues, i.e. measures for more effective investigations of any offence committed by means of a computer system or entailing evidence in electronic form;
- Fostering efficient international cooperation with general principles of cooperation as well as specific provisions for more effective cooperation that permit State Parties to apply procedural tools also internationally with regard to cybercrime and e-evidence. It also entails a network of contact points available on a 24/7 basis to facilitate rapid cooperation.

Membership to the Convention has been steadily increasing (by June 2018, 71 countries were Parties, Signatories or invited to accede, compared to 57 in January 2013). The EU and its Member States have been strong advocates for the Convention, maintaining that it provides technology-neutral definitions of cybercrime offences and lays out procedures for investigation and prosecution on the national level and for international police-to-police and judicial cooperation, as well as setting out rule-of-law safeguards. The Convention is backed by a treaty-based body, the Cybercrime Convention Committee (T-CY), which assesses implementation and issues guidance notes as new threats and technological paradigms arise. Russia and China oppose the Budapest Convention, while countries as Brazil, South Africa and Iran tend to support negotiating a new cybercrime instrument at the UN level. Launching such negotiations could have the effect of suspending the implementation of legislative reforms already underway, with no guarantee of success. It also risks diverting resources from capacity building and seeing the safeguards set in the Budapest Convention lowered. While a UN treaty has been discussed on and off since 1990, there appears to be no consensus in sight to move ahead. To date, most States favour the use of existing instruments backed by capacity building.

The EU position has been captured in several Council Conclusions which recall that: *'international law, including international conventions such as the Council of Europe Convention on Cybercrime and relevant conventions on international humanitarian law and human rights, such as the International Covenant on Civil and Political Rights [and] the International Covenant on Economic, Social and Cultural Rights, provide a legal framework applicable in cyberspace. Efforts should therefore be made to ensure that these instruments are upheld in cyberspace; therefore the **EU does not call for the creation of new international legal instruments** for cyber issues'*. It reiterates that the Budapest Convention **'provides a solid basis among a diverse group of countries to use an effective legal standard for the different national legislation and for international cooperation addressing cybercrime'**.

Sources: Council of Europe website; Council Conclusions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; Council Conclusions on Cyber Diplomacy; Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

In addition, **Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography** provided vital help in this challenging field, criminalizing new developments such as online child 'grooming' or predation. This legal instrument aimed to establish minimum standards in all Member States. It advocates a holistic approach, taking into account requirements for the investigation and prosecution of offences, assistance and protection of victims, and prevention. In 2016, the Commission adopted two reports on the measures taken by Member States to implement the Directive and measures against websites that contain or propagate child pornography. Some issues remain that are not covered in the Directive, such as the absence of mandatory reporting by industry in cases where child sexual material is detected in their infrastructure, or the need for additional investigative tools to tackle challenges such as anonymisation, P2P networks and the darknet.

The EU also targets new areas as the linkage between crime and the digital space becomes increasingly intertwined, e.g. trafficking in human beings gains a new dimension with people being traded online, or wars between drug cartels moving from the streets to online fora.

Cooperation amongst key stakeholders

The linked challenges of different jurisdictions and laws have also brought to the fore procedural issues, in particular ensuring adequate investigative powers for law enforcement agencies and effective cross-border cooperation. To complement its policy and legislative objectives, the EU also supports operational actions to improve those capacities as well. Specialised agencies like Europol and Eurojust play an important role – both as a collective voice of cybercrime investigators and focal points for data analysis and fusion, operational support to investigations in Member States and platforms to bridge the law enforcement, judicial, private sector and technical communities.

The **European Cybercrime Centre at Europol (EC3)** was set up in 2013 to strengthen the law enforcement response to cybercrime in the EU by sharing operational analysis with Member States and by enhancing cooperation and providing expertise for cross-border cybercrime investigations. Each year, EC3 publishes the Internet Organised Crime Threat Assessment (IOCTA),³¹ a flagship strategic report on emerging threats and developments in cybercrime. EC3's operational work focuses on supporting investigations in three areas: (1) cyber-enabled and high-tech crimes, in particular by organised groups that generate large criminal profits (Analysis Project Cyborg); (2) the online sexual exploitation and abuse of children (Analysis Project Twins); and (3) international electronic and online payment fraud (Analysis Project Terminal). It also hosts the Joint Cybercrime Action Task Force (J-CAT)³² that works on the most important international cybercrime cases and is comprised of EC3 staff, cyber liaison officers from several EU Member States and non-EU cooperation partners Australia, Canada, Colombia, Norway, Switzerland and the United States.

From the judicial perspective, the Council took steps in 2016 to formalise the **European Judicial Cybercrime Network (EJCN)**,³³ supported by Eurojust, to *'facilitate and enhance cooperation between the competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace'* by sharing information and best practices and fostering dialogue among stakeholders who have a role in ensuring the rule of law in cyberspace.

BOX 8: JOINT INVESTIGATIONS AND OPERATIONS

In December 2016, Europol in partnership with law enforcement agencies and private companies took down an international criminal business known as Avalanche, which had been active since 2009. Avalanche offered criminal infrastructure and services that its associates used to launch cybercrime campaigns that included so-called banking Trojans, ransomware and phishing. Using a Crime-as-a-Service (CaaS) operating model, Avalanche consisted of more than 20 different firms, each representing one of the malware families the network was supporting. It also provided a complex command-and-control infrastructure that strengthened the network's resilience to detection. Building on previous successful botnet takedown operations against ZeroAccess (2013), GameoverZeus (2014) and Ramnit (2015), Operation Avalanche involved coordination across more than 30 different jurisdictions. It illustrates well how cybercrime divisions and their respective law enforcement authorities are better able to understand and neutralise a variety of technologically advanced criminal operations. Nonetheless, tracking down cybercriminals remains one of the core challenges facing law enforcement due to a wide range of legal, technical and internet governance issues.

Source: Europol (2017), Responding to cybercrime as scale: Operation Avalanche – A case study, Issue brief 2017(3).

In addition, the EU supports several initiatives aimed at improving cooperation on cybercrime aspects. For example, in 2012 the Commission co-launched with the US the **Global Alliance against Child Sexual Abuse Online** to raise international standards and improve investigations and mechanisms. The initiative grouped

31 Europol, *Internet Organised Crime Threat Assessment*, The Hague, 2017.

32 See Europol's website for additional information about the, *Joint Cybercrime Action Taskforce*.

33 Council of the European Union, *"Conclusions of the Council of the European Union on the European Judicial Cybercrime Network"*, 10025/16, 9 June 2016.

54 countries that committed to improve their national framework to reduce child sexual abuse online, to improve victim protection, identify and prosecute offenders, raise awareness and reduce the availability of child pornography online and the re-victimization of children. In 2016, the Global Alliance was merged with the UK-led **WeProtect Initiative**, which was created in 2014 with partners from several countries, NGOs and technology companies. The initiative was renamed the **We Protect Global Alliance to End Child Sexual Exploitation Online (WePROTECT Global Alliance)**.³⁴ The rationale for the merger was to capitalise on the strengths of each initiative and avoid duplication, maximising its global impact. By 2018 70 countries had joined together with major international organisations, global technology companies and leading civil society organisations.

2.3. International cooperation in cyberspace

International engagement has become an important element of the EU's external action. Its primary objective is to support and promote a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply for the social well-being, economic growth, prosperity and integrity of our free and democratic societies.³⁵

The scope of the EU's cyber diplomacy is outlined in the Council Conclusions on Cyber Diplomacy that were adopted in 2015. They elaborate the EU position on a range of relevant issues, including 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 the prosperity of the EU, cyber capacity building and development as well as strategic engagement with key partners and international organisations. The document also stresses the positive contribution that a common and a comprehensive approach could make towards mitigating threats, preventing conflicts and ensuring greater stability in cyberspace. A set of guidelines for 'common and comprehensive' EU cooperation with international partners endorsed by the EU Member States includes, among others:

- Promotion and protection of core EU values online, including freedom of expression and access to information; an active contribution to the enforcement of international human rights obligations in cyberspace; promoting exchange of good practices; the protection of the rights of victims of serious and organised crime in cyberspace by promoting effective investigations and prosecutions;
- Mitigation of cybersecurity threats and ensuring stability in cyberspace through norms of behaviour and application of existing international law in the field of international security;
- Strengthening the multi-stakeholder model of internet governance;
- Enhancing competitiveness and the prosperity of the EU through promoting the EU Digital Single Market, digital trust, and enabling ICT-driven growth while at the same time ensuring equal rules on market access;
- Fostering open and prosperous societies through cyber capacity-building measures.

In 2017, the Member States agreed to develop a framework for a joint EU diplomatic response to malicious cyber activities, the **Cyber Diplomacy Toolbox**. The document recognises the need for a coherent and coordinated EU effort to promote security and stability in cyberspace by upholding existing international law, promoting norms of responsible state behaviour and reducing the risk of misperception, escalation and conflict that may stem from ICT incidents. Options for action – depending on the assessment along a predefined set of principles – include statements by the Council and High Representative, Council Conclusions, diplomatic demarches, signalling through dialogues and restrictive measures, among others.³⁶ These measures should encourage cooperation, help mitigate threats and deter potential aggressors in the long term.

The EU also pursues its objectives through **bilateral cyber dialogues** with key strategic partners such as Brazil, China, India, Japan, South Korea, and the United States, coordinated by the European External Action Service in close cooperation with the Commission services. The scope of these dialogues varies depending on the maturity of the bilateral relationship. Close relations and staff-to-staff consultations are also in place with other international organisations, including the OSCE, CoE, ASEAN and OAS.

³⁴ See <https://internet.weprotect.org/>.

³⁵ Council of the European Union, "Council conclusions on malicious cyber activities", Brussels, 16 April 2018.

³⁶ P. Pawlak, "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", EU Institute for Security Studies, Brief n° 24, 2017.

BOX 9: EU CYBER DIPLOMACY TOOLBOX: GUIDING PRINCIPLES

A joint EU diplomatic response to malicious cyber activities has to:

- Focus on protecting the integrity and security of the EU, Member States and citizens
- Consider the broader context for EU external relations with the state concerned
- Contribute towards the achievement of CFSP objectives as set out in the Treaties
- Be based on a shared situational awareness
- Ensure proportionality to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity
- Respect applicable international law and not violate fundamental rights and freedoms

Source: Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")

Application of existing international law and norms of responsible state behaviour

Regarding norms of state behaviour in cyberspace, the EU supports the achievements of the aforementioned UN Groups of Governmental Experts. Council conclusions on cyber diplomacy *'encourage the EU and Member States to 'strongly uphold' the principle of state responsibility for internationally wrongful acts'*. In the **Council Conclusions on malicious cyber activities** adopted in April 2018, the EU stressed that the use of ICTs for malicious purposes is *'unacceptable as it undermines our stability, security and the benefits provided by the internet and the use of ICTs'*. Consequently, the EU upholds the position that existing international law is applicable to cyberspace and emphasises that respect for international law, in particular the UN Charter, is essential to maintaining peace and stability. The EU underlines that States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts.

BOX 10: EU POSITION ON NORMS AND THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE

With regard to norms of behaviour and application of existing international law in the field of international security, the Council encourages the EU and its Member States to:

- Focus efforts in a coherent and coordinated manner and contribute actively to the achievement of a global common understanding on how to apply existing international law in cyberspace and to the development of norms for responsible state behaviour in cyberspace with a view to increasing transparency and trust, consistent with existing international law provisions;
- Strongly uphold the principles regarding State responsibility for internationally wrongful acts and to take the initiatives necessary at national, regional and international level to ensure that they are fully respected and enforced in cyberspace;
- Strongly uphold the position that existing international law is applicable in cyberspace.

Source: Council Conclusions on Cyber Diplomacy

Confidence-Building Measures

The added value of Confidence Building Measures (CBMs) stems from their capacity to defuse potential misunderstandings, reduce tensions and prevent a conflict from escalating. Concrete examples of CBMs in cyberspace include the exchange of national views on aspects of national and transnational threats to and in the use of ICTs, the facilitation of co-operation among national agencies and the exchange of information and consultations.

The EU recognises that there is a key role for regional organisations in this field, particularly since they provide a framework for discussion between neighbouring States that may have strained relations and where an unexplained cyber incident could easily escalate into conflict. More specifically, the EU and its Member States contributed to negotiations at the OSCE that concluded in the adoption of two sets of CBMs in December 2013 and March 2016 that are designed to enhance inter-state cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation, and conflict.³⁷ Currently, an informal working

³⁷ OSCE, 2016.

group established under the auspices of the OSCE Security Committee is working towards identifying ways of strengthening the work of the OSCE as a practical platform for the constructive and efficient implementation of CBMs. The EU has also been engaging with the ASEAN Regional Forum (ARF) to encourage the development of cyber confidence-building measures in Asia.

Human rights online

In line with the EU's fundamental values of human rights and the rule of law, one key principle in the 2013 EU Cybersecurity Strategy is that *'the same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain'*. This is further reaffirmed in the 2015 EU Council Conclusions on Cyber Diplomacy, which underline that *'individuals' human rights and fundamental freedoms as enshrined in the relevant international instruments must be respected and upheld equally online and offline'*. In an era where some governments consistently restrict online access and relevant rights – even shutting down the internet completely – it is crucial to proactively work to promote and protect freedom of expression online and offline. To this end, the EU adopted in 2014 a set of **Human Rights Guidelines on Freedom of Expression Online and Offline**. The **2015–2019 EU Action Plan on Human Rights and Democracy** also includes a number of commitments in this field, such as integrating the respect for freedom of opinion and expression in external policies and programmes, inter alia, in relation to cybersecurity and cybercrime; as well as working with partner countries to ensure that legislative and procedural measures in the field of surveillance of communications is in line with international human rights law.

An important global initiative in this area is the **Freedom Online Coalition (FOC)** that was established in 2011, bringing together governments that are committed to cooperate in supporting internet freedom and protecting human rights online. As of mid-2018, the Coalition counts 30 members (including 14 EU Member States) with a rather balanced geographical representation, and a vital role in shaping the global human rights online agenda.

Cyber capacity building

The EU has invested substantially in strengthening or building cyber capacities of third countries, either working directly with those countries or through international organisations. For the EU, external cyber capacity-building efforts serve multiple objectives which are mutually reinforcing. A key ambition is to help eradicate safe havens for cybercriminals and to ensure that developing countries can fully benefit from the spread of new technologies. In order to achieve this vision, the EU supports the building of functioning and accountable institutions, as well as strengthening legislative frameworks in partner countries. Recognising that not all countries have reached the same level of capabilities – political, technical, institutional, regulatory or otherwise – the EU has also provided support to initiatives aimed at developing cybersecurity strategies, setting up national CERTs/CSIRTs, building resilience into critical infrastructure and awareness-raising.

The importance of external cyber capacity building as a dimension of cyber policy is noted in the 2013 **EU Cybersecurity Strategy** which defined it as a strategic building block of its international engagement. The 2015 **Council Conclusions on cyber diplomacy** also pointed to the need to strengthen cybersecurity and the fight against cybercrime through international cooperation and assistance in the field of cyber capacity building. This position has been reaffirmed in the 2017 **Joint Communication on resilience, deterrence and defence: building strong cybersecurity for the EU** which acknowledges that efforts to strengthen resilience in third countries contribute to meeting the EU's development commitments and to increasing the level of cybersecurity globally, with positive consequences for the EU. The Joint Communication further defined that a priority for capacity building will be *'the EU's neighbourhood and developing countries experiencing fast growing connectivity and rapid development of threats'*.

In a broader relevant context, the 2014 **Council Conclusions on internet governance** encouraged Member States and the EU to promote technological, policy and regulatory capacity building related to the Internet through the support of development cooperation programmes, exchange of best practices and the promotion of a multi-stakeholder process and the importance of ICTs for the Sustainable Development Goals.³⁸ The increasing role of digital technologies in all spheres of life has also triggered interest in **mainstreaming**

38 Council of the European Union, "Council conclusions on Internet Governance", Brussels, 27 November 2014.

digital solutions in EU development policy. The relevant 2016 Council Conclusions³⁹ stress the importance of national and regional exchanges of good practices, development of strategies and legislation for cybersecurity and against cybercrime, actions to protect critical infrastructure and the establishment of computer emergency response teams as well as for countering violent extremism and the use of the internet for terrorist purposes. In addition, the **New European Consensus on Development** put forward the concept of **Digital4Development** as a solid, comprehensive and targeted approach that would enhance the transformative potential of EU development policy interventions.⁴⁰

Consequently, the main elements of the EU's cyber capacity building, since 2013, can be described as:

- Engaging with international partners and organisations to support building legal, organisational and technical skills to counter cyber threats;
- Assisting various policy communities – political, legal, technical – in strengthening their capacities through training, developing or adapting relevant national policies, strategies, and institutions;
- Supporting the development of secure technologies and networks in partner countries, including by facilitating public-private partnerships for cybersecurity in emerging markets and less developed countries;
- Sharing EU good practices that respect fundamental rights (including the protection of intellectual property and personal data).

Given that the theme of cyber capacity building has gained prominence in international fora and there is a proliferation of initiatives undertaken bilaterally, regionally and internationally, a set of **Council Conclusions on EU External Cyber Capacity Building Guidelines** were adopted in June 2018, offering political guidance on the scope, principles, priorities and approach for the EU's engagement in this field. The Conclusions underline that external cyber capacity-building initiatives by the EU and its Member States should prioritise addressing cybercrime and increasing cybersecurity in partner countries and regions, with a focus on reforms across the main pillars of cyber resilience, through:

- supporting an overarching strategic framework;
- promoting legislative reforms and increasing the capacities of the criminal justice system;
- developing and increasing incident management capabilities;
- developing education, professional training and expertise in this field and promoting cyber hygiene and awareness as well as a culture of security assessment of digital products, processes and services; in compliance with European and international standards and best practices and applying a whole-of-society approach.

BOX 11: PRINCIPLES FOR THE EU EXTERNAL CYBER CAPACITY-BUILDING INITIATIVES

The EU's core values and principles for cybersecurity – as defined in the 2013 EU Cybersecurity Strategy – should serve as the underlying framework for any external cyber capacity-building action, to ensure that it:

- incorporates the understanding that the existing international law and norms apply in cyberspace;
- is rights-based and gender-sensitive by design, with safeguards to protect fundamental rights and freedoms;
- promotes the democratic and efficient multi-stakeholder internet governance model;
- supports the principles of open access to the internet for all, and does not undermine the integrity of infrastructure, hardware, software and services;
- adopts a shared responsibility approach that entails involvement and partnership across public authorities, the private sector and citizens and promotes international cooperation.

Source: Council Conclusions on EU External Cyber Capacity Building Guidelines

Internet governance

With the increasing digitalisation of societies, governance structures for the internet as a global resource are ever more important. The Internet itself has become a key infrastructure with a global dimension. While in early days its governance mostly focused on coordinating the internet infrastructure (e.g. interoperability

³⁹ Council of the European Union, "Council Conclusions on 'Mainstreaming digital solutions and technologies in EU development policy'", Brussels, 28 November 2016.

⁴⁰ European Commission, *New European Consensus on Development our World, our Dignity, our Future*, OJ C210, 30 June 2017.

between the domain-name system and IP addresses), today broader considerations are brought to the fore, including market implications, security and trust dimensions, human rights and public safety aspects.

Internet governance is a **'catch-all' term** that encapsulates the different cooperative and regulatory frameworks that make up the internet as well as its technical and policy structures. It was defined at the **World Summit on Information Society**⁴¹ as *'the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programs that shape the evolution and use of the internet'*.

The EU has always advocated that the internet should be treated as one single unfragmented space, where all resources should be accessible in the same manner, irrespective of the location of the user or provider. The transnational and multidimensional nature of the internet has allowed it to flourish, triggering innovation and the benefits of the digital revolution. This **multi-stakeholder approach**, as opposed to a **government-led** one, should be further strengthened and improved to address legitimacy, transparency, accountability and inclusiveness concerns. In recent years we have seen how practices such as filtering traffic at borders (e.g. the 'Great Firewall of China') and the fragmentation of the internet (known as 'Balkanisation') can compromise economic growth and the free flow of information.

This is an extremely complex and highly polarized policy area with more players involved and numerous intersecting themes. They include security and trust, innovative and disruptive business models, net neutrality, digital access and literacy, the internet of things, blockchain technology and the shared and accountable management of critical internet technical resources. The discussion also takes place in many fora such as the UN General Assembly and the World Summit on the Information Society review (WSIS+10), the UN Economic and Social Council (ECOSOC), the International Telecommunication Union (ITU), the UN Educational, Scientific and Cultural Organisation (UNESCO), the UN Conference on Trade and Development (UNCTAD), the Internet Governance Forum (IGF) and the Internet Corporation for Assigned Names and Numbers (ICANN). As a result, a more inclusive dialogue is needed with all players, including those with very different ideas, and more capacity and confidence building to ensure everyone sees the benefits of a bottom-up, multi-stakeholder and inclusive approach to internet governance.⁴²

BOX 12: KEY INTERNET GOVERNANCE ACTORS AND INITIATIVES

The **Internet Governance Forum (IGF)** meets annually and serves as a global platform for open and inclusive multi-stakeholder dialogue on internet governance policy. It was one of the main outcomes of the World Summit on the Information Society. Since its first meeting in 2006, the IGF has become integral to the internet ecosystem, with a vibrant multi-stakeholder community to share ideas and best practices on internet governance issues without the pressure of formal negotiations and decision-making.

The **Internet Corporation for Assigned Names and Numbers (ICANN)** is an American not-for-profit corporation established in 1998 to manage the internet's naming, addressing and protocols system (the internet's 'phone book', so called IANA functions) that allows the use of names for navigating the internet instead of Internet Protocol numbers. It originally operated under a MoU with the U.S. Department of Commerce. That expired in 2016, allowing for the formal transition of its functions to the global multi-stakeholder community.

An important EU-supported initiative that contributes to making the internet governance process more transparent and accessible is the **Global Internet Policy Observatory (GIPO)**. The European Commission in 2014 proposed developing this online tool to monitor and analyse internet policy as well as technological and regulatory developments across the world. GIPO is designed to help make internet policy more understandable and accessible, especially in relation to positions being discussed at internet governance fora. It has a capacity-building dimension since it is meant to help all stakeholders, including those in developing countries and the most disadvantaged, enhance their knowledge and expertise on internet governance issues, so that they will be better equipped to take part in discussions that shape the future of the internet.

Sources: Websites of IGF, ICANN and GIPO.

41 Internet Telecommunications Union, "The Tunis Agenda for the Information Society", Tunis, 18 November 2005.

42 Calderaro, Andrea, *Internet Governance Capacity Building in Post-Authoritarian Contexts. Telecom Reform and Human Rights in Myanmar*, 1 May 2015.

2.4. Defence in cyberspace

The EU has taken steps to strengthen its defences against malicious cyber activities that have become one of the key elements in hybrid operations directed at EU Member States and institutions. As noted, the first elements of the EU's cyber defence policy were laid down in the EU Cybersecurity Strategy of 2013, with a focus on:

- Operational cyber defence requirements and development of cyber defence capabilities and technologies to address all aspects of capability development, including training and exercises;
- EU cyber defence policy framework to protect networks within CSDP missions and operations;
- Civil-military dialogue in the EU and coordination between all actors at EU level;
- Dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence.

Recognising that the cyber domain has become critical for military- and security-related EU activities, the **Cyber Defence Policy Framework** adopted in November 2014 provided a roadmap for developing cyber defence capabilities for CSDP and the protection of CSDP-relevant communication and information networks. Cyber defence was also integrated in the **Capability Development Plan** by the European Defence Agency, with several projects launched to this end.

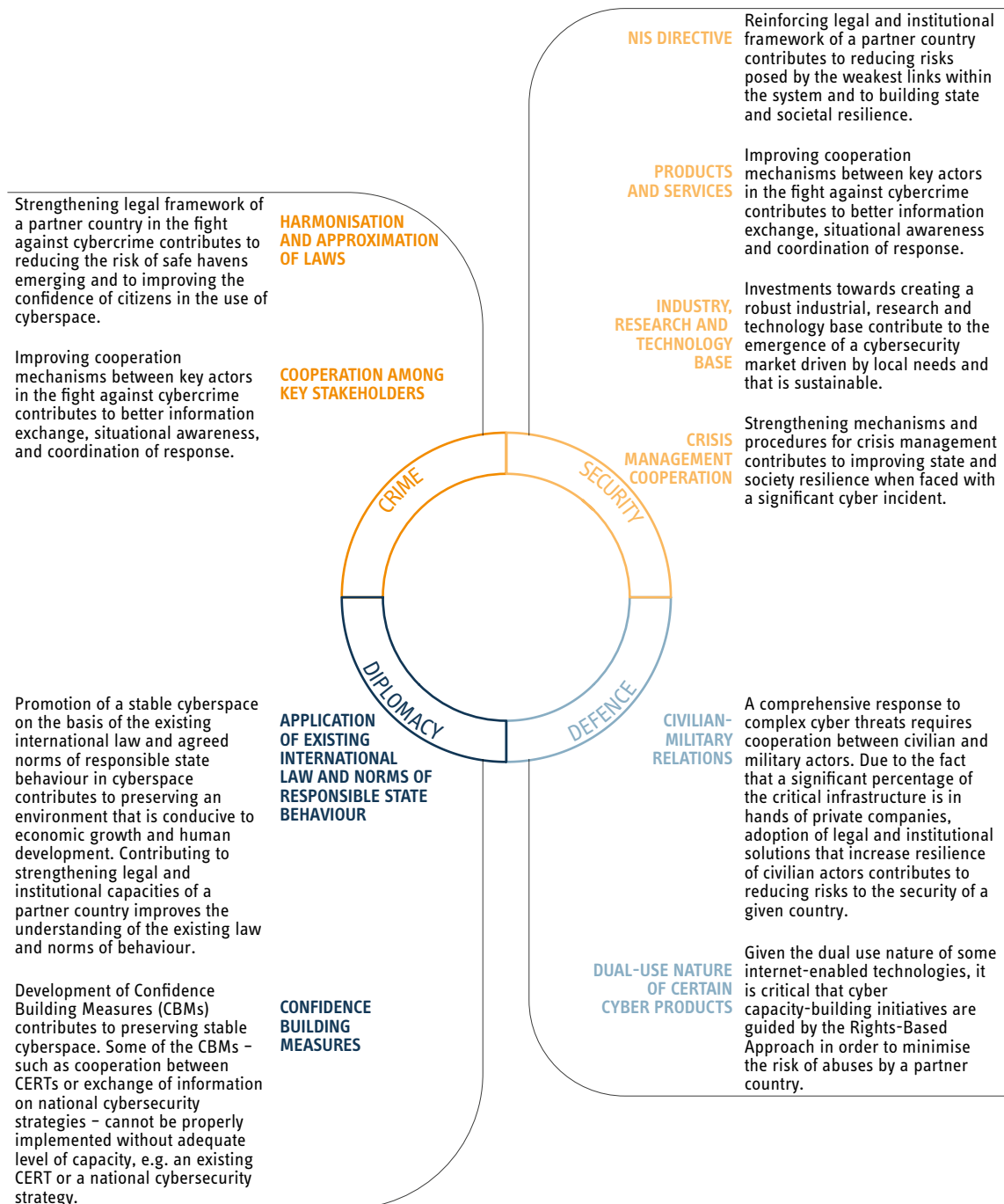
Moreover, the **EU concept on cyber defence for EU-led military operations and missions** adopted in 2016 aims to provide a general framework for integrating cyber defence aspects into the planning and conduct of EU-led military operations and missions. It also addresses doctrinal, organisational and personnel aspects. In 2017, the EU accelerated the implementation of the **Permanent Structured Cooperation (PeSCo)**, which allows like-minded Member States to pursue further cooperation on defence without needing the consent of the others.⁴³ In March 2018 the Council adopted formally a first set of 17 projects, including a Cyber Threats and Incident Response Information Sharing Platform, Cyber Rapid Response Teams and a project on Mutual Assistance in Cyber Security.

As regards relations with NATO, the **EU-NATO Joint Declaration** signed at the alliance's Warsaw Summit in 2016 expressed an urgent need to expand cooperation with the EU and the importance of boosting the abilities of both to counter hybrid threats, including by enhancing resilience, timely information and intelligence sharing and cooperating on strategic communication and response. It was followed by an implementation plan and set of proposals, of which four are specific to cybersecurity and defence:

- Exchange of concepts on the integration of cyber defence aspects into planning and conduct of missions and operations;
- Harmonise training requirement and open training courses for mutual staff participation;
- Foster Cyber Defence Research and Technology Innovation cooperation;
- Strengthen cooperation in cyber exercises.

In 2017, the Estonian Presidency of the European Union conducted the EU CYBRID 2017 table-top exercise at the ministers of defence level. It was followed by the independent yet coordinated crisis response exercises of the two organisations that incorporate cyber elements, namely the EU's Parallel and Coordinated Exercise (PACE) and NATO's Annual Crisis Management Exercise (CMX). In addition, the Computer Emergency Response Team – European Union (CERT-EU) and NATO's Computer Incident Response Capability (NCIRC) have signed **technical arrangements** on strengthening cyber defence information sharing.

43 European External Action Service, "Permanent Structured Cooperation (PESCO) – Factsheet", Brussels, 5 March 2018.

FIGURE 8: Linkages between policies and cyber capacity building

3. Policy dilemmas

Given the breadth and scope of cyber-related policies it is only natural that some might pursue divergent approaches that eventually need to be reconciled by political decisions. Such tensions should not be avoided but rather recognised and addressed from the very beginning to avoid impeding the overall objectives.

3.1. Security and human rights

Different definitions of security (whose? from what?) and the involvement of numerous actors with specific cultures in cyberspace (law enforcement, data protection agencies, human rights organisations) result in a complex policy dilemma: **How to ensure security in cyberspace while recognising and strengthening human rights online?** Legitimate actions aimed at strengthening security of the state (e.g. through new

legislation or increased competences for government agencies) may not adequately address – or may even undermine – the security and safety of individuals and the protection of their rights in cyberspace (e.g. the right to privacy and the protection of personal information). This is particularly relevant in the context of decisions by the European Court of Human Rights that governments have an obligation to protect individuals also online, including through criminal law as outlined in the Budapest Convention on Cybercrime.⁴⁴

One challenging issue is **encryption**. Its main function is to transform information into either a code or a cipher that makes the data illegible to anyone without adequate credentials. In computing, encryption is used primarily to ensure the confidentiality and integrity of data, canons that inform the protection of network and information systems. Encryption can protect the security of non-personal data (e.g. trade secrets) as well as the identities of vulnerable persons such as whistleblowers, human rights defenders or civil society campaigners in authoritarian regimes. Encryption is considered a condition for fostering trust of financial transactions and exchanges online⁴⁵ and the best way to ensure the confidentiality of private communications over the internet, thus supporting the right to respect for communications enshrined in the Charter of Fundamental Rights of the European Union.

At the same time, however, encryption became a way to frustrate the work of law enforcement and intelligence agencies. Obtaining encrypted information without the cooperation of the owner or custodian of the data may require considerable time and computing power to break the code (so-called brute-force attack). This can be a big problem when investigating cybercrime because electronic data are ‘volatile’, easily transferred or destroyed very easily. Similarly, encrypted communications make it difficult for law enforcement to perform targeted surveillance of suspects. As a result, law enforcement agencies have voiced the desire to find solutions, e.g. by weakening the standard of commercial encryption, creating back doors on (privately owned) network systems or making available to police the information needed for deciphering the data or message (i.e. legitimately reading the encrypted message).

In the interim, some in law enforcement have sought the cooperation of tech companies through public-private partnerships, or they have resorted to hacking into the machines of suspects and planting malware to obtain evidence. Research on cryptography in the past decades has demonstrated that so-called ‘cryptography backdoors’ and exceptional access for law enforcement create opportunities for malicious intruders⁴⁶, undermine the privacy of communications and ultimately citizens’ trust⁴⁷, and open doors for criminal and malicious non-state actors.⁴⁸ A growing concern about security has prompted many producers of devices and online services to invest significant efforts towards ensuring even stronger protection for their customers, resulting in some high-profile court cases by tech companies against the government.

Questions about encryption are inherently tightly linked to **the right to privacy and data protection**. Personal data should be protected so as to prevent or limit the adverse effect that the improper or unlawful use could have on the individual; damage could be physical, material (financial loss) or non-material (reputation, profiling), or it could affect other rights (e.g. freedom of association). Privacy allows the autonomous development of a person, individually and socially. Both are deemed important for democracy. Consequently, data protection and privacy are entitlements recognised in and protected by domestic law, regional and international conventions⁴⁹ and soft law (such as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the EU Charter of Fundamental Rights, and the OECD Privacy Guidelines). The Court of Justice of the European Union also acknowledged in the case of *Digital Rights Ireland*⁵⁰ (and subsequent case law) that confidentiality of the contents of communications is part of the respect for private and family life, whereas the existence of rules on confidentiality, integrity and availability of data is part of the essence of the right to the protection of personal data.⁵¹

44 See case of *K.U. v Finland*.

45 L. Gill, T. Israel, C. Parsons, “Shining a light on the encryption debate”, The Citizen Lab, 14 May 2018.

46 The Royal Society, “Progress and research in cyber security. Supporting a resilient and trustworthy system for the UK”, *The Royal Society Science Policy Centre*, London, 2016.

47 European Union Agency for Network and Information Society (ENISA), “ENISA’s Opinion paper on encryption. Strong Encryption Safeguards our Digital Identity”, Heraklion, 2016.

48 H. Abelson et al., “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications”, *Massachusetts Institute of Technology*, Cambridge, 2015.

49 Such as Art. 12 of the Universal Declaration on Human Rights; art. 17 of the International Covenant on Civil and Political Rights; and, in Europe, art. 8 of the European Convention on Human Rights.

50 Court of Justice of the European Union, Judgment of 8 April 2014 in *Digital Rights Ireland* and *Seitlinger and Others*, Joined cases C-293/12 and C-594/12.

51 M.G. Porcedda, “Patching the patchwork: appraising the EU regulatory framework on cyber security breaches”, *Computer Law & Security Review: The International Journal of Technology Law and Practice* (2018).

On the other hand, the rules on the protection of personal data may clash with the fight against cybercrime, where an individual's online communications or encrypted data may constitute valuable evidence. In this respect, strong encryption can appear as an obstacle to the work of law enforcement. However, weakening encryption may hinder anonymity by making individuals, their personal data and their communications potentially visible and open to scrutiny. Accessing data for investigatory purposes also calls into question the existing relationship between law enforcement agencies, private companies that may be collecting and processing data as part of their business, and the individuals who use the services offered by those businesses. To address some of these challenges, the European Commission proposed in 2018 new rules that would create **European Production and Preservation Orders for getting access to electronic evidence in criminal matters**. The proposal also would harmonise rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, while providing safeguards for the rights and freedoms of all concerned.⁵²

The EU also considers the relationship between security and the **protection of human rights online** to be a key pillar of its foreign and development policy. In 2014, the Council of the European Union adopted the **EU Human Rights Guidelines on Freedom of Expression Online and Offline** to incorporate these principles in its dealings with partner countries. The document states clearly that *'all human rights that exist offline must also be protected online, in particular the right to freedom of opinion and expression and the right to privacy, which also includes the protection of personal data'*.⁵³ This is particularly important in the context of the shrinking space for civil society across the world and an increase in efforts by some governments to control and manipulate information on social media.⁵⁴ The latter point is relevant in the context of the discussion about **disinformation and 'fake news'**, which are considered⁵⁵ a challenge to modern democracies and democratic processes.⁵⁶ In 2018, the European Commission proposed measures to tackle online disinformation, including a **Code of Practice on Disinformation**.⁵⁷ However, while in some cases the use of such measures is justified, there are also numerous instances of governments using disinformation as an excuse to fight political opponents or restrain freedom of expression online through internet shutdowns, website blocking or arrests for internet activity.⁵⁸

3.2. Sovereignty and governance

A difficult challenge that cuts through all cyber-related policy areas is reconciling differing understandings of **sovereignty, legitimacy and approaches to internet governance**. One of the key premises in this debate is the state's responsibility for the actions originating from its territory. According to the 2013 UN GGE report, *'state sovereignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'*. This implies, for instance, that states should not knowingly allow their territory to be used for wrongful acts abroad using ICTs. Consequently, many countries have adopted an approach whereby the government plays a predominant role in governing cyberspace. Given the strategic importance and potential impact of cyber incidents on the functioning of a state this is not surprising. However, certain governments have used the principle of sovereignty as justification for a very limiting definition of the role that multi-stakeholder approaches involving the technical community, civil society organisations and the private sector can play in the process. Instead, they have placed government bodies and agencies at the centre of cyber-related decision-making. In fact, there is an increasing trend by countries, quoting security concerns, to curb global connectivity of their citizens through censorship and other restrictions. Such practices hinder both the realisation of the economic and societal benefits of the digital ecosystem and the public's confidence to it. On the opposite end of the spectrum, the European Union has repeatedly confirmed the importance of having all

52 European Commission, "Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings", COM(2018) 226 final, Strasbourg, 17 April 2018; European Commission, "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters", COM(2018) 225 final, Strasbourg, 17 April 2018.

53 Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline", Brussels, 12 May 2014.

54 S. Kelly, et al., "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy", Freedom House, 2017.

55 European Commission, "Flash Eurobarometer 464: Fake News and Disinformation Online", Brussels, 2018.

56 The European Commission defines disinformation as *verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm*.

57 European Commission, "Tackling online disinformation: Commission proposes an EU-wide Code of Practice", Press Release, Brussels, 26 April 2018.

58 An internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information. See: [Access Now](#).

stakeholders involved in internet governance and its commitment to strengthening the **multi-stakeholder model**,⁵⁹ which is supported by like-minded countries. In between these two factions there are many countries that are now developing their digital and cyber policies, with several countries remaining cautious on introducing a technology that so clearly empowers society (including civil society, opposition groups and government critics) and fosters networked rather than hierarchical power structures. The situation is still rather fluid and the discussion is becoming increasingly intertwined with other international cyber discussions such as the one on international security.

The idea of state sovereignty in cyberspace has been also used to challenge the existing international legal order. The 2013 United Nations Group of Governmental Experts (UN GGE) report clearly stated – for the first time – 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, stable, accessible and peaceful ICT environment’*. Efforts to understand how to interpret existing law in a cyber-specific context continue, especially following the failure of the UN GGE to present a consensus report. The work of the UN GGE was later reflected on in other international groupings: the **G7 Ministers of Foreign Affairs** called on states to publicly explain their views on how international law applies to state activities in cyberspace, for example. But not everyone shares this interpretation. Russia’s Information Security Doctrine, adopted in December 2016, acknowledges that universally recognised principles and norms of international law form the legal framework of the doctrine but does not include any specific reference to whether existing laws apply to cyberspace. Similarly, **China’s International Strategy of Cooperation on Cyberspace** merely contains a commitment to *‘study the application of international law in cyberspace from the perspective of maintaining international security, strategic mutual trust and preventing cyber conflicts’*. Even more importantly, such statements need to be interpreted in a broader context, including the respect for other principles of international law and human rights.

The difference in approaches gave birth to discussions about new international legal instruments. Since 2011, under Sino-Russian leadership, members of the Shanghai Cooperation Organisation (SCO) have been working on a draft International Code of Conduct for Information Security that is broadly seen as **a direct challenge to the vision promoted by the EU, US and like-minded partners**. The narrative has been spreading also with regard to the fight against cybercrime. **The Council of Europe Convention on Cybercrime (Budapest Convention)** adopted in 2001 is the only legally binding instrument providing a framework for international cooperation in the fight against cybercrime. Promoted by the EU and a group of like-minded states and organisations, it has served as a benchmark for setting global standards in the fight against cybercrime and for access to electronic evidence. At the same time, certain countries either reject the Convention (Russia) or question at times its global aspirations arguing that it was not negotiated at UN level (ex. India, Brazil). The calls for a new international cybercrime instrument are a direct consequence. The **open-ended Intergovernmental Expert Group on Cybercrime (IEG)**, established in 2010 by the UN Congress on Crime Prevention and Criminal Justice (CCPCJ), was tasked with examining options for strengthening international efforts. A draft study presented by the United Nations Office on Drugs and Crime (UNODC) in 2013 included a contested summary that put forward seven options, including the development of multilateral tools for international cooperation regarding electronic evidence in criminal matters and a new instrument on cybercrime. However, the IEG concluded that while there was broad support for capacity building there were “diverse views” on all other options.

3.3. Accountability and transparency in cyberspace

Whereas national security remains the competence of governments alone, it is generally acknowledged that state bodies need to work with other stakeholders in the governance of cyberspace. This brings to the fore the question of transparency and accountability.

The issue is particularly pertinent with regard to **accountability and intelligence oversight**. Intelligence services play a vital role for cybersecurity but keeping nations safe from online threats has become increasingly complex. Massive investments in security technology have furthered the convergence of software that

59 Commission of the European Communities, “Communication from the Commission to the European Parliament and the Council - Internet Governance: the next steps”, COM(2009) 277 final, Brussels, 18 June 2009; European Commission, “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, Brussels, 7 February 2013; Council of the European Union, “Council Conclusions on Cyber Diplomacy”, Brussels, 11 February 2015.

transcends national borders and disciplines. For example, while many democracies distinguish in legislation between police and intelligence powers and require strict separation between them, it has become increasingly difficult to adhere to this distinction in practice. Predictive policing, military reconnaissance and signals intelligence often use the same data acquisition and analytical tools and the enrichment of their datasets with other government and commercial data renders formal distinctions less meaningful. This has important ramifications for oversight and many laws and oversight systems lag far behind.⁶⁰ Democracies have a strong interest in seeing that intelligence and security services perform their important tasks in an effective, lawful and legitimate way. This requires comprehensive and modern security legislation and independent and resourceful oversight bodies. Overseers in parliament typically review the actions, programs, policies and budget of the intelligence community, whereas overseers within the judiciary or in administrative bodies authorize and review the use of digital powers that can impinge on human rights. Effective checks and balances provide legitimacy for and public trust in the government and the intelligence community. Reviewing the legality and propriety of special powers, independent review bodies ought to challenge malfeasance and, where necessary, punish abuses. **Both in legislation and in actual oversight practice, different needs constantly have to be weighed against each other.** For example, there is the need for government secrecy and the public's right to information. Overseers need adequate access to the servers and digital infrastructure of the national intelligence community to comprehend, let alone verify the information they get from national security circles. Granting overseers such access also turns them into an attractive target for foreign cyber operations. Hence, the pursuit of rigorous oversight does imply security risks.

In addition, the use of **hacking capabilities** both by intelligence agencies and law enforcement (so-called hacking back) has been expressly permitted by legislation in some European jurisdictions in recent years. Government hacking can be referred to as *'a government's exploitation of existing vulnerabilities in soft- and hardware to access data in transit and data at rest, or to manipulate a target's device (e.g. switching on sensors or webcams). A vulnerability can be defined as a flaw in soft- or hardware which individually or linked with others enables third parties to perform unauthorized - and possibly covert - operations on a device or against a digital account.'*⁶¹ Expert community differentiates between vulnerabilities already known by the manufacturer (n-days) and those unknown to it (0-days). Consequently, disclosure is the process leading from a 0-day to a n-day. Even if disclosed and fixed, a vulnerability may still be exploited by law enforcement agencies and intelligence community. That brings several challenges for security governance: the oversight bodies are facing renewed difficulties building the in-house technical understanding to ensure their effectiveness, while lawmakers are grappling with questions as to how and when such techniques should be permitted in the national interest.

3.4. Innovation, growth and security

The discussion about the compatibility and complementarity of security and development objectives (e.g. economic growth, inclusiveness, protection of human rights) is not new or unique to cyber issues or cyber capacity building. The EU has long acknowledged that *'security is a precondition for development'*⁶² and that *'without development and poverty eradication there will be no sustainable peace'*⁶³. **Whereas the impact of innovation and technology as drivers of growth is undeniable, the exponential growth in complexity of new ICTs, the speed of technological advancement and its impact on society challenge traditional regulatory approaches and value systems.** The uncertainty about the societal and security impact of new technologies coupled with the proliferation of mobile devices, the internet of things, artificial intelligence and blockchain technology further accentuate the tension between innovation, growth and security. Several applications of new technologies have lately attracted particular attention:

- **Blockchain technologies**⁶⁴ and **cryptocurrencies** entered the discussion about cybersecurity primarily due to their growing use in online transactions, including illicit activities. The disruptive and innovative aspect of the blockchain technology lies in the fact that trust is distributed among multiple parties, removing the need for a trusted third party – a role that banks or governments play in traditional systems. One

60 T. Wetzling, "Options for more effective intelligence oversight", *Discussion paper*, November 2017, Stiftung Neue Verantwortung.

61 S. Herpig, "Government hacking: computer security vs. investigative powers", Stiftung Neue Verantwortung, June 2017.

62 Council of the European Union, "A Secure Europe in a Better World - European Security Strategy", Brussels, 8 December 2003.

63 Council of the European Union, "Security and Development - Conclusions of the Council and the Representatives of the Governments of the Member States meeting within the Council", Brussels, 20 November 2007.

64 A blockchain is a database with credentials distributed among different participants protected by cryptography algorithms and organised in transactional blocks mathematically linked to each other. Its most important feature is that it cannot be modified without the consensus of thousands of participants.

of the most popular uses for blockchain technology is with cryptocurrencies (e.g. ripple, bitcoin, Ethereum). Cryptocurrencies can facilitate access to the banking system at a low cost, and excluding traditional intermediaries. But like any other internet-enabled mechanism, cryptocurrencies are vulnerable to cyber attacks. Due to the anonymity they can provide, cryptocurrencies have also become a means of payment for criminal organisations and terrorists.

- **Internet of Things**⁶⁵ (IoT) is another important development with significant implications for cybersecurity. Increasingly, technology makes it possible for the objects to react to external stimulus and interact with other devices (i.e. exchanging information) without any human intervention. Applications span all sectors, including in factories, urban infrastructure, the health sector and environmental controls. However, as many of these devices have very weak security, they pose a serious threat to the whole internet ecosystem. Some organisations, for instance, have created a Product Security Incident Response Team (PSIRT) that focuses on the identification, assessment and disposition of risks associated with security vulnerabilities in things an organization produces and/or sells.⁶⁶ Governments and standardization bodies are also working on standards and labelling schemes that impose requirements on producers and developers and contribute to raising their awareness about potential risks related to sub-optimal security. At the same time, there is a debate in regional and international bodies concerning identifiers for the Internet of Things. There is a concern that such a solution might place oversight for the interconnection of all objects, devices and networks in the hands of governments, which would gain unprecedented levels of information about citizens and the capacity to exercise censorship and manipulate information, track information to its source and remove it, disconnect devices, shut down communication or even locate an individual.
- **Data science** is increasingly used for addressing challenges posed by cybersecurity and cybercrime, in particular making sense of complex crime scripts, attack patterns, or harm ensuing from attacks.⁶⁷ Data science is an expression that encompasses techniques used to analyse data, typically in large quantities (also called big data), and extract value from them. Its current applications include the use of software (off-the-shelf or by coding) to scrape data from computer programs or to crawl through open-source intelligence on the Web; data analytics, i.e. the combination of statistics to analyse large data sets, and visualization software to represent the results; and machine learning, whereby a computer system improves its performance of automated functions by 'learning' from troves of data fed by operators. Researchers also point to risks associated with data science. For instance, the accumulation and potentially infinite reuse of data could violate the data protection principles of data minimization and purpose specification. As the collection and flows of data increase, the risk of reversal of anonymisation of data grows too, with ensuing consequences for individuals and liability for those who process the data.⁶⁸ Furthermore, the large data sets become very attractive for cyber criminals (or state-sponsored attackers), who may be targeting buckets (cloud-computing infrastructures) where large data sets are held, to the clear detriment of cybersecurity (and data protection). As a result, data science may be both offering solutions to societal issues, such as the fight against cybercrime, and further complicating them.⁶⁹ The law currently offers only partial solutions and data science is not regulated, particularly when it comes to law enforcement uses.

This conflict has been particularly vivid in the context of the revisions of the **Wassenaar Arrangement** - an export-control framework among 42 countries (as of mid-2018) covering conventional arms and certain dual-use goods and technologies. Following media reports that some repressive regimes used Western-developed surveillance tools to spy on dissidents and human rights activists, governments involved negotiated to add 'intrusion software' and 'IP network communications surveillance systems' to the list of technologies governed by the Wassenaar Arrangement. Security researchers, however, pointed to the negative impact that such a solution might have on sharing of information of security vulnerabilities.

65 Internet of Things is the ecosystem of the devices using Internet as platform for communications, exchange of information and interactions.

66 Forum of Incident Response and Security Teams, "Draft PSIRT Services Framework", 2017.

67 M. G. Porcedda, D.S. Wall, "Data Science, Data Crime and the Law" in V. M-ak, E. Tjong Tjin Tai & A. Berlee (Eds), *Research handbook on Data Science & Law*, London, Edward Elgar, 2018.

68 M. G. Porcedda, D.S. Wall, op. cit

69 Ibid.

PART II

A FRAMEWORK FOR THE EU'S EXTERNAL CYBER CAPACITY BUILDING

The EU has been consistent in highlighting that security is a precondition for development, and at the same time there cannot be sustainable peace without development and poverty eradication. Building state and societal resilience became one of the priorities in the **Global Strategy for the EU's foreign and security policy** presented in June 2016. According to the strategy, *'a resilient state is a secure state, and security is key for prosperity and democracy. But the reverse holds true as well. [...] A resilient society featuring democracy, trust in institutions and sustainable development lies at the heart of a resilient state'*. The strategy calls for enhanced efforts towards more flexible development policies that are aligned with the EU's other strategic priorities, a better use of common security and defence policy instruments and diplomatic action that is 'joined up' across the EU's external policies, between Member States and EU institutions and between the internal and external dimensions of EU policies.

The new **European Consensus on Development**, adopted in June 2017, also notes that development should contribute to achieving the priorities of EU external action, including by fostering a dynamic and multi-dimensional approach to resilience. In this sense, cyber capacity building – encompassing both cybersecurity and combatting cybercrime – fits within a broader EU engagement with partner countries in areas such as counterterrorism, border management or security sector reform.

The EU's international engagements are aimed at promoting the vision of a free, open and secure Internet and supporting capacity building in partner countries to implement this vision.¹ The immediate objective is to build resilience in partner countries so as to strengthen their ability to benefit from the digital economy. This objective has been recognised in the **EU Cybersecurity Strategy of 2013** and more recently in the **Joint Communication on 'Resilience, deterrence and defence: Building strong cybersecurity for the EU'** of November 2017.

Recognising the importance of access to and use of open and secure ICTs for enabling economic growth and innovation as well as accelerating progress and driving political, social and economic development, the **2015 Council Conclusions on Cyber Diplomacy** stressed the importance of cyber capacity building. The main aspects highlighted in the Conclusions include:

- Developing a coherent and effective model for cyber capacity building;
- Integrating cyber capacity building into wider global approaches in all cyberspace domains;
- Supporting new initiatives that focus on the link between access to and use of open and secure ICT and fostering open societies and an enabling environment for economic growth and social development;
- Promoting sustainable cyber capacity building with international partners as well as streamlining and prioritising funding, including by making full use of the relevant EU external financial instruments and programmes;
- Promotion of the Council of Europe Convention on cybercrime internationally;
- Building resilience by developing capacities and new initiatives to tackle growing cyber threats and challenges, leveraging the expertise of national cyber organisations such as Computer Security Incident Response Teams, high-tech crime units and other competent national bodies.

1 Council of the European Union, "Cyber capacity building: towards a strategic European approach", Brussels, 30 June 2016.

Table 2: Cyber capacity-building in EU strategic documents

Cybersecurity Strategy (2013)	'Review' of the Cybersecurity Strategy (2017)
<ul style="list-style-type: none"> Invites the Commission to use the Instrument for Stability (now IcSP) to develop the fight against cybercrime as well as for capacity-building initiatives including police and judicial cooperation in third countries from where cybercriminal organisations operate; (...) to facilitate coordination of capacity-building programmes to avoid duplication and provide for synergies Calls upon the Commission and the HRVP (...) in cooperation with Member States and relevant private organisations and civil society to make full use of relevant EU aid instruments for ICT capacity building, including cybersecurity Calls on Member States, the Commission and the High Representative to work towards achieving a coherent EU international cyberspace policy by (...) supporting capacity building in third countries through training and assistance for the creation of relevant national policies, strategies and institutions, with a view to enabling the full economic and social potential of ICTs, supporting the development of resilient systems in those countries and mitigating cyber risks for the EU Institutions and Member States while making use of existing networks and forums for policy coordination and information exchange. 	<ul style="list-style-type: none"> The EU will continue to promote a rights-based capacity-building model, in line with the Digital4Development approach. The priorities for capacity building will be the EU's neighbourhood 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. 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.

In light of the proliferation of cyber capacity-building initiatives since the original 2013 Strategy and the subsequent Cyber Diplomacy Conclusions in 2015, the issue has grown in importance, also due to the 2017 Digital4Development policy framework. In order to offer political guidance to the EU and to Member States, the Council adopted in June 2018 **Conclusions on EU External Cyber Capacity Building Guidelines**.

The Council Conclusions recognise that the EU's external cyber capacity-building efforts serve multiple objectives which are mutually reinforcing, most notably:

- supporting cyber resilience building in partner countries that contributes to an improved global digital ecosystem;
- fostering strategic alliances aimed at supporting the notion of a global, open, free, stable and secure cyberspace in line with the EU's core values and principles, the rule of law, human rights and fundamental freedoms;
- encouraging the creation of formal and informal cooperation frameworks between partner countries and regions and the EU and its Member States; and
- promoting the EU's development commitments and the implementation of the 2030 Agenda for Sustainable Development.

BOX 13: PRACTICAL GUIDELINES ON CAPACITY BUILDING

- European Commission, [Why, what and how and Toolkit for capacity development](#).
- European Commission, [Operational Human Rights Guidance for EU external cooperation actions addressing terrorism, organised crime and cybersecurity](#).
- OECD, [Evaluating development activities. 12 lessons from the OECD DAC](#).
- Austrian Development Agency, [Manual capacity development. Guidelines for implementing strategic approaches and methods in ADC](#).
- German Agency for International Cooperation, [Capacity works. Success stories. Examples of best practices](#).
- German Agency for International Cooperation, [Capacity works. The management model for sustainable development](#).

1. What is capacity building?

The concept of capacity building emerged in the 1970s in the context of institution building and gained a broader recognition in the 1990s in the field of development aid and international cooperation. While there is no single understanding² of what capacity building is, the main purpose of capacity building is to stimulate change by developing or strengthening the capabilities and competencies of individuals, institutions, governments and societies at large. To achieve its objectives, the process of capacity building needs to be driven 'from within', with external actors providing support. That implies that at the core, partner countries bear the primary responsibility for strengthening their own capacities to attain their development goals. Decades of experience have led to the conclusion that capacity building is the engine of human development and that achieving the desired objectives, including those in the Sustainable Development Goals, requires state and societal capacity to design and implement strategies that adequately address the multitude of crises.³

Over time, capacity building has emerged as one of the main instruments in the field of security, in particular in the context of security sector reform, border management, counterterrorism and the rule of law. The **OECD Development Assistance Committee (DAC)** has recognised certain categories of security spending as compliant with the reporting directives for official development assistance (ODA) for peace and security. The primary criterion when assessing ODA eligibility is having a focus on promotion of the economic development and welfare of a developing country. The United Nations' **2030 Agenda for Sustainable Development** highlights the link between security and development and underlines the importance of just, peaceful and inclusive societies both as a sustainable development goal and in support of other development objectives.

BOX 14: CAPACITY-RELATED DEFINITIONS

The concept of 'capacity building' is often contrasted with one of 'capacity development' (UNDP, 2002). Whereas the former is generally criticised for assuming the lack of indigenous capacities, the latter is believed to recognise that a certain level of capacity always exists. The 2005 Paris Declaration on Aid Effectiveness and the 2008 Accra Agenda for Action have stressed the importance of capacity development for aid effectiveness and the central responsibility of partner countries for systematic identification of capacities that require strengthening. As the needs and nature of development cooperation evolved, the concept of capacity building and capacity development have been used interchangeably to describe an indigenous, country-driven, long-term process that requires the involvement of all sectors of society, with external support no longer limited to enhancing individual skills but also addressing institutional, organizational and societal dimensions (United Nations Economic and Social Council, 2002).

- **'Capacity'** is the ability of people, organisations and society as a whole to manage their affairs successfully. **Capacity development** is the process whereby people, organisations and society as a whole unleash, strengthen, create, adapt and maintain capacity over time' (OECD, 2006).
- **'Capacity building'** encompasses the country's human, scientific, technological, organizational, institutional and resource capabilities. A fundamental goal of capacity building is to enhance the ability to evaluate and address the crucial questions related to policy choices and modes of implementation among development options, based on an understanding of environment potentials and limits and of needs perceived by the people of the country concerned' (United Nations Conference on Environment and Development, 1992).
- **'Capacity development'** is the process by which people and organisations create and strengthen their capacity over time. Consequently, support to capacity development is the inputs and processes that external actors – whether domestic or foreign – can deliver to catalyse or support capacity development of persons, an organisation or a network of organisations' (European Commission, 2005).
- **Cyber capacity building** is the development and reinforcement of processes, competences, resources and agreements that is necessary for communities, businesses and governments to cope with the rapid changes and challenges of fast-changing world. Cyber capacity building is global in nature, since the internet transcends conventional borders (Global Forum on Cyber Expertise, 2017).

² United Nations Educational, Scientific, and Cultural Organization, "Capacity Development for Education for All – Translating Theory into Practice", Paris, 2011.

³ Davis, T. Lemma & K. Wignaraja, "Capacity development. A UNDP primer", United Nations Development Programme, New York, 2009.

2. What is cyber capacity building (CCB)?

Advancements in digital technologies are at the heart of economic and societal change across the world. In 2001, the Human Development Report addressed this trend by arguing that ICTs can contribute to human development and poverty reduction.⁴ However, the benefits are not reaped equally, as only around half of the world's population has access to the internet.⁵ This '**digital divide**' stretches across regions, sexes, age groups and urban/rural populations as well as between developing and developed countries.⁶ In recognition of this, the development community is also addressing the need to strengthen institutions, develop skills and ensure an adequate regulatory climate. There is also an increasing awareness of the need to enhance cyber resilience as an overarching theme for capacity building.

The development community's contributions to cyber capacity building have been manifold, drawing upon extensive experience in capacity building for poverty reduction and sustainable development.⁷ Donors and development actors coined an operational definition of capacity building that enabled them to identify challenges in sustainable development. These include accounting for cross-sectoral influences; drafting baseline needs assessments; establishing streamlined measures aimed at institutional change and individual skill building; and developing an ability to assess capacity development efforts.⁸ These challenges contributed towards conceptualising and operationalising capacity building. The development community thus understood capacity building to be a locally owned process of change that builds on existing foundations towards the development of sustainable outcomes, whilst accounting for issues such as governance, political dynamics and local resources. But this understanding has not informed cyber capacity-building efforts undertaken by other communities which then resulted in a significant gap in knowledge and discrepancies in conceptual approaches to capacity building between development actors and the technical, law enforcement and diplomatic communities.

Governments and international organisations alike have been voicing louder concerns regarding cybersecurity as a political and security challenge with global ramifications. Consequently, several international and regional organisations intensified their efforts to address cyber-related concerns in their own work. For example, the **Council of Europe** defines the scope of its relevant capacity-building actions as measures enabling criminal justice authorities to meet the challenge of cybercrime and electronic evidence. This entails strengthening the knowledge and skills and enhancing the performance of criminal justice organisations, including their cooperation with other stakeholders. It should be aimed at protecting individuals and society against crime and at protecting the rights of individuals, at promoting security, confidence and trust in ICT, at strengthening human rights, democracy and the rule of law in cyberspace and at contributing to human development.⁹ For the **International Telecommunication Union (ITU)**, cyber capacity building is defined as strengthening the human and institutional capacity of developing countries to adapt to an evolving ICT sector. The underlying assumption in the ITU's approach is that building broad telecommunication/ICT literacy enables citizens to access and contribute information, ideas and knowledge to create an inclusive information society. Providing assistance in human and institutional capacity building that improves telecommunication and ICT skills to support the development and use of networks and applications continues to be a priority for the ITU Telecommunication Development Sector (ITU-D).¹⁰

Capacity building appears to be a common thread across all cyber-related processes. Indeed, the **UN Group of Governmental Experts (UN GGE)** on Developments in the Field of Information and Telecommunications in the Context of International Security recognised capacity building as bridging uneven levels of security, including critical information infrastructure protection, and developing relevant skills and adequate institutional frameworks.¹¹ In parallel, an international platform aimed at tackling cyber issues, known as the **London Process**, has been focusing on capacity building: the **Global Conferences on Cyberspace (GCCS)** convened as part of this process have been gradually including capacity building in discussions surrounding

4 K. Malik, Human Development Report 2013 - The Rise of the South: Human progress in a Diverse World, New York, United Nations Development Programme, 2013.

5 International Telecommunication Union, "ICT Facts and Figures 2017", Geneva, 2017.

6 World Bank Group, World Development Report: Digital Dividends, Washington D. C., 2016.

7 P. Pawlak, 2014.

8 B. Lucas, "Current thinking on capacity development", GSDRC Helpdesk Research report No 960, Birmingham.

9 Council of Europe, "Capacity Building on cybercrime", Discussion paper, 2013.

10 International Telecommunication Union, "Our Mandate, Mission and Strategy", 2018.

11 United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", New York, 24 June 2013.

cybersecurity. That led in 2015 to the creation of the **Global Forum on Cyber Expertise (GFCE)**, a platform for countries, international organisations and private companies, together with NGOs, the technical community and academia, to exchange best practices and expertise around CCB.¹² Similar endeavours have also been carried out regionally. EU Member States are focusing on a more European approach to CCB to effectively respond to cybersecurity threats and develop resilience.¹³ The **OAS** has been acting as a focal point to ensure adequate coordination in CCB efforts throughout its member states. The **ASEAN** has also called for a regional approach to cybersecurity, including CCB. The **Meridian Process** – a forum for senior decision-makers dealing with protecting critical information infrastructure – also made CCB a leitmotif in their global conferences. There also is consensus in the international community around CCB as an enabler in the fight against cybercrime.¹⁴ Organisations promoting judicial and law enforcement cooperation (e.g. Interpol, the UNODC and the Council of Europe) to fight cybercrime have also included CCB in their initiatives.

BOX 15: DAC-ABILITY OF CCB SPENDING

Recognising new challenges and the evolving security environment, the OECD Development Assistance Committee (DAC) decided in 2016 to update and clarify reporting directives for official development assistance (ODA) for peace and security.* As the risks and the security environment evolve, traditional development actors no longer hold a monopoly on or are not well-equipped to provide the support required. Consequently, other actors – including the military and law enforcement agencies – have stepped in. Whereas certain aid categories targeting the latter are already acceptable under ODA rules, support to the military is still an open question.

Clear guidance on the ‘DAC-ability’ of cybersecurity assistance and capacity building for cyber defence hasn’t materialised, although further discussions about the ODA Casebook might result in the inclusion of cyber defence later. The key issue is the dual use nature of cyber tools, and the difficulty in constraining the potential misuse of equipment or skills delivered for purely defensive purposes. However, it is not impossible to compile a catalogue of institutional, legal or human capabilities where the lines between offensive-defensive and civilian-military actions are less thorny. In fact, any large-scale cyber attack is very likely to demand a comprehensive and integrated civil-military approach. Therefore, the establishment of Incident Management Centres or training in digital forensics anywhere would be welcomed by cybersecurity experts as a step towards strengthening the resilience of society as a whole.

* OECD, “Communiqué: DAC High Level Meeting”, Paris, 19 February 2016.

3. Elements of an EU approach to external cyber capacity building

On the basis of relevant EU cyber policy documents and development methodology, it is possible to identify three perspectives, each offering a distinct perspective as a starting point for reflection about the design and implementation of concrete action:

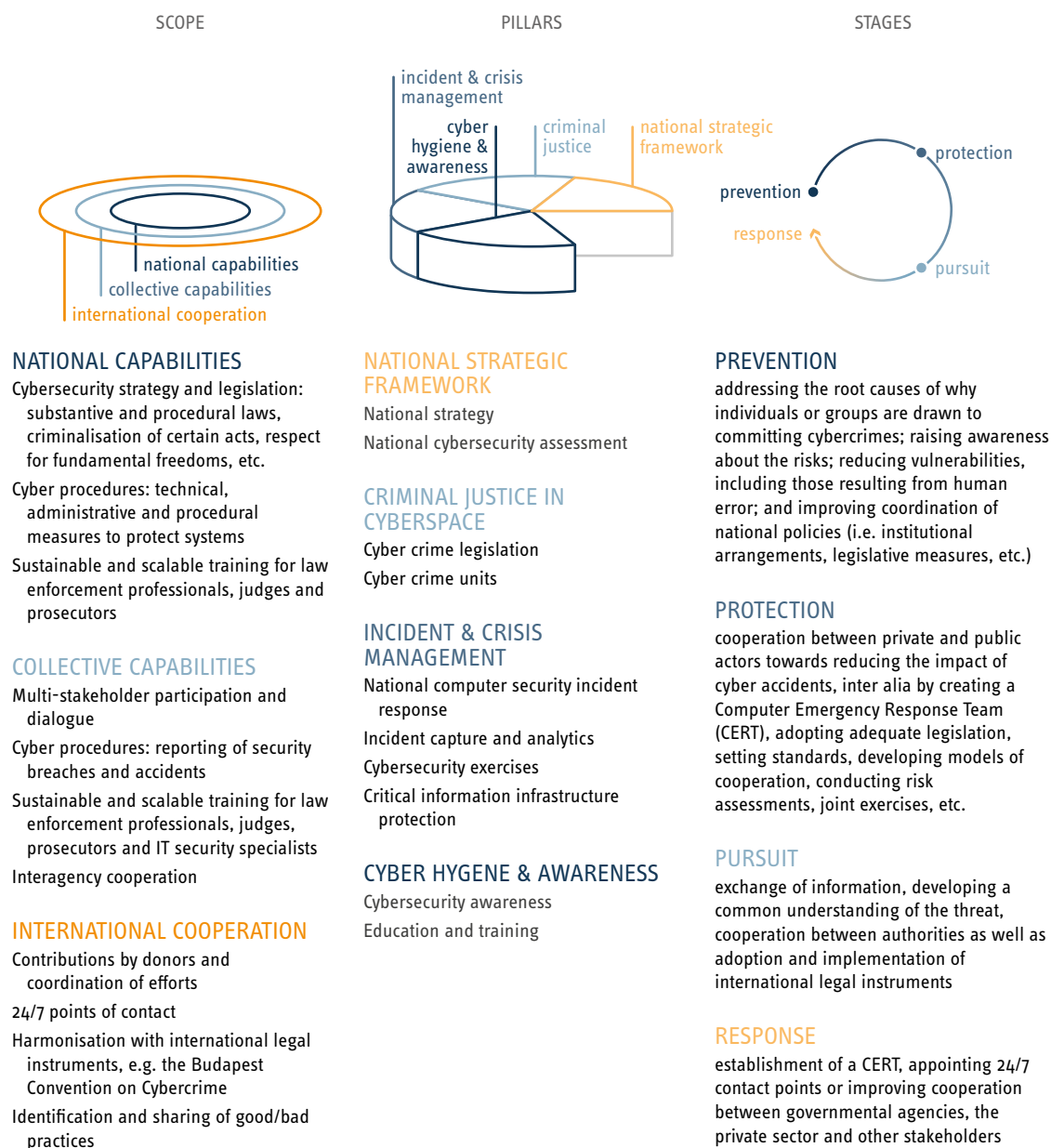
- **Scope** (Whose capacities does the action intend to support: individuals, governments, society, regional organisations or the international community?) – Defining the scope of an action is important as it provides information about the level of ambition and will have big implications on the policy and context analysis;
- **Policy stages** (Which specific stage of the policy cycle does the action intend to address?) – Capacity building actions can start with a decision on whether to approach a given problem by strengthening prevention, protection, pursuit or maybe the response capacities of a partner country or organisation.
- **Policy pillars** (What is the policy area to which the action intends to contribute?) – The most common path starts with the definition of a problem and the policy area to which it belongs. It might be that the action will require operations in more than one policy area.

It is important to note that these three perspectives are not competing but simply provide guidance for launching the CCB process.

12 See the GFCE website for more information.

13 Council of the European Union, “EU Code of Conduct on Complementarity and Division of Labour in Development Policy – Conclusions of the Council and of the Representatives of the Governments of the Member States meeting within the Council”, Brussels, 15 May 2007.

14 United Nations, “Report on the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice”, Doha, 12-19 April 2015.

FIGURE 9: Elements of a cyber capacity-building design

3.1. Strategic scope of cyber capacity building

Support for cyber capacity building can focus on three strategic levels, each with their own characteristics and challenges:

- **Strengthening national capabilities** – Even though responsibilities for cyberspace are spread among many stakeholders, the state still plays an important role in creating a legal and policy environment that helps to protect the benefits of an open and secure internet. Law-making, law enforcement and defence are the exclusive prerogatives of the state. The state can perform this role either through government action (when it can act alone) or by providing the right incentives for other stakeholders (when it does not have the right resources). Such actions come in different forms – adopting a national security strategy and secondary legislation, building national computer emergency response teams, implementing legal and political reforms or entering into international agreements. Consequently, many organisations, including the EU, have committed substantial resources to capacity-building projects aimed at law enforcement and judicial training, cybercrime or high-tech crime units, computer forensic capabilities and CERT/CSIRT employees.

- **Developing collective capability** – Bringing together different communities to address security challenges in cyberspace is hard given the complexities – different organisational missions and objectives (providing security versus making a profit), working methods (public service versus various private sector business models) or conflicting time frames (longer period for policy making or legislation versus the need for quick action). The task is further complicated by the need to recognise different – albeit legitimate – approaches to dealing with cyber threats, mainly military, trade or law enforcement. Consequently, cyber capacity-building actions focused on collective capability aim to reinforce selected actors within the cybersecurity ecosystem and thus contribute to a more effective implementation of the whole-of-society approach.
- **Facilitating international cooperation and partnerships** – Coordinated international efforts are necessary to ensure a minimum level of cyber capacity across the globe. This often proves difficult given the competing objectives and narratives about what needs to be protected, why and how. It is therefore essential to deepen international consensus and strengthen cooperation with regard to prevention, protection, pursuit and response, including through international and regional organisations. As ongoing projects demonstrate, different approaches are possible, including the designation of priority geographic areas, partnerships based on the threat level and connectivity growth or simply due to a country's potential for becoming a hub for developing bottom-up regional initiatives.

3.2. Policy stages: capacity to do what?

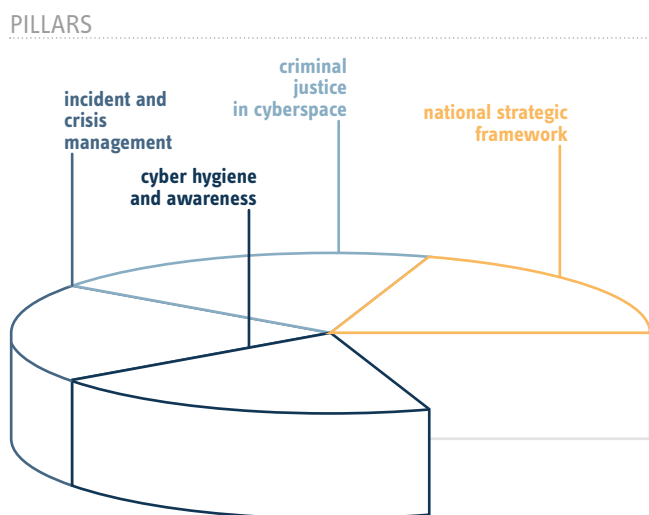
With regard to concrete security objectives, the process of capacity building can be organised along four stages that jointly prescribe a partner country's level of state and societal resilience:

- **Prevention** – Even though cyberspace is characterised by systemic complexity, most of the risks associated with cyberspace involve human intervention. Therefore, understanding relations between people and technology is a crucial aspect. To that end, capacity-building activities may be geared towards addressing the root causes of why individuals or groups are drawn to committing cybercrimes; raising awareness about risks; reducing vulnerabilities, including those resulting from human error; and improving coordination of national policies (i.e. institutional arrangements, legislative measures, etc.);
- **Protection** – Protecting citizens and infrastructure from an attack or accident is an important element. Concrete actions may include cooperation between private and public actors towards reducing the impact of cyber accidents, inter alia by creating a CERT/CSIRT, adopting adequate legislation, setting standards, developing models of cooperation, conducting risk assessments, joint exercises, etc.;
- **Pursuit** – As an incident can result either from negligence or premeditated action, the attribution of liability and potential sanctions is an important part of the discussion. In criminal cases – aimed at obtaining economic or other benefits – efforts may focus on exchange of information, developing a common understanding of the threat, cooperation between authorities as well as adoption and implementation of international legal instruments;
- **Response** – Once a cyber event occurs, actions are taken to minimise and manage the negative consequences on the economic and social wellbeing of citizens, companies or institutions. Potential capacity-building activities in this area might include establishing a CERT, appointing 24/7 contact points or improving cooperation between governmental agencies, the private sector and other stakeholders.

3.3. Pillars of the EU approach: capacity in what?

Decisions about the scope of engagement and which specific policy stage is to be reinforced are inherently linked to the choice of concrete policy area(s) to be supported. Taking into account the EU's current practice in cyber capacity building and drawing comparisons with approaches adopted by other organisations or countries, four pillars of cyber capacity building emerge: (i) national strategic framework, (ii) criminal justice in cyberspace, (iii) incident and crisis management, and (iv) cyber hygiene and awareness.

FIGURE 10: Policy pillars of external cyber capacity building



National strategic framework

Developing a national strategic framework remains a key enabler for building cyber resilience and tackling cyber threats. The aim of national strategic frameworks is to ensure that emerging cybersecurity-related challenges, such as critical infrastructure protection, online criminal activity and skills gaps, are addressed in a comprehensive and coherent way. Many states have adopted different approaches to a strategic framework, often in the form of a national cybersecurity strategy document that establishes a range of objectives and priorities to foster cyber resilience.¹⁵ An effective strategic framework has to be malleable to distinctive political and regulatory environments. It does so whilst developing the overarching aims, means, and responsibilities used to define the basic institutional structure that could accommodate for the development of a cybersecurity ecosystem and its governance framework. The strategic framework must be flexible and actionable, with periodic reviews that contribute towards recalibrating the strategic outlook and accounting for evolving threat landscapes. In practice, this would translate to specific and time-bound action plans or road maps with concrete implementation steps.

¹⁵ See the ENISA website on "National Cyber Security Strategies".

BOX 16: STEPS AND ELEMENTS OF CYBERSECURITY STRATEGY

There are resource materials available on how to develop a national cybersecurity strategy. **ENISA published its first National Cyber Security Strategy Good Practice Guide in 2012**, which has since been updated several times.

The guide presents six steps for the design and development of a strategy:

- Set the vision, scope, objectives and priorities
- Follow a risk assessment approach
- Take stock of existing policies, regulations and capabilities
- Set a clear governance structure
- Identify and engage stakeholders
- Establish trusted information-sharing mechanisms.

In addition, 15 objectives for the implementation are described:

- Develop national cyber contingency plans
- Protect critical information infrastructure
- Organise cybersecurity exercises
- Establish baseline security measures
- Establish incident reporting mechanisms
- Raise user awareness
- Strengthen training and educational programmes
- Establish an incident response capability
- Address cybercrime
- Engage in international cooperation
- Establish a public-private partnership
- Balance security with privacy
- Institutionalise cooperation between public agencies
- Foster R&D
- Provide incentives for the private sector to invest in security measures

Source: ENISA, 2016.

Criminal justice in cyberspace

An effective criminal justice response is necessary to protect the rule of law and the rights of individuals in cyberspace as well as the security, confidence and trust in ICT. Criminal justice action must be based on law and thus the starting point of capacity-building activities is most often supporting the preparation of domestic legislation – both substantive (criminalising conduct) and procedural (powers to investigate cybercrime and other offences involving evidence on computer systems). Attention must be paid to ensure that offences are narrowly defined to avoid overcriminalisation and that procedural powers are limited by rule-of-law safeguards. This may be followed by activities enabling key criminal justice institutions (police investigators, computer forensic experts, prosecutors or judges) to implement such legislation through specialisation or specialised units and training. Since any law enforcement officer, prosecutor or judge may encounter cases involving electronic evidence, training on cybercrime and e-evidence needs to be embedded into the curricula of training institutions for the judiciary and law enforcement. Much electronic evidence is stored by private sector entities such as service providers. Promoting public-private cooperation should thus be a key feature of capacity-building programmes. The same is true for international cooperation as electronic evidence may be stored in multiple jurisdictions. Formulating a strategy or policy on cybercrime and e-evidence helps ensure coherence and the involvement of all relevant stakeholders. This could be a stand-alone strategy or part of a cybersecurity strategy.

BOX 17: ELEMENTS OF CYBER CAPACITY BUILDING IN THE FIGHT AGAINST CYBERCRIME

The Council of Europe in 2013 released a paper encouraging a stronger role for development cooperation organisations in capacity building on cybercrime. It offered pointers, arguments and resources for organisations prepared to provide support, for those requiring assistance, and for those designing cooperation projects. It suggests that capacity-building programmes for cybercrime prevention and criminal justice can address a large range of needs:

- Cybercrime policies
- Development of domestic cybercrime legislation on the basis of international standards
- Cybercrime reporting
- Prevention measures
- Specialised high-tech crime / cybercrime units
- Law enforcement training
- Judicial training
- Support for public/private cooperation
- Support for enhanced international cooperation
- Protection of children online
- Financial investigations and prevention of fraud and money laundering
- Prevention and control of terrorist use of ICT.

Source: Council of Europe, "Capacity Building on Cybercrime", Discussion Paper, 2013.

BOX 18: PUBLIC AND PRIVATE CERT/CSIRT COMMUNITIES

NIS Directive Cooperation Group and EU CSIRT Network: The EU Cooperation Group was established to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, with a view to achieving a high common level of Network and Information Security (NIS) in the Union. The CSIRT Network is comprised of Member State CSIRTs and CERT-EU, also to contribute to building trust and to promote swift and effective operational cooperation. The **EU Blueprint** for cyber-incident management aims to structure and organise the response to large-scale cybersecurity incidents and crises.

Forum of Incident Response and Security Teams: FIRST is a global network of CERTs/CSIRTs that was created in 1990 from the idea that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide-ranging attacks were important for security and incident-response teams. FIRST brings together product-security teams from the government, commercial, and academic sectors, among others. It has been involved in recording lessons from activities undertaken by network members, including publishing best practices on setting up a CERT or CSIRT.

Meridian Process: A global network of governmental bodies on CIIP, the Meridian Process aims to exchange ideas and initiate cooperative actions for governmental bodies on Critical Information Infrastructure Protection (CIIP). It explores the benefits and opportunities of cooperation between governments and provides an opportunity to share best practices from around the world. It is open to all countries, allowing for the creation of a community of senior government policymakers in CIIP by fostering ongoing collaboration.

Regional network of CERTs in the Asia-Pacific: APCERT aims to maintain a trusted network of computer-security experts in the Asia-Pacific to improve the region's awareness and competence in relation to cyber incidents. It focuses on: (i) enhancing Asia-Pacific regional and international cooperation on information security; (ii) jointly developing measures to deal with large-scale or regional network security-incidents; and (iii) assisting other CERTs/CSIRTs in the region to conduct efficient and effective computer emergency response.

Sources: Websites of NIS Cooperation Group, FIRST, Meridian, APCERT.

Incident and crisis management system

The varying scale and frequency of cyber incidents make them difficult to handle. The ability to manage unknown threats and crises is key to be able to absorb unforeseen shocks and adapt accordingly. Many countries are therefore establishing CERTs/CSIRTs to centralise and focus threat mitigation efforts, as well as establishing rapid response and reliable reporting channels between relevant public authorities and private sector entities (including operators of essential services and digital service providers.) Having effective response mechanisms can often be the first line of defence against cyber attacks. Capacity building in this domain is primarily about supporting and protecting critical infrastructure and information infrastructure as well as incident reporting and response. An effective incident management system contains crisis management mechanisms, standards and procedures. This also includes trusted and secure incident reporting channels between actors, both public and private. Putting in place risk management practices also enables actors to mitigate the potentially cascading effects of cyber risks.

Cyber hygiene and awareness

The human factor is often the weakest link in cybersecurity, whether this concerns design thinking or individual responses to cyber-attacks such as ransomware or social engineering.¹⁶ Awareness-raising through media campaigns and civic engagement will allow for a greater level of cyber hygiene as well as foster an inclusive cybersecurity culture. Ensuring effective cyber awareness and hygiene vertically across all layers of society and horizontally, including individuals, organisations and communities, is also a key ingredient for cyber resilience. A cyber-savvy workforce is more resistant to cyber threats than one where expertise is fragmented. A combined public and private effort to raise awareness, promote internationally agreed technical standards, and share best practices helps to bridge the gap between top-down, high-level policy guidance with experience across business sectors of companies that deal with cyber threats on a daily basis.

BOX 19: SAFER INTERNET DAY INITIATIVE

Safer Internet Day (SID) is an international event taking place in February every year to promote a safer and more responsible use of online technology and mobile phones by children and young people. Starting as an initiative of the EU Safe Borders project in 2004 and taken up by the Insafe network, SID has grown beyond its traditional geographic zone and is now observed in more than 100 countries across six of the world's seven continents. The goal is to raise awareness and to help through concrete actions to create a safer and better online environment, with the involvement of children, students, teachers, parents, industry, policy makers, decision takers and other stakeholders.

Source : European Commission.

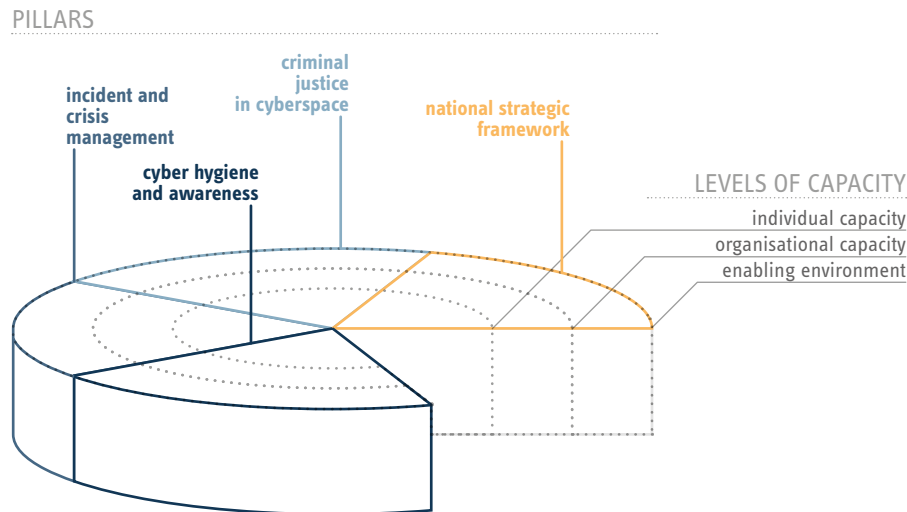
Overall, cyber awareness and hygiene aims to inform and educate users and organisations on how best to mitigate cyber threats. Knowledge and skills should be shared and pooled among actors and sectors to ensure a sufficient level of understanding.

16 C. Boulton, "Humans are (still) the weakest cybersecurity link", CIO, 19 April 2017.

3.4. Levels of capacity: capacity of who and/or what?

It is generally accepted that capacities are distributed at three main levels: individual, organisational and the enabling environment. Therefore comprehensive cyber capacity-building actions need to take into account, and ideally address, capacity gaps at all three levels.

FIGURE 11: Levels of external cyber capacity building



Individual capacity

Capacity building for individuals is the process of equipping them with the understanding, skills and access to information, knowledge and training to perform effectively. The focus is on needs, skills and capabilities, personal attitudes, psychology, motivations, values, etc. This level is usually considered to be the weakest link and therefore of primary importance.

Organisational capacity

Capacity building for an organisation is focused on the elaboration of management structures, processes and procedures internally and managing relationships between different organizations and sectors (public, private and community). It focuses on practices, roles, mandates, decision-making structures, division of labour, sharing of responsibilities, methods of management, means of functioning and use of resources – intellectual, material, economic and technological. Given the high level of inter-dependency between some organisations – e.g. the reliance of hospitals on energy providers – it is important to ensure that organisational capacities are approached in a systemic way that deals with vulnerabilities of the whole cyber ecosystem and does not treat organisations in isolation.

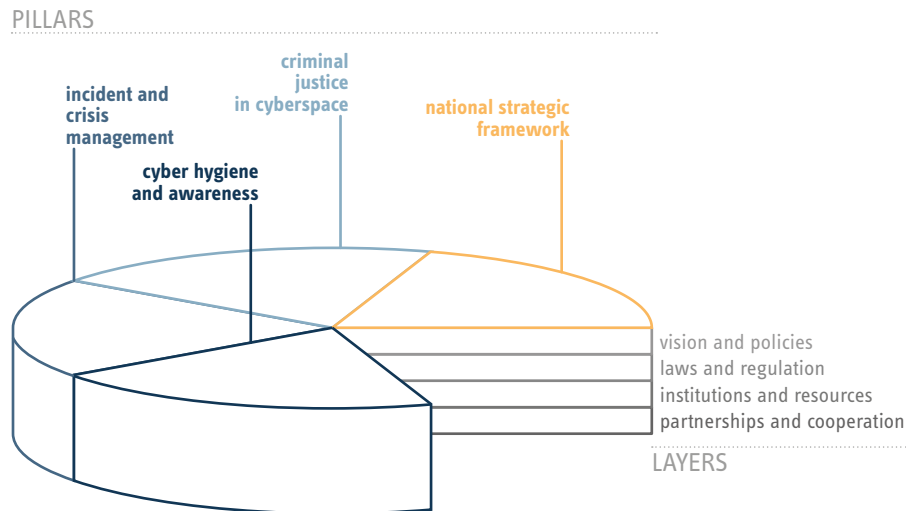
Enabling environment

Creating an enabling environment is about generating the right set of legal, regulatory, economic and societal changes that ultimately support organizations, institutions and agencies at all levels and in all sectors in enhancing their capacities. The assessment of capacities at this level looks at society, laws, policies, procedures, norms, standards, power structures, systems, the environment and culture. The enabling environment is often ignored in capacity-building projects although it is the context within which projects are conceived and implemented that will ultimately decide their success or failure. No matter how well designed, no cyber capacity-building project will have a chance of delivering sustainable results if there is no political support or the legal tradition conflicts with the proposed solutions.

3.5. Layers of capacity: what type of capacity?

The experience of the development community with capacity-building projects provides a useful basis for defining primary layers of cybersecurity capacity building that need to be taken into account.¹⁷

FIGURE 12: Layers of external cyber capacity building



Vision and policies

Developing national capabilities to address vulnerabilities in cyberspace requires identifying clearly what needs to be protected and how. The strategic objectives can include strengthening state and societal resilience, protecting economic growth or protecting national security or any other developmental goal. To define a vision and values, a government needs to have capacity to adequately assess the situation. Once defined, a vision provides the foundations for the development and implementation of policies, but it does not translate into policies automatically. It is through individuals and organisational arrangements that this process takes place, and in a given context. That implies developing capacities to formulate policies and shape the environment, including capacity to explore different perspectives, set objectives, elaborate sectoral and cross-sectoral policies and manage priority-setting mechanisms. Ultimately, a vision and associated policies should reflect a certain value system and contribute to the emergence of a unique cyber culture in the society.

Laws and regulations

A robust legislative framework needs to incorporate reforms in its substantive and procedural criminal law to address cybercrime and electronic evidence, in line with international legal standards and existing international commitments on human rights. Moreover, necessary legal measures may include the definition and protection protocols and standards for critical information infrastructure, information society services and essential services. Laws and regulations translate concepts and strategies into rules, principles, rights and obligations on the part of individuals, organisations and society at large. Due to the complex nature of internet-related laws and regulation, many countries face difficulties adjusting their existing legal orders. Linkages between issues and the fast pace at which technology evolves also make it hard sometimes to fully grasp the implications of proposed solutions. Consequently, the adoption and implementation of legal and regulatory frameworks requires strengthening capacities at all levels, including individual (developing legal skills, adjusting university curricula), organisational (cooperation mechanisms within the justice system, strengthening the organisational capacity to implement laws and regulations), and creating the enabling environment. Numerous initiatives to improve legal capacities when building an enabling environment, dealing with cybercrime, adopting a national cybersecurity strategy or protecting critical national infrastructure have already been completed or are underway. The biggest challenge remains their successful implementation. In

17 United Nations Development Programme, "Capacity Development: Practice Note", New York, 2008.

addition, there is a risk that frameworks developed regionally may jeopardise the efforts towards interoperability and the harmonisation of practices at a global level.

Institutions and resources

Putting laws and regulation into practice, and implementing and enforcing policies requires well-functioning and coordinated institutions and procedures. Broadly, this is important (i) when implementing a national cybersecurity strategy, (ii) for preventing, detecting and responding to potential cyber attacks (i.e. a national level CERT/CSIRT), (iii) for having the necessary capability to undertake cybercrime investigations and digital forensics (i.e. set up of high tech crime units). As countries adopt different models in line with their cultural and political backgrounds (i.e. some have set up such bodies in their ministry of defence, others in the telecommunications ministry), it is essential to gain a thorough understanding of each specific domestic context. Management structures as well as coordination mechanisms and other institutional factors must also be explored. Elements such as leadership, the management of relationships and accountability mechanisms are often decisive in ensuring that a project or undertaking is successful.

Establishing an institutional structure with clearly prescribed cybersecurity responsibilities is also important. The specific arrangement depends on the nuances of national culture, history, law and methods of public administration. While the involvement of different parts of government is essential to ensure a whole-of-government approach, the ultimate coordinating role should be clearly assigned. Addressing capacity needs at different layers also requires adequate resources. This can be a challenge for developing countries where other priorities compete for funding, human resources, equipment or training, education and awareness raising. That means that another important element is the capacity to plan, implement, manage and evaluate projects and programmes, including the capacity to prepare a budget and to estimate capacity development costs; manage human and financial resources and procurement; set indicators for monitoring and monitor progress; measure results and collect feedback to adjust policies; codify lessons and promote learning; and ensure accountability to all relevant stakeholders.

BOX 20: PUBLIC-PRIVATE PARTNERSHIPS

A public – private partnership (PPP) is a long – term collaborative engagement between two or more public and private actors. Acknowledging the importance and possible contribution that such partnerships might have in the cyber domain, a cybersecurity community is still looking for the models and approaches that would allow to leverage such collaboration in the most efficient and effective way.

European Union legislation and policy documents encourage the need for private-public cooperation in the field of cybersecurity as well as the importance of trust building through public-private partnerships. To that effect, ENISA has worked on incentives and actual recommendations on how to setup and run a PPP:

- Public Private Partnerships (PPP) – Cooperative models;
- EP3R 2009–2013 Future of NIS Public Private Cooperation;
- Good Practice Guide on Cooperative Models for Effective PPPs;
- Desktop Research on Public Private Partnerships.

The World Economic Forum has published '**Cyber Resilience: Playbook for Public-Private Collaboration**' that aims to help leaders develop a baseline understanding of the key issues and policy positions relating to cybersecurity and resilience. The Playbook is intended to guide intra-state public-private collaboration on cybersecurity policy. It contains two distinct sections in service of that mission: the reference architecture for public-private collaboration and the cyber policy models.

For more information see the [WEF website](#).

Cooperation and partnerships

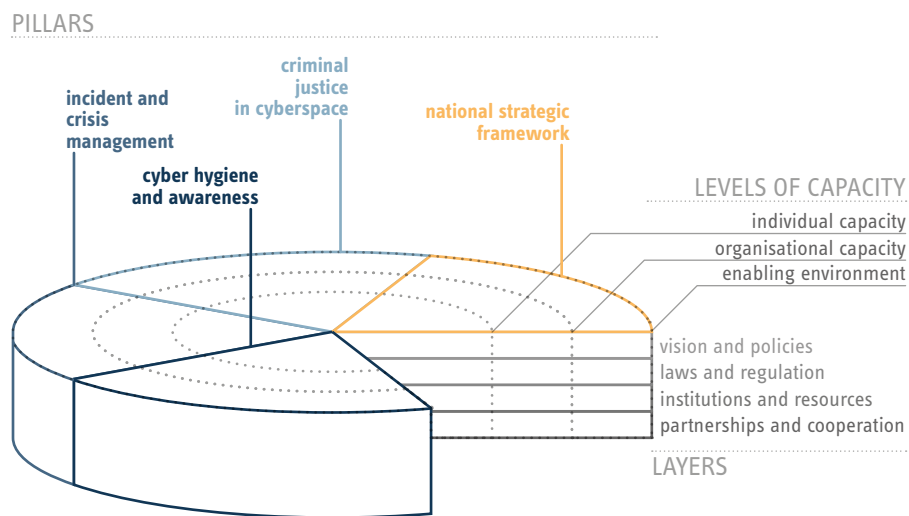
Developing robust and sustainable partnerships between the government and other actors in society (i.e. the private sector, civil society organisations, research institutes) is key for ensuring the whole-of-society approach. Resources for cyber resilience building are distributed at many levels (i.e. individual, community, state) so it is crucial that responsibilities at each are clearly defined. This implies a capacity to engage stakeholders at the national and international levels, such as to identify, motivate and mobilize stakeholders;

create partnerships and networks; promote engagement of civil society and the private sector; manage large-group processes and open dialogue; mediate divergent interests; and establish collaborative mechanisms. Public-private partnerships play a particularly important role in this respect as they contribute to building trust and improve the understanding between public-private, private-private and public-public entities.¹⁸

3.6. Comparison to other approaches

What emerges at the end of the process is a framework for cyber capacity-building actions that requires tackling all three elements – pillars, levels of capacity and policy layers – in a comprehensive and integrated way.

FIGURE 13: Elements of an EU approach to external cyber capacity building

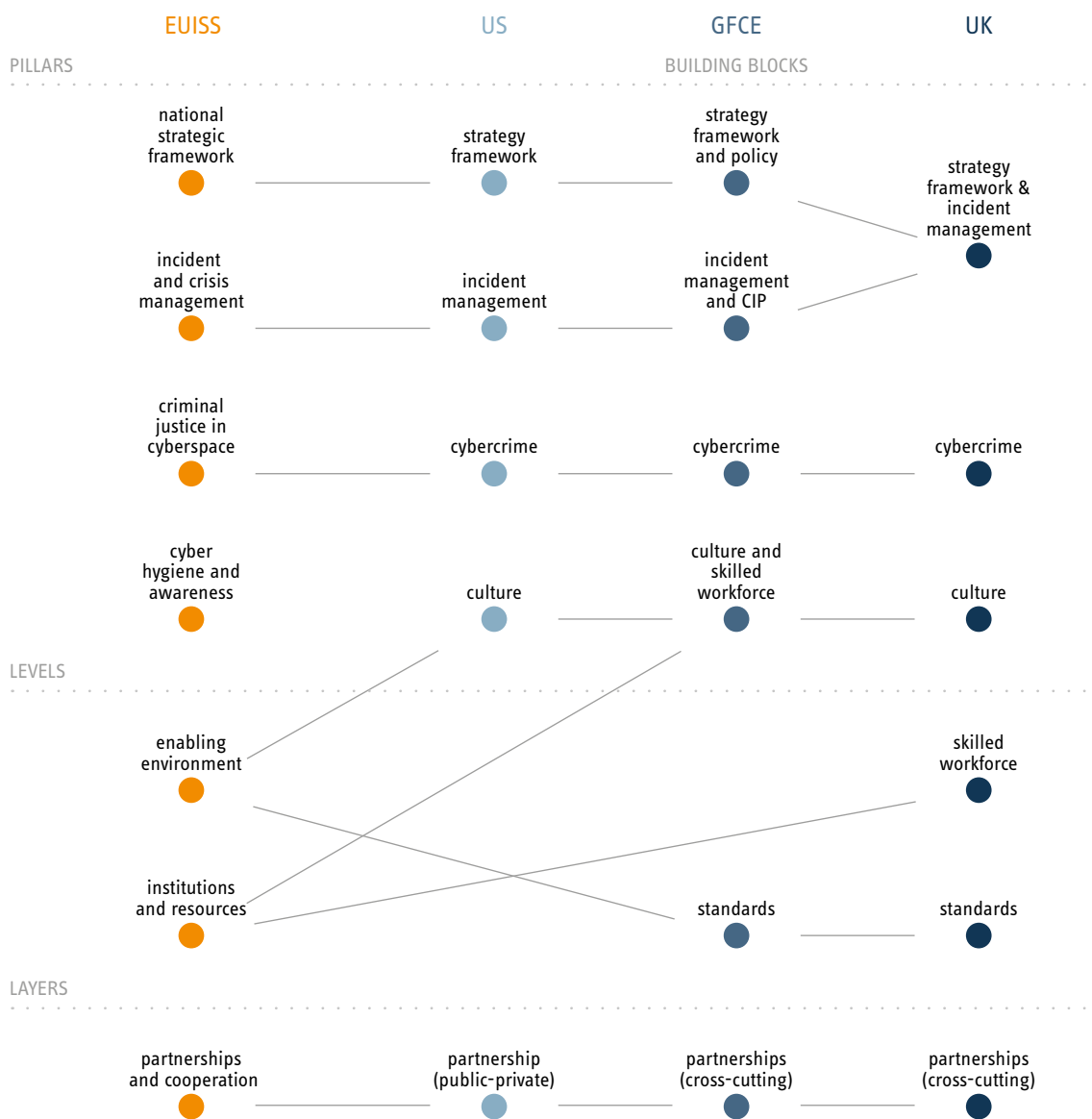


The proposed approach also builds on cyber capacity-building pillars / building blocks proposed by other countries or organisations. While these approaches were developed with different objectives in mind (maturity assessment, defining priorities for CCB, designing capacity-building actions), they all identify similar elements of cyber capacity building:

- **United Kingdom** – The approach developed by the United Kingdom builds heavily on the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Global Cyber Security Capacity Centre at the University of Oxford. The model is intended to measure the existing cybersecurity capacities of countries so that they can develop their cybersecurity capacity-building strategies on this basis. It is based on five crucial dimensions of cyber capacity: cybersecurity policy and strategy; cyber culture and society, cybersecurity education, training and skills; legal and regulatory frameworks; standards, organisations, and technologies.
- **United States** – The illustration of the United States approach to cyber capacity building is based on the presentations by the Department of State in various venues and the 2011 US International Strategy for Cyberspace, which distinguish the following building blocks: national strategy, incident management, cybercrime, cyber culture, and public-private partnerships. The main ideas and concepts were further developed by the MITRE Corporation specifically on strategy development.
- **Global Forum on Cyber Expertise** – The Global Agenda for Cyber Capacity Building builds upon themes of cyber capacity building: cybersecurity policy and strategy; incident management and infrastructure protection; cybercrime; cybersecurity culture and skills; cybersecurity standards. Each theme constitutes an important foundation for national, regional, and global cybersecurity developments. They are closely related and constitute key foci for cyber capacity-building efforts as identified by the GFCE, and are mutually reinforcing.

18 ENISA, "Public Private Partnerships (PPP) – Cooperative models", Athens, 14 February 2018.

FIGURE 14: Comparison of building blocks of cyber capacity building



Inspired by a preliminary comparison proposed by Robert Collett

4. An operational framework for CCB cooperation

A specific Cyber Capacity Building Framework (CCBF) proposed in this study is based on the analysis of several general capacity-building/development frameworks adopted by various development and donor agencies as well as best practices and guidelines proposed by organisations working on cyber policy. Because the CCBF is rooted in methodologies of the development community, there are clear overlaps with the dominant approaches – like the EU’s Project and Programme Management Cycle (PPMC) - based on the Logical Framework Approach (LFA) and the Theory of Change (ToC).

The proposed approach is underpinned by the process of change that includes the following elements:

- **A clear definition of a developmental goal or set of goals** - It is important that an intervention is clearly embedded within a broader developmental context and contributes to one or several objectives set forth by a partner country or a region. In other words, the first question to be answered is: What is the change that we want to achieve and why? At this stage, the development goal is articulated or, if previously set, then reviewed and validated.

- **Designing a change process that supports the attainment of the selected goal or set of goals** - Once a developmental goal has been identified, the process of designing the best path to achieve it begins. It includes an assessment of the capacities and resources needed and the identification of the gap between existing capacities and those needed to achieve the goal. Indicators for measuring respective capacities are identified and targets set. As part of the needs assessment process, the assumptions and risks that are relevant in the process of capacity development and the larger developmental goal are also identified.
- **Formulating a programme design** - Once a desired change has been defined and validated, the process of formulating the program design begins. This stage is focused on identifying the agents of change and specific capacities to be strengthened or built, as well as the identification of related risks and underlying assumptions. Identification of methods in support of the partner country or region in its efforts will constitute the backbone of the change process.
- **Implementation** - Once an intervention begins, the focus shifts towards monitoring the progress towards predefined outcomes and targets. Periodic reviews constitute an important element in deciding whether any adjustments to the programme are required.
- **Completion** - The final stage of the programme – although hopefully not the final stage of the capacity building, which by then should be driven primarily by the partner country or region – is the assessment of the progress toward the development goal.

BOX 21: LOGICAL FRAMEWORK APPROACH AND THEORY OF CHANGE

The focus on change that is generated and sustained from within is the main feature of any capacity-building approach. Since the 1990s, the European Commission has adopted several project design and management tools accompanied by manuals and guidelines for their application. The existing approach, defined in Project and Programme Cycle Management, aims to improve the relevance, feasibility and effectiveness of programmes and projects supported with EU funds, including how well they are managed. The EU's approach is based on two main elements:

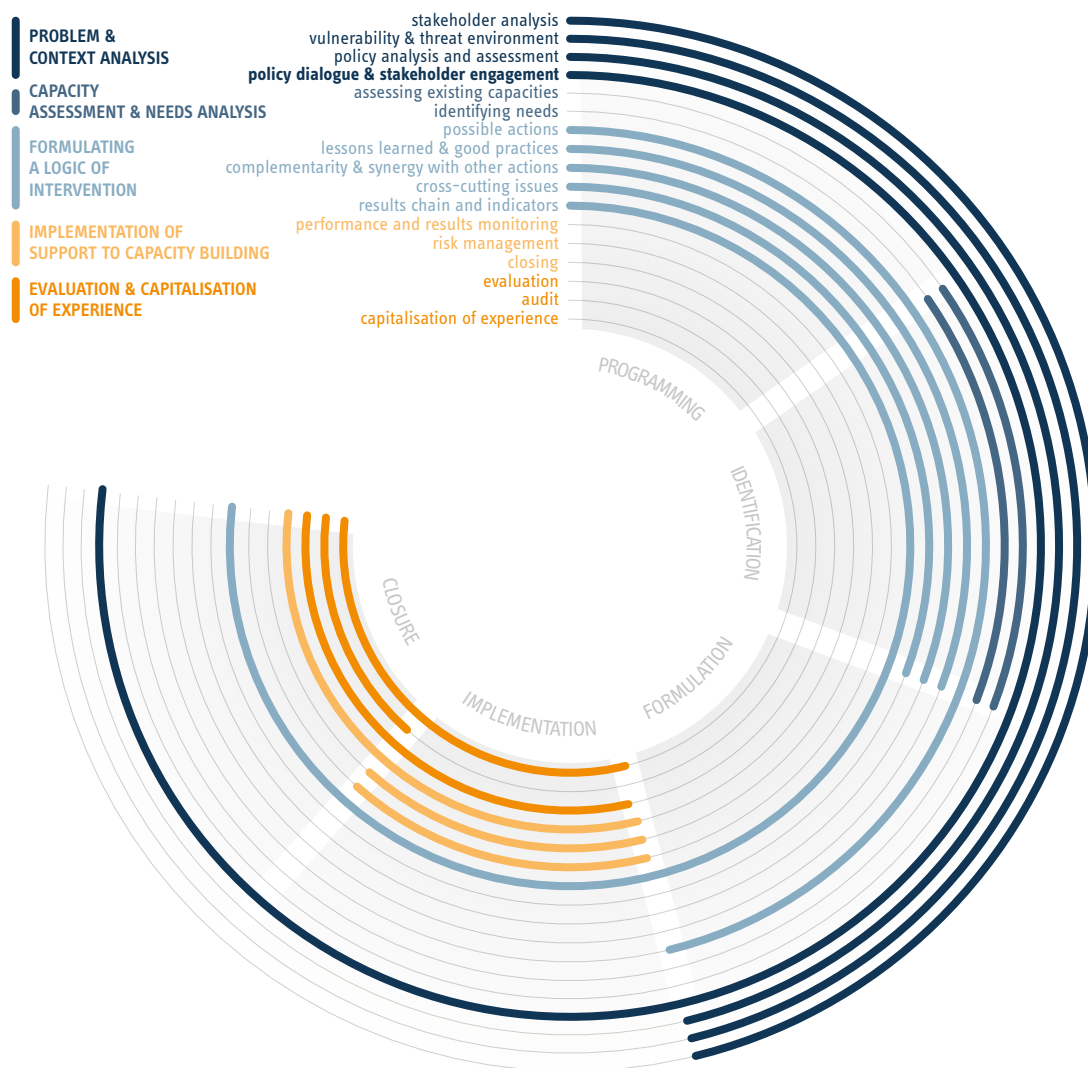
- The **Logical Framework Approach** is an analytical process and set of tools. The problems affecting a given country/sector are presented using cause-and-effect relationships (the 'problem tree'). The problem tree can be mapped to solutions presented through activities-and-results relationships (the 'objective tree'). The strength of the LFA is its focus on the concept of "Intervention Logic" (IL). The IL describes what effects are intended to be (i) achieved (outputs), (ii) directly influenced (outcomes) and (iii) indirectly influenced (impact). The IL forces the critical revision of the evidence on which the rationale is based and the conditions (in the form of assumptions) necessary for the change to happen.
- **Theory of Change** is a coherent set of ideas that serve as a roadmap in the change process. It is different from a Logical Framework Approach in that it seeks to describe at every level how and why certain activities and outputs lead to an intended result.

The international development community is still debating the relationship between the Theory of Change (which is usually illustrated through a logic model) and the Logical Framework Approach (which is illustrated through a Logical Framework Matrix or a Logframe). In practice, the Theory of Change shows the big picture, with all possible ways leading to the expected change, and the reasons (evidence) for them. The Logical Framework Approach focuses on a specific project or programme that leads to expected results through a highly structured way. This makes the monitoring of the corresponding project or programme easier.

Donor organisations have followed their own frameworks for capacity building and development programming. All of them, however, acknowledge the importance of mapping the logic of the capacity development programmes, which is presented either as a programme logic map or a logical framework matrix. These tools help clarify the relationship between a stated development goal, the related objective(s) of the capacity-building programme (supported by a specific set of indicators, baselines and targets), and the stakeholders (agents of change) who will affect the process.¹⁹

When making decisions about the engagement in a cyber-related project it is important to take into account the distinction between capacity building as an explicit aim of an intervention (outcome) and capacity building as a process that is implicitly embedded in any intervention (a stage of a project).

FIGURE 15: Cyber capacity building in the Project and Programme Management Cycle



19 S. Otoo, N. Agapitova, and J. Behrens, *The Capacity Development Results Framework: A strategic and results-oriented approach to learning for capacity development*, New York, World Bank Institute, 2009.

FIGURE 16: Checklist for cyber capacity-building stages

5. Preparatory stage: decisions about an engagement

High vigilance is necessary when implementing external cyber capacity-building actions to ensure coherence with key EU values, interests and principles (e.g. freedom of expression online/offline, multi-stakeholder internet model, promotion of existing international law, a rights-based approach). The increased financing for cyber under the EU external financing instruments raises challenges on ensuring policy coherence and optimal operational choices, especially in light of the global polarisation on cyber issues and the fact that implementing organisations are limited and not always aligned with EU principles. It is therefore important to enhance the knowledge base both in terms of policy and on the methodology to be followed when designing/ implementing cyber capacity-building programmes.

5.1. Mitigating risks

Recognising different logics underpinning the EU's cybersecurity capacity-building efforts is an important step in identifying potential risks for the EU stemming from the engagement with a partner country or region. More specifically, risks exist at the level of:

- **Policy** – different intervention logics, if not addressed from the outset, may undermine the coherence of EU action and result in sub-optimal outcomes in terms of economic opportunities created, competitiveness or sustainability. Ignoring differences in policy objectives together with the lack of coordination among different parts of the EU may, for instance, lead to ‘forum shopping’ whereby potential partners look for the point of entry in the EU that is most sympathetic or least demanding towards the partner’s positions, views or policies.
- **Politics** – insufficient attention to objectives, values and principles recognised in other policy areas may create political risks for the EU as such, in particular when fundamental concepts like the protection of human rights are likely to be compromised. The major risk for the EU is therefore a pursuit of short-term objectives in one policy area or ignoring the views of other actors within the EU family, which might undermine the EU’s standing in the long term.
- **Society** – it is also important to adequately reflect on a policy’s impact and the potential for negative spill-overs into other areas. This is particularly the case with digitalisation-focused approaches that, if not designed properly, may contribute long term to increasing the partner’s vulnerability to risks, as well as that of the EU. For instance, the focus on digitalisation in the health care, energy or education sectors promoted as part of the Digital4Development framework might result in negative consequences if potential societal or security risks stemming from the proposed solutions are not properly addressed.
- **Institutions** – additional risks are linked to sustainability. This is particularly true in the case of actions that focus on institution building or developing regulatory frameworks, where the adoption of whole-of-government and whole-of-society approaches that take into account international best practice is of crucial importance.

To minimise these risks, it is therefore important to put in place adequate risk analysis and mitigation strategies that are founded on EU values, interests and principles.

5.2. V-I-P approach to cyber capacity building

The strategies to mitigate political, societal or institutional risks for the EU cybersecurity capacity-building initiatives need to be grounded in the existing values, interests, and principles enshrined in the Treaties and in key policy documents. These are not alternative approaches but rather complementary dimensions of a single approach that, while placing the partner country/region at the centre of an intervention, also acknowledge different elements that drive the depth and breadth of the EU’s engagement.

Values-based dimension

The CCB initiatives are not implemented in a vacuum. Any EU engagement with third countries and regions needs to ensure the respect for EU values as identified in the Treaties, EU policy documents and other international documents endorsed by the EU and its Member States. While different policies and policy communities may be driven by their own distinct value systems, it is important to ensure that all EU CCB engagements with third countries/partners meet at least the minimum threshold of respecting, protecting, upholding and enabling human rights as well as promoting peaceful coexistence in cyberspace.²⁰

Interests-based dimension

Most projects are driven by a developmental logic that has for an objective supporting the progress of a partner country or region. But in some instances, EU interests are included among the criteria for prioritisation, in a clear recognition that cybersecurity capacity building is rarely a one-way exercise. More often than not, CCB actions are launched to achieve a specific result – such as reducing cybercrime or strengthening the protection of critical infrastructure in a partner country – as a means towards also improving the EU’s own security. By the same token, the EU may decide not to act if the action in question might undermine EU values.

²⁰ For instance, a draft intelligence cooperation law in Netherlands – which nonetheless was rejected in referendum – defined a set of criteria that must be weighted before the intelligence services engage with other intelligence agencies: democratic embedding of a service (i.e. what is the legal basis for the service operations and what are the oversight mechanisms), human rights situation in a country (i.e. has the country signed human rights treaties and are the basic freedoms guaranteed), professionalism and reliability (i.e. what are past experiences with relevant services), legal powers and possibilities of a service (i.e. what is the scope of activities permitted by law), and level of data protection (i.e. how does the service deal with the storage, retention and deletion of collected data).

Principles-based dimension

The EU's CCB actions and their implementation take into account approved and tested guiding principles under each of the logics mentioned earlier. This aspect is particularly important as it determines how the value-based and interest-based approaches are operationalized in practice.

While recognising the diversity of approaches underpinning different logics of CCB, the following four principles – defined in the 2011 Busan Partnership for Effective Development Cooperation and recently recognised in the Delhi Communique by the Global Forum on Cyber Expertise – are particularly relevant in the context of the EU's cybersecurity capacity building in partner countries:

- **Ownership of cybersecurity capacity-building priorities** - Countries – understood as a broader stakeholder community of governmental and non-governmental actors – should play a key role in setting their priorities with a focus on sustainable development. In the case of capacity-building projects, this principle is the major one given that the primary role of any external actor is merely to provide support to capacity building.
- **A focus on results and sustainability** - Having a sustainable impact should be the driving force behind investments and efforts in cyber capacity building. That is particularly relevant in the context of the current discussions in the EU about Digital4Development, and about mainstreaming digital solutions in EU development cooperation that are much broader than cyber capacity building. In that respect, principles such as 'do no harm', 'do maximum good' and the 'duty of care' should provide guidance in defining what the desired results are and how they can be achieved.
- **Partnerships for development and shared responsibility** - Development depends on the participation of all stakeholders while recognising the diversity and complementarity of their functions. This is particularly relevant in the context of cyber-related policies, where the focus is on promoting the multi-stakeholder model of governance. The whole-of-society and whole-of-government approaches promoted by the European Union constitute a useful methodology for operationalising this principle.
- **Transparency and accountability** - In general, any development cooperation action must be transparent and accountable to all citizens. In the context of building trust in ICT solutions, transparency and accountability are the primary conditions for societal support and sustainability. It is therefore important to ensure that any cyber capacity-building action is implemented in a political, legal or institutional environment that favours transparency and accountability, including the handling of data by public authorities, service providers and system developers.

In cyber capacity building, these general development principles can be supplemented with cybersecurity-specific principles identified in EU policy documents, in particular the Charter of Fundamental Rights of the European Union:

- **Equal respect for human rights online and offline** - Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in EU Treaties and the EU's core values. Ensuring respect for the same rights online as off is the primary condition for addressing challenges resulting from trade-offs between policy objectives with the seemingly conflicting logics of security and development. This implies that EU cybersecurity policy should involve a citizen-centric approach upholding rights to liberty and individual security; respect for private and family life, home and communications; freedom of expression and information; and protection of personal data.²¹
- **Bridging digital security divide** - Everyone should be able to have access to the internet, to an unhindered flow of information and equal access to other tools that enable and empower them to use internet in a secure and safe way. That includes the 'analogue complements' that ensure competition among businesses, adaptability of workers' skills, accountable institutions and access to knowledge. At the same time, software and hardware producers have a duty of care towards consumers and must follow due diligence with respect to cybersecurity for the whole product lifecycle, starting from the design phase.²²

21 European Commission, "Cybersecurity in the European Digital Single Market", Scientific Opinion No. 2/107 by the High Level Group of Scientific Advisors, Brussels, 2017.

22 Ibid.

- **State responsibility and respect for international law** - Whereas the primary objective of cyber capacity building is to enable a partner country to harness the developmental benefits of access to the digital domain, it would be irresponsible to ignore potential misuse of the provided support for harming a partner's own population, or using it in ways contradictory to the peaceful use of cyberspace.

BOX 22: EXAMPLES OF VALUES, INTERESTS AND PRINCIPLES IN THE EU DOCUMENTS

EU values linked to

- *The nature of the internet* - Free, open, secure internet; Open, secure, interoperable, and reliable access; Open and neutral internet; Single, open, neutral, free and unfragmented internet; Accessibility, transparency, security;
- *Security, safety and stability online* - Safety and security online; Trust and confidence in ICT; Robustness and stability of global internet; Peace and stability in cyberspace;
- *Freedoms, democracy and good governance* - Democratic and efficient governance; Rule of law; Respect for human rights; Equality and inclusiveness; Economic freedom and entrepreneurship; Open markets.

EU interests

- Sustainable development and security
- Inclusive growth and inclusive societies
- Bridging the digital divide / digitalisation
- Promotion of EU norms and values
- Reducing harm to the EU and strengthening resilience

Principles linked to

- *Development* - Policy coherence; Flexibility and adaptability; Conflict sensitivity; Data and evidence-driven approach; Local ownership; Risk-informed programming; Inclusive partnerships; Results orientation; Development effectiveness; Transparency and accountability; Complementarity and synergies; Rights-based approach; 'Do no harm', 'Do maximum good'; 'Duty of care'; Sustainability and scalability;
- *Diplomacy* - International cooperation and dialogue; State responsibility and respect for international law; Necessity and proportionality; Lawfulness;
- *Resilience* - Whole-of government and whole-of-society approach; Due diligence;
- *Access* - 'No one left behind'; Multilingualism;
- *Market* - Interoperability (of services and movements of data); Net-neutrality.

5.3. Rights-Based Approach

The Rights-Based Approach (RBA) incorporates human-rights principles and standards as both a means and a goal of cooperation, and integrates the achievement and fulfilment of human rights into design, implementation, monitoring and evaluation of all policies and actions. It is a working method that requires a shift in the way international cooperation and development interventions are conceptualised and implemented so that they contribute to the realisation of human rights.

Already in 2011 with the Agenda for Change Communication, and concretely with the 2012 EU Strategic Framework and Action Plan on Human Rights and Democracy, the EU made the RBA a required and essential component of all EU action, across all sectors. The 'Tool-Box – A Rights-Based Approach, Encompassing All Human Rights For EU Development Cooperation' adopted by the European Commission in 2014 describes the various relevant concepts and elaborates five fundamental working principles: applying all rights; participation and access to the decision making process; non-discrimination and equal access; accountability and access to the rule of law; and transparency and access to information.

TOOL 1: VALUES-INTERESTS-PRINCIPLES (VIP) CHECKLIST

<p>Values</p> <p>Global, open, free, stable, secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply to social well-being, economic growth, prosperity and integrity of all free and democratic societies.</p>	<p>Interests</p> <p>Sustainable development, security, inclusive growth and societies, digitalisation, promotion of EU norms and values, strengthening resilience.</p>	<p>Pinciples</p> <p>Ownership, result-orientation, sustainability, partnership, shared responsibility, transparency and accountability, human rights offline and online, bridging digital security divide, state responsibility and respect for international law.</p>
---	---	---

↓
LAYERS OF CAPACITY

visions and policies	laws and regulations	institutions and resources	partnerships and cooperation
----------------------	----------------------	----------------------------	------------------------------

↓
ASSESSMENT CHECKLIST

<ul style="list-style-type: none"> > What is the overall political situation in a country, in particular its attitudes and practice towards international humanitarian law, human rights, the rule of law, effective democratic oversight and accountability? > Are the country's policies compatible with EU values, interests and principles? 	<ul style="list-style-type: none"> > Is it possible that the provided support might directly or significantly contribute to: use of the death penalty; unlawful or arbitrary arrest or detention; torture; unfair trial or denial of justice; unlawful interference with democratic rights; persecution on grounds of religion, race, gender, ethnicity or sexual orientation? 	<ul style="list-style-type: none"> > Are there any human rights concerns about the institutional partner that will participate in the project/programme? > What accountability and transparency mechanisms are in place? 	<ul style="list-style-type: none"> > Are there any justified concerns about linkages between the country/institution that will participate in the programme and cybercrime groups or organised crime networks in general?
---	--	--	---

↓
QUESTIONS

- > Are there any reputational or political risks as a result of the delivery of the project or programme?
- > Are the EU's interests, values, and principle reflected and protected throughout the delivery of the project or programme?

↓
IF THE ASSESSMENT IS THAT...

<ul style="list-style-type: none"> > There are no concerns with the country / institution; > There is less than serious risk of a direct or significant impact of the action on human rights; and/or > The EU's values, interests and principles are reflected and protected. 	<ul style="list-style-type: none"> > There is some reputational or political risk for the EU to work with a country / specific institution; > There is a potential risk that the assistance might directly or significantly contribute to the violation of human rights; and/or > The EU's values, interests and principles might be adversely affected by the project/programme; but can be mitigated effectively. 	<ul style="list-style-type: none"> > There is serious reputational or political risk for the EU to work with a country / specific institution; > There is a serious risk that the assistance might directly or significantly contribute to the violation of human rights; > The EU's values, interests and principles will be adversely affected by the project/programme; and > The mitigation measures will not be effective.
---	---	---

↓
...THEN

<p>The programme or a project can be approved following regular procedures, including the risks/assumptions analysis.</p>	<p>The programme or a project needs to include risk mitigation measures already at the design stage. Support measures include regular or periodic review/assessment of human rights compliance, assurances from the host government, training on human rights, monitoring, vetting of participants, any other mitigation measure.</p>	<p>Engagement on cyber capacity-building should be deprioritised. The programme or a project could be approved by institutional leadership following the analysis of political and reputational risks associated with the project or programme.</p>
---	---	---

On the basis of this toolbox, the **Operational Human Rights Guidance for EU external cooperation actions addressing terrorism, organised crime and cybersecurity** was developed in 2015 to support the integration of RBA in security-related actions. In the field of cyber capacity building, the main policy trade-off that needs to be addressed is between safeguarding, promoting and protecting human rights online

and security objectives. As elaborated in the RBA guidance, ‘*the issues that must be balanced are to safeguard access and openness, to respect, protect and fulfil human rights online, and to maintain the reliability, resilience and interoperability of the Internet and other ICTs*’. Main rights concerns in relation to cybersecurity would include privacy, freedom of expression, freedom of association, discrimination, fair trial and access. In addition, a key dimension of the RBA is to continuously assess whether there are any flow-on human rights risks from the planned or ongoing cyber capacity-building intervention, in particular due to the ‘**dual use**’ of cyber technologies, whereby increased digital capacities may be abused in some countries to facilitate repression.

6. Step one – Problem and context analysis

No organisation or network of organisations functions without constantly being influenced by the context and at the same time influencing it.²³ With the increasing presence of cyber-related topics in international discussions and a growing focus on digitalisation for development, issues linked to cyber-resilience are also entering the agenda of the development community and international cooperation. Nonetheless, any engagement on cyber-related aspects needs to be preceded by a thorough analysis of the policy context in a given country and region and an assessment of the relevance of these issues for achieving the country/regional developmental goals. A thorough understanding of the context requires mapping and analysis of sectoral and other relevant policies, institutions and stakeholders, with the goal of focusing on priority areas and/or problems to be addressed. That implies that, in line with the EU’s own guidelines, **a decision about engagement should reflect and be consistent with national/regional development plans and priorities and strategies of partners as well as EU policy objectives** as expressed in various strategies and programming documents. However, given the relative novelty of the subject, it is also possible that many challenges linked to building a cyber-resilient state and society were not sufficiently taken on board when such documents were prepared. Therefore, in addition to those sources, the reflection about a potential CCB engagement should first check with stakeholders and partners for any analysis or strategic planning done in the past that is linked to the overall objective.

6.1. Stakeholder analysis and engagement

Stakeholders are the individuals, groups or organisations that have an interest in, influence or are influenced by the activity of the cooperation partner or the problem that the EU contribution intends to solve or reduce.²⁴ Stakeholders may also include governmental actors such as ministries and the private sector, community representatives and civil society organisations. Engagement of stakeholders should take place through all stages of the project. Some activities that help to ensure meaningful engagement include consultative processes, communication concerning initiatives, dialogue and coordination efforts.²⁵

A key component of the context analysis is a thorough mapping of stakeholders who shape developments in cyber-related sectors and who are affected or might be affecting the change process. This aspect of project design/implementation is particularly relevant in the case of cyber-related initiatives due to the focus on a multi-stakeholder approach to internet governance. The multi-stakeholder nature of internet governance is a recurrent theme in many policy documents and has been addressed at length by analysts and researchers. The Internet was developed and operates across borders with input from the public and private sectors, academia and civil society, harnessing the expertise of each. So the multi-stakeholder approach is widely accepted as the optimal way to make policy decisions for a globally distributed network.²⁶

Furthermore, a project that does not demonstrate a strong sense of stakeholder ownership and commitment is bound to fail. A properly conducted stakeholder analysis allows for a more accurate identification of the problem and how a specific action fits within national development priorities, and supports the identification of change agents and potential solutions. The **focus on ownership** is a key component given that external actors do not build capacities but only provide support to capacity-building processes. These observations are particularly relevant for cyber capacity building, where the prevailing paradigm is based on **whole-of-society and whole-of-government approaches**. To avoid an overly complex analysis, it might

23 European Commission, “Institutional Assessment and Capacity Development: why, what and how?”, Luxembourg, 2005.

24 K. Schulz, I. Gustafsson, & E. Illes, “Manual for Capacity Development”, SIDA, Stockholm, 2005.

25 See the European Commission’s “Operational human rights guidance for EU external action addressing terrorism, organized crime and cybersecurity”.

26 Internet Society, “Internet Governance: Why the Multistakeholder Approach Works”, 2016.

be more useful to identify stakeholders from the vantage point of the objective to be achieved rather than the existing institutional arrangements, competences and roles.

TOOL 2: QUESTIONNAIRE FOR STAKEHOLDER ANALYSIS

A structured stakeholder analysis may be guided by the following questions:

- **Key actors** - Who are the main actors and what are their main strengths and weaknesses, in particular regarding the capacity to assume their mandate and their working relationship with the government? What factors might prevent them from exercising influence over the policy process?
- **Multistakeholder approach** - Does the cyber-related policy recognise the multi-stakeholder nature of the internet or is the process centralised through the government? Does the private sector or civil society participate in the process through consultations or other similar mechanisms? Is there a well-functioning civil society? For instance, do civil-society organisations have the means to engage in a meaningful discussion on cybercrime, in particular in the context of preserving civil liberties? What is the ownership structure of critical infrastructure – state, private or other form of arrangements – and how does it influence policy making?
- **Power structures** - What are the power structures within the policy-making process? Is there an agency or a government body responsible for the design of cyber policies? How would changing the capacities of the actors affect their positions within the power structure in the cyber sector? What would be the desired and undesired consequences of the intended change? What would be the impact on vulnerable groups?
- **Coordination and methods** - What are the coordination mechanisms in place? Are cross-sectorial consultations with other actors part of the process? Are the whole-of-government and whole-of-society approaches reflected in the way the policy process is structured? How are conflicts within the policy circles addressed?

A meaningful engagement with stakeholders also requires strategies for managing expectations from the very early stages. For instance, many governments still associate cyber-related capacity building with the delivery of hardware or infrastructure. These are not cyber capacity-building projects per se. It is important therefore to communicate the precise objectives and anticipated results of the projects and to monitor changes in the positions and attitudes of specific actors. In such a dynamic environment it is critical to establish appropriate channels and tools to nurture relationships.

Finally, capacity building is an inherently political instrument that in situations of unbalanced power relations can have unwanted consequences.²⁷ Understanding the existing power relations – i.e. what the current capacities of stakeholders are and how capacity building will affect them – is an important element of stakeholder analysis. Because capacity building is very likely to result in shifting power relations between stakeholders, it is important to analyse who will be affected, in what ways and how other actors might react. Stakeholder analysis, therefore, can contribute to increasing the understanding of ways in which different groups may relate to the result.²⁸ While some actors who are expected to benefit become agents of change and change accelerators, others may demonstrate more reluctance towards proposed solutions and act as spoilers. One of the main challenges working in the multi-stakeholder environment, therefore, is identifying relevant institutions and organisations and ensuring their willingness to engage. This process will be more or less complicated depending on the mission and objectives of an action and the respective organisations. For instance, civil society organisations with limited resources are probably more likely to engage in activities that are at the core of their business and offer some sort of return – either financial or reputational. Private-sector companies, on the other hand, which usually have more resources, are more likely to engage in a broader scope of activities that may help to advance their positions and interests, even if indirectly. There is also a possibility of actors engaging in a negative way; a project hardly ever gains universal acceptance.

27 K. Schulz, I. Gustafsson, & E. Illes, *op. cit.*

28 *Ibid.*

Non-governmental organisations may criticise a project's impact on civil liberties while the private sector may simply object to the costs.

TOOL 3: MAPPING OF ACTORS ACTIVE IN RESPECTIVE POLICY PILLARS

Stakeholder and basic characteristics	Key interests	Capacity to support the process of change
<p>National governments</p> <p>Elected officials that have authority to govern and enact change</p>	<ul style="list-style-type: none"> Improving strategic posture Developing cyber resilience Improving criminal response and reducing cybercrime rate Using ICT for growth and development Minimising the impact of cross-border crisis and cyber threats Building partnerships and coalitions to address threats in a collective manner 	<ul style="list-style-type: none"> Legislative and sanctioning powers The right of policy initiative Public funding and oversight Convening power
<p>National courts</p> <p>Act as tribunal in criminal prosecution; jurisprudence</p>	<ul style="list-style-type: none"> Providing justice to perpetrators and victims Ensuring rule of law and protection of human rights 	<ul style="list-style-type: none"> Law-shaping and law-making Sanctioning powers
<p>Law enforcement agencies</p> <p>Responsible for the enforcement of the law, policing duties, and social order</p>	<ul style="list-style-type: none"> Bringing perpetrators to justice Reducing cybercrime 	<ul style="list-style-type: none"> Identification of potential new threats and vulnerabilities Awareness raising Organisation of joint investigations and operations Convening power
<p>National CERT/CSIRT</p> <p>Responsible for risk and incident handling, threat detection and communication</p>	<ul style="list-style-type: none"> Minimising the negative impact of incidents and handling Providing timely threat intelligence to policymakers and the whole cyber ecosystem 	<ul style="list-style-type: none"> Threat intelligence and vulnerability analysis capabilities Operational responsibility for protecting the networks
<p>Government agencies</p> <p>Permanent/semi-permanent entity, responsible for oversight and administration of specific functions (i.e. civic engagement, dissemination)</p>	<ul style="list-style-type: none"> Improving strategic posture Developing cyber resilience Improving criminal response and reducing cybercrime rate Using ICT for growth and development Minimising the impact of cross-border crisis and cyber threats Building partnerships and coalitions to address threats in a collective manner 	<ul style="list-style-type: none"> Legislative and sanctioning powers The right of policy initiative Public funding and oversight Convening power
<p>International organisations</p> <p>Multi-national membership and reach, both governmental and non-governmental</p>	<ul style="list-style-type: none"> Strengthening international response to cyber threats and vulnerabilities Streamlining resources to avoid duplication Supporting members in achieving their goals 	<ul style="list-style-type: none"> Law, regulation and policy-making powers Platforms for international discussions and deliberations International crisis management mechanisms Sanctions to enforce international law
<p>Private sector</p> <p>Entities not under direct State control</p>	<ul style="list-style-type: none"> Minimising the impact of cyber attacks on their business, clients and costumers Strengthening trust in online environment 	<ul style="list-style-type: none"> Funding for training and awareness raising Drivers of change and innovation Important interlocutors/partners for governments, including for critical infrastructure protection, cyber-crime, e-evidence (PPPs).

Stakeholder and basic characteristics	Key interests	Capacity to support the process of change
<p>Technology companies</p> <p>Focuses primarily on the development and manufacturing of technology (infrastructure, services and products)</p>	<ul style="list-style-type: none"> Monitoring potential impact of regulation and policy initiatives on clients and shareholders Providing secure products and service Contributing to the threat and risk identification process Fostering societal trust in technology 	<ul style="list-style-type: none"> Technical and financial resources for innovative solutions Direct intelligence about threat environment and consumers behaviour Digital forensics
<p>Operators of essential services</p> <p>Providers of services that are critical to the functioning of a society</p>	<ul style="list-style-type: none"> Maintaining proper and uninterrupted functioning of critical sectors and protecting infrastructure Source of information about breaches and threats 	<ul style="list-style-type: none"> Technical and financial resources for innovative solutions
<p>Digital service providers</p> <p>Providers of content and media online (i.e. online marketplace, search engine, and cloud computing service)</p>	<ul style="list-style-type: none"> Maintaining proper functioning of services Protecting company's image and trust in its products/services Shaping legislation and policies to the advantage of the shareholders 	<ul style="list-style-type: none"> Report breaches and inform affected parties Possess technical and financial resources for innovative solutions
<p>Civil society</p> <p>Community of citizens linked by common interests and collective activity</p>	<ul style="list-style-type: none"> Protection of human rights Consumer protection 	<ul style="list-style-type: none"> Mobilisation and engagement Influence on broader parts of society Information about grassroots processes

TOOL 4: MAPPING OF INTERNATIONAL STAKEHOLDERS

National strategic framework	Criminal justice in cyberspace	Incident and crisis management	Cyber awareness and hygiene
<p>organisation</p> <p>mission</p> <p>activities</p>			
<p>ITU</p> <p>To strengthen the human, institutional and organisational capacity of developing countries in a manner that prepares them for the challenges of a digital economy through engagement and awareness, national cybersecurity assistance, computer incident response team program, information sharing, cyber drills, human capacity building, in-country technical assistance</p>			
<ul style="list-style-type: none"> strategic & conceptual support standards and procedures 		<ul style="list-style-type: none"> CERT support technical support policy support 	<ul style="list-style-type: none"> awareness raising information dissemination civic engagement multi-stakeholder engagement
<p>UNDP</p> <p>To ensure that cybersecurity programmatic assistance is provided on an “on demand” basis to developing nations</p>			
<ul style="list-style-type: none"> strategic & conceptual support 			<ul style="list-style-type: none"> education
<p>ECOWAS</p> <p>To establish a single Digital Market in West Africa and regional integration; to strengthen the security and resilience of vital ICT infrastructure; to secure and encourage use of ICT</p>			

National strategic framework	Criminal justice in cyberspace	Incident and crisis management	Cyber awareness and hygiene
<ul style="list-style-type: none"> • strategic & conceptual support • regulatory convergence • compliance 	<ul style="list-style-type: none"> • technical support • online child protection • harmonisation of legislation 	<ul style="list-style-type: none"> • critical infrastructure protection 	<ul style="list-style-type: none"> • information dissemination • awareness raising • civic engagement • multi-stakeholder engagement

OECD

To develop policy analysis and recommendations for governments and other stakeholders to better address security challenges in the digital environment from an economic and social perspective (trust, big data and the knowledge economy; internet policy and governance)

<ul style="list-style-type: none"> • strategic & conceptual support 		<ul style="list-style-type: none"> • policy support 	<ul style="list-style-type: none"> • information dissemination • awareness raising • civic engagement • multi-stakeholder engagement
--	--	--	--

OAS

To increase access to knowledge and information on cyber threats and risks; to enhance the technical and policy capacity of governments and critical infrastructure operators to detect cyber threats, respond to cyber incidents, and combat organized crime; and to promote more robust, effective and timely information-sharing, cooperation and coordination among cybersecurity stakeholders at the national, regional and international level

<ul style="list-style-type: none"> • strategic & conceptual support • institutional set-up • standards and procedures 	<ul style="list-style-type: none"> • technical support • harmonisation of legislation • law enforcement cooperation • training 	<ul style="list-style-type: none"> • threat detection • critical infrastructure protection • crisis management exercises • best practice sharing 	<ul style="list-style-type: none"> • information dissemination • awareness raising • civic engagement • multi-stakeholder engagement
--	--	--	--

OSCE

To work on confidence-building measures (CBMs) to reduce the risks of conflict stemming from the use of ICTs; to build expertise and capacities to tackle cyber/ICT security threats from non-state actors, such as organized criminals and terrorists as well as the protection of fundamental freedoms online; to promote adequate and timely responses by national authorities to these evolving threats, ranging from better forensics to innovative approaches to prevent ICTs from becoming tactical facilitators for terrorists; to create synergies with other organizations and entities working in these fields

<ul style="list-style-type: none"> • strategic & conceptual support • international law & norms • confidence building measures 	<ul style="list-style-type: none"> • technical support • online child protection • training 	<ul style="list-style-type: none"> • policy support 	<ul style="list-style-type: none"> • information dissemination • awareness raising • civic engagement • multi-stakeholder engagement
---	--	--	--

ASEAN

To enhance regional ability to respond to the evolving cyber threat landscape and to build a secure and resilient ASEAN cyberspace; to develop technical, policy and strategy-building capabilities within ASEAN Member States. Focus areas under the programme includes cyber policy, legislation, strategy development as well as incident response (ASEAN Committee on Consumer Protection)

<ul style="list-style-type: none"> • institutional set-up • standards and procedures • international law & norms • regulatory convergence • compliance 	<ul style="list-style-type: none"> • technical support • online child protection • harmonisation of legislation 	<ul style="list-style-type: none"> • incident reporting & response • information sharing • best practice sharing • policy support 	<ul style="list-style-type: none"> • information dissemination • awareness raising • civic engagement • multi-stakeholder engagement • education
---	--	---	---

INTERPOL

To support cybercrime investigations; to develop innovative new technologies; to assist countries in exploiting digital evidence; to conduct training sessions; to assist countries in reviewing their cyber fighting capacities

National strategic framework	Criminal justice in cyberspace	Incident and crisis management	Cyber awareness and hygiene
<ul style="list-style-type: none"> • institutional set-up • standards and procedures • compliance 	<ul style="list-style-type: none"> • prosecution and investigation • evidence gathering • online child protection • law enforcement cooperation • training 		<ul style="list-style-type: none"> • awareness raising • multi-stakeholder engagement • information dissemination

African Union

To continuously set up and update sound policy to match the technological evolution in one hand and build the hard infrastructures that will strengthen integration through internal and external connectivity of the continent and secure the access of citizen to networked Information Society and lead to the digital economy; to promote a culture of Cybersecurity and develop National and Regional cybersecurity policies through multi stake holders approach

<ul style="list-style-type: none"> • institutional set-up • standards and procedures • strategic & conceptual support 	<ul style="list-style-type: none"> • technical support • online child protection • harmonisation of legislation 	<ul style="list-style-type: none"> • incident reporting & response • information sharing • best practice sharing • policy support 	<ul style="list-style-type: none"> • information dissemination • awareness raising • civic engagement • multi-stakeholder engagement • education
--	--	---	---

CTO

To assist member countries and the wider stakeholder community leverage ICTs for development by providing technical support and advisory services, delivering capacity building and organising international events; to develop a Commonwealth Approach for Developing National Cybersecurity Strategies based on the Commonwealth Cyber governance Model

<ul style="list-style-type: none"> • strategic support • institutional set-up 	<ul style="list-style-type: none"> • technical support • online child protection • harmonisation of legislation 	<ul style="list-style-type: none"> • incident reporting & response • information sharing • best practice sharing • critical infrastructure protection 	<ul style="list-style-type: none"> • information dissemination • awareness raising • multi-stakeholder engagement • education
---	--	---	---

World Bank

To offer integrated solutions in the ICT project portfolio to address cybersecurity gaps in their country clients; to develop integrated solutions in order to increase countries' response capacity to cyber-threats menacing their public systems and infrastructure, especially those projects that have eGovernment, eServices, eIDs, Cloud, among other components

<ul style="list-style-type: none"> • strategic & conceptual support • institutional set-up 		<ul style="list-style-type: none"> • infrastructure support • policy support 	<ul style="list-style-type: none"> • awareness raising • multi-stakeholder engagement • information dissemination • education
--	--	--	---

Meridian Process

To create a community of senior government policymakers in CIIP by fostering ongoing collaboration

<ul style="list-style-type: none"> • strategic & conceptual support • institutional set-up • best practice sharing 		<ul style="list-style-type: none"> • policy support 	
---	--	--	--

GFCE

To identify successful policies, practices and ideas and multiply these on a global level; to develop practical initiatives to build cyber capacity together with partners from NGOs, the tech community and academia GFCE members; to stimulate new funding streams and the sharing of expertise and experiences in four key areas: cybersecurity, cybercrime, data regulation and e-development.

National strategic framework	Criminal justice in cyberspace	Incident and crisis management	Cyber awareness and hygiene
<ul style="list-style-type: none"> • strategic & conceptual support • institutional set-up • best practice sharing 			<ul style="list-style-type: none"> • multi-stakeholder engagement
<p>FIRST</p>			
<p>To cooperatively handle computer security incidents and promote incident prevention programs; to develop and share technical information, tools, methodologies, processes and best practices; to encourage and promote the development of quality security products, policies & services; to develop and promulgate best computer security practices; to promote the creation and expansion of Incident Response teams and membership from organizations from around the world</p>			
<ul style="list-style-type: none"> • standards and procedures • strategic & conceptual support • institutional set-up 		<ul style="list-style-type: none"> • incident reporting & response • information sharing • best practice sharing • critical infrastructure protection • CERT support • technical support 	
<p>AfricaCERT</p>			
<p>To propose solutions to challenges for Internet Health in Africa’s Internet Ecosystem; to assist African countries in establishing CSIRTs; to promote best practices; to foster and support education and outreach programs in ICT Security in and among African countries</p>			
<ul style="list-style-type: none"> • standards and procedures • strategic & conceptual support • institutional set-up 		<ul style="list-style-type: none"> • incident reporting & response • information sharing • best practice sharing • critical infrastructure protection • CERT support • technical support 	
<p>AP-CERT</p>			
<p>To maintain a trusted contact network of computer security experts in the Asia Pacific region; to improve the region’s awareness and competency in relation to computer security incidents</p>			
<ul style="list-style-type: none"> • standards and procedures • strategic & conceptual support • institutional set-up 		<ul style="list-style-type: none"> • incident reporting & response • information sharing • best practice sharing • critical infrastructure protection • CERT support • technical support 	
<p>TF CSIRT</p>			
<p>To promote collaboration and coordination between CSIRTs whilst liaising with relevant organisations at the global level such as FIRST, ENISA, other regional CSIRT organisations; to develop and provide services for CSIRTs, promote the use of common standards and procedures for handling security incidents, and coordinate joint initiatives where appropriate</p>			
<ul style="list-style-type: none"> • standards and procedures • strategic & conceptual support • institutional set-up 		<ul style="list-style-type: none"> • incident reporting & response • information sharing • best practice sharing • critical infrastructure protection • CERT support • technical support 	

6.2. Vulnerability and threat environment

Given a rapidly evolving security context and competing developmental objectives, cyber-related security concerns are not always adequately addressed in development plans and strategies. The systematic analysis of the cyber environment is challenging and requires significant resources, so the quality of intelligence varies depending on countries and regions. In developing and the least-developed countries, data is often unavailable. To address these problems, some regional organisations have established partnerships with research institutes or the private sector.

TOOL 5: CHECKLIST FOR VULNERABILITY ASSESSMENT

What is the level of internet penetration?

It allows one to understand how many individuals are potentially exposed to cyber threats and what the potential cost to society could be. Statistics on the number of users, households and types of connection are collected by the ITU and are available on their website.*

What is the structure of access to internet and the online environment?

The risks are different depending on the digital environment in a country. For instance, in many African countries access to internet is primarily provided via mobile phones, which means that online services are more tailored for this specific form, including mobile banking, etc. Reports on the digital environment in a specific country might be also available from regional and international organisations like the World Bank.

What is the level of connectivity and to what extent is the country's critical infrastructure dependent on ICT platforms?

Depending on how connected the country is, its exposure to digital risks might be higher or lower accordingly. Being connected does not pose a threat as such but simply signals that there is a risk and certain level of vulnerability. This information is usually available in a descriptive form and might be collected from respective ministries, service providers, etc. For instance, The Global Information Technology Report series published by the World Economic Forum in partnership with INSEAD and Cornell University measures the drivers of the ICT revolution globally, using the Networked Readiness Index (NRI). The Index currently assesses the state of networked readiness using 53 individual indicators. For each of the 139 economies covered, it allows for the identification of areas of priority to more fully leverage ICTs for socioeconomic development.

What are the main risks and threats in cyberspace?

Answering this question allows one to place a situation in a given country in a broader context. Ideally, such information would be available from government agencies, however this is rarely the case. More often, such information is generated by the private sector. While acknowledging that such studies might sometimes be biased to promote certain policies or products, the following reports are potentially useful: Internet Security Threat Report by Symantec, Global Security Intelligence Report by Microsoft, Data Breach Investigations Report by Verizon.

* ITU, 2017.

While assessing vulnerabilities and threats is complex, there are certain questions that might provide a good understanding about the situation in a given country (see Tool 5). With the issue gaining traction in the international debates, one cannot exclude situations where requests for support are motivated less by a genuine need and threat assessment than a politically motivated priority setting. Such requests may be also driven by misplaced policy objectives whereby a focus on incident management, for instance, might jeopardise attention to the developmental nature of the capacity-building projects. It is therefore essential that the EU has a well-developed understanding of the situation in a country. These questions may be one of the first steps in establishing dialogue with the partner country and/or region. Even if such data is not always readily available, asking for it might be a useful step in identifying needs. For instance, information about potential attacks and vulnerabilities should normally be provided by the Computer Emergency Response Teams at different levels – national, regional, sectoral – or law enforcement and intelligence agencies. Difficulty in obtaining such data – even in a very generic form – might be an indication that such institutions do not exist or their capacities are not sufficient.

BOX 23: REGIONAL REPORTS ON CYBERSECURITY TRENDS AND POLICY RESPONSES

- The **African Union Commission** and Symantec released a report on ‘Cybersecurity trends and government responses in Africa’, which included the Rise of Ransomware and Cryptolocker; Social Media, Scams, and Email Threats; Smartphones and the Internet of Things; Business Email Scams; and Vulnerabilities. This report is unique in that it incorporated the perspectives of African Union Commission Member State governments and online threat data from Symantec’s comprehensive cyber threat monitoring network. The report should serve as a baseline from which to recognize progress made by African governments and areas in need of improvement. It is also meant to assist in guiding and strengthening in a multi-stakeholder fashion efforts aimed at building a safe, secure and stable digital world.
- **Organization of American States** and **Inter-American Development Bank** have published a report ‘Cybersecurity: are we ready in Latin America and the Caribbean?’. The report presents a comprehensive depiction based on the Cybersecurity Capacity Maturity Model for Nations (CMM) by the Global Cybersecurity Capacity Centre. National stakeholders can utilize this information to gain a better understanding of their country’s cybersecurity situation in a regional context. It can also help governments and cybersecurity experts explore new ideas for strengthening cybersecurity in their respective countries and across the hemisphere. Overall, the findings represent a snapshot in time which can be used as a reference point as countries develop their cybersecurity capabilities. Utilizing surveys and other data provided by experts and officials from 32 OAS Member States, the report examines each country’s cyber maturity in five dimensions: (i) Cybersecurity policy and strategy; (ii) Cyber culture and society; (iii) Cybersecurity education, training and skills; (iv) Legal and regulatory frameworks; and (v) Standards, organizations, and technologies. The country-by-country approach helps to develop a more nuanced understanding of each state’s cybersecurity regime and assists policymakers and technicians to strategically improve existing efforts and to design and implement new initiatives.

6.3. Policy analysis and assessment

A thorough policy analysis and assessment is a prerequisite for an adequate identification of the needs of a country or a region (See Tool 6). Its ultimate objective is to help determine what would be the most effective way of providing support to a partner country/region. Even if cyber-related elements are included in the development programmes, they need to be assessed against the overall national development plans and strategies. This is important to ensure credibility, relevance and sustainability of a given project or programme. For instance, an engagement with a partner country aimed at improving the competence of law enforcement officials with regard to handling electronic evidence and addressing cybercrime might be important for a country with a rapidly growing online presence, but it needs to be embedded in a broader developmental plan to strengthen good governance and the rule of law or to contribute towards economic development. In other words, only cyber capacity-building engagements designed with a structured reform outlook, expressly to contribute towards broader developmental goals, have a chance of having a meaningful impact.

A properly conducted sectoral policy analysis provides the foundation for a more in-depth investigation of the role of cyber capacity building within a broader framework. Once the role of cyber resilience within the broader developmental context is better understood, the focus of the analysis needs to shift towards concrete questions to determine the adequacy of the support to capacity building as a method of engagement. Most importantly, does the partner country recognise the need for cyber capacity building as an important aspect of its overall developmental strategy? If yes, have any specific priorities been set? In many cases, addressing these issues will require access to data and information that is not always readily available. Therefore, the following data sources may be helpful:

- **Policy objectives:** a national security strategy, national cybersecurity strategy, legal and regulatory acts addressing cybercrime, protection of critical information infrastructure, etc. Additional information could be inferred from the country’s participation in regional and international organisations, including the adoption of the Council of Europe’s Convention on Cybercrime or other arrangements applicable in the country’s region;
- **Relevance:** impact assessments, risk analysis, needs assessments, lessons learned from past projects;
- **Credibility:** national budgets, political commitment, national development plans;
- **Human rights:** ‘Freedom on the Net’ report published by the Freedom House, annual reports by Amnesty International and Human Rights Watch, court cases in the national system and regional courts such as the European

Court of Human Rights. Human rights violations and internet shutdowns are also monitored through campaigns such as #KeptItOn organised by NGO Access Now.

TOOL 6: QUESTIONNAIRE FOR POLICY ANALYSIS AND ASSESSMENT

What are the policy objectives?

It is important to understand the overall place of the cyber-related issues in the country's national development strategy. First, does the country have a defined cyber policy? If yes, what are its objectives? Cyber issues do not appear in a vacuum but are usually driven by a specific developmental objective, which can offer a specific prism through which cyber issues are perceived and addressed. While some countries view them as a catalyst towards economic and human development, others might place more focus on the security dimension. Additional questions to address include the consistency and coherence of different dimensions of cyber policy.

Is the policy relevant?

One of the main aspects in public policy analysis is assessing how relevant is the specific approach for addressing a given policy challenge. That implies clarifying whether the policy is risk informed, what concrete challenges does it address and how compatible it is with relevant EU policies.

Is the public policy credible to national and international stakeholders?

To be credible, any government policy needs to be implemented and supported with adequate human and financial resources. It also requires mechanisms for translating stated objectives into concrete outcomes. Policy assessment should therefore look into budgets and other documents that might give an indication of the government's commitment. It also is important to draw from experience and lessons identified from past projects or other donors and partners. Looking into past experiences also helps to assess the effectiveness of policy implementation.

Is local ownership assured?

Capacity building is a process driven by domestic actors with external partners only providing a supporting role. To ensure that this support is delivered in an effective and efficient way, partners need to understand the structural and institutional factors that shape present capacity and provide drivers as well as constraints to change (European Commission, 2005). Given that countries have different models for cooperation with external partners – working exclusively through the government, support to projects selected directly by the donor organisation, etc. – it is important to understand the opportunities and limitations of each approach.

What are the existing institutional capacities?

In addition to looking into content, policy analysis should address issues linked to the policy formulation process, coherence, monitoring and evaluation, modes of cooperation between donors and the government and open/close processes for stakeholder engagement. All this requires a certain degree of institutional capacity, therefore assessment of these elements will also allow conclusions to be drawn about a country's overall institutional capacity.

Do sector coordination mechanisms exist?

The predominant view in the EU is that cyber capacity building needs to follow the whole-of-government and whole-of-society approaches. Adequate coordination mechanisms guarantee that the general policy orientation adopted by a country is based on a broader consensus, with correspondingly higher chances of successful implementation. Coordination across the sector is also a good way to ensure that a specific interest or category of interests is not overemphasised, resulting in a distortion of the developmental orientation of the country/region.

Does the existing policy framework guarantee compliance with human rights commitments?

Finally, the policy needs to be assessed for compliance with international human rights commitments, the principles of rule of law and good governance. Certain elements of this analysis are already addressed at an early stage when the decision on whether to engage with a specific country is first considered. Any doubts about the country's commitment to values promoted by the European Union should be clearly spelled out and the risks associated with a project in such an environment properly assessed.

6.4. Policy dialogue and engagement

Policy dialogue is part of the development assistance toolkit that aims to support a partner's domestic reforms. It complements financial support and technical assistance to achieve results and accountability. It is long term and runs throughout the programme cycle. The main purpose of the dialogue is to explore issues of mutual importance, measure opinions and build shared understandings based on mutual respect, sincerity, openness and freedom of expression.²⁹

Table 3: Different forms of stakeholder dialogues

Types of dialogue	Key stakeholders	Content / Scope	Objective
Policy making – domestic level	Government, private sector and civil society	Sector and national policies, conflict resolution, government accountability, sustainability of policies	Defining issues and option analysis, ensuring credibility of policies by involving stakeholders in design, defining success criteria and scrutinising implementation
Donor – Country (government)	Donor, government, CSOs and private sector	Mutual accountability, indicators for managing support, joint identification of priorities and implementation modalities	Reducing transaction costs, holding government and donors to account, improving development effectiveness, mutual accountability
Donor – donor	Donors / Agencies	Building synergies and division of labour, pooling resources, coherence, sharing of good practices	Reducing transaction costs, increasing coherence of donor response to government's policies, improving aid effectiveness, sharing risks

One key challenge in the area of cyber capacity building is to ensure that dialogue is established with the right partners, i.e. those sections of the government responsible for a specific aspect of cyber policy. There are no one-size-fits-all solutions and institutional arrangements are often made on the basis of historical or political experiences. For example, whereas in some countries the Ministry of Defence might be responsible for cyber-policy coordination – including crime and security – in others its role might be strictly limited. This step is later supported through the stakeholder analysis. Joint learning with other organisations and exchange of information with other donors is indispensable.³⁰

²⁹ K. Schulz, I. Gustafsson, & E. Illes, "Manual for Capacity Development", SIDA, Stockholm, 2005.

³⁰ Ibid.

BOX 24: DIFFERENT MODELS FOR MANAGING CYBER POLICIES

The organisational arrangements of individual countries place a strong emphasis on appointing a co-ordination point at the policy and operational levels. This role can be performed by a specific agency for cybersecurity attached to a co-ordination body (e.g. the French ANSSI), a ministry (Canada, Germany, Netherlands) or in some cases a cabinet office (e.g. Australia, Japan, United Kingdom) or executive (e.g. the 'Cybersecurity Czar' reporting to the White House) to give it more political leverage.

- **Finland** – The Ministry of Finance's Government Information Security Management Board (VAHTI) is responsible for co-ordination with respect to cybersecurity within the government.
- **France** – The National Agency for the Security of Information Systems (ANSSI) is attached to the Secretary General of Defence and National Security (SGDSN), who reports to the Prime Minister.
- **Germany** – The Federal Ministry of the Interior has a lead role in cooperation with other ministries, in particular the Foreign Office and ministries of Defence, Economics and Justice. A National Cyber Response Centre was created to optimise operational cooperation within the government.
- **Spain** – The National Security Department in the Cabinet Office plays the role of secretariat for the National Council for Cybersecurity which gathers all relevant agencies and bodies, including those dealing with Critical Infrastructure Protection, the National Cryptologic Centre and the Cyber Ambassador Office. The National Council for Cybersecurity is also the advisory body to the broader National Security Council, chaired by the Prime Minister.
- **Netherlands** – The Ministry of Security and Justice and a National Cyber Security Centre are responsible for strategic guidance and implementation. A National Cyber Security Council, on the other hand, brings together representatives from the public and private sectors as well as academia to help improve the understanding of cybersecurity developments.

7. Step two – Capacity assessment and needs analysis

Once the public policy and context are better understood, the next step is to define specific objectives of a possible intervention and assess the capacities required to achieve them. Broadly speaking, capacity can be defined as the ability to perform tasks and produce outputs, to define and solve problems and make informed choices.³¹ Capacity building is hence the process by which people and organisations create and strengthen these abilities over time. Because capacity building should be inherently a domestically driven process, external donors and partners can only provide support, meaning the inputs and processes to catalyse or support the capacity of people, an organisation or a network of organisations (e.g. in a sector).³² Part of the capacity assessment is identifying the capacity gap – the difference between existing capacities and those needed to attain the identified objectives. Ideally the capacity and needs assessment should be endogenous, driven by the government or other stakeholders. In cases where such assessments are unavailable and the capacity and needs assessment is performed by external actors, a minimum level of ownership should be ensured by basing the analysis on domestically generated data and through the policy dialogue. Regular consultations with civil society organisations and private sector actors identified through the stakeholder analysis can also serve as valuable sources of information.

7.1. Assessing the existing capacities

Assessing the existing capacity is about taking a snapshot of where a given country or region stands in terms of cyber resilience, which will serve as a baseline from which the progress will be assessed. However, since capacities evolve and depend on a multitude of environmental factors, the assessment cannot be a one-off exercise but needs to be a continuous process. Ideally, capacity assessment should also be a part of a CCB activity to ensure stronger buy-in and involvement of the country/region concerned.

31 European Commission, "Institutional Assessment and Capacity Development: why, what and how?", Luxembourg, 2005.

32 Ibid.

TOOL 7: CHECKLIST FOR CYBER CAPACITY ASSESSMENT

Vision and policies	<ul style="list-style-type: none"> • Is there a comprehensive cybersecurity strategy and/or legal/policy framework to deal with cybercrime and ensure the security of critical national infrastructure? If yes, what do you need to implement them effectively, also in terms of international cooperation? If not, what are the obstacles and what do you need to overcome them? • What is the level of cyber competencies amongst the general population? Are there education and training programmes available? What do you need to improve the overall level of knowledge about cybersecurity risks and building cyber resilience?
Laws and regulation	<ul style="list-style-type: none"> • How does existing legislation influence the capacities of institutions, companies and individuals to innovate and exercise their rights? What do you need to make the legal framework work for the benefit of the citizens? What do you need to minimise digital security risks for companies or individuals?
Institutions and resources	<ul style="list-style-type: none"> • Is there a national entity in charge of preventing, detecting and responding to cyber attacks and/or a body responsible for the implementation of a national cybersecurity strategy? Do you need one and what do you need to make it happen? What do you need to identify and respond more effectively to potential risks? • How does your organisation fit within the broader architecture? Do you think your mandate and resources match the role that your organisation is expected to play in implementing cybersecurity policies? What do you need to do better? • Are responsibilities amongst main stakeholders clearly assigned and understood? What do you need for agencies to work better together? What do you need from other stakeholders? • Is home-grown expertise available? What are the main obstacles to generating a qualified work force, and what is needed to overcome them? What is the level of competence within your own organisation? What do you need to make the best use of existing resources and/or to generate new ones?
Partnerships and cooperation	<ul style="list-style-type: none"> • Is there a framework for certification of internationally recognised cybersecurity standards in the public sector or among critical infrastructure operators? If yes, do you need to improve the performance? If not, what do you need to set it up? • Are there established channels of communication with the public on cyber-related issues to strengthen confidence on the internet? What do you need to communicate and better promote a cybersecurity mind set?

Capacity assessment is a very sensitive process and needs to be designed and carried out in collaboration with the partner countries and organisations.³³ Participatory self-assessments not only contribute to capacity development on their own but also bring forward the acceptance of ownership for the required change process.³⁴ The founding principle of any capacity assessment should be to assume that there are existing capacities that can be built upon. This is important as acknowledging the existence of resources/capacities within a state and society might strengthen both ownership and sustainability. But a capacity needs assessment may also be problematic if capacities are assessed and understood differently by the stakeholders. It is important therefore to explore during the stakeholder analysis what respective actors mean by capacity and how they see power relations that shape it. For instance, governments and civil society or the private sector might assess the distribution of resources/capacity differently, which will also lead to a different understanding of the power relations. An important part of this process – conducted at the moment of stakeholder analysis – is to identify agents of change who are best placed and best qualified to initiate and manage the change process. Such institutions, organisations or individuals can contribute to the achievement of a developmental goal in multiple ways.³⁵ For instance, placing knowledge and information in the hands of new or different stakeholders can change power relations, so that learning can lead to changes in the efficiency of a policy and its effect and therefore be an important component of a capacity-building strategy.

33 K. Schulz, I. Gustafsson, & E. Illes, "Manual for Capacity Development", SIDA, Stockholm, 2005

34 Ibid.

35 S. Otoo, N. Agapitova, and J. Behrens, *The Capacity Development Results Framework: A strategic and results-oriented approach to learning for capacity development*. New York: World Bank Institute, 2009.

BOX 25: MODELS AND INDEXES FOR CYBER CAPACITY ASSESSMENT

Cybersecurity Capacity Maturity Model for Nations (CMM) designed and implemented by the Global Cyber Security Capacity Centre, University of Oxford and its strategic partners. The CMM facilitates the (self-)assessment of the maturity of a country's cybersecurity capacity across five dimensions: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training and skills; legal and regulatory frameworks; standards, organizations, and technology. For each dimension indicators are used to measure cybersecurity maturity along a five-stage spectrum: start-up, formative, established, strategic and dynamic.

For more information, visit the [GCSCC website](#).

The **Global Cybersecurity Index (GCI)** developed by the International Telecommunication Union (ITU) is an initiative to measure the commitment of countries to cybersecurity. GCI focuses on five categories: legal, technical, organizational, capacity building and cooperation. ITU has also published an overview of existing cybersecurity indices, a non-exhaustive list of outstanding surveys, indices and publications from private and public organisations.

For more information, visit the [ITU website](#).

Cyber Readiness Index (CRI) by the Potomac Institute for Policy Studies is designed to inform national leaders on the steps they should consider to protect their countries and potential GDP growth by evaluating each country's maturity and commitment to cybersecurity and resilience. The CRI also defines what it means for a country to be "cyber ready" and documents the core components into an actionable blueprint focusing on seven elements: national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development, diplomacy and trade, and defence and crisis response.

For more information, visit the [Potomac Institute website](#).

National Cyber Security Index (NCSI) by the e-Governance Academy is a global index that measures countries' preparedness to prevent fundamental cyber threats and their readiness to manage cyber incidents, crimes and large-scale crises. The aspects of national cybersecurity covered by the Index include legislation in force, cooperation mechanisms, etc.

For more information, visit the [EGA website](#).

The **Cyber Maturity in the Asia-Pacific Region** report is the flagship annual publication of the ASPI International Cyber Policy Centre. This report assesses the national approach of Asia-Pacific countries to the challenges and opportunities of cyberspace along several dimensions: governance and legislation, law enforcement, military capacity and policy involvement, and business and social engagement in cyber policy and security issues. The 2017 report covers 25 countries.

For more information, visit the [ASPI website](#).

The Software Alliance (BSA) is the organisation behind the EU cybersecurity dashboard, which illustrates the cybersecurity landscape based on criteria such as legal foundations, operational capabilities, public-private partnerships, sector-specific plans and education.

For more information, visit the [Software Alliance website](#).

The analysis of existing capacities should serve not only to provide an overview of the capacities directly linked with the specific objective in question but also those that might be elevated to support it. For instance, while the existence of a CERT is not directly linked to the goal of reducing cybercrime, effective information exchange mechanisms between a CERT and law enforcement might have a significant impact on the capacity to respond to the cybercrime phenomenon. A proper assessment should also address the capacity of actors that will be affected by the action. For instance, in projects aiming at building the capacity of law enforcement agencies, attention must be paid to the impact they will have on privacy and data protection and the capacity of actors in those policy areas, in line with the 'do no harm' and 'do maximum good' principles.

There is no blueprint for how detailed a capacity assessment should be. It depends on the purpose – which decisions will it lead to – and specific circumstances. An assessment can easily drown in insignificant details

and overlook critical, sensitive factors.³⁶ The literature offers several considerations that should guide a needs assessment process:

- Assessment of the environment, i.e. broader structural and institutional factors, and socio-political analysis should draw on local expertise and academia. Except in very small operations, donors should only as a last resort conduct their own process;
- The closer an assessment is to the core of an organisation or sector, the more important it is that the country in question is in charge and committed to the assessment process;
- Broad participation is not always good, in that it may raise expectations and stir up conflicts. On the other hand, it may greatly enhance the transparency of processes and results.³⁷

7.2. Determining desired capacities

Characterised by a higher dynamism than other policy area, cyber capacity building poses particular difficulties with regard to determining a desired level of capacities.³⁸ This is primarily because the technology and threat landscape evolve constantly and require constant adaptation. It is therefore important to set realistic goals for building capacities that support the attainment of the developmental goal within a specific time-frame. Interventions also need to assume that setting an adequate level of capacities is a moving target and requires flexibility. To mitigate risks linked to such a dynamic process, it is important to ensure that feedback loops and monitoring mechanisms are adapted to such a context. Ensuring that the process is locally driven and embedded in a broader national development strategy is one mechanism to ensure effectiveness and sustainability of cyber capacity building.

The approach proposed here suggests the capacity level to be achieved through a concrete action is linked to the existing capacities. This means the level of ambition should reflect the maturity of the capacities already available in a country. The further existing capacities are from the ideal case scenario, the higher the probability that resources needed for attaining that goal are not available. That means that achieving a desired objective and making it sustainable may require a significant commitment from the external partners, which would undermine the very nature of capacity building, where external partners play a secondary role. Furthermore, since capacity building is a domestically driven process, any engagement should aim to build as much as possible on existing capacities, with the external support aimed at taking them to the next level. For instance, assisting a partner country in adjusting its legislation in line with the provisions of the Network Information Security Directive would be unrealistic and would set too high expectations if basic institutions, legal frameworks or the cybersecurity culture are not sufficiently advanced. To be a meaningful planning tool, goals should be specific and linked to the level at which the project or programme will have an impact.³⁹

³⁶ European Commission, "Institutional Assessment and Capacity Development: why, what and how?", Luxembourg, 2005.

³⁷ Ibid.

³⁸ Multiple needs assessments approaches have been developed over year in the field of development. See for instance a review of the most popular capacity assessment tools published by the UNDP (2005) or a description of general tools and techniques for assessing capacity and organisational capacity provided in DFID (2003).

³⁹ K. Schulz, I. Gustafsson, & E. Illes, "Manual for Capacity Development", SIDA, Stockholm, 2005..

TOOL 8: CYBER CAPACITY ASSESSMENT LIST FOR LAYERS AND LEVELS OF CAPACITY

Level	Layer	Questions
Individual capacity:	Vision and policies	<ul style="list-style-type: none"> How are individual roles defined in the developmental objectives and policies?
Abilities	Laws and regulation	<ul style="list-style-type: none"> Do individuals have skills required to put laws into practice, e.g. law enforcement agents, prosecutors, judges?
Needs and performance	Laws and regulation	<ul style="list-style-type: none"> Do individuals have sufficient understanding of the laws and regulation?
Personal attitudes	Laws and regulation	<ul style="list-style-type: none"> Do individuals have sufficient understanding of the laws and regulation?
Psychology	Laws and regulation	<ul style="list-style-type: none"> Do individuals have sufficient understanding of the laws and regulation?
Motivations and incentives	Institutions and resources	<ul style="list-style-type: none"> Do individuals have the right skills to access, gather and disaggregate data and information about cybersecurity threats and possible solutions?
Inclinations	Institutions and resources	<ul style="list-style-type: none"> Do the mechanisms exist (e.g. training, awareness raising) to help individuals acquire the knowledge and understanding of the vision and values that drive the country's cybersecurity policy?
Skills and capabilities	Institutions and resources	<ul style="list-style-type: none"> Do the mechanisms exist (e.g. training, awareness raising) to help individuals acquire the knowledge and understanding of the vision and values that drive the country's cybersecurity policy?
Know-how	Institutions and resources	<ul style="list-style-type: none"> Do the mechanisms exist (e.g. training, awareness raising) to help individuals acquire the knowledge and understanding of the vision and values that drive the country's cybersecurity policy?
Values	Partnerships and cooperation	<ul style="list-style-type: none"> Are there mechanisms in place – government-to-government or public-private partnerships – that strengthen the development of individual capacities?
Organisational capacity:	Vision and policies	<ul style="list-style-type: none"> Are the institutional roles, mandates and decision-making procedures defined clearly enough to allow for articulation of capacity assets and needs?
Practices	Vision and policies	<ul style="list-style-type: none"> Are the institutional roles, mandates and decision-making procedures defined clearly enough to allow for articulation of capacity assets and needs?
Roles	Vision and policies	<ul style="list-style-type: none"> Do the institutional practices and norms reflect the overall vision of the country?
Mandate	Vision and policies	<ul style="list-style-type: none"> Do the institutional practices and norms reflect the overall vision of the country?
Decision-making structures	Laws and regulation	<ul style="list-style-type: none"> Do organisations exist to oversee laws and regulatory framework in the cyber domain? Do laws and regulations provide effective incentives? Are the roles of organisations and institutions in the field of cyber-resilience clearly prescribed? Are they adequately resourced?
Divisions of labour	Laws and regulation	<ul style="list-style-type: none"> Do organisations exist to oversee laws and regulatory framework in the cyber domain? Do laws and regulations provide effective incentives? Are the roles of organisations and institutions in the field of cyber-resilience clearly prescribed? Are they adequately resourced?
Sharing of responsibilities	Laws and regulation	<ul style="list-style-type: none"> Do organisations exist to oversee laws and regulatory framework in the cyber domain? Do laws and regulations provide effective incentives? Are the roles of organisations and institutions in the field of cyber-resilience clearly prescribed? Are they adequately resourced?
Methods of management and means of functioning	Institutions and resources	<ul style="list-style-type: none"> Are institutional responsibilities and decision-making procedures defined in a clear way? Are the mandates supported with adequate resources?
Use of resources	Institutions and resources	<ul style="list-style-type: none"> Are institutional responsibilities and decision-making procedures defined in a clear way? Are the mandates supported with adequate resources?
Incentives	Partnerships and cooperation	<ul style="list-style-type: none"> Do the existing policy-making mechanisms contribute to the whole-of-government and whole-of-society approach?
Enabling environment:	Vision and policies	<ul style="list-style-type: none"> Does the legal and institutional environment provide conditions that facilitate information sharing and support cooperation?
Society	Vision and policies	<ul style="list-style-type: none"> Does the legal and institutional environment provide conditions that facilitate information sharing and support cooperation?
Laws	Vision and policies	<ul style="list-style-type: none"> Does the legal and institutional environment provide conditions that facilitate information sharing and support cooperation?
Policies	Vision and policies	<ul style="list-style-type: none"> Does the cultural and value system in the country promote cybersecurity?
Procedures	Vision and policies	<ul style="list-style-type: none"> Do the adopted strategies and policies and the underpinning visions contribute to the development of the culture of cyber resilience by creating incentives, motivation, etc.?
Norms	Vision and policies	<ul style="list-style-type: none"> Do the adopted strategies and policies and the underpinning visions contribute to the development of the culture of cyber resilience by creating incentives, motivation, etc.?
Standards	Laws and regulation	<ul style="list-style-type: none"> Is there social acceptance for laws and regulation in the cyber domain?
Power structures	Laws and regulation	<ul style="list-style-type: none"> Does the general organization of the country provide guarantees for the rule of law and good governance needed to implement any laws or regulatory frameworks?
Systems	Laws and regulation	<ul style="list-style-type: none"> Does the general organization of the country provide guarantees for the rule of law and good governance needed to implement any laws or regulatory frameworks?
Environment	Laws and regulation	<ul style="list-style-type: none"> Does the general organization of the country provide guarantees for the rule of law and good governance needed to implement any laws or regulatory frameworks?
Culture	Institutions and resources	<ul style="list-style-type: none"> Are checks and balances in place to ensure that different interests and value systems regarding cyber resilience are represented?
	Partnerships and cooperation	<ul style="list-style-type: none"> Does the institutional and legal set up in the country provide opportunities for participation in the policy-making process?

8. Step three – Formulating a logic of intervention

Analyzing existing and desired capacities helps to identify a capacity gap preventing a country or region from reaching a higher level of development. Identification of an existing capacity gap also allows for assessing whether the stated goals are achievable with the available inputs and given timeframe.⁴⁰

On the basis of the policy analysis, identification of stakeholders, capacity assessment and policy dialogue with partner countries and other stakeholders, it is possible to formulate a plan for capacity building. While designing an intervention, it is important to keep in mind that external actors play a supporting role and their actions should primarily facilitate and catalyse indigenous processes. A good plan builds on existing assets to address gaps identified in a capacity assessment⁴¹ and is essential to the success of any development enterprise.⁴² Therefore, the external actor should first aim to identify domestic projects and programmes that may provide lessons for the planned action or for which synergies and complementarity could be created. Past experiences in capacity building demonstrate that overconfidence in transferring solutions from rich countries instead of using the specific local situation as the point of departure may result in failure.⁴³

Based on previous experience and engagements, external actors might contribute with insights into potential actions that could multiply the effects of capacity-building initiatives. In some instances it might be important to define short-term activities to help generate support while the foundation for long-term objectives is being laid. Ideally, therefore, the plan for support of capacity building should contain a combination of quick-impact initiatives and medium- to long-term ones. Sequencing is needed also because available resources are usually limited. The inherent risk is that the focus on quick gains becomes dominant at the expense of more strategic, longer-term objectives.⁴⁴ For instance, recurrent training and awareness-raising initiatives for police officers might undermine broader initiatives aimed at strengthening the capacity of the justice system altogether. Since the process of setting priorities is inherently political, it should be managed carefully and transparently, with the involvement of relevant stakeholders to avoid resistance to change during implementation.

Another step in formulating the plan to support capacity building – after the objective has been defined – is outlining the change in the targeted capacity indicators that the project intends to achieve. Experience suggests that the wording of the objective should be very specific. It should make clear what the programme will do, why, for whom and how the implementers and other stakeholders will know if it succeeded.⁴⁵ The capacity development objective provides the basis for a logical flow that constitutes the foundation of the intervention logic. This flow connects the objective to the capacity factor indicator to be improved and determines the appropriate methodological approach for learning as well as the capacity development activities to be designed.⁴⁶ Indicators should be set to monitor progress of the implementation itself, the expected results (outcomes) and the achievement of objectives (impact). Note that outcome and impact indicators defined within the programme are likely to be relevant after its implementation. The process itself of defining progress indicators is useful as a way of generating policy discussion, enhancing monitoring and evaluation and as a learning exercise.

Designing an intervention logic requires answering what makes us think that the intended change will really happen. That calls for identifying the key assumptions of the intervention logic and the evidence underpinning them. In addition, an intervention logic answers the following questions: What outcomes are sought, for whom and why? What has been done in this field before to build on? How change might happen, over what period of time, based on what assumptions? How will we measure progress and evaluate achievements? What indicators measuring acquired or built capacities do we need, and what are the risks? It comprises two main elements: Theory of Action (i.e. what steps need to be taken to achieve the results) and Theory of Change (i.e. why and how change might happen). The process of designing an intervention logic comprises three main steps: analysis of context and issues, exploration of change processes and underlying

40 Ibid.

41 Davis, T. Lemma & K. Wignaraja, "Capacity development. A UNDP primer", United Nations Development Programme, New York, 2009.

42 Ibid.

43 K. Schulz, I. Gustafsson, and E. Illes, 2005.

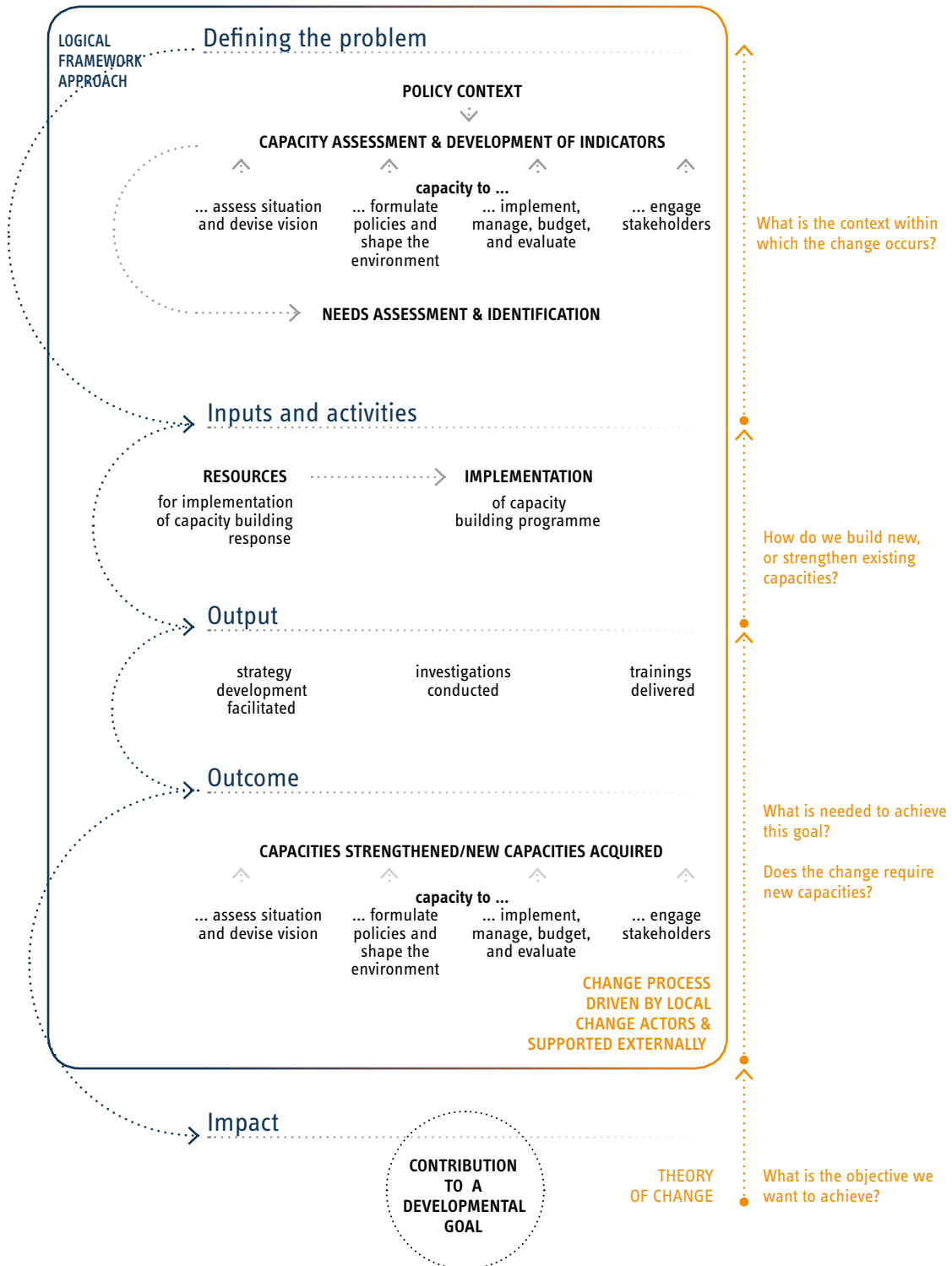
44 European Commission, "Institutional Assessment and Capacity Development: why, what and how?", Luxembourg, 2005.

45 S. Otoo, N. Agapitova, & J. Behrens, *The Capacity Development Results Framework: A strategic and results-oriented approach to learning for capacity development*, New York, World Bank Institute, 2009.

46 Ibid.

assumptions, and assessment of the evidence. The intervention logic should take into account the capacity gap identified earlier.

FIGURE 17: Combining the Legal Framework Approach with the Theory of Change



TOOL 9: A GRID FOR DETERMINING THE EXISTING LEVEL OF CYBER CAPACITY

	Vision and policies	Laws and regulation	Institutions and resources	Partnerships and cooperation
Advanced	A country has a well-defined and clearly articulated vision of cyberspace reflecting the needs and objectives of all stakeholders and expressed in a national strategic framework.	A country has a comprehensive regulatory and legal framework to strengthen state and societal resilience to malicious activities in cyberspace (esp. cybercrime), in line with international legal standards.	Responsibilities for the implementation of the national vision for cyberspace are clearly prescribed and supported with adequate human and financial resources.	Contributes to and shapes global governmental and multi-stakeholder cybersecurity initiatives.
Developed	A country has a well-defined and clearly articulated vision of cyberspace reflecting the needs and objectives of all stakeholders and expressed in a national strategic framework.	A country has a comprehensive regulatory and legal framework to strengthen state and societal resilience to malicious activities in cyberspace (esp. cybercrime) inspired by but not necessarily fully compliant with international legal standards.	Responsibilities for the implementation of the national vision for cyberspace are clearly prescribed with some resources provided.	Actively participates and contributes to global governmental and multi-stakeholder cybersecurity initiatives.
Developing	A country has a patchwork of policies for cyberspace but without a clearly defined coordination mechanism.	A country has a patchwork regulatory and legal framework to deal with certain types of vulnerabilities.	Some institutional capacities and resources exist to implement existing policies as well as regulatory and legal frameworks, with limited resources.	Participates in global governmental and multi-stakeholder cybersecurity initiatives.
Basic	A country has some policies for cyberspace but without a clearly articulated vision.	A country does not have or has a narrowly defined regulatory and legal framework to deal with certain types of vulnerabilities.	Institutional capacities to implement existing policies as well as regulatory and legal frameworks are weak and resources insufficient.	Participates in selected regional and global governmental and multi-stakeholder cybersecurity initiatives.

8.1. Possible actions

The set of objectives for capacity building and their sequence is tailored to the capacity factors that are to be improved, to agents of change who are to make those improvements, and to the envisioned change process.⁴⁷ Based on experience from development projects, some specific outcomes essential to all capacity-building efforts are raised awareness, enhanced skills, improved consensus and teamwork, fostered collaboration, formulated policy or strategy and implementation thereof.⁴⁸ Each of these outcomes and objectives can be achieved through activities undertaken at the level of an individual, organisation or environment.

47 S. Otoo, N. Agapitova, & J. Behrens, *op.cit.*

48 *Ibid.*

TOOL 10: EXAMPLES OF POSSIBLE ACTIONS AND RESULTS STATEMENTS

Focus of possible actions	Potential result statements
Raised awareness	<ul style="list-style-type: none"> • Awareness raising campaigns delivered • Participant understanding of an issue or situation improved • Participant attitude improved • Participant confidence improved • Participant motivation improved
Enhanced skills	<ul style="list-style-type: none"> • New skills/knowledge acquired • New skills/knowledge applied • Training on technical skills and competences delivered • Training on leadership skills and competences delivered • Education and scholarship schemes provided • Support for cybersecurity research provided
Improved consensus / teamwork	<ul style="list-style-type: none"> • A coordinating body for cybersecurity issues appointed • Developed standard operating procedures (SOPs): technical, administrative, procedural measures for network management and protection • Discussion initiated/resumed/activated • Participatory process initiated/expanded • Action steps/plan formulated/improved • Collaboration increased/improved
Fostered coalitions / networks	<ul style="list-style-type: none"> • Mentoring and peer-to-peer learning put in place • A 24/7 point of contact appointed and procedures for interagency coordination strengthened • Public-private partnership arrangements elaborated • Risk assessment and management exercises organised • Discussion initiated/resumed/activated • Participatory process initiated/expanded • Informal networks created/expanded • Formal partnerships or coalitions created/expanded
Formulated policy / strategy	<ul style="list-style-type: none"> • National cybersecurity strategy formulated and/or implemented • Cybercrime and cybersecurity legislation adopted: substantive and procedural laws, criminalisation of certain acts, ensuring respect of fundamental freedoms, inclusion of positive/negative incentives in private and administrative laws • Stakeholders involved in process • Policy/strategy needs assessment completed • Stakeholder agreement reached • Action steps/plan formulated • Monitoring and evaluation plan designed • Policy/reform/strategy/law proposed to decision makers
Implemented strategy / plan	<ul style="list-style-type: none"> • Incident response capabilities / CSIRTs established • Implementation steps formulated and initiated • Monitoring and evaluation initiated • Implementation know-how improved • Budgetary resources for CCB allocated

Source: Developed on the basis of the Capacity Development Results Framework, World Bank.

8.2. Result chain and indicators

The use of indicators allows for performance management and enhances possibilities for following up the operational process, acquiring relevant information and contributing to learning.⁴⁹ Indicators are quantitative or qualitative variables that can be observed to provide information on the progress of a specific project or programme over time and at all levels:

49 K. Schulz, I. Gustafsson, & E. Illes, 2005.

- Output indicators provide a measure of the direct products that the planned activities are expected to generate. This includes the number of trainings organised, publications delivered, participants in the events, new courses offered, high-level officials who received written products, etc.
- Outcome indicators measure the direct effect on the political, social or economic spheres as well as potential changes in perception, behaviour or engagement of the target groups. The indicators need to be chosen so as to reflect the ties between outputs and outcomes. Indicators at this level include for instance an improvement in the performance of participants in the training sessions.
- Impact indicators measure the degree to which a project or programme have contributed to the overall stated objective. These include an increase in economic growth, improvement of the rule of law in cyberspace, etc.

8.3. Lessons learned

Design and implementation of an intervention is expected to build on lessons (positive and negative) from similar experiences and good practices identified on previous occasions. In recent years, the EU and other donor organisations have engaged in cyber capacity-building efforts. The timing is ripe, therefore, to start learning from those engagements to avoid reinventing the wheel and to use scarce resources in a more efficient and effective way. The international community has committed significant resources to address the problem of information fragmentation. In 2017, the Global Forum on Cyber Expertise – comprising over 60 partners representing governments, international organizations and private companies – published Global Good Practices in policy areas such as national capacity assessment, CERTs/CSIRTs, incident capture and analytics, critical-information infrastructure protection, cybersecurity awareness and standards.⁵⁰ Valuable lessons can be also drawn from the EU's engagement in cyber capacity-building projects. For instance, the EU's long-standing partnership with the Council of Europe has resulted in many projects with regional and global scope.⁵¹

Important lessons can be also drawn from the EU's engagement in the promotion of digital technologies for development:

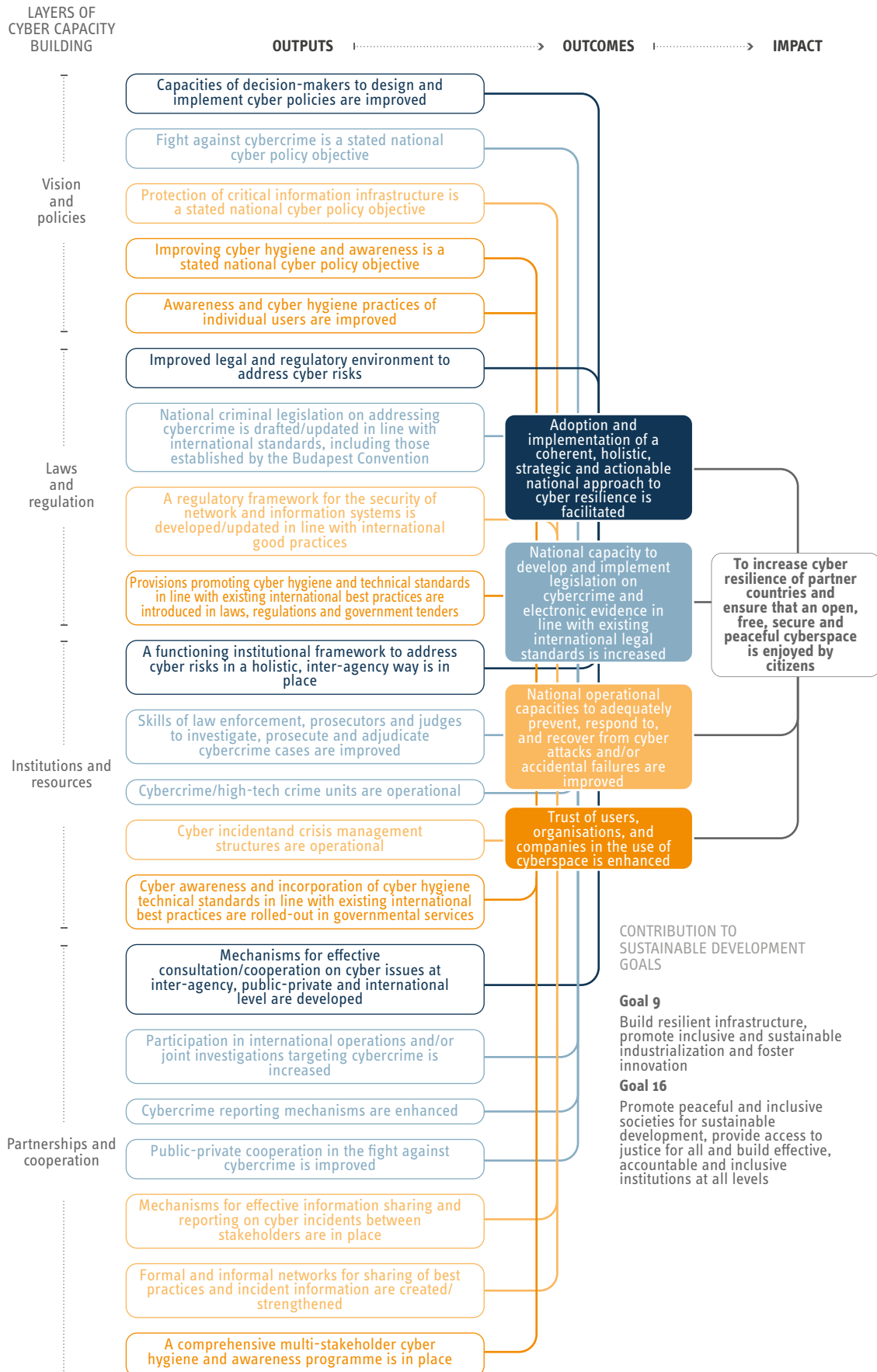
- A series of infrastructure-network projects aimed at connecting European research and education institutions with peer institutions in partner countries have evolved into research collaboration platforms: E@PConnect for the Eastern Partnership countries, EUMEDCONNECT in the Mediterranean, AfricaConnect, CAREN2 for Central Asia, RedClara for Latin America, and C@ribnet in the Caribbean.
- EU initiatives have contributed to the promotion of creativity and cultural diversity in the digital environment such as 'Creative Tracks' – a dynamic online platform connecting young entrepreneurs in cultural and creative sectors in the EU and developing countries.

Several projects focus on policy harmonisation through support for regulatory reforms and creating appropriate frameworks with independent national regulators, developing market liberalisation and encouraging private sector investment. These are most often more technical, but vigilance is necessary to ensure that such initiatives adequately address potential digital risks.

50 See Global Good practices identified by the GFCE community

51 See Council of Europe, "Cybercrime – Worldwide Capacity Building".

TOOL 11: EXAMPLES OF RESULT CHAIN AND INDICATORS FOR CCB



Source: The Capacity Development Results Framework. A strategic and results-oriented approach to learning for capacity development, The World Bank Institute.

TOOL 12: MAPPING OF SOURCES FOR IDENTIFICATION OF GOOD PRACTICES AND LESSONS

The **Global Forum on Cyber Expertise** provides a platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. Together with partners from NGOs, the tech community and academia, GFCE members develop practical initiatives to build cyber capacity. GFCE members and partners develop joint initiatives to strengthen cybersecurity, fight cybercrime, protect online data and support e-governance.

For more information, visit the [GFCE website](#).

The GFCE Inventory provides a central reference point for international and regional capacity-building efforts. It documents programmes, projects and initiatives by international and regional organisations, governments, companies and NGOs that aim to enhance cybersecurity capacity worldwide. The **Cybersecurity Capacity Portal** of the Global Cyber Security Capacity Centre, University of Oxford, which hosts the GFCE Inventory is a one-stop-shop for cyber capacity-related information, including the ongoing projects, initiatives, events, publications. For more information see the Cybersecurity Capacity Portal.

In 2017, the GFCE published Global Good Practices focused on the following topics:

- National Cyber Security Assessments
- National Computer Security Incident Response
- Incident capture and analytics
- Critical Information Infrastructure Protection
- Legal Frameworks
- Law enforcement in cyberspace
- Cyber Security Awareness
- Standards

For more information, visit the [GGP website](#).

The World Bank's **Digital Development Partnership** (DDP) helps operationalize the 2016 World Development Report on Digital Dividends and offers a platform for digital innovation and development financing. The DDP brings public and private sector partners together to catalyse support to developing countries in articulating and implementing digital development strategies and plans. This partnership makes digital solutions available to developing countries with an emphasis on the following areas: Data and indicators; Digital economy enabling environment; Cybersecurity; Internet access for all; Digital government; Mainstreaming digital services, solutions, and platforms.

For more information, visit the [DDP website](#).

The **Global Centre for Cybersecurity** is an autonomous organization under the auspices of the World Economic Forum. The aim of the centre is to establish a global platform for governments, businesses, experts and law enforcement agencies to collaborate on cybersecurity challenges. The centre focuses on: consolidating existing cybersecurity initiatives of the World Economic Forum; establishing an independent library of cyber best practices; helping partners enhance knowledge on cybersecurity; working towards an appropriate and agile regulatory framework on cybersecurity; serving as a laboratory and early-warning think tank for cybersecurity scenarios.

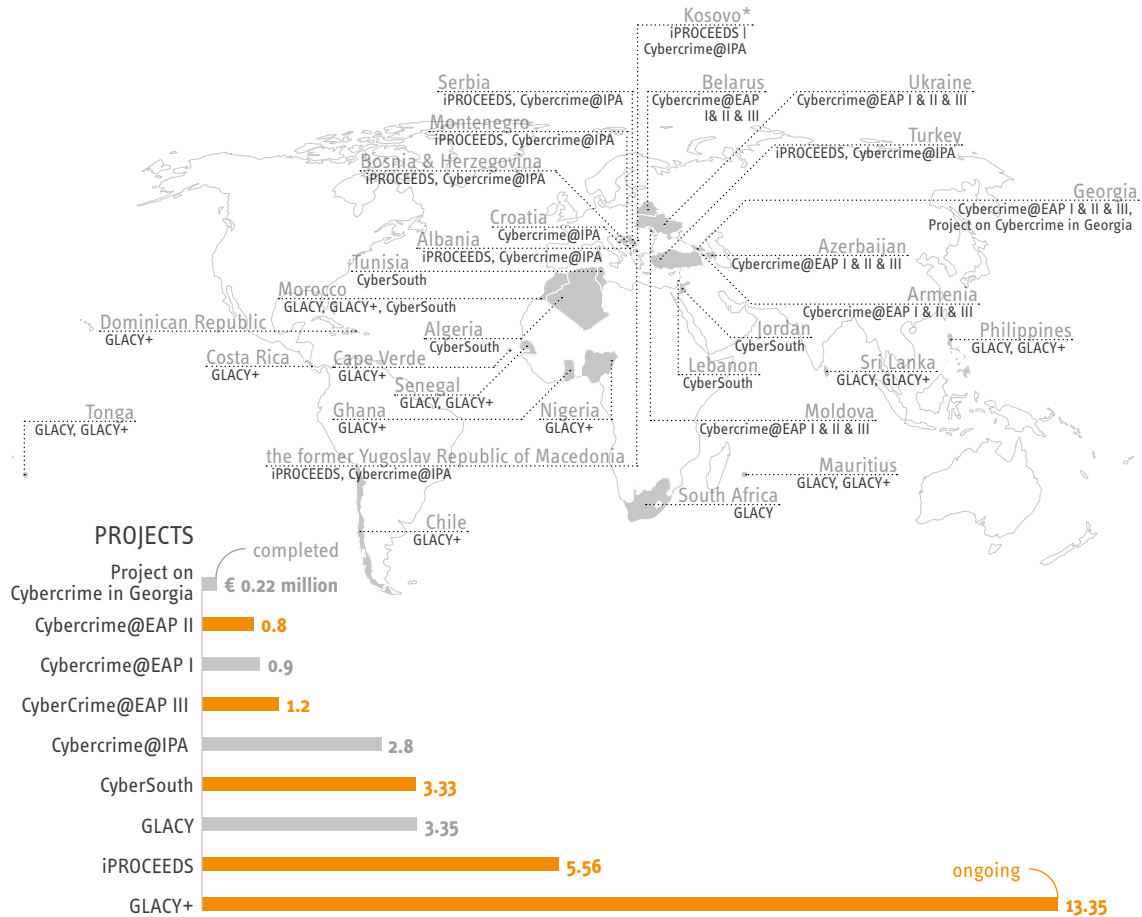
For more information, visit the [WEF website](#).

8.4. Complementarity and synergy with other actions

Like in other policy areas, one of the main challenges of cyber capacity building is the lack of coordination between agencies and donors. The **2018 Council Conclusions on EU External Cyber Capacity Building Guidelines**, recognise that the increasing number of stakeholders globally involved in this field '*creates opportunities for synergies and burden-sharing but also poses challenges in terms of coordination and coherence*' and encourages the EU and its Member States '*to continuously engage with key international and regional partners and organisations as well as with civil society, academia and the private sector in this field with the aim of avoiding duplication of effort given the limited resources*'. Several coordination and information-exchange platforms exist, with the **Global Forum on Cyber Expertise** having the coordination of capacity-building efforts at the core of its mandate by pulling together information about ongoing initiatives, best practices, guidelines, etc. At the EU level, the 2017 Joint Communication on Building a Strong

Cybersecurity for the EU, included a proposal to establish an **External Cyber Capacity Building Network** that shall endeavour to mobilise the collective expertise of EU Member States for EU-funded external cyber capacity-building programmes, undertake mapping of the EU and Member States relevant activities, and support effective cooperation and coordination with other actors.

FIGURE 18: Projects on cybercrime implemented by CoE with EU funding



*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

Data: European Commission.

Aside from the coordination difficulty, another challenging dimension in relation to capturing the breadth of cyber actions related to the very broad range of cyber-related policies, therefore it is often difficult to comprehensively capture projects or initiatives that may not be **cyber-specific** but would be highly **cyber-relevant**. For instance, projects aimed at improving IT infrastructure in a partner country do not fall under the scope of 'cyber capacity building' but would most often be accurately captured as digitalisation projects. However, they should have cybersecurity elements embedded. Moreover, given that an increasing number of services rely on internet-based platforms, crime also increasingly gains a cyber flavour. Numerous projects that focus predominantly on building capacity of law enforcement agencies, or the security sector more broadly, are also receiving basic training in the domain of cybercrime and electronic evidence, even though the project's main objective might refer broadly to the rule of law or justice system. As a consequence, monitoring all engagements with cyber capacity-building elements is complicated. Nonetheless, it is important to make sure that any planned intervention is designed following a mapping of the existing initiatives and also includes a **'cyber-specific' or 'cyber-relevant' marking**, as appropriate, to facilitate reporting and potential synergies with other actions. Most notably, cyber-relevant capacity-building actions would entail those addressing human rights freedoms online; internet governance; the development of ICT infrastructure, policies and regulations; as well as justice and security sector reform programmes, including on countering terrorism and organised crime, with a strong digital evidence and forensics component.

8.5. Cross-cutting issues

The proposed actions need to integrate the human rights, gender, and environmental considerations. In the field of cyber capacity building, all three areas play a very important role as they make an important contribution towards empowering specific communities - human rights defenders, civil society organisations – or demographic groups, in particular women and youth.⁵²

Gender

A growing body of research and analysis points to a gender gap in access to the internet. Equally worrying is the data about women's access to cybersecurity professions. It is therefore essential that any cyber capacity-building intervention promotes women's and girls' participation with the ultimate aim of promoting equal access and inclusion in cyberspace. For this reason, specific indicators should be developed in the logic of intervention. This dimension is important also given that it is women who usually benefit most from access to services and information, which allows them to undertake economic activity and consequently improve the situation of entire households.

Moreover, cyber-violence against women and girls is emerging as a global problem with serious implications for societies and economies around the world. Cyber violence against women and girls (cyber-VAWG) is under-reported both in western countries with high internet penetration as well as in the Global South. This emerging trend requires a gender sensitive development of the response to cybercrime, not only at the stage of legislation but also in the investigation, prosecution and adjudication of crimes entailing cyber-VAWG.

Tailored monitoring and reporting can help demonstrate how the intervention is pursuing gender equality in its implementation, therefore ensuring that there are mechanisms to capture gender-disaggregated data should be a considered from the outset in cyber capacity-building actions.

Environment and climate change

Various EU legal and policy documents call for integrating the environment and climate change issues in EU international cooperation and development programmes, with the aim of promoting sustainable development. The link between the environment and cybersecurity or ICT more broadly has not been fully explored. Some obvious impacts result from infrastructure projects or the extraction of natural resources and rare earth minerals for manufacturing, as well as the energy needed to operate server rooms, etc. Guidelines published by the European Commission on 'Integrating the environment and climate change into EU international cooperation and development' offer a set of concrete tools that might prove useful in integrating environmental concerns into cyber-related policies.⁵³

8.6. Cyber resilience as a cross-cutting issue: mainstreaming

The development of e-government and the application of ICT in various areas of human activity are believed to be important instruments in the pursuit of sustainable development. Governments across the world are devoting substantial resources to upgrading their infrastructure, telecommunication systems or energy networks using elements of ICT. This makes it increasingly difficult to treat cybersecurity as a distinct policy area. The transformational power of ICT can be easily undermined if risks associated with mobile and internet tools in particular are not adequately managed. Disruptions may have disastrous consequences so the need to ensure robustness against cyber-attacks is of primary importance. At the same time, the right policy environment for ICT roll-outs must be created and policy reforms empowering citizens and businesses alike must be addressed.

Over the last 10 years, the European Union has devoted approximately €350 million to digital initiatives in EU partner countries, with over €110 million allocated for on-going digital projects. Countries in the European

52 OECD, "Mainstreaming cross-cutting issues – 7 Lessons from DAC Peer Reviews", Paris, 2014.

53 European Commission, "Tool and Methods Series: Guidelines n°6 - Integrating the environment and climate change into EU international cooperation and development. Towards sustainable development", Brussels, 2016.

Neighbourhood received 31%, Africa 19%, Asia 43% and Latin America 7%.⁵⁴ On the basis of existing policies and partnerships, the Commission is mainstreaming digital technologies across four main priority areas:

- Promoting access to affordable and secure broadband connectivity and to digital infrastructure;
- Promoting digital literacy and skills;
- Fostering digital entrepreneurship and job creation;
- Promoting the use of digital technologies as an enabler for sustainable development.⁵⁵

TOOL 13: CHECKLIST FOR CROSS CUTTING ISSUES

Gender assessment

Context

- What gender equality issues exist in the country and how they relate to the proposed action? For instance, what is the proportion of females employed in the field of cybersecurity, cybercrime, etc.?

Policy

- Is there a national gender strategy and to what extent does the proposed action support national gender strategy?
- Are the key gender policy priorities integrated in government cybersecurity programmes?

Intervention

- How does the project/action tackle gender equality issues?
- Which gender-sensitive indicators does the proposed action intend to use to monitor progress?
- Will the data generated by the proposed action be disaggregated by sex and age?

Gender equality assessment for cyber-related projects should adequately reflect the fact that most of the cyber-related professions are currently mostly occupied by men and actions promoting more women in cyber-related professions should be encouraged. This is particularly the case of actions supporting the capacity development in law enforcement.

Rights-based approach assessment

Context

- What are the main issues regarding human rights linked to cyber capacity building? What are the proposed measures to tackle them?
- What is the overall human rights record of a country and how does the situation relates to the proposed action?

Policy

- Within the context of cyber capacity building, are there existing or potential gaps between human rights standards and day to day reality identified, including human rights concerns raised by international treaty bodies, negative development trends potentially leading to human rights violations; evidence of disparities to the detriment of vulnerable groups?

Intervention

- Has the capacity of rights holders/vulnerable groups to claim their rights in the context of the proposed action been assessed?
- Has the capacity to state institutions to fulfil their duties and responsibilities with regard to rights holders/vulnerable groups been assessed?
- Do the objectives of the proposed action ensure that the rights of vulnerable groups and inequality and discrimination issues are taken into account?

54 European Commission, "Commission Staff Working Document - Digital4Development: mainstreaming digital technologies and services into EU Development Policy", SWD(2017) 157 final, Brussels, 2 May 2017.

55 Ibid.

Human rights assessment for cyber-related projects should adequately address the following issues in particular: privacy, freedom of expression, freedom of association, discrimination, and fair trial rights. Particular attention should be paid to compliance with the provisions of Article 15 of the Budapest Convention on Cybercrime and UN treaties.

Environmental and climate related screening

Context

- What are the main environmental issues in the country?
- What is the overall impact of cyber-related policies on the country's environmental policies?

Policy

- What are the main issues and/or opportunities regarding environment, biodiversity and climate change linked to cyber capacity building?

Intervention

- How does the project/action tackle environment-related issues?

Environmental and climate related issues are usually addressed superficially in the assessment of cyber capacity-building projects. However, potential impact of cyber projects on environment and climate cannot be ignored, in particular with regard to the energy consumption linked to the introduction of some solutions (e.g. large data bases, amount of digital data generated, etc.). Introduction of new technologies and their secure use might also have positive impact on the environment. For instance, the use of sensors for the emissions controls, etc. In that sense, there is also a direct link between security of such systems and a potential impact of their malfunctions on the environment (e.g. release of toxic or radioactive substances, etc.).

This should be read in conjunction with the *DG DEVCO Template for the assessment of cross cutting issues*.

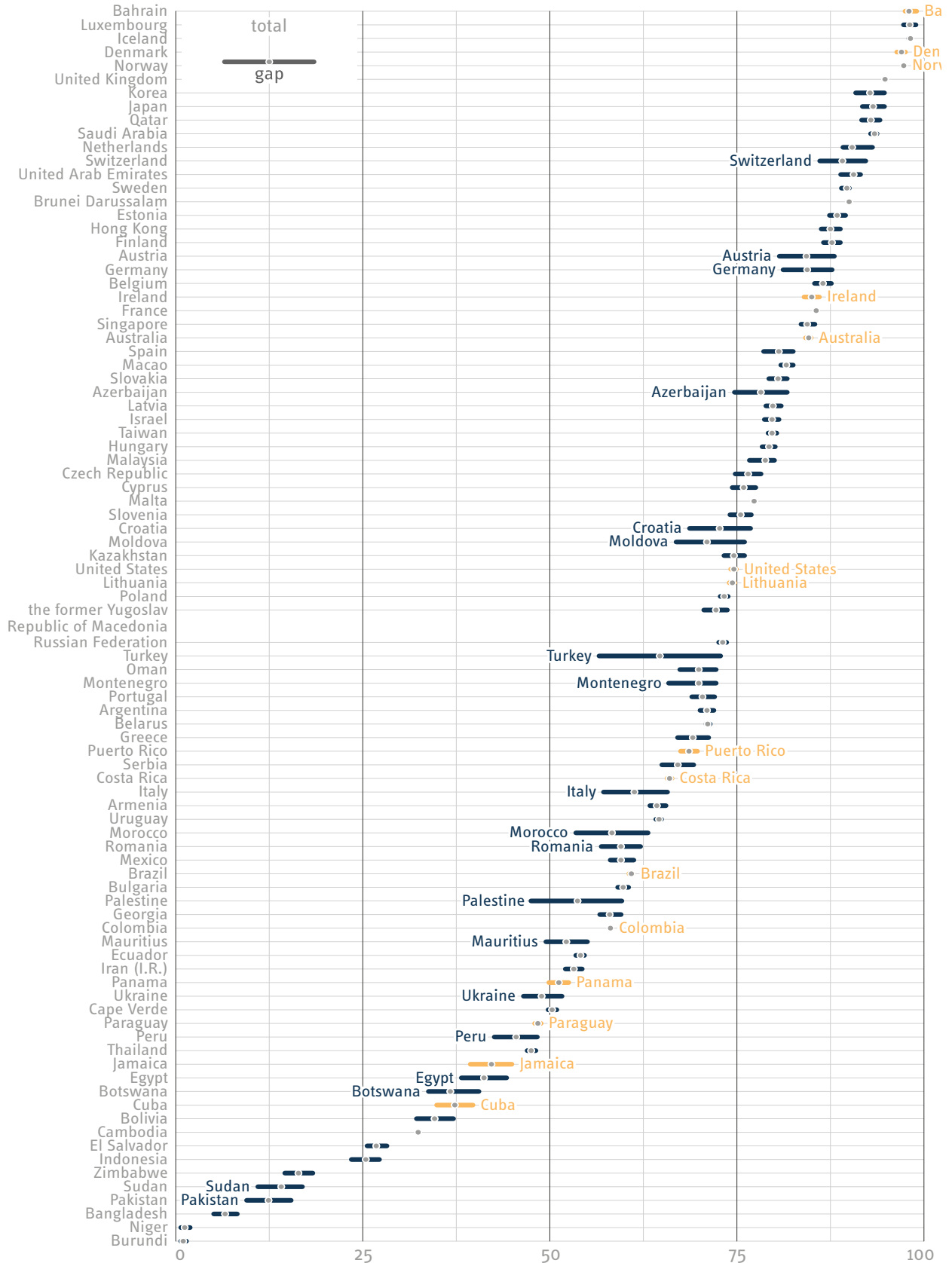
The increasing reliance on ICTs implies that unless properly addressed, vulnerabilities in the cyber domain might impede economic and human development in affected areas. It is important therefore, for any project with an ICT component to properly assess the potential impact of cyber insecurity. That could be included under specific risks to the project. The challenge is even more urgent given the focus on digitalisation as a main pillar of EU engagement with external partners. Recognising that resources are limited, the Commission has prioritised Africa as the region where both the digital divide and opportunities are the greatest. In its 2014 Communication 'A stronger role of the private sector in achieving inclusive and sustainable growth in developing countries', the Commission highlighted the importance of digital technologies '*as a tool for achieving the financial inclusion of the poor, especially in Africa where they are already dramatically changing the financial landscape*'.⁵⁶

The **EU's 2017 Digital4Development framework** elaborated on this challenge, noting that '*due to the cross-sectorial nature of digitalisation, promoting cybersecurity as a transversal issue is essential in development cooperation, namely through incorporation of cybercrime components in criminal justice sector reform programmes as well as integration of cyber resilience elements in projects dealing with critical infrastructures (ex. ICT, transport, energy) and digital/e-government initiatives*'. In fact, even though this Operational Guidance is mainly for programmes that have a cyber-specific focus, it is also intended to provide guidance on actions that have cyber-relevant dimension and activities. The rationale is to promote a holistic and consistent policy approach, taking in to account that external capacity-building programmes that touch on justice and security, in particular in fighting terrorism and organised crime, often address aspects of electronic evidence and cyber-enabled systems, infrastructure and services.

⁵⁶ European Commission, "Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A stronger role of the Private Sector in Achieving Inclusive and Sustainable Growth in Developing Countries", COM(2014) 263, Brussels, 13 May 2014.

FIGURE 19: Internet access by gender

- 18 out of 90 countries, **more women** than **men** use the internet.
- 20 countries, the gap exceeds 5 %points.



Data: ITU, 2017.

9. Step four – Implementation, including monitoring and reporting

All the thinking, planning, assessing, analysing and designing is tested in implementation - bringing a project to life and ensuring that it follows a desired path. This is also the stage where the involvement of the partner is most relevant. Partner countries feel a strong sense of ownership of initiatives when their own systems and procedures are used for implementing programmes and projects.⁵⁷

9.1. Performance and results monitoring

Monitoring is intended to be continuous and flexible to allow for adjustments when faced with changed needs or priorities, or simply as the understanding of the situation evolves.⁵⁸ Indicators and benchmarks for success are usually developed when the programme or project are formulated. Given the broad scope of potential cyber capacity building and the highly contextualised nature of any external support, designing a set of universal indicators is not only difficult but may also be counterproductive. Therefore, it is better to choose indicators that are closely linked to a specific project.

One of the main challenges in establishing indicators in general is ensuring that they are closely tied to the results. This is because of the problem with direct contribution, whereby the causal link between specific activities and outcomes is not always easy to establish. Other factors may intervene, such as the political and economic environment or support from other donors or actors. For instance, a programme with an overall objective defined as strengthening cyber resilience may find it difficult to monitor the progress and establish the direct causal link with a broad range of activities focused on, among others, training of law enforcement officers or passing cybercrime legislation. While monitoring the results on the level of activities is definitely an easier task, it does not necessarily allow for an adequate evaluation of the relevance, efficiency and effectiveness.

A result framework is used to measure results achieved against strategic development objectives articulated at different levels – from outputs to outcomes and impact.⁵⁹ Several Directorates-General within the European Commission have developed their own result-oriented frameworks. For example, DG International Cooperation and Development developed the **EU Result Framework** (EURF) to strengthen its capacity to monitor and report results, thus enhancing accountability, transparency and visibility of EU aid, as articulated in the 2011 Agenda for Change Communication.⁶⁰ Another example is the **Partnership Instrument Monitoring System** (PIMS) by the Service for Foreign Policy Instruments, which is designed to support PI stakeholders in monitoring the results of PI actions. The PI focuses on processes and the political nature of the results. The DG for Neighbourhood and Enlargement Negotiations (DG NEAR) has developed its own Guidelines linking planning/programming, monitoring and evaluation.⁶¹ Three converging sources for DG NEAR evaluations are the regulations governing external action in the framework of ENI and IPA II, the Better Regulation Guidelines, and the OECD-DAC criteria.⁶²

The EU Results Framework (EURF)

In the Agenda for Change and the related Council Conclusions, the EU and the Member States committed themselves to promote common, results-based approaches to strengthen their capacity for monitoring and evaluating development results. The Busan High-level Forum specifically called for the promotion of results and mutual accountability agreements. Furthermore, it stressed the central role of developing countries in drafting such frameworks, which should respond to their needs and be grounded in their development policies. Recognising the importance of demonstrating results and improving effectiveness in support of stronger development outcomes, a number of donors, including the European Union, have designed and implemented specific results frameworks.⁶³ The EURF tool is based on three levels, with the focus on:

57 Davis, T. Lemma & K. Wignaraja, "Capacity development. A UNDP primer", United Nations Development Programme, New York, 2009.

58 S. Otoo, N. Agapitova, and J. Behrens, 2009.

59 The use of input-output-outcome-impact corresponds to the internationally practices OECD-DAC results terminology.

60 European Commission, "Commission Staff Working Document - Launching the EU International Cooperation and Development Results Framework", SWD(2015) 80 final, Brussels, 26 March 2015.

61 European Commission, "Guidelines on linking planning/programming, monitoring and evaluation", DG NEAR, Brussels, July 2016.

62 The overall objectives and priorities are defined, among others, in the Annual Enlargement package and Budget Support Guidelines – Programming, Design and Management a modern approach to budget support, 2012.

63 European Commission, "Commission Staff Working Document - Paving the way for an EU Development and Cooperation Results Framework", SWD(2013) 530 final, Brussels, 10 December 2013.

- **Wider development progress** made by partner countries that reflects medium and long-term developmental outcomes/impact resulting from the collective action of the country concerned, external donors and other development actors, including private sector and external actors (level 1). Indicators at this level are agreed by the international community and draw on many sources of data gathered by international organisations, thus allowing for comparison across countries and time periods. Indicators at this level have been agreed internationally, such as the SDGs, and are in line with the EU development policy priorities 2014-2020, among others. Data to report against level 1 indicators come from international statistical sources (UN, World Bank, IMF). DG DEVCO has developed methodological notes for all level 1 indicators.⁶⁴
- **Aggregated results** linked to EU projects and programmes in countries in which the EU is engaged (level 2). These results demonstrate how the EU contributes to development progress in sectors that reflect the EU's development policy priorities. The indicators included in the EURF are linked with the sector choices and indicators in the programming documents. Methodological notes developed for this level provide definitions and explain what types of interventions should be included when reporting against an indicator.
- **Organisational performance** (level 3) with indicators providing primarily data about how a given donor organisation manages operational processes and resources to contribute to achieving development results. The EURF indicators at this level include information on such areas as quality of project design, performance during implementation, disbursement rates, etc.

Result Oriented Monitoring (ROM)

The Result Oriented Monitoring (ROM) system aims to assist the Commission's services and its representations (through the EU delegations) in partner countries and regions in monitoring and reporting on the implementation of projects and programmes financed within the EU's external assistance.⁶⁵ Specific evaluation criteria in EU-funded projects and programmes have been defined on the basis of the relevant OECD DAC criteria and include:

- **Relevance** – the extent to which the objectives of an action are consistent with beneficiaries' requirements, country needs, global priorities and partner and donor policies. Retrospectively, the question of relevance often becomes a question of whether the objectives or intervention logic are still appropriate given changed circumstances;
- **Efficiency** – measures how economic resources/inputs (funds, expertise, time) are converted into outputs;
- **Effectiveness** – the extent to which the objectives were achieved, or are expected to be achieved, taking into account their relative importance;
- **Sustainability** – the continuation of benefits after major development assistance has been completed, the probability of continued long-term benefits, and the resilience to risk of net benefit flows over time.

⁶⁴ The full set of methodological notes for different levels of indicators is available at <https://capacity4dev.ec.europa.eu/eu-rfi>.

⁶⁵ European Commission, "ROM Handbook: Instructions and guidance for ROM reviews and support to end-of-project results reporting for projects and programmes financed by the European Union within the framework of its external assistance", DG DEVCO, Brussels, 2015.

TOOL 14: CHECKLIST OF EVALUATION CRITERIA

Relevance	<ul style="list-style-type: none"> • Does the action presently respond to the needs of the target groups/end beneficiaries? • Do all stakeholders still demonstrate effective commitment (ownership)? • Is the action adapted to present institutional, human, financial capacities of the partner government and/or other key stakeholders? • Is there an effective government-led system of sector coordination involving the relevant local stakeholders and donors? • Have all relevant circumstances and risks been taken into account to update the intervention logic?
Efficiency	<ul style="list-style-type: none"> • Have the chosen implementation mechanisms proven conducive for achieving the expected results? • Do government and other partners in the country effectively steer the action? • Do the resources actually made available correspond to the needs of the action? • Are there any delays in the implementation and if yes, what has caused them and have the plans been adapted accordingly? • Do implementing partners, partner government(s) and other key stakeholders adequately monitor the action?
Effectiveness	<ul style="list-style-type: none"> • Is the progress of each output conforming to plan? • Is the quality of outputs satisfactory? • Are the outputs still likely to lead to expected outcomes? • Does the action effectively support the partner's policy and actions?
Sustainability	<ul style="list-style-type: none"> • Are key stakeholders acquiring the necessary institutional and human capacities to ensure a continued flow of benefits? • Is the role of EU actors sufficiently respectful of the leading role of the partners so as to enhance their capacities? • Have the relevant authorities taken the financial measures to ensure the continuation of services after the end of the action? • Has the private sector been involved to ensure the sustainability of the action?

Challenges linked to result monitoring and reporting

Several studies have analysed difficulties associated with implementing results-based approaches, including:

- **Contribution** - Due to all the factors that influence a project's implementation, credibly attributing results to a donor organisation becomes difficult, with the performance assessment moving away from inputs (i.e. resources invested in activities) towards various levels of results. Instead, the only conclusion that can be drawn is about how a given organisation is contributing towards the achievement of a partner country's developmental goal. In the specific case of cyber capacity-building projects, that implies that assessing the EU's contribution towards strengthening the rule of law or resilience in a partner country might be very difficult, as most likely this outcome stems from a convergence of the activities of many donors.
- **Performance incentives** - The focus on delivering outputs (i.e. training, workshops, etc.) rather than contributing towards sustainable country results leads to supply-driven rather than demand-driven decision making for programme management. Such approaches tend to neglect the contribution that a focus on capacity building could ultimately have. For instance, in addition to focusing on simply monitoring outputs such as 'the number of workshops' or 'the number of prosecutors trained' (supply-driven approach), a better approach would also assess outcomes, such as an improvement in the quality of e-evidence collected (demand-driven approach) with indicators such as 'number of criminal prosecutions supported by e-evidence', or 'percentage of convictions using e-evidence upheld on appeal'.
- **Harmonisation of results-based approaches** - With several donor organisations and partners introducing their own result monitoring approaches, there is a risk of different needs assessments emerging, which could result in divergent prioritisation. This is seen in the various ways security aspects are covered in some cyber-related projects currently underway that are funded by different donors. It is therefore important that parties involved in the implementation of cyber capacity-building projects work towards harmonising their approaches and improving their understanding of each other's work. This can be achieved with a more thorough analysis of synergies and complementarities between donor engagements.

- **Data and statistics** - A significant hindrance to a more comprehensive use of results-based approaches is the lack of relevant and accurate data and statistics. Without this information, performance measurement (i.e. through the use of objective indicators) becomes very difficult, especially at the outcome and impact stages. Most available data is produced by the private sector, which raises serious questions about their impartiality.⁶⁶

9.2. Project risk management

Risks are any external factors beyond the control of those designing and implementing the programme or project that have the potential to prevent or inhibit it from achieving its desired results. Country and sector-level risks - including those linked to the political climate, the respect for human rights, the socio-economic context and governance - could hamper the success of the envisaged action, the development of capacities as well as the sustainability of the results.

9.3. Closing

An important aspect of capacity-building programmes is negotiating from the start clear strategies and timeframes for an exit and making sure that they are included in any formal arrangement. Such an approach helps to manage expectations from the beginning and clearly illustrates that the external actor's role is limited to supporting the partner only until a certain capacity level is achieved. It is also one of the mechanisms to promote sustainability by ensuring that the partner country assumes ownership of the process early on. From the very beginning, programmes and project contracts and contracts of individual experts may include exit clauses and link exit strategies to performance measures, monitoring systems and incentives. Coaching and monitoring should be part of the hand-over before experts depart. Monitoring of performance also helps in making sure that the phasing out of external expertise and systems is done in a professional and mutually beneficial manner, with minimum disruption. Certain projects by their nature have the exit built in. For instance, 'train the trainer' programmes are built on the idea that the partner country acquires enough capacity to ensure the continuity of the process. It does happen, however, that such projects cease to exist once the material support from a donor organisation or other external partner stops.

⁶⁶ United Nations Economic and Social Council, "Effectiveness of the UN development system and its operational activities: capacity of the system to provide country level support and develop national capacities", Conference room paper, New York, 2004.

TOOL 15: FRAMEWORK FOR RISK MAPPING

The categories of risks that can be identified, assessed in terms of probability and impact on the implementation of projects, and eventually mitigated or avoided, include:

- **Political risks** - Support and willingness for change among the political elites is usually a pre-requisite for any intervention. However, it is important that the action monitors other initiatives undertaken by the government that might be contrary to the EU's values or interests. In the case of cybersecurity, this could be an expressed support to new international conventions or the shift from a multi-stakeholder to state-centric approach in internet governance.
- **Operational risks** - Given the need to involve groups of actors with different objectives, cultures, resources and level of engagement, there is a risk that competing claims, views or inexperience hamper the implementation of the action. So it is important to thoroughly map the relevant stakeholders and their interests and understand their motivations and inter-/intra-group dynamics. There is also a risk linked to continuity of operations, which is closely linked to having several donors or external actors operating in a partner country/region. For instance, it might be difficult to support the operations of a CERT if it was built according to a model supported by a different donor that incompatible with the EU's approach.
- **Legal risks** - One of the main pillars in building cyber resilience is strengthening the legal and regulatory environment of a country or region. However, given differences in the overall level of legal approximation between the EU and partner countries, there are potential negative spill-overs that cannot be ignored. This is particularly the case with technologies that can be used by governments for surveillance of civilians or compromise human rights online, including the safety of human-rights defenders. Similarly, strengthening capacities of law enforcement agencies without a comprehensive analysis of the whole legal system from the perspective of the rule of law and democratic standards may have negative consequences. For instance, new law enforcement capacities in the field of cybercrime might also be used to prosecute civil-liberties activists or minorities. Finally, there is also a risk that support provided in one domain (developing a strategy) may lead to actions by a partner country or region that go against the spirit of the initial intervention (e.g. development of model laws, etc.)
- **Security risks** - Placing cybersecurity or cybercrime on the agenda of governments can also attract the attention of those who might feel targeted, such as criminal groups, hackers, etc. Therefore, actions may need to be accompanied by adequate mitigation strategies. This is particularly relevant given that most of the solutions used at all levels are based on off-the-shelf technologies that are vulnerable to attacks.
- **Resource-related risks** - These are associated with funding, including the failure to secure budgets or other types of resources like an adequate staff. Problems linked to budgets are particularly present in developing countries where resources are more limited. Given the limited number of experts in the field of cybersecurity and cybercrime and the increasing competition for expertise between public and private actors, there is also a risk of losing well-trained and experienced staff to other job offers.
- **Reputational risks** - The nature of cyber capacity-building actions requires the involvement of different groups of actors. That means there is a potential for damage to the EU's reputation stemming from differing values and principles. One way to diminish this is to ensure that actions are accompanied by adequate plans and communication strategies. In the field of cyber capacity building this is particularly relevant with regard to the choice of involved partners and the implementers.

For the discussion about risks related to the implementation of the rights-based approach (RBA) see for instance Operational human rights guidance for EU external action addressing terrorism, organized crime and cybersecurity.

10. Step five – Evaluation of the Provided Support

The purpose of evaluation is to assess, against indicators selected in the planning stage, how successful the project has been in meeting its stated objectives, to reflect upon the relevance of project activities, to identify lessons learned in terms of impact, sustainability, effectiveness and efficiency and to assess whether any can provide guidance for further work in the field of CCB.

One of the main deficiencies noted in analysing cyber capacities building initiatives is access to credible evidence in support of the effectiveness of undertaken actions. This problem is characteristic of capacity building in general, where measurement of success cannot be reduced to an increase in human, financial or physical resources, for example. The link between capacity development and impact is also not always evident, as the latter may depend on several factors over time, change in capacity being one of them.⁶⁷ Lessons from other capacity-building domains suggest that several concrete steps can be taken to improve the quality of evaluation. Capacity-building programme objectives should be based on a clear vision for success rather than vague language such as 'improve, enhance, strengthen, or increase capacity'. Likewise the measurement should be based on clear evidence of actual changes rather than such things as the completion of training activities, procuring tools or augmenting staff.⁶⁸ In addition, the evaluation process should also include assessment of the extent of achievement of learning outcomes, the status of the targeted capacity indicators and progress toward the development goal. In some cases, these assessments may be followed by a long-term assessment of capacity indicators.⁶⁹

The completion of a project or a programme and its evaluation should provide inputs for decisions regarding the next steps, including continuation, scaling up or new funding sources for the project. Where necessary, this also involves decisions about whether and how programme participants could be further supported, including by joining other programmes.

The identification of lessons is also important to ensure that the outcomes and experiences associated with the intervention feed into future policies and practices. An often-ignored element in lesson identification is mapping instances of failure or projects that do not bring desired outcomes. It is important to document not only positive but also negative elements of the process.

67 Davis, T. Lemma & K. Wignaraja, 2009.

68 Ibid.

69 S. Otoo, N. Agapitova, and J. Behrens, 2009.

TOOL 16: CHECKLIST FOR IDENTIFICATION OF LESSONS

Lessons learned may be identified and documented at any point during the project's life cycle in order to promote certain desirable outcomes or avoid making the same mistakes. Any record of lessons learned should include information about the project and contact information, a clear statement of the lesson, a background of how lesson was learned, and benefits of using the lesson and suggestion how the lesson may be used in the future.

Thinking about lessons should provide answers to the following questions:

- What was learned about the project in general? What is the contribution of the project towards the overall goal? Were risks identified and mitigated? If not, why not? What bottlenecks or hurdles were experienced that impacted the project?
- What was learned about project management? Was the schedule met? If not, why not? Did the project management methodology work? If not, why not?
- What was learned about communication? What changes would assist in speeding up future projects while increasing communication?
- What was learned about budgeting? Where costs budgets met? If not, why not?
- What was learned about stakeholders? Have the relevant groups of actors been involved? Which elements of the stakeholder analysis contributed to this outcome?
- What was learned about what went well? What was learned about what did not go well?
- What was learned about what needs to change? What can be done in future projects to facilitate success?
- How will/was this incorporated into the project? What procedures should be implemented in future projects?

Based on Lessons Learned guide developed by the Centers for Disease Control and Prevention (CDC).

PART III

APPLICATIONS OF THE OPERATIONAL GUIDANCE TO SPECIFIC PILLARS

1. National strategic framework

The primary aim of a national strategic framework – whether in the form of a single document or a series of plans linked to a national developmental objective – is to provide high-level direction and define priorities for building cyber resilience. In that sense, a national strategic framework is closely linked to other pillars of capacity building in that it provides an overarching vision and methodology for how various elements relate to each other. A national cybersecurity strategy (NCSS) is a high-level framework that establishes strategic principles, guidelines and objectives – and in some cases specific measures – to be achieved in a specific timeframe to mitigate risks associated with cybersecurity.⁷⁰ Some countries have already developed national strategies and used the lessons learned to adopt successive versions. Given the multiplying effect of the process around a strategic framework – in that it brings various stakeholders around the same table to work on a common vision for a country – providing support for developing cybersecurity strategies or defining adequate frameworks has become one of the main aspects in cyber capacity building.

1.1. Policy analysis

The importance of developing a national strategic framework or cybersecurity strategy has been broadly recognised. Several regional and international organisations (ITU, OAS) and donors (EU, UK, US) view cyber strategy or strategic frameworks as a key element in the development of cyber capacities. Several countries have or are in the process of developing such strategies. Even though the content may differ, the primary value lies in that developing such a framework triggers strategic reflection in a country, brings different players together and pushes different policy communities to work on a joint vision – a process that does not always occur naturally. In that sense, the process is a *de facto* capacity-building exercise.

Cybersecurity strategies are most commonly products of such process and are usually the best way to communicate with domestic audiences and external partners. They provide clarity on vision, concepts, policy objectives, instruments and resources. But in some cases, policy documents or laws may become *de facto* strategies due to their clarity and scope. For instance, the EU's Network and Information Security Directive is a *quasi-strategy* that for the first time sets a clear vision for the Member States and provides guidelines towards its achievement. Some of the most common elements of national strategies identified in the literature include to:

- Achieve cyber resilience: develop capabilities and cooperate efficiently with the public and private sector; raise awareness about threats and responses; strengthen training and education;
- Secure critical information infrastructure: national cyber contingency plans; establish or strengthen incident-reporting mechanisms and response capability, including organising cybersecurity exercises and protection of critical information infrastructure;
- Reduce cybercrime;
- Develop the industrial and technological resources for cybersecurity: foster research and development;
- Contribute to the establishment of an international cyberspace policy: establish channels for cooperation and information exchange.

⁷⁰ European Union Agency for Network and Information Security (ENISA), "NCSS Good Practice Guide. Designing and implementing National Cyber Security Strategies", Heraklion, November 2016.

Most of these elements can be traced in the EU's Cybersecurity Strategy presented in 2013, which for the first time provided an overall framework for the EU action in this domain. Specific policy frameworks regarding defence cooperation, public-private partnerships, the fight against cybercrime, and cyber diplomacy – to name a few – were added later. Based on the experience from implementing that strategy and taking into account new developments in the cyber domain, in September 2017 the European Commission presented a modernisation package that included an update to the Cybersecurity Strategy and a proposal to transform ENISA into a fully fledged European Cybersecurity Agency.

1.2. Engagement

When deciding on engaging in capacity-building initiatives aimed at developing a cyber strategic framework there are several elements to take into account. First is the need to ensure that different voices are heard and interests taken into consideration throughout the process. That implies that the private sector and civil liberties organisations must be able to pursue their legitimate objectives and express their views as freely as possible, respecting the rights and freedoms of others. One way to verify if this is indeed the case is by checking the country's commitment to the to the promotion and respect for human rights both online and offline. In practical terms, this often translates into reconciling the government's security concerns and the human rights or freedom of operation concerns raised by civil society and the private sector, respectively. This dichotomy is very clear in the discussion about extremist content online, where the line between security and freedom of expression is very blurred. Another consideration is the overall approach that drives the process of strategic reflection. In light of talk about a conflict in cyberspace, offensive and defensive cyber capabilities and the stability of cyberspace, it is essential to consider whether a country's overall posture is peaceful and aligned with the EU's key interests and values.

1.3. Risk mapping

National risk assessment is the main element in the process of designing a new or upgrading an existing strategic framework. It consists of risk identification, risk analysis and risk evaluation.⁷¹ Since security of the state and its citizens is the primary responsibility of government, risk assessments are usually conducted by an appointed national authority, security authorities and in some cases by the operators of critical infrastructure. Very often, however, countries opt for an all-hazard approach encompassing threats ranging from hacktivism, cybercrime, espionage and technical failures to inter-state conflict. While risks play an important role in determining cybersecurity strategy objectives, it is also important to recognise the opportunities ICTs offer for country's development and growth. Risk mapping should therefore be oriented towards the analysis of how potential system vulnerabilities may undermine the attainment of the overall developmental objective.

1.4. Key stakeholders

To be operational and relevant, a strategic framework for building cyber resilience requires the clear identification of stakeholders and their respective roles, including regarding oversight, direction and execution of the strategy. Given the large scope of the issues involved, these can include critical infrastructure operators, law enforcement and the judiciary, the ICT sector and academic and research institutions. The collaborative process can be challenging as roles and responsibilities often overlap, giving rise to disagreements about who should do what. To minimise potential turf wars, it is essential to codify such issues through a formal and structured process that generates buy-in. Recognising the need for different perspectives and the diverse resources required to tackle cybersecurity challenges effectively, the European Union is also promoting a whole-of-government and whole-of-society approach as means to create incentives for stakeholders to share information and provide strategic insights into policy. One of the dimensions that might be particularly contentious is what governance structure a strategic framework or strategy should put in place. Some countries have adopted a centralised approach with a central cybersecurity authority with wide responsibilities and competencies across sectors, while others have more decentralised approaches characterised by strong cooperation between public authorities. In addition, trust is often limited among different actors with conflicting priorities and interests. Therefore, engaging trusted information-sharing communities (e.g. FIRST) might sometimes help to increase confidence among stakeholders.

71 See ENISA's "Glossary - Current risk".

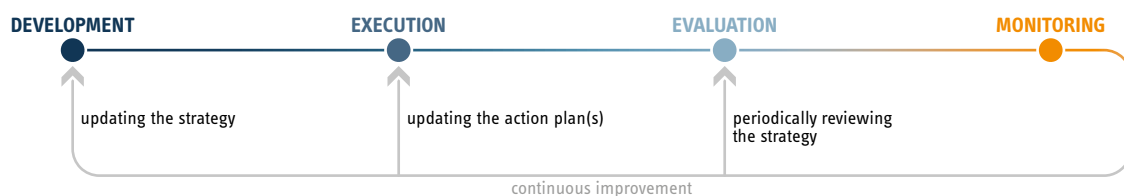
1.5. Capacity assessment and needs analysis

A national cyber strategic framework needs to be firmly grounded in the local context and tied to a country's national development agenda. Therefore, before embarking on the long process of developing a new strategic framework, it is important to take stock of existing policies, regulations and capabilities. This step maps the achievements in cybersecurity around which new initiatives can be defined. Such approach also promotes the ownership and sustainability of the process in the longer term.

Although a perfect template does not exist, there are certain elements that constitute a bare minimum for a good strategic framework:

- **Vision, objectives, and priorities** - What overall objective is the strategy supposed to help achieve (growth, security, development, etc.) and within what timeframe? What are the country's goals and aspirations? How will the strategy be implemented?
- **Scope** - What are the key sectors that the strategy wishes to cover? The scope should be defined following a risk assessment approach that aims to gain a holistic understanding about risk to the nation and consequently focuses on the most important cybersecurity challenges. The aspects to be assessed include:
 - **Cybersecurity** - What are the main cybersecurity challenges for the strategy and how will it address them? Who are the main actors in this process and what are their roles?
 - **Cybercrime** - What are the main cybercrime challenges for the strategy and how will it address them? Who are the main actors in this process and what are their roles?
 - **Cyber hygiene and culture** - Does the strategy provide instruments and tools for ensuring high levels of cyber hygiene and building a cybersecurity culture?
 - **Democracy and human-rights protection** - How is a country going to ensure that rights of citizens are protected both online and off?
 - **International stability** - What are the country's views on the main aspects of the stability regime in cyberspace, such as the application of existing international law, norms of responsible state behaviour and Confidence Building Measures? Is a country's military posture offensive or defensive?
- **Governance structure** - Who is responsible for the strategy lifecycle and strategy documentation? Ideally, strategy implementation should be linked to existing governance mechanisms such as those involved in budget formulation and legislation.
- **Cooperation and outreach** - Who are the main actors for implementing the strategy and how are they going to work together? Is civil society and the private sector involved and if yes, how? How is the strategy going to be communicated to a broader domestic and international audience?

FIGURE 20: National cyber strategy development cycle



Data: ENISA, 2014.

BOX 26: ANALYSING NEEDS – NATIONAL STRATEGIC FRAMEWORK PILLAR

Vision and policies

- Is there a national cybersecurity strategy or other similar framework?
- What are major threats and risks – defined in the strategy or established otherwise?
- What are the essential elements of the country's aspiration?

Laws and regulation

- Are there laws and regulations pertinent to cybersecurity (i.e. electronic communications, data protection, information security)?
- Are there already sector-specific strategies for critical infrastructure protection or crisis management or other regulatory measures aimed at improving cybersecurity (e.g. mandatory incident reporting)?
- Do other forms of soft regulations exist (e.g. public-private partnerships)? Have they achieved their goals?

Institutions and resources

- What are the roles and responsibilities of existing public agencies mandated to deal with cybersecurity policies, regulations and operations (i.e. energy regulators, communications regulators, data-protection authorities, national cybercrime centres)? Are there overlaps or gaps in their mandates and activities?
- Is a clear governance structure in place defining the roles, responsibilities and accountability of all relevant stakeholders?

Partnerships and cooperation

- What cooperation mechanisms for the public and private sectors and civil society are in place?
- How and why do these stakeholders contribute to the objectives of the strategic framework?
- Are there sufficient incentives for the private sector and civil society to participate?
- Do trusted mechanisms for information sharing and rules that govern the mechanism exist (e.g. non-disclosure agreements, traffic-light protocols, antitrust rules)?

While performing capacity and needs assessment, it is worth keeping in mind how countries and their needs and priorities differ. If several documents form a strategic framework, the capacity assessment should aim to clarify how they relate to each other and propose ways to create synergies or eliminate contradictions. This is particularly relevant for legal and regulatory frameworks. Such an analysis should also consider whether a country needs a single national cybersecurity strategy or whether other solutions could be envisaged. For instance, the assessment may conclude that the existing framework is sufficient for an effective cybersecurity policy except in the area of international cooperation. In such a case a strategy for external engagements on cybersecurity, building on the existing framework, might be a sufficient response. Indeed, recommendations should avoid creating unduly burdensome structures or processes that could divert scarce resources from more immediate problems, especially if a given country is just at the beginning of the road. In searching for concrete solutions, look into approaches adopted by other countries and avoid reinventing the wheel. In such cases, however, it is critical that the strategy implementation plan is developed by the authorities who will be in charge of the process and is tied directly to available means.

1.6. Building an intervention logic

The primary aim of initiatives aimed at cyber capacity building is **to contribute to developing a comprehensive strategic framework that reinforces state and societal resilience in partner countries.**

A national strategy or a strategic framework conveys the main cybersecurity challenges a nation is facing and formulates the approach to counter these challenges. The drafting process itself provides a country with an opportunity to assess its own vulnerabilities, define approaches to tackle them and determine the level of the existing capacity. A national strategy is also an opportunity to clarify a country's approach to developments in the cyber domain, which contributes to transparency and ultimately builds trust. A built-in implementation monitoring and review mechanism is also a good way to strengthen the country's capacity to perform regular cybersecurity assessments. Ideally, development of a national cybersecurity strategy should apply a whole-of-government and whole-of-society approach allowing various stakeholders to contribute.

Table 4: Identifying a point of entry for cyber capacity building: national strategic framework

	Vision and policies	Laws and regulation	Institutions and resources	Partnerships and cooperation
Advanced	Regular threat analysis and assessment of emerging issues (i.e. ethical aspects, societal impact) Cybersecurity exercises Feedback and evaluation mechanisms	Sector specific implementation action plans or roadmaps (finance, energy, transportation, health)	Create maturity self-assessment tools Set up a mechanism for review of adopted solutions	Confidence-Building and Stability Measures Joint exercises Information sharing, intelligence sharing
Developed	Integrated risk management process Action plans for the implementation of the strategy Comprehensive cross-policy approach to building resilience National cyber contingency plans	A comprehensive and coherent legal framework in support of the objectives of a cybersecurity strategy Baseline security measures for a sector Incident reporting mechanisms, including communication Legal framework fully respects and promotes human rights online	Prescription of roles and responsibilities of governmental actors and other stakeholders Defining tasks and related metrics Robust and effective structures to promote cybersecurity and respond to cyber attacks Cyber training and educational programmes	Cooperative arrangements for engagement with domestic and international partners at multiple layers of government, economy, society Adherence to bilateral, regional and international treaties and conventions
Developing	National cybersecurity strategy Communicating the strategy Raising user awareness	Recognition of cyber issues in sectoral laws and regulation Adherence to existing international standards	Prescription of roles and responsibilities of governmental actors Coordination mechanism Incident response capacity - CERT	Formal and informal mechanisms for consultation with a broader stakeholder community
Basic	Assessing the importance of cyber issues for national development or other country priorities Identification of critical sectors	Identifying overlaps and gaps in existing laws and regulations, including cybercrime	Identification of the existing functions and gaps Appointment of a person/institution in charge of coordinating national efforts	Mapping of relevant domestic stakeholders and international partners

There is no one-size-fits-all solution to the development of a national strategic framework. However, the experiences of other countries provide very useful lessons. The most common elements that have proven to be effective include plans for Critical Information Infrastructure Protection (CIIP) with a focus on identifying vital infrastructure and risk mitigation; national contingency plans describing processes and action for handling cyber crises; the importance of comprehensive cyber laws and regulation; cybersecurity exercises; and building skills and standards to develop a culture of cyber resilience. One also needs to acknowledge challenges that may have an impact on cyber capacity-building initiatives. A frequently mentioned one is linked to quantification and measuring results. Strategies often aim to improve confidence in doing business or accessing services online, but indicators for measuring results are often not readily available and can be challenging to construct in reliable manner.⁷² The link between elements of the strategies and the explanation of how they support strategic outcomes is often difficult to establish without ambiguity.

72 N. Robinson & V. Horvath, "Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts", Report prepared for the European Parliament, 2013.

TOOL 17: EXAMPLES OF ELEMENTS FOR THE CONSTRUCTION OF A LOGFRAME:

RESULTS CHAIN	INDICATORS	SOURCES AND MEANS OF VERIFICATIONS	ASSUMPTIONS AND RISKS
<p>IMPACT</p> <ul style="list-style-type: none"> > To increase cyber resilience of partner countries and ensure that citizens enjoy an open, free, secure and peaceful cyberspace 	<ul style="list-style-type: none"> > Country position in the ITU Global Cybersecurity and Cyberwellness Index > Country position in the World Economic Forum's Network Readiness Index > Country position in the Freedom on the Net Report by Freedom House 	<ul style="list-style-type: none"> > Global Cybersecurity and Cyberwellness Index > Network Readiness Index > Freedom on the Net report 	<ul style="list-style-type: none"> > Stakeholders remain committed to the change process and adaptations it requires > The overall financial and technical capacity of the partner country will not decline > The Action is not disrupted by adverse events such as political instability or a fragile security situation
<p>OUTCOMES(S)</p> <ul style="list-style-type: none"> > Adoption and implementation of a coherent, holistic, strategic and actionable national approach to cyber resilience is facilitated 	<ul style="list-style-type: none"> > A comprehensive national strategic framework is adopted > An implementation plan (or roadmap) for delivering on the strategic commitments is developed and systematically updated > Existence of locally-based organisations that contribute to effective dialogue with central authorities and cybersecurity actors 	<ul style="list-style-type: none"> > Strategy or national framework documents and/or Official Journal > Text of the implementation plan > Expert study/mapping to be commissioned by the Action (at the beginning and end of implementation) 	<ul style="list-style-type: none"> > Stakeholders have a clear understanding of their roles and responsibilities > Good cooperation among ministries and agencies and acceptance of change; conflicts over turf are minimised > National governments actively seek the involvement of the private sector; manufacturers, etc. > Trained staff remain even beyond the capacity building activity > Ability of the implementing partners to mobilise the right expertise in time for the roll out of activities
<p>OUTPUTS(S)</p> <ul style="list-style-type: none"> > Capacities of decision-makers to design and implement cyber policies are improved 	<ul style="list-style-type: none"> > Status of national cybersecurity strategy designed/updated with the support of the Action > Status of a risk management framework/ guidelines for national authorities designed/updated with the support of the Action > Frequency of inter-agency cooperation meetings at strategic/ management level > Number of decision-makers trained by the Action on the importance of cyber policies as well as design and implementation of national cybersecurity strategies (disaggregated by sex and age) 	<ul style="list-style-type: none"> > Text of the strategy > Text of the guidelines > Administrative data to be requested from the relevant national institutions at the beginning and periodically until the end of the Action's implementation > Action's reports/database of trained participants (disaggregated by sex and age) 	<ul style="list-style-type: none"> > Text of the legislation/ regulations > Action's reports/ database of mentored staff (disaggregated by sex and age)
<p>Laws and regulation</p> <ul style="list-style-type: none"> > Legal and regulatory environment to address cyber risks is improved 	<ul style="list-style-type: none"> > Status of laws/regulations addressing cyber risks (for ex. set-up of a national cybersecurity agency) designed/updated with the support of the Action > Number of staff in Ministries/ Parliament mentored on legislative/regulatory measures addressing cyber risks implemented with the support of the Action (disaggregated by sex and age) 	<ul style="list-style-type: none"> > Text of the legislation/ regulations > Action's reports/ database of mentored staff (disaggregated by sex and age) 	

NATIONAL STRATEGIC FRAMEWORK

Institutions and resources

- > Status of the identification of a national coordinating inter-agency body/authority on cyber issues (ex. Task Force, National Council)
- > A functioning institutional framework to address cyber risks in a holistic, inter-agency way is in place
- > Text of the national strategy and/or legislation/ regulation
- > Provisions of the national budget
- > Administrative data to be requested from the relevant national institutions at the beginning and periodically until the end of the Action's implementation

Partnerships and cooperation

- > Mechanisms for effective consultation/ cooperation on cyber issues at inter-agency, public-private and international level are developed
- > Number of public consultations organised in relation to the development of national strategic framework
- > Number of private sector entities (esp. critical infrastructure/ services) participating in consultations for the development of the national strategic framework
- > Text of MoUs or press releases
- > Number of cooperation MoUs signed between national governments and private sector actors
- > Text of recommendations/ press releases
- > Status of recommendations by civil society organisations on the development of the national strategic framework

Indicative activities

- > Technical assistance on drafting of policy documents/ laws/ regulations/ guidelines on the basis of international standards and good practices
- > Training courses, workshops and other activities aimed at enhancing skills and promoting good practices, including defining modalities for implementation
- > Table top exercises and mock operations
- > Awareness raising campaigns

Pre-conditions

- > Partner country recognises the need for a strategic framework and commits to actively engage and support the implementation of activities
- > Partner country commits to the peaceful use of cyberspace

There are also significant risks linked to implementation. Developing a strategy or strategic framework and putting it into action is a lengthy and difficult process. Meanwhile, the fast pace of technological progress requires constant adaptation, risking an ‘implementation fatigue’ that makes it difficult to maintain the support of everyone involved. Strategies themselves also require constant monitoring and adaptation. Consequently, developing a set of near-term tasks and defining quick-wins depending on the level of existing capacities might be beneficial for the process. At the same time, it is important to recognise that there are no shortcuts that would allow for skipping periodic progress reviews, checking in with stakeholders or confirming the validity of objectives, as such reviews are key to ensuring the relevance of the national strategic cyber framework.

A lack of clear communication about the aims of the strategy and division of labour and responsibilities may decrease the level of commitment among stakeholders and undermine the effectiveness of capacity-building initiatives in the long term. Developing consultation and coordination mechanisms that ensure involvement of all actors (e.g. the private sector, critical infrastructure operators) and close cooperation among public entities (e.g. through an adequate governance mechanism, information exchanges, etc.) can help mitigate some of these challenges.

The question of developing adequate governance structures plays an important role given the need to coordinate roles and resources spread across government and society. Whether the approach is centralised or decentralised, the governance mechanism established for a strategic framework will most likely change the power relations between stakeholders, resulting in resistance. This is another reason why approaching cyber capacity building through a whole-of-society and whole-of-government approach is important as it may reduce some of the tension. Meanwhile, legal and regulatory fragmentation also can undermine the effectiveness of national efforts to strengthen cyber resilience. Working towards a coherent legal and regulatory framework, ideally in line with existing international standards, is an obvious method for minimising such risks.

It is also important to keep in mind that cyber capacity building is a continuous process that requires frequent adaptation. The same is true for national strategic cybersecurity frameworks and strategies, which should be considered living documents. The assessment of cybersecurity strategies and frameworks presents a few distinct challenges, such as need for investment in budget and resources, a lack of good practices and the difficulty of measuring impact.⁷³

2. Criminal justice in cyberspace

Cybercrime is a term which covers criminal acts specific to the internet, such as attacks against information systems and different methods of spreading malware. Computers are also used as tools to commit more traditional crimes, such as fraud or the dissemination of illegal content. The experience of the fight against organised crime (i.e. trafficking, financial crime, etc.) shows that a robust criminal justice system with comprehensive and enforceable legislation, clearly prescribed institutional and operational roles, skilled law enforcement agents, prosecutors and judges as well as respect for the rule of law are indispensable. The situation is no different in the case of cybercrime and the challenges related to access to electronic evidence.

2.1. Policy analysis

The growing complexity of cybercrime⁷⁴ increasingly poses a threat to law enforcement response capability. As other forms of crime (i.e. trafficking, money laundering, etc.) increasingly gain a ‘cyber’ dimension, it is becoming ever more difficult for law enforcement and judicial bodies to effectively address those challenges without tackling that component.

At the same time, the multi-jurisdictional nature of cybercrime and the ways to address it adds further layers of complexity with regard to how it is investigated and adjudicated by the authorities. Certain legal instruments and investigative tools are already available and legislative reforms have been initiated or completed in recent years in a number of countries. However, the strengthening of institutional capacities to ensure

⁷³ European Union Agency for Network and Information Security, “An evaluation Framework for National Cyber Security Strategies”, Heraklion, 2014.

⁷⁴ See Europol, Internet Organised Crime Threat Assessment 2017.

the completion of legal reforms appears to be a persistent challenge, including the application of legislation and practical measures to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence. Developing the necessary knowledge base and relevant training programmes for law enforcement and judicial authorities is therefore key, bearing in mind respect for the rule of law. The need for assistance has been stressed in numerous international fora including the UN Congress on Crime Prevention and Criminal Justice. Nations and international organisations also contribute to the expansion and strengthening of mutual legal assistance initiatives and schemes (e.g. the Budapest Convention on Cybercrime, the Commonwealth's Harare Scheme on Mutual Assistance in Criminal Matters).

The broad interest in international cooperation against cybercrime is reflected in the EU. At the strategic level, the EU's fight against cybercrime is driven by three strategies, the EU Cybersecurity Strategy (2013), the European Agenda on Security 2015-2020, and the Joint Communication on "Resilience, Deterrence and Defence". The EU Cybersecurity Strategy of 2013 calls for global capacity building to prevent and counter cyber threats, including cybercrime and terrorist use of the internet. An update to the Strategy presented in 2017 recognises that to increase the EU's chances of bringing perpetrators to justice, it needs to urgently improve the capacity to identify those responsible for cyber attacks. The same document also states clearly that the borderless nature of the internet requires using an optimal legal standard for national legislations addressing cybercrime, like the one provided by the Budapest Convention. Rather than the creation of new international legal instruments for cybercrime issues, the EU calls on all countries to design appropriate national legislation and pursue cooperation within this existing international framework.

2.2. Engagement

Since the fight against cybercrime is a security priority for the EU and many partner countries, it often serves as a catalyst for cyber capacity building becoming the engagement of first choice.

However, a decision about engagement in capacity building in the criminal justice pillar should not be automatic given the potential risks and conflicts of interest. For instance, faced with an increasing use of the internet by terrorist organisations for propaganda, recruitment and funding, several countries have called for closer international cooperation against terrorist use of cyberspace. At the same time, several governments have used the fight against terrorism online as a tool against their own political opponents and human rights organisations. In addition, governments resort to internet shutdowns – i.e. intentional disruptions in the delivery of the internet or mobile apps – as means to control the flow of information during a specific event.⁷⁵

In addition to human rights concerns, there are also political risks to be considered. Some countries are pushing for the adoption of new international legal instruments on cybercrime, which contradicts the EU's approach, so it would be counterproductive to support countries that subscribe to this line of reasoning, but should instead engage in policy dialogue.

Finally, it is important to ensure that the scope of capacity-building initiatives is clearly defined. Given the frequent overlaps in objectives between projects and programmes, it is essential to avoid decisions in one area that might have a negative impact in another. For instance, it is important to ensure that actions to strengthen incident management capacities, a national cybersecurity strategy or simply the infrastructure do not contain elements that might contradict the need for a criminal justice approach to cybercrime and therefore impede capacity-building efforts. It is therefore essential to ensure complementarity between the different strands of cyber capacity building with a comprehensive, whole-of-government and whole-of-society approach. That includes relying on the extensive expertise available among the research community, private sector and civil society organisations.⁷⁶ Considering also that there is a trend towards over-securitisation of cyber issues by certain stakeholders, it is crucial to promote a criminal justice approach in capacity-building actions that aim at addressing cybercrime and electronic evidence.

⁷⁵ See Access Now, "Keep it on".

⁷⁶ See for instance: a series of publications by Global Partners Digital devoted to human rights in the digital environment and encryption policy for human rights defenders; annual Freedom on the Net reports by Freedom House; Digital Rights in Africa report by Paradigm Initiative.

2.3. Risk mapping

Capacity building in the field of cybercrime – like in other cyber-related policy areas – will always be subjected to the capacity-expectations gap whereby even most advanced countries are never fully prepared for an ever-evolving threat landscape. Countries will face different threats depending on their technological ecosystem: whereas in Africa mobile financial services might be the primary target, in parts of Asia crime has shifted towards cryptocurrencies. The best way to achieve effective and sustainable capacity building is to ensure local ownership of the process to the greatest extent possible.

2.4. Key stakeholders

An effective fight against cybercrime requires the involvement of the whole society and all levels of government. Nevertheless, it is the latter with its power to sanction unlawful behaviour that bears the primary responsibility for the security and safety of its citizens and businesses. Consequently, governmental actors and bodies – law enforcement agencies, prosecutors, judges, and in some cases the security/intelligence services or the military – have significant stakes in cyber capacity building. A criminal justice perspective also highlights the role of judges and judicial networks, public defenders trained to deal with cybercrime cases, home-groomed experts who can serve with their expertise in the courts, and public or non-governmental organisations with the capacity to defend the rights of victims and those accused in the courts. A relatively new aspect (including in the United States, UK, and the Netherlands) that reflects the evolution in the debate over how to deal with cybercriminals is the possibility of engaging with so-called ‘white hat hackers’ or ‘ethical hackers’ – individuals who use their hacking skills to identify security vulnerabilities in hardware, software or networks while respecting the rule of law.⁷⁷

Furthermore, the involvement of the private sector (e.g. operators of critical infrastructure, vendors, and Internet Service Providers) is key for addressing cybercrime. Their role is a hybrid one in that they are both custodians of information about the digital lives of their clients (e.g. patterns of behaviour, location, etc.) which they are contractually obliged to protect, and a potential source of information for law enforcement agencies. Most companies, in particular small- and medium-sized enterprises which might not survive a major data breach or cyber attacks, are likely to accept a government role in ensuring protection, because cybersecurity cannot be addressed in silos. Only governments have the tools to stimulate cybersecurity education and awareness-raising and to pass laws and regulations. Finally, civil society organisations are important contributors to the debate, but are less likely to support efforts aimed at strengthening law enforcement and judicial bodies without commensurate reinforcement of civil liberties and oversight mechanisms. Some of these power struggles have played out in public during discussions about government surveillance programmes or encryption. In that respect, cyber capacity-building actions may serve as a bridge between communities with different worldviews.

2.5. Capacity assessment and needs analysis

Assessing the capacity of law enforcement or judicial bodies is a demanding and sensitive task as it touches the core of state sovereignty and might expose a country to criticism. The quality of the information provided through such a process may not always be high because of trust issues and the intrusiveness of looking into, for example, financial resources or command and control structures. While duplication of efforts is not recommended, external partners need to hedge against such possibilities and collect information about states capacities from independent, open sources.

⁷⁷ David S. Wall, “Cybercrime. The transformation of crime in the information age”, Polity, 2007.

BOX 27: ANALYSING NEEDS – CRIMINAL JUSTICE IN CYBERSPACE**Vision and policies**

- What are major threats? Prevalent types of cybercrime? Sources or targets of cybercrime?
- Is there a national cybercrime strategy? How is cybercrime defined?
- Are there any statistics on cybercrime and electronic evidence available? How is it collected and by whom?
- Is there a cybercrime reporting mechanism and how does it work?
- Is there a national education and skills development policy dealing with cybercrime awareness and prevention? Who is responsible for its implementation?

Laws and regulation

- Is there substantive legislation targeting cybercrime or drafts thereof?
- What is considered cybercrime? Are offences against confidentiality, integrity and availability (CIA) criminalised?
- Is the country a member of the Budapest Convention? What is its position on the Convention?
- Are there any mutual legal assistance treaties in place with EU MS?
- Does the law distinguish between white- and black-hat hacking? Does the law take into account the age of offenders?
- Is there procedural legislation addressing cybercrime, or drafts thereof?
- What are the rules for data protection? Is there an independent data protection supervisory authority?
- What laws regulate the communication of service providers' obligation to retain data? Who authorises requests for data? What are the conditions and safeguards for access?
- Is there any legislation requiring service providers to report or remove illegal materials from on their servers?

Institutions and resources

- What is the size of law enforcement staff allocated to cybercrime cases, the structure of any specialised units? Is there a specialised department that deals with digital forensics?
- Do the following specialised units exist and if so what are their resources: child protection, economic crime, financial intelligence, organised crime, other?
- Are there specialised units or staff dealing with cybercrime and electronic evidence cases in the prosecutor's office?
- Are there specialised judges to hear cases involving cybercrime and electronic evidence?
- What are the responsibilities and resources of CERTs/CSIRTs? What is their relationship with law enforcement (do they share data on cyber attacks e.g.)?
- How do organisations responsible for the fight against cybercrime work with each other and other players in cases involving cybercrime and electronic evidence? Which is the lead organisation?
- How are the resources for cybercrime mobilised and distributed?

Partnerships and cooperation

- What are the mechanisms for cooperation between and amongst public authorities and industry, in particular communication Service Providers, in cases involving cybercrime or electronic evidence (i.e. SOPs, MoUs)
- Which institution(s) is/are responsible for international police and judicial cooperation and what are the roles?
- Has a 24/7 point of contact been appointed? With what roles and capacities?

2.6. Building an intervention logic

The primary purpose of initiatives aimed at cyber capacity building under the pillar ‘Criminal Justice in cyberspace’ is to **contribute to increasing quality and strengthened capacity of the criminal justice system to adequately address cybercrime while ensuring protection of fundamental rights and the rule of law**. These efforts are driven by the conviction that differences in legal frameworks and ineffective international cooperation resulting from limited capacities may lead to the emergence of online criminal hot spots and safe havens where investigations, evidence collection and prosecution would be impeded.

Partner countries are generally interested in and committed to cyber capacity-building initiatives, given their concern over cybercrime and the limited abilities of many to deal with it. Given differing definitions and priorities set by individual partner countries, however, there is a risk that requests for assistance may not always be in line with the EU’s interests and values. It is therefore important to clarify any differences in language and work towards similar understandings of the problem from the very beginning of the engagement process. Even though cybercrime capacity building is a relatively new field, more than a decade of experience has shown that an effective response is linked to two areas. They are a state’s capacity to 1) **develop and implement legislation on cybercrime and access to electronic evidence in line with the existing international legal commitments and standards**, and 2) **effectively participate in international networks and public-private partnerships aimed at the fight against cybercrime**. This is because, whereas cyber criminals know no borders, law enforcement agencies and judges operate in a highly fragmented world. Their powers are restricted by national jurisdictions and differences in legal frameworks concerning, for instance, criminalisation of conduct and provisions to investigate cybercrime and gather e-evidence.⁷⁸

Building an intervention logic for criminal justice in cyberspace faces several difficulties⁷⁹. First, the evolving nature and complexity of the cybercrime threat landscape – for instance the emergence of Crime-as-a-Service (CaaS) as Malware-as-a-Service (MaaS) – makes it hard to align legal frameworks in a timely and effective manner. This is further aggravated by a still-limited case law and limitations of the existing operational processes such as Mutual Legal Assistance Agreements. Such circumstances make cooperation with the private sector and non-traditional law enforcement agencies vital in combating cybercrime.⁸⁰ Some of the most successful operations against cybercriminal networks resulted from a close cooperation between governmental agencies and the private sector.⁸¹ However, such cooperation frameworks also suffer from a lack of standardised rules of engagement. So countries need to make decision makers more aware of the cyber threat landscape, ensure that national criminal (substantive and procedural) law frameworks and policies are in line with international standards and provide law enforcement, prosecutors and judges with the necessary legal, technical and operational skills needed to investigate cybercrime cases.

The experience from the GLACY project, with over 165 activities conducted over three years (2013-2016), demonstrates that the capacities of criminal justice authorities to address cybercrime and electronic evidence were strengthened through:

- Adoption or elaboration of laws to better converge with international standards;
- Mainstreaming of cybercrime and e-evidence modules into the curricula of judicial training academies;
- Providing training, access to training materials and other tools to cybercrime units;
- Improving mechanisms for international cooperation, including by linking cybercrime units, prosecution services and 24/7 points of contact with their counterparts;
- Improving information sharing and interagency and public/private cooperation;
- Strengthening the government’s ability to assess progress made in the investigation, prosecution and adjudication of cybercrime and other cases involving electronic evidence.⁸²

⁷⁸ Council of the European Union, “Joint paper by Europol and Eurojust on ‘Common challenges in combating cybercrime’”, Brussels, 13 March 2017.

⁷⁹ World Bank has published a toolkit, “Combating Cybercrime: Tools and Capacity Building for Emerging Economies”, which aims at building capacity to combat cybercrime among policy-makers, legislators, public prosecutors and investigators, as well as among individuals and in civil society at large in developing countries by providing a synthesis of good practices in the policy, legal and criminal-justice aspects of the enabling environment necessary to combat cybercrime. Included in this Toolkit is an Assessment Tool that enables countries to assess their current capacity to combat cybercrime and identify capacity-building priorities.

⁸⁰ World Economic Forum, “Recommendations for Public-Private Partnership against Cybercrime”, Geneva, 2016.

⁸¹ See: Europol, “Andromeda Botnet Dismantled in international cyber operation”, *Press Release*, 4 December 2017; “‘Avalanche’ Network dismantled in international cyber operation”, *Press Release*, 1 December 2016.

⁸² Capacity-building on cybercrime and e-evidence. The experience of EU/Council of Europe joint projects 2013-2017, UN IEG Conference Room Paper 2, 6 April 2017 (doc. UNODC/CCPCJ/EG.4/2017/CRP.2)

Table 5: Identifying a point of entry for cyber capacity building: criminal justice in cyberspace

	Vision and policies	Laws and regulation	Institutions and resources	Partnerships and cooperation
Advanced	<p>Adoption of sector-specific policies targeting crime committed with or facilitated by computer systems</p> <p>Exploit all possibilities within existing bilateral, regional and international agreements on cooperation in criminal matters</p>	<p>Adapt legislation on financial investigations, the confiscation of crime proceeds, money laundering and the financing of terrorism to the online environment</p> <p>Develop emergency procedures for requests related to risk of life and similar exigent circumstances</p>	<p>Improve procedures for cybercrime investigations and the handling of electronic evidence by implementing national and international standards and good practices.</p> <p>Commit skilled staff and resources for Mutual Legal Assistance</p>	<p>Capacity to identify and facilitate exchange of good practices between specialised units at regional and international level</p> <p>Legislation and agreements allowing for public/private information sharing and development of guidelines for information sharing</p>
Developed	<p>Evaluate on a regular basis the effectiveness of the criminal justice response to cybercrime and maintain statistics</p> <p>Evaluate the effectiveness of international cooperation through collection of data on requested/provided assistance, timeliness of responses and procedures used.</p> <p>Accession to Budapest Convention on Cybercrime</p>	<p>Regular evaluation of the effectiveness of legislation and collection of statistical data on cases investigated, prosecuted and adjudicated</p> <p>Implementation of procedural law provisions to secure electronic evidence by law enforcement to ensure lawful access to data held by private-sector entities</p>	<p>Ensure judicial oversight of intrusive powers and respect for principles of proportionality and necessity by law enforcement agencies</p> <p>Establishment of specialised prosecution units/teams</p> <p>Regular review of functions and resources of such units</p> <p>Establish 24/7 points of contact</p>	<p>Engage in international cooperation, making use of the existing bi- and multi-lateral and regional arrangements such as the Cybercrime Convention Committee (T-CY)</p> <p>Foster a culture of cooperation between LE and ISPs and other private sector entities through MoUs</p>
Developing	<p>Cybercrime and cybersecurity policies or strategies are pursued with the objective of ensuring an effective criminal justice response.</p>	<p>Substantive criminal law provisions on cybercrime and procedural law provisions to secure electronic evidence by law enforcement are in place</p> <p>International standards on data protection in line with ETS 108, protection of children against sexual violence (Lanzarote Convention) are in place</p>	<p>Set up, training and providing continuous support to digital forensics units</p> <p>Adapting existing or developing new training materials</p>	<p>Establish online platforms for reporting cybercrime or integrating such reporting into existing platforms</p> <p>Identify lessons and good practices</p>
Basic	<p>Create awareness of the challenges of cybercrime and gathering electronic evidence at all levels</p>	<p>Ensure that human rights and rule of law requirements are met</p> <p>Evaluate the scope and effectiveness of existing legislation</p>	<p>Establish specialised cybercrime units and points of contact</p> <p>Have a training strategy for domestic law enforcement, investigators and the judiciary</p>	<p>Establish clear rules and procedures domestically for law enforcement access to data held by service providers and the private sector</p> <p>Show a commitment to international cooperation as reflected in interest in accession to Budapest Convention on Cybercrime</p>

TOOL 18: EXAMPLES OF ELEMENTS FOR THE CONSTRUCTION OF A LOGFRAME:

ASSUMPTIONS AND RISKS	SOURCES AND MEANS OF VERIFICATIONS	INDICATORS	RESULTS CHAIN
<ul style="list-style-type: none"> > Stakeholders remain committed to the change process and adaptations it requires > The overall financial and technical capacity of the partner country will not decline > The Action is not disrupted by adverse events such as political instability or a fragile security situation 	<ul style="list-style-type: none"> > Global Cybersecurity and Cyberwellness Index > Network Readiness Index > Freedom on the Net report > Text of the law. An expert analysis may also need to be commissioned by the project to assess the stated provisions > Council of Europe Treaty Office > Administrative data of the Ministry of Interior / Ministry of Justice to be requested at the beginning and periodically until the end of the Action's implementation > Reports by cybercrime units and prosecution offices > Public perception survey to be conducted at the start and end of the Action (disaggregated by sex and age) 	<ul style="list-style-type: none"> > Country position in the ITU Global Cybersecurity and Cyberwellness Index > Country position in the World Economic Forum's Network Readiness Index > Country position in the Freedom on the Net Report by Freedom House > Status of legal provisions / regulations on cybercrime and electronic evidence > Accession to/ratification of the Budapest Convention > Percentage of cybercrime complaints that are investigated > Percentage of population that expresses confidence in the capacity of the law enforcement and judicial bodies to tackle cybercrime effectively 	<ul style="list-style-type: none"> > To increase cyber resilience of partner countries and ensure that citizens enjoy an open, free, secure and peaceful cyberspace > National capacity to develop and implement legislation on cybercrime and electronic evidence in line with existing international legal standards is increased
<ul style="list-style-type: none"> > Stakeholders have a clear understanding of their roles and responsibilities > Good cooperation among ministries and agencies and acceptance of change; conflicts over turf are minimised > National governments actively seek the involvement of the private sector, manufacturers, etc. > Trained staff remain even beyond the capacity building activity > Ability of the implementing partners to mobilise the right expertise in time for the roll out of activities 	<ul style="list-style-type: none"> > Text of the strategy > National and international reports (ministries, regional organisations) about country's cyber policies and their implementation, including cybercrime strategies and threat assessments > CoE assessments (initial and final situation reports), Octopus Cybercrime Community Wiki > UNODC Cybercrime Repository > Text of the legislation > Council of Europe Treaty Office > CoE assessments (initial and final situation reports), Octopus Cybercrime Community Wiki > UNODC Cybercrime Repository > National and international reports (ministries, regional organisations) about country's cybercrime legislation and its implementation 	<ul style="list-style-type: none"> > Cybercrime is listed as a priority in a national strategic framework / cyber strategy designed/updated with the support of the Action > Status of laws/regulations on cybercrime and electronic evidence legislation aligned with the Budapest Convention that are drafted/updated with the support of the Action 	<ul style="list-style-type: none"> > Fight against cybercrime is a stated national cyber policy objective > National criminal legislation on addressing cybercrime is drafted/updated in line with international standards, including those established by the Budapest Convention
			<ul style="list-style-type: none"> > National criminal legislation on addressing cybercrime is drafted/updated in line with international standards, including those established by the Budapest Convention
IMPACT	OUTCOME(S)	OUTPUT(S)	

CRIMINAL JUSTICE IN CYBERSPACE

Institutions and resources

- > Cybercrime/high-tech crime units are operational
 - > Number of domestic and international cybercrime investigations launched and cases adjudicated by national authorities
 - > Administrative data of the Ministry of Interior / Ministry of Justice to be requested at the beginning and periodically until the end of the Action's implementation
- > Skills of law enforcement, prosecutors and judges to investigate, prosecute and adjudicate cybercrime cases are improved
 - > Number of police officers, prosecutors and judges trained by the Action (disaggregated by sex and age)
 - > Status of incorporation of cybercrime modules in law enforcement and judicial training academies
 - > Text of national budget/Official Journal

Partnerships and cooperation

- > Participation in international operations and/or joint investigations targeting cybercrime is increased
 - > Number of joint operations and/or investigations conducted with other countries with the support of the Action
 - > Number of requests handled by national 24/7 points of contact
 - > Reports by 24/7 points of contact
 - > Reports by cybercrime units
- > Cybercrime reporting mechanisms are enhanced
 - > Number of international police-to-police requests
 - > Action progress reports
 - > Text of MoUs or press releases
- > Public-private cooperation in the fight against cybercrime is improved
 - > Status of public/public-private reporting mechanisms developed with the support of the Action
 - > Number of MoUs with private sector and relevant civil society organisations signed

Potential activities

- > Technical assistance on drafting/updating substantive and procedural criminal provisions on cybercrime and electronic evidence based on international standards (Budapest Convention)
- > Training, workshops and other activities aimed at enhancing skills and promoting good practices, including cooperation across government agencies and the private sector
- > Table top exercises and mock operations

Pre-conditions

- > Partner country recognises the need for reforming/updating its criminal justice system and commits to actively engage and support the implementation of activities
- > Partner country commits to the peaceful use of cyberspace

The experience of the GLACY project allowed for formulation of several lessons, including that capacity building:

- Responds to needs and can produce immediate effect;
- Favours multi-stakeholder cooperation;
- Contributes to human development;
- Helps reduce the digital divide.
- Consequently, support to cybercrime capacity building needs to focus on mainstreaming cybercrime and electronic evidence in the criminal justice system, continuous law reform and development, strengthening institutional capacities, law enforcement and judicial training, cooperation between law enforcement and service providers and more efficient regional and international cooperation.

3. Incident and crisis management system

The EU's cyber capacity-building engagement with partner countries should take into consideration the development of a robust system for managing cybersecurity incidents and crises. A cybersecurity incident can be defined as 'any event having an actual adverse effect on the security of network and information systems'.⁸³ A cyber crisis, on the other hand, is defined as 'an abnormal and unstable situation that threatens an organisation's strategic objectives, reputation or viability'.⁸⁴ Finally, incident/crisis response and management are efforts aimed at protecting an organisation's information by developing and implementing processes to detect an attack, contain the damage, eradicate the attacker's presence and restore the integrity of the network and systems.⁸⁵ A systemic approach to building cyber resilience is important given the potential complexity and impact of threats and the resources required to mitigate them. No actor – whether at the national or international level – has the capacity to cope with cyber vulnerabilities alone. It requires significant coordination by all parties involved.

3.1. Policy analysis

Establishing an incident and crisis management system requires defining what should be protected and how. Certain assets, the loss or compromise of which would have a major detrimental impact on the availability, delivery or integrity of essential services, are categorised as critical information infrastructure, in recognition of their importance for human development (i.e. economic growth, well-being, security). However, efforts at improving access to ICT and the growing focus on the Digital4Development agenda have underestimated the risks and challenges associated with this process. The OECD recommendations on digital security risks (2015) was one of the first documents to recognise that 'digital security risk should be treated like an economic rather than a technical issue, and should be part of an organisation's overall risk management and decision making'. The 2016 World Development Report on Digital Dividends made another important contribution to the debate by calling for a revision of the 'perimeter security' paradigm, putting users and not devices at the centre of the discussion. The 2030 Agenda for Sustainable Development, adopted at the UN in 2015, further recognised the importance of building resilient infrastructure by adopting Goal 9a, which is focused on facilitating sustainable and resilient infrastructure development through enhanced financial, technological and technical support.

The EU Cybersecurity Strategy in 2013 stressed that '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 and joint incident management exercises. The Strategy also committed the EU to more intensive international cooperation aimed at strengthening critical information infrastructure protection (CIIP) cooperation networks involving governments and the private sector. The risks to critical infrastructure have also been recognised in the Joint Communications on 'Countering Hybrid Threats' and the 'Strategic Approach to Resilience in the EU's external action'. Both policy documents outline proposals to help counter hybrid threats and foster resilience of national critical infrastructure. Furthermore, the Joint Communication 'Resilience, Deterrence and Defence: Building

⁸³ Article 4, NIS Directive.

⁸⁴ Snowden, "Managing a Cyber Crisis: What is the most effective way to prepare leadership for a high tech threat?", Register Larkin, 2014.

⁸⁵ European Union Agency for Network and Information Security (ENISA), "Strategies for Incident Response and Cyber Crisis Cooperation", Heraklion, 2016.

strong cybersecurity for the EU', presented in September 2017, recognised that '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'. Finally, the EU Network and Information Security Directive (NIS Directive) demonstrates the importance of developing confidence and trust among the Member States and to promote swift and effective operational cooperation by establishing a EU network of CERTs/CSIRTs. The Directive states that each Member State shall designate one or more CERTs/CSIRTs responsible for risk and incident handling in accordance with a well-defined process. The Directive gives high-level requirements that designated CERTs/CSIRTs must observe and tasks that they must perform.

3.2. Engagement

Capacity-building initiatives aimed at supporting and strengthening protection of Critical Information Infrastructure and a country's crisis response capacities are less politically sensitive and less prone to abuses. Nonetheless, human rights and civil liberties concerns should not be ignored even in a purely technical cooperation project. At the same time, due diligence is required when it comes to a country's overall posture and intentions with regard to international cooperation. Whereas the transnational nature of cyber crises provides strong incentives for engagement and for reducing the risk posed by the weaker links in the network, such decisions should take into account each country's commitment to preserving stability in cyberspace, in particular respect for existing international law, rules of responsible state behaviour and an active contribution to building confidence and trust. Several international processes offer some guidance in this respect.

BOX 28: G8 PRINCIPLES FOR PROTECTING CRITICAL INFORMATION INFRASTRUCTURES

1. Countries should have emergency warning networks regarding cyber vulnerabilities, threats and incidents.
2. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.
3. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.
4. Countries should promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.
5. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
6. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.
7. Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.
8. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.
9. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.
10. Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.
11. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

Source: G8 Justice & Interior Ministers, 2003.

In 2003, the G8 concluded that nations should protect their critical information infrastructure. According to the G8, that includes identification of threats and vulnerabilities, minimising damage and recovery time, identifying the cause of a disruption and analysis by experts and/or investigation by law enforcement. Effective CIIP also requires communication, coordination and cooperation nationally and internationally among all stakeholders.

The UN Group of Governmental Experts (UN GGE) dealing with questions of international security in cyberspace has also put forward proposals for norms of responsible state behaviour in cyberspace, including that states should: not knowingly allow their territory to be used for internationally wrongful acts using ICT; consider how to best cooperate to exchange information and assist each other; respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts; and not conduct or knowingly support activity to harm the information systems of CERTs/CSIRTs. The UN GGE and OSCE have also proposed a set of voluntary Confidence Building Measures which aim to prevent escalation between countries in case of a serious cyber crisis. Some of the proposed measures are: facilitation of cooperation between relevant national bodies; sharing information on national organisation, strategies, policies and programmes; and consultations to prevent political and military tensions and to protect critical national ICT infrastructure.

3.3. Risk mapping

In light of the devastation an attack on critical information infrastructure could cause, a partner country should be able to perform a cyber threat assessment – either autonomously or through international collaborative arrangements. This is particularly important in the context of hybrid conflicts and the possible use of cyber tools for malicious purposes. A lower level of dependence on digital infrastructure might not necessarily imply a lesser impact from such an attack, especially if it concerns a critical service such as energy or transportation. The risk of escalation and miscalculation stemming from potential attack adds to the importance of focusing on building resilience of critical infrastructures and networks.

3.4. Key stakeholders

The main stakeholders in cyber incident and crisis management are the government agencies in partner countries as well as the operators of critical information infrastructure. To ensure meaningful engagement, it is important to identify the responsible public agencies and ministries. The key responsibility for crisis response may be with the Ministry of Defence. There may also be a CERT/CSIRT, the organisation that receives reports of security breaches, analyses them and responds to the senders. They may operate as part of a parent organisation such as a university, government or a company, or be responsible for an entire country or some critical infrastructure as is the case with national and governmental CERTs/CSIRTs.⁸⁶ Since cyber incidents may be a result of criminal activity, it is also key to establish how law enforcement agencies are tied in the process of crisis management, particularly given the importance of digital evidence. Whereas in some countries critical infrastructure may be state owned, in most cases it is operated by private companies. Stakeholder analysis should therefore assess the mechanisms for cooperation between the public and private sectors. Probably the most challenging aspect is the role of military. It is essential to clarify how civilian-military relations are organised and what oversight mechanisms are in place. Finally, because the failure of critical information infrastructure may be catastrophic, it is very likely that initiatives will enjoy high level of buy-in from the partner country, especially if the cause was a premeditated attack orchestrated by another country or a non-state group. Given the sensitivity of the issues and their close link to national security, it is essential to play a supporting role and ensure the maximum degree of local ownership. There is also a small group of international actors who might play a useful role when it comes to cyber incident and crisis management, including regional organisations like the African Union or the Organisation of American States, OECD and World Bank and trusted technical communities such as the Forum for Incident Response and Security Teams (FIRST), the Trusted Introducer GEANT (TF CSIRT) or the Meridian Process.

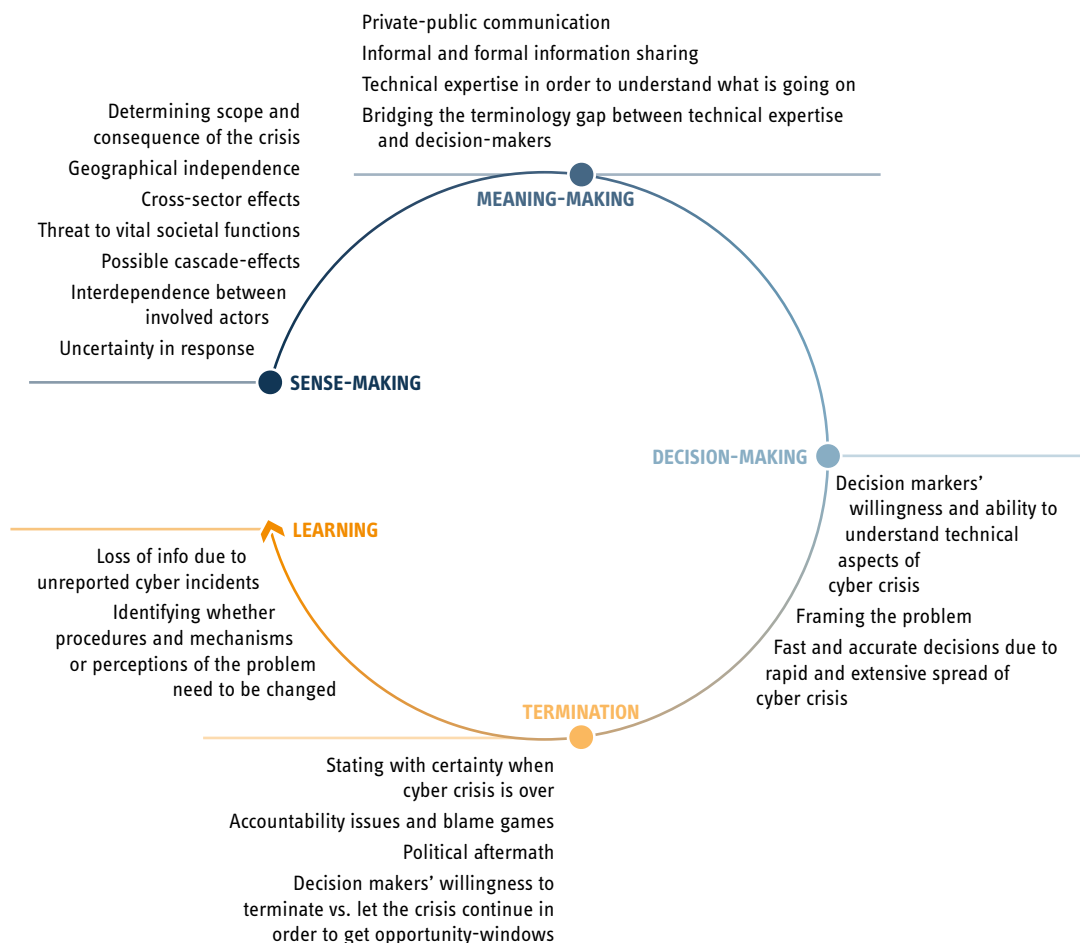
86 Ibid.

3.5. Capacity assessment and needs analysis

Managing cyber incidents or crises is a complex process composed of several stages and tasks depending on the level of country's dependence on digital infrastructure. Capacity assessment, therefore, needs to include a thorough analysis of the national digital ecosystem, the main dependencies within the system and the extent to which a country relies on their proper functioning.

It has been generally accepted that a functioning CERT/CSIRT is a bare minimum in developing a cyber crisis management system. According to the ITU, there are currently 103 national CERTs/CSIRTs established worldwide.⁸⁷ Consequently, as one of the first steps it is important to establish if a country has a CERT and if yes, what is its mandate (e.g. the official national point of contact), what external and internal support services it provides (e.g. requests for assistance, guidance for improving the infrastructure, incident handling and management), and how it is organised, including the resources at its disposal. Other elements include the availability of a 24/7 duty officer as well as its position and membership in CERT/CSIRT communities such as FIRST or regional networks like APCERT or CERT-Africa.

FIGURE 21: Cyber crisis management cycle



Since not all countries have a CERT/CSIRT or a very mature one, they have become a main focus of cyber capacity-building initiatives, in addition to the development of a national cybersecurity strategy and a legal framework to fight cybercrime. Consequently, international actors have developed guidelines and best practices for establishing a CERT/CSIRT, including the Global Forum on Cyber Expertise⁸⁸, ENISA⁸⁹, Meridian

87 See International Telecommunication Union, "CIRT Programme".

88 Global Forum on Cyber Expertise, "Global Good Practices: National Computer Security Incident Response Teams", 2017.

89 European Union Agency for Network and Information Security (ENISA), "CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs", Heraklion, 2015.

Process⁹⁰ and the Internet Governance Forum⁹¹. There are also best practices available that deal with organising human and technical resources and processes to effectively comply with the pre-defined CSIRT/CERT mandate⁹² or provide guidance on how to assess its maturity.⁹³

Once a CERT/CSIRT has been established and its maturity determined, the capacity assessment should focus on the sustainability dimension, which includes budgetary, technical and human resources required for its proper functioning, including the availability of specialised training. The CERT/CSIRT community provides continuous training on current threats and trends and organises hands-on technical courses.⁹⁴

BOX 29: ANALYSING NEEDS - INCIDENT AND CRISIS MANAGEMENT SYSTEM

Vision and policies

- How is the incident/crisis framed? The choice of words and definitions can alter the perception of an event and hence the response.
- What is the scope of and methodologies for responding to a cyber crisis?
- How does incident and crisis management fit within the overall vision of a country?
- Is there a threat and/or vulnerability monitoring system in place?
- Do current cyber crisis-management practices include learning processes and capacity building?
- Are informative awareness-raising activities conducted?

Laws and regulation

- Are critical infrastructure and critical information infrastructure protection clearly defined?
- Have the dependencies between CII sectors and other critical services been clearly defined?
- How does decision-making take place?
- How do the scope and methodologies differ from those in general crisis management?
- Is legislation dealing with incident and breach management in force or has it been proposed?

Institutions and resources

- Is there an organisation set up to collect and respond to threat intelligence, e.g. a national CERT or other CERTs/CSIRTs?
- Who are the main stakeholders and are their responsibilities clearly prescribed? What resources do they have at their disposal?
- Is there a national crisis management coordination system in place?
- Are the existing mechanisms systematically exercised?

Partnerships and cooperation

- What are the mechanisms through which actors other than governments are involved?
- What is the state of public-private partnerships?
- What is the nature of cooperation between crisis management structures, CERTs/CSIRTs, law enforcement agencies and policymakers?
- Is the country an active member of international crisis management networks?
- Does the country subscribe to the proposed norms of responsible state behaviour in cyberspace and participate in the implementation of Confidence Building Measures?

Beyond the institutional level, it is important that capacity assessment looks into the country's ability to manage cyber crises in a systematic way. That includes the capacity of other domestic actors and the effectiveness of existing coordination mechanisms as well as the cooperation with international partners, including CERT teams from other countries. The latter aspect is particularly important given that cyber crises may

90 E. Luijff, T. Van Schie & T. Van Ruijven, "Companion Document to the GFCE-Meridian Process Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers", GFCE-MERIDIAN, 2017.

91 Internet Governance Forum, "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security", Istanbul, 2014.

92 European Union Agency for Network and Information Security (ENISA), "Introduction to Return on Security Investment: Helping CERTs assessing the cost of (lack of) security", Heraklion, 2012.

93 European Union Agency for Network and Information Security (ENISA), "Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity", Heraklion, 2016, 28p. European Union Agency for Network and Information Security (ENISA), "CSIRT Capabilities: How to assess maturity? Guidelines for national and governmental CSIRTs", Heraklion, 2015.

94 See ENISA's training materials or FIRST's symposia, workshops, and technical colloquia.

transcend national territorial and legal boundaries. These capacities are acknowledged through membership in trust-based networks and tested through drills and exercises which assess a community's preparedness for cyber crises, technology failures and critical information infrastructure incidents. An exercise can be used to test various elements of the cybersecurity plan involving the technical, operational, co-operational and strategic levels.⁹⁵

3.6. Building an intervention logic

Critical information infrastructure (e.g. financial services, energy, transportation networks, or healthcare system) constitutes in many cases the backbone of a country's economic growth and human development. Therefore, the primary aim of cyber capacity-building initiatives focused on an 'incident and crisis management system' is to **contribute to strengthening state and societal capacity to manage cyber incidents and crises in a timely, effective and efficient manner**. To achieve that objective, countries need to establish institutions with clearly prescribed responsibilities and processes for crisis management and cooperation between various stakeholders.

The primary focus is to define and protect national critical information infrastructure that underpins critical functions of the government and society, including health care, energy, transportation, etc. With countries increasingly reliant on the use of ICT to optimise the operation of ports, energy grids or manufacturing facilities, it is paramount to identify vulnerabilities in the inter-linked networks and information systems that could be exploited for political reasons or financial gains.

Critical infrastructure encompasses large complexes controlled and monitored by Industrial Control Systems (ICS), including SCADA systems (Supervisory Control and Data Acquisition). To reduce costs, many ICS products use commercial off-the-shelf software and apply standard embedded systems platforms. The downside of such a solution, however, is that ICS are vulnerable to network-based attacks. While the principal responsibility for security falls on individual countries, the international community cannot ignore the negative internal and external implications of potential attacks on critical infrastructure in developing parts of the world.

Even though the probability of large-scale attacks is still considered relatively low, the magnitude of potential consequences (e.g. from an attack on a nuclear power plant) means that all governments have a stake in the matter. The capacity of many developing countries to monitor and manage such incidents in cyberspace is, for now, rather limited but can be improved with investment in technological and organisational measures, including the setting up of CERTs, acquiring the right equipment and receiving specialised training. Effective cybersecurity capacity building entails, inter alia, a functioning national CERT which delivers a comprehensive list of functions such as monitoring, response, mitigation, continuity capacities of national networks, feeds information to law enforcement agencies, and acts as interface between government bodies and the private sector.

However, establishing a CERT is just the beginning. The maturity of a CERT can only grow by performing the tasks assigned to the team combined with a culture of continuous improvement, supported by proper education and training. A country must put in place specific policies, procedures and workflows that support the CERT's goals and tasks. This also encompasses developing capacities of CERTs/CSIRTs and other crisis management bodies to participate in international partnerships and cooperation. Good connections to the international community and regional networks of CERTs/CSIRTs (e.g. FIRST, CERT Africa, etc.) help in solidifying expertise and ensuring that through a closer integration with the international community, national crisis management bodies have greater access to information and expertise.

⁹⁵ European Union Agency for Network and Information Security (ENISA), "National and International Cyber Security Exercises: Survey, Analysis and Recommendations", Heraklion, 2012.

TOOL 19: EXAMPLES OF ELEMENTS FOR THE CONSTRUCTION OF A LOGFRAME:

RESULTS CHAIN	INDICATORS	SOURCES AND MEANS OF VERIFICATIONS	ASSUMPTIONS AND RISKS
<p>IMPACT</p> <ul style="list-style-type: none"> > To increase cyber resilience of partner countries and ensure that citizens enjoy an open, free, secure and peaceful cyberspace 	<ul style="list-style-type: none"> > Country position in the ITU Global Cybersecurity and Cyberwellness Index > Network Readiness Index > Freedom on the Net report 	<ul style="list-style-type: none"> > Global Cybersecurity and Cyberwellness Index > Network Readiness Index > Freedom on the Net report 	<ul style="list-style-type: none"> > Stakeholders remain committed to the change process and adaptations it requires > The overall financial and technical capacity of the partner country will not decline > The Action is not disrupted by adverse events such as political instability or a fragile security situation
<p>OUTCOME(S)</p> <ul style="list-style-type: none"> > National operational capacities to adequately prevent, respond to, and recover from cyber attacks and/or accidental failures are improved 	<ul style="list-style-type: none"> > Status of policy provisions and/or regulations defining the responsibilities and resources of institutions competent for prevention, protection and recovery from cyber attacks and/or accidental failures > Status of a risk framework / guidelines for national authorities designed/updated > Status of cyber-related inspection and/or audit services within the individual institutions and bodies responsible for incident and crisis management 	<ul style="list-style-type: none"> > Text of the policies and/or regulations. An expert analysis may also need to be commissioned by the project to assess the stated provisions > Text of risk framework / guidelines > Text of the policy and/or regulation on the establishment of the inspection/audit services for cybersecurity 	<ul style="list-style-type: none"> > Stakeholders have a clear understanding of their roles and responsibilities > Good cooperation among ministries and agencies and acceptance of change; conflicts over turf are minimised > National governments actively seek the involvement of the private sector, manufacturers, etc. > Trained staff remain even beyond the capacity building activity > Ability of the implementing partners to mobilise the right expertise in time for the roll out of activities
<p>OUTPUT(S)</p> <ul style="list-style-type: none"> > Protection of critical information infrastructure is a stated national cyber policy objective 	<ul style="list-style-type: none"> > Protection of national critical information infrastructure is listed as a priority in a national strategic framework / cyber strategy designed/updated with the support of the Action 	<ul style="list-style-type: none"> > National reports identifying/mapping critical digital services, networks and infrastructure > National and international reports (ministries, regional organisations) about country's cybersecurity policies, risk management and their implementation 	
<p>Laws and regulation</p> <ul style="list-style-type: none"> > A regulatory framework for the security of network and information systems is developed/updated in line with international good practices 	<ul style="list-style-type: none"> > Status of legislation on setting up a national CERT/CSIRT and its oversight > Status of regulatory guarantees for CIIP drafted/updated with the support of the Action > Status of national cooperation framework/ guidelines in case of large scale cyber incident or crisis (crisis management mechanism) drafted/updated with the support of the Action 	<ul style="list-style-type: none"> > Text of the law setting up a national CERT/CSIRT and its oversight > Text of the regulatory framework for CIIP > National and international reports (ministries, regional organisations) about country's cybersecurity policies and their implementation 	

INCIDENT AND CRISIS MANAGEMENT

Institutions and resources

- > Cyber incident and crisis management structures are operational
 - > Status of governance framework for CIIP and cyber incident management created/developed with the support of the Action
 - > The national CERT/CSIRT has established parameters for organisational structure, human resources, tools and processes with the support of the Action
 - > Status of the national budget allocated to bodies and agencies responsible for cyber incident and crisis management
 - > Number of incident management/response cases monitored and handled by national CERT/CSIRT
 - > Number of CERT/CSIRT employees mentored/trained with the support of the Action (disaggregated by sex and age)
- > Text of national strategy/cyber crisis governance framework
- > National CERT/CSIRT mandate and responsibilities (website)
- > Assessment of Security Incident Management Maturity Model (SIM3)
- > Text of national budget/Official Journal
- > National CERT/CSIRT annual activity report/website
- > Action's reports/database of trained staff (disaggregated by sex and age)

Partnerships and cooperation

- > Mechanisms for effective information sharing and reporting on cyber incidents between stakeholders (private sector and government bodies) are in place
 - > Number of MoUs between key private sector entities (CI operators, vendors) and governmental bodies
 - > Number of active users of information sharing platforms/mechanisms established with the support of the Action
 - > National CERT/CSIRT membership to FIRST and TFCCSIRT
- > Formal and informal networks for sharing of best practices and incident information are created/strengthened
 - > Text of MoUs or press releases
 - > Administrative data to be requested from the cybersecurity institutions at the beginning and periodically until the end of the Action's implementation
 - > FIRST and TFCCSIRT websites

Potential activities

- > Technical assistance on policy, organisational, technical and cooperational dimensions of CIIP and cyber incident/crisis management
- > Training, workshops and other activities aimed at enhancing skills and promoting good practices
- > Table top exercises and mock operations

Pre-conditions

- > Partner country recognises the need for a strategic framework and cyber incident management, and commits to engage and support the implementation of activities
- > Partner country commits to the peaceful use of cyberspace

Table 6: Identifying a point of entry for cyber capacity building: incident and crisis management

	Vision and policies	Laws and regulation	Institutions and resources	Partnerships and cooperation
Advanced	Capacity to implement cyber crisis management principles and procedures Capacity to evaluate results and identify lessons, good practices	Comprehensive plans, procedures and protocols for emergency and incident response	Autonomous delivery of tools for strengthening cybersecurity Clearly prescribed roles of civilian and military actors Programmes and/or mechanisms for sharing good practices and lessons	Public and private CII operators perform joint exercises / stress tests Leadership and agenda-setting in regional or international networks
Developed	Implementation of the National Cyber Crisis Management Strategy Crisis communication structures are in place	Clearly defined norms and principles for critical infrastructure operators Voluntary and/or mandatory incident notification	Coordinated national cybersecurity response system to prevent, detect, deter, respond and recover from cyber incidents Training and exercises in the field of cyber crisis management CERT has a complete set of capabilities in place and has established a stable place in the community	States and other stakeholders develop and share strategic cyber crisis-management procedures and best practices Information sharing and collaboration between private and public organizations Participation in watch, warning and incident response information sharing
Developing	National Cyber Crisis Management Strategy	Legal framework setting minimum standards for network information security	Crisis management structure with clearly defined command chain, SOPs, etc. A focal point for managing cyber incidents/crises CERT has baseline capabilities (operations) in place and trust among the CERT community	Point(s) of contact within government agencies, the private sector and international partners Membership in FIRST or other regional networks
Basic	Cyber incident and crisis management is recognised in national cybersecurity strategy Mechanisms for regular assessment of vulnerability	CERT has a clear mandate on a specific regulatory basis	CERT is being established and trying to earn recognition in the CERT community (based on individual trust building). Availability of affordable tools, software, etc. for cybersecurity	Stakeholders share a basic understanding of what cyber crisis management is

Cyber exercises are an important tool to assess the preparedness of a community to respond to cyber crises, technology failures and critical information infrastructure incidents. Exercises enable competent authorities to target specific weaknesses, increase cooperation across the CII sector, identify interdependencies, stimulate improvements in continuity planning and generate a culture of cooperative effort to boost resilience. Supporting cybersecurity exercises is therefore a major objective of cyber capacity building in the medium- to long term.⁹⁶ Experience has shown that exercises are an effective way for the public and private sectors to train and test various scenarios regarding crisis management processes and structures, contingency plans and communications on a local, national, regional and international level. This, however, is only likely to lead to improvements if accompanied by a proper lessons identification mechanism, including evaluation and recommendations. Ultimately, exercises also contribute to strengthening coordination between CERTs/CSIRTs and other relevant actors (i.e. national critical infrastructure operators, law enforcement, politicians), enhance awareness, test information sharing mechanism and establish communication and information exchange channels between stakeholders.

A parallel path to building cyber resilience focuses on creating an integrated and comprehensive cyber crisis management system with clearly prescribed responsibilities, procedures and resources. Such a system should also include strong incident capture and analytics capacities, in particular to examine the cyber threat landscape and to glean insights into the effectiveness of countermeasures. However, overcomplicated response plans and procedures may delay the effectiveness of incident response and de-escalation procedures.

Cyber crisis response and management is impossible without sharing of information regarding cybersecurity threats, vulnerabilities, exploits, incidents and risks and collaboration with a broad stakeholder community. That helps information security professionals to investigate incidents, mitigate them and develop technical and organisational responses to prevent repeat occurrences.⁹⁷ In addition, policy-makers can better understand the relative state of cybersecurity and craft suitable policy responses if such information is shared between the public and private sectors. There is a degree of uncertainty with respect to the legal basis of much CERT cross-border coordination since most of it happens on an informal basis. Evidence from ENISA research indicated that in practice, data protection, data retention and obligations to work with law enforcement constituted the greatest set of challenges for cross-border CERT cooperation.⁹⁸

Finally, there is a whole set of risks that need to be addressed in the design of capacity-building actions. These range from difficulty of attracting and retaining skilled IT security personnel, the lack of a full appreciation at the political level of the importance of investing resources in incident response activities and the risk of incompatibility with other donor activities. Ultimately, even best equipment may be ineffective if unmanned, untested, not updated or if a properly trained team is not in place.

4. Cyber hygiene and awareness

People are often mentioned as the weakest link and the most important asset in the cybersecurity chain. Increasingly sophisticated types of cybercrime – e.g. new methods of spear-phishing and social engineering – put the users on the losing end and make it very difficult for policymakers and companies to keep up. However, most attacks are made possible due to human error or irresponsible behaviour. More worryingly, such behaviour does not always stem from the lack of information but also from conscious decisions to ignore established practices for enhancing security and safety online, e.g. on password protection or opening links from unknown sources. There are several reasons for that, including the general anxiety that the technical aspects of cybersecurity often cause and the lack of a clear research base on how to best improve cyber hygiene. Consequently, raising public awareness and engagement on cybersecurity is often challenging. Yet the

96 See: European Union Agency for Network and Information Security (ENISA), "National and International Cyber Security Exercises: Survey, Analysis and Recommendations", Heraklion, 2012; European Union Agency for Network and Information Security (ENISA), "Emergency Communications Stocktaking: A study into Emergency Communications Procedures", Heraklion, 2012; European Union Agency for Network and Information Security, "Report on Cyber Crisis Cooperation and Management: Comparative study on the cyber crisis management and the general crisis management", Heraklion, 2014; ENISA, "Technical Guideline on Incident Reporting: Technical guidance on the incident reporting in article 13a", Heraklion, 2014.

97 See Dependability Development Support Initiative (2002) Roadmap: Warning and Information Sharing.

98 European Union Agency for Network and Information Security (ENISA), "A flair for sharing – encouraging information exchange between CERTs. A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe", Heraklion, 2011.

effort is seen as one of the pillars in building cyber resilience and ultimately fostering economic and social development.⁹⁹

4.1. Policy analysis

The basic premise of awareness raising is to focus the attention of a targeted group (e.g. end users, companies, institutions) on cybersecurity as a legitimate concern.¹⁰⁰ Cyber hygiene complements such efforts by developing automatic impulses based on proactive thinking about cybersecurity-related aspects of their on-line behaviour (e.g. using products/tools that fit our hygiene needs, performing these hygienic tasks correctly and establishing a routine).

Available research findings suggest that while many countries and organisations consider cyber hygiene to be important it is still not a priority for many unless there is a pressing, external need to comply, including through government regulation or terms of contract.¹⁰¹ Given that cybersecurity nowadays is everybody's responsibility, it is essential that individual users at home or at work understand the threat and are equipped with the tools and skills necessary to detect and protect themselves against attacks, including appropriate risk-based cybersecurity programmes and intelligence about the evolving risk landscape.

Market-based models for promoting cyber hygiene have had limited success,¹⁰² so various regional and international organisations as well as individual actors have addressed the need to establish a culture of cybersecurity. Several resolutions adopted by the UN General Assembly¹⁰³ stress that individual users and organisations should be aware of the need for security of information systems and networks, and that they bear a share of the responsibility for the security of such systems to the extent appropriate to their individual roles. This includes the need to regularly review and adapt their own policies, practices, measures and procedures.

At the EU level, promoting cyber hygiene and awareness is a key objective in the joint communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, presented in 2017. According to the document, '*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*'. In 2017, ENISA presented an overview of programmes and methods used by individual Member States, including a list of best practices.¹⁰⁴ Recognising that there is no EU-wide standard or commonly agreed approach to cyber hygiene, the report stressed the importance of promoting cyber hygiene schemes, particularly those targeting small- and medium-sized enterprises, throughout the EU. Another challenge identified in the report is the trend to base national awareness programs on the pull method (i.e. to have information available on request) rather than a push approach that provides information and guidance in a more pro-active way.

Overall, most programmes and initiatives focused on cyber hygiene and awareness aim to promote 'good health online'. That involves identifying, prioritising and responding to risks in five main spheres: perimeter, network, individual devices, the cloud and the supply chain.¹⁰⁵ Several delivery methods exist to ensure reaching broad audiences, including through brochures, newsletters, handbooks, training and awareness courses, interactive cybersecurity websites, exercises and viral marketing campaigns.¹⁰⁶ To address the growing need for cybersecurity professionals, several countries faced with a skills shortage organise regular competitions for students and professionals to find cyber talent and encourage people to pursue a career in cybersecurity. The importance of such initiatives cannot be overstated in the context of the rapid development of the Internet of Things, where basic mechanisms and operations are often based on weak security standards and hyper connectivity.

99 See GFCE, Global Agenda for Cyber Capacity Building.

100 NIST, Information technology security training requirements: A role- and performance-based model, NIST — SP 800-16, USA, 1998.

101 European Union Agency for Network and Information Security, "Review of Cyber Hygiene practices", February 2016.

102 See the 2016 National Cybersecurity Strategy of the United Kingdom.

103 Resolution 55/63 (2000) and 56/121 (2001) on combatting criminal misuse of information technologies, 57/239 (2002) on the creation of a global culture of cyber security, 58/199 (2003) on the creation of a global culture of cyber security and the protection of critical information infrastructure.

104 European Union Agency for Network and Information Security, "Review of Cyber Hygiene practices", February 2016.

105 Ibid.

106 European Union Agency for Network and Information Security, "The new users' guide: How to raise information security awareness", November 2010.

4.2. Engagement

Engagement in cyber hygiene and awareness raising initiatives with partner countries represents a relatively low political risk, assuming the primary focus is on improving the public's sensitivity and knowledge base concerning cyber vulnerabilities. Therefore, cyber awareness raising campaigns are usually a good ground for strengthening cooperation with partner countries on cybersecurity issues. However, there are instances where such projects may not be that straightforward, particularly when they are aimed at individuals and organisations operating in a constraining regulatory environment (for instance, human rights defenders, journalists or members of political opposition parties). In such cases, governments may perceive such activities as hostile and an attempt to limit their sovereignty in their own territory. Some governments may want to use such initiatives as a pretext to acquire new skills that may then be used in a more strategic way to promote political views and values that might be in conflict with the EU's own approach. It is therefore critical that such risks are identified and assessed from the very beginning.

Engagement on cyber hygiene and awareness raising may also be one of the riskiest areas from the effectiveness point of view since there are many factors outside of the implementer's control. Even well-designed and executed campaigns can bring very limited results if the target group does not engage and commit to the objective. This is also linked to the constantly evolving threat landscape.

4.3. Risk mapping

A growing number of successful cyber attacks and resulting losses have been broadly attributed to the lack of cyber hygiene and poor security management. The threat landscape in the cyber domain also changes on a daily basis, which makes it very difficult for any organisation to keep their online security policies up to date. In addition, techniques for gaining access to systems and data are becoming more sophisticated. Social engineering – the process of psychologically manipulating people into performing actions or divulging confidential information – nowadays take the shape of sophisticated phishing campaigns or a convincing story delivered to a customer over the phone. In that sense, poor cybersecurity hygiene and a low awareness about potential threats and vulnerabilities make it easier for adversaries to gain access to personal and financial information as well as steal ideas, research formulas or blueprints that may decide the fate of an entire company or organisation. The evolution of the Crime-as-a-Service infrastructure and autonomous attack tools enable adversaries to easily operate on a global scale by exploring vulnerabilities that had already been identified and patched (as was the case of both WannaCry and NotPetya attacks in 2017). At the same time, the growing number of internet-enabled devices in use – often with non-existent or poor security solutions – contributes to higher vulnerability. The issue is particularly relevant for organisations involved in national security, which often still rely on off-the-shelf solutions or commercial providers of cloud services such as hosting, email and domain services.

4.4. Key stakeholders

According to some estimates, about 80 percent of exploitable computer vulnerabilities are the direct result of poor or no cyber hygiene.¹⁰⁷ Given the open nature of the cyber ecosystem, the responsibility for security is distributed among all internet users at all levels: individual, organisation and society. Therefore, the pursuit of a whole-of-government and whole-of-society method in this specific policy area is particularly pertinent.

Individuals are primarily responsible for taking basic and proactive steps to secure their networks and devices, including through software updates, strong, secure passwords and modern firewall and security techniques. Several of these steps can be enforced through security and data protection policies adopted by organisations and institutions in their relations with employees or clients. In that sense, organisations and institutions as well as service providers and technology designers play an important role in instilling collective responsibility. State institutions play a crucial role in providing the impulse and providing leadership for national efforts aimed at improving cyber hygiene and awareness. The ultimate goal is to develop a culture of cybersecurity throughout the internet ecosystem. A concentrated national outreach to reiterate the role of individuals might improve their feeling of empowerment and generate stronger buy-in towards proposed actions and initiatives.

¹⁰⁷ See MITRE's [website](#) for further information.

Promoting cyber hygiene and conducting awareness campaigns are resource intensive and therefore even committed organisations are not always fully able to do so. That highlights the importance of integrating existing resources and opens the door to a stronger role by government bodies and consumer organisations that have the expertise and legitimacy to coordinate large-scale efforts at the regional or national level. The list of actors with required expertise (and interests) in improving cyber hygiene is long: academic and research institutions, ICT sector (telecom companies, ISP and mobile players), critical infrastructure operators, law enforcement professionals and civilian agencies, technical professionals (system and network engineers, system administrators, software developers), justice and police professionals (judge, prosecutor, regulator) and policymakers across all branches of government.

4.5. Capacity assessment and needs analysis

Assessing the needs and existing capacities linked to cyber hygiene and awareness is particularly difficult compared to other four pillars. Hygiene and awareness is not solely about access to information and a general knowledge of broadly defined cyber threats but about how people and organisations adapt their attitudes and behaviour on the basis of acquired information and knowledge. Therefore, it is not enough to look at polls to check what percentage of the public is aware of the risks online. What matters for capacity building on cyber hygiene and awareness is the assessment of structural elements that allow citizens and organisations to assess their vulnerabilities and the risks to their operations, and to respond with concrete actions. That means, for instance, looking into how aspects of child protection online are reflected in school curricula, the regularity of resources committed to awareness raising, or systematic reviews of gaps in knowledge or awareness concerning cybersecurity and information security issues among selected groups.

BOX 30: ANALYSING NEEDS - CYBER HYGIENE AND AWARENESS

Vision and policies

- Are major threats and risks to the public assessed regularly?
- Is there a national cyber awareness-raising programme or campaign, e.g. a cyber month?
- Is cyber awareness and hygiene mainstreamed into other policy areas, in particular on digital skills, education, etc.?

Laws and regulation

- Are there laws and regulations pertinent to cyber hygiene and awareness raising (e.g. electronic communications, data protection, information security)?
- Are there existing sector specific strategies for awareness raising or other regulatory measures aimed at improving cybersecurity (e.g. mandatory incident reporting)?
- How are cyber hygiene and awareness raising included in terms and conditions or other contractual arrangements for services provided by public- and private-sector organisations?
- Do other forms of soft regulations exist (e.g. public-private partnerships)?

Institutions and resources

- What are the roles and responsibilities of government agencies, consumer organisations, ombudsmen, etc. to deal with cyber hygiene and awareness raising? What are the overlaps or gaps in their mandates and activities?
- Does a country devote sufficient resources (financing, manpower, etc.) or other means to facilitate cyber hygiene and awareness-raising initiatives?

Partnerships and cooperation

- What cooperation and coalition-building mechanisms between public and private sector / civil society are in place?
- How do these stakeholders contribute to the objectives of the strategic framework and what are their respective responsibilities?
- Are there sufficient incentives for the private sector and civil society to participate in the process?

4.6. Building an intervention logic

Building a resilient society requires the engagement of diverse groups of stakeholders with different levels of awareness and expertise regarding cyber-related issues. It is therefore essential to improve cyber hygiene and awareness as the main component of a cybersecurity culture, based on a sense of shared responsibility for cyber resilience among stakeholders at all levels. Ultimately, a strong cybersecurity culture contributes to strengthening state and societal resilience and allows end users – citizens, enterprises, organisations – to enjoy more fully and safely the economic, social and political opportunities in cyberspace.¹⁰⁸

The underlying assumption steering these efforts is that good cyber hygiene practices will ultimately increase immunity across businesses and organisations, reducing the risk that a weak link within a supply chain or network will be used to compromise other members. Supporting countries in raising the level of cyber hygiene and awareness to the highest possible level can also improve trade and political relations as it increases mutual trust in capacities and security standards. Thus, cyber hygiene and awareness contribute to the development of a cybersecurity culture, a key element in the analysis at the level of the enabling environment. According to ENISA, the desire for a strong cybersecurity culture within organisations stems from the recognition that the shared beliefs, values and actions of employees regarding cybersecurity are directly related to how vulnerable an organisation is to a malicious cyber operation. To facilitate the process whereby employees become ‘human firewalls’ against cyber attacks, organisations need to create a work environment that reinforces and encourages complying with security policies as an important aspect of doing one’s job.¹⁰⁹

A stronger cybersecurity culture can be achieved by pursuing specific objectives. First is increasing and reinforcing awareness of cybersecurity among the public, private sector and government employees, both in terms of associated risks and threats as well as existing solutions and protective measures. For instance, the Information System Authority of the Republic of Estonia (RIA) launched in 2018 the CybExer Cyber Hygiene online training platform for all Estonian civil servants to test and improve their awareness of threats emerging from the digital environment. One obstacle to broader investment in cyber hygiene and awareness raising is the perception that cybersecurity is expensive (i.e. need expensive tools, skilled professionals, ISO 27001 certification on information security) and consequently will erode company profits.

Second, enhancing digital literacy and a cybersecurity mind set across the government and society is important to ensure that development interventions, enhanced by the use of digital technologies, generate positive outcomes for the target groups and leave no one behind. This can be achieved through increased investment in cybersecurity-related education programmes as well as general education about information-security threats for end users. Concrete initiatives can focus on the development of dedicated cybersecurity curricula, education- and awareness-raising materials, development of specific skills through training, streamlining the applicability of degrees and mutual recognition of certifications. Such initiatives would also contribute towards closing a global cybersecurity skills gap.

Furthermore, cybersecurity standards and practices provide agencies, sectors and businesses with a well-established body of knowledge and harmonised approach to increase preparedness, response and recovery capacities, which also contributes to enhancing cooperation, mutual understanding and information exchanges. Some professional level of both general and sector-specific cybersecurity expertise is needed in every critical sector: end-to-end network and systems security for servers (telecommunications); defence against financial cybercrime and ID theft (banking/finance); digital forensics and e-crime investigation units (civil and military forces); and operational control networks for pipelines for oil, gas and water (energy/water utilities). Public bodies and agencies, especially those providing essential services, should ensure that their staff are trained in cybersecurity-related areas. Because standards and practices play such an important role in strengthening cyber resilience, it is key to ensure that compliance is closely monitored and reported. However, there is also a significant risk that the additional time and resources needed to comply with all the requirements imposed by regulatory bodies might prove troublesome for small and medium-sized enterprises or companies relying on global supply chains.

¹⁰⁸ For an overview and concrete proposals regarding the design, implementation and result-based monitoring of cyber hygiene and awareness raising initiatives, see a series of publications by ENISA available at <https://www.enisa.europa.eu/topics/cybersecurity-education>.

¹⁰⁹ ENISA (2018) *Cyber Security Culture* in organisations.

TOOL 20: EXAMPLES OF ELEMENTS FOR THE CONSTRUCTION OF A LOGFRAME:

RESULTS CHAIN	INDICATORS	SOURCES AND MEANS OF VERIFICATIONS	ASSUMPTIONS AND RISKS
<p>IMPACT</p> <ul style="list-style-type: none"> > To increase cyber resilience of partner countries and ensure that citizens enjoy an open, free, secure and peaceful cyberspace 	<ul style="list-style-type: none"> > Country position in the ITU Global Cybersecurity and Cyberwellness Index > Country position in the World Economic Forum's Network Readiness Index > Country position in the Freedom on the Net Report by Freedom House 	<ul style="list-style-type: none"> > Global Cybersecurity and Cyberwellness Index > Network Readiness Index > Freedom on the Net report 	<ul style="list-style-type: none"> > Stakeholders remain committed to the change process and adaptations it requires > The overall financial and technical capacity of the partner country does not decline > The Action is not disrupted by adverse events such as political instability or a fragile security situation
<p>OUTCOME(S)</p> <ul style="list-style-type: none"> > Trust of users, organisations, and companies in the use of cyberspace is enhanced 	<ul style="list-style-type: none"> > Percentage of citizens who express confidence in the use of cyberspace > Percentage of organisations and companies that express confidence in the use of cyberspace > Percentage of internet penetration in the country 	<ul style="list-style-type: none"> > Public perception on the basis of baseline and final study to be commissioned by the Action (disaggregated by sex and age) > National data at the beginning and end of the Action 	<ul style="list-style-type: none"> > Stakeholders have a clear understanding of their roles and responsibilities > Good cooperation among ministries and agencies and acceptance of change; conflicts over turf are minimised > National governments actively seek the involvement of the private sector; manufacturers, etc. > Trained staff remain even beyond the capacity building activity > Ability of the implementing partners to mobilise the right expertise in time for the roll out of activities
<p>OUTPUT(S)</p> <ul style="list-style-type: none"> > Vision and policies > Improving cyber hygiene and awareness is a stated national cyber policy objective > Awareness and cyber hygiene practices of individual users (e.g. employees, citizens, students) are improved 	<ul style="list-style-type: none"> > Cyber hygiene and awareness is listed as a priority in a national strategic framework / cyber strategy > A national Cyber Awareness Month takes places annually > Number of national or local trainings or awareness raising strategies designed and implemented with the support of the Action 	<ul style="list-style-type: none"> > Improving cyber hygiene and awareness is a stated national cyber policy objective > Text of the strategy > National Cyber Awareness Month website and/or press releases > Number of persons reached by awareness raising campaigns implemented with the support of the Action > National surveys (web, phone) on cybersecurity awareness and hygiene undertaken at the start and end of the Action > Industry reports on phishing and malware spread in country at the start and end of the Action 	

CYBER HYGIENE AND AWARENESS

Laws and regulation

- > Provisions promoting cyber hygiene and technical standards in line with existing international best practices (i.e. ICT security standards and cryptographic controls, procurement standards for ICT, etc.) are introduced in laws, regulations and government tenders
- > Status of relevant laws/regulations
- > Text of the laws/regulations
- > Text of government ICT procurement tenders

Institutions and resources

- > Cyber awareness and incorporation of cyber hygiene technical standards in line with existing international best practices are rolled-out in governmental services
- > Status of the national budget allocated to the roll-out of cyber awareness and hygiene programmes
- > Number of staff mentored/trained with the support of the Action on cyber hygiene practices and technical standards
- > Text of the national budget/ Official Journal
- > Administrative data requested by the relevant national authorities
- > Action's reports/database of mentored/trained staff (disaggregated by sex and age)

Partnerships and cooperation

- > A comprehensive multi-stakeholder cyber hygiene and awareness programme is in place
- > Number of institutions, organisations, and individuals participating in an awareness raising campaign or training
- > Number of collaborative awareness raising campaigns (e.g. Cyber Month) and programmes developed and rolled-out with the support of the Action
- > Number of institutions, organisations, and individuals participating in an awareness raising campaign or training
- > Action's reports/database of event participants (disaggregated by sex and age)

OUTPUT(S)**Potential activities**

- > Training, workshops and other activities aimed at enhancing skills and promoting good practices, including defining modalities for implementation
- > Table top exercises and mock operations
- > Awareness raising campaigns
- > Best practice guides and lessons learned manuals

Pre-conditions

- > Partner country recognises the need for a strategic framework and the importance of cyber hygiene, and commits to actively engage and support the implementation of activities
- > Partner country commits to the peaceful use of cyberspace

Table 7: Identifying a point of entry for cyber capacity building: cyber hygiene and awareness

	Vision and policies	Laws and regulation	Institutions and resources	Partnerships and cooperation
Advanced	<p>Academic and research institutions participate in development of education and training curricula</p> <p>Ensuring best practices are reviewed and updated on an annual basis</p> <p>Cybersecurity is mainstreamed into skills programmes, e-government and awareness campaigns</p> <p>Clear policies around data breach notifications to the public and users and follow up information campaigns</p>	<p>Implementation of the 'duty of care', 'security by design', and 'data protection by default and by design' principles</p> <p>Adoption of certification and labelling to guide consumers</p> <p>Capacity to develop and implement guidelines for Secure Development Lifecycle*</p> <p><small>* The SDL is a process that standardises security best practices across a range of products and/or applications.</small></p>	<p>Consumer protection or ombudsman bodies assume responsibility in cyber domain</p> <p>Training and skill development</p> <p>Governmental support to low-income citizens and businesses with limited means</p> <p>A one-stop-shop to help victims of cyberattacks, providing information on latest threats and bringing together practical advice and cybersecurity tools</p>	<p>The tech and software industry recognise their role beyond that of device or service providers and implement security at all stages of the development lifecycle</p> <p>CERT Resilience Management Model** that supports cyber hygiene is in place</p> <p><small>** https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html</small></p>
Developed	<p>Education and building culture that focuses on resilience of systems</p> <p>Programmes and plans for cybersecurity related education and skill development exist and are implemented</p>	<p>Building trustworthy systems (cryptography standards)</p> <p>Use of electronic identification and trust services by citizens, businesses and public administrations to access online services or manage electronic transactions.</p> <p>Cybersecurity standards for government and the private sector, in line with existing international best practices</p>	<p>Awareness building and education programmes focused on cyber resilience</p> <p>SMEs have access to technologies that increase their resilience to cyberattacks</p> <p>Raising awareness of online abuse and gender-based violence</p> <p>Government invests in research and development activities to develop solutions to cyber risks</p> <p>Security accreditation and certification of skilled personnel</p>	<p>Coordinated national and international campaigns</p> <p>Multi-sector and multi-stakeholder cybersecurity training and awareness programmes</p>

	Vision and policies	Laws and regulation	Institutions and resources	Partnerships and cooperation
Developing	National information security training, educational and awareness-raising programmes Mechanisms for assessing individual risks, identifying high-risk assets and scaling their security	Development and application of appropriate standards to products	Development of training modules and professional cybersecurity roles for CSO/CISO, network security specialists, digital forensics and incident response analysts, information-security assessor, security architect, vulnerability analysts, information security systems and software development Developing best practices and guidelines	Ethical standards are endorsed and promoted at all levels among the broad stakeholder community Civil society, the private sector and research community participate in governance of cyber domain Participation in relevant regional and international initiatives
Basic	A national awareness programme exists to encourage all participants to secure their own cyberspace	Basic cyber hygiene and awareness raising mechanisms are included in service contracts and terms of use, e.g. password management policies, limiting the use of certain functions, encryption	A catalogue of roles and relevant educational backgrounds needed	Citizens and users have access to quality information on how to manage their devices A national cybersecurity month, week or day is organised regularly to engage public and private partners

Finally, increasing involvement and establishing clear communication channels with stakeholders at all levels facilitates information exchange and consequently builds safer communities online. This is particularly relevant for law enforcement, private-sector companies and individual users. An example of such engagement is the ‘No More Ransom’ campaign launched by the Dutch police force’s National High-Tech Crime Unit, Europol’s European Cybercrime Centre and cybersecurity companies to help users prevent ransomware infections and decrypt data if they are victims of an attack.

There is also a set of cross-cutting assumptions and risks that need to be factored into any efforts aimed at strengthening cyber hygiene and awareness.¹¹⁰ As technology changes, it is very difficult – if not impossible – to ensure that awareness-raising initiatives are up to date. In these instances having broad coalitions and cooperation networks increases the possibility that the right type of information is available and shared in a timely manner. Experience also suggests that over-education is a common pitfall, as there tends to be a threshold as to how much information the public can absorb from a single source within a given period of time. Some challenges are linked to changing or un-learning established patterns of behaviour, given that cybersecurity is still too often approached as an afterthought. A lack of managerial or political support for cyber hygiene or awareness-raising projects contributes to the perception of cybersecurity as a luxury rather than an integral part of society’s or an organisation’s DNA. In that context, any decision or concrete action that contributes to improving cyber resilience in a country, community or company can be evidence of growing awareness and hygiene. The problem, however, lies in establishing a causal link between concrete initiatives and such outcomes.

¹¹⁰ Ibid.

REFERENCES

- Abelson, H. et al. (2015) “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications”, *Massachusetts Institute of Technology*, Cambridge.
- Boulton, C. (2017) “Humans are (still) the weakest cybersecurity link”, CIO.
- Calderaro, A. (2015) “Internet Governance Capacity Building in Post-Authoritarian Contexts. Telecom Reform and Human Rights in Myanmar”, SSRN.
- Commission of the European Communities (2009) “Communication from the Commission to the European Parliament and the Council - Internet Governance: the next steps”, COM(2009) 277 final, Brussels.
- Council of Europe (2001) “Convention on Cybercrime” CETS 185, Strasbourg.
- Council of Europe (2001) “Explanatory Report to the Convention on Cybercrime CETS 185”, Strasbourg.
- Council of Europe (2013) “Capacity Building on cybercrime”, Discussion paper, Strasbourg.
- Council of Europe, “Cybercrime – Worldwide Capacity Building overview”.
- Council of the European Union (2003) “A Secure Europe in a Better World – European Security Strategy”, Brussels.
- Council of the European Union (2007) “EU Code of Conduct on Complementarity and Division of Labour in Development Policy – Conclusions of the Council and of the Representatives of the Governments of the Member States meeting within the Council”, 9558/07, Brussels.
- Council of the European Union (2007) “Security and Development - Conclusions of the Council and the Representatives of the Governments of the Member States meeting within the Council”, 15097/07, Brussels.
- Council of the European Union (2013) “Council Conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, 12109/13, Brussels.
- Council of the European Union (2014) “Council conclusions on Internet Governance”, 16200/14, Brussels.
- Council of the European Union (2014) “EU Human Rights Guidelines on Freedom of Expression Online and Offline”, Brussels.
- Council of the European Union (2015) “Council Conclusions on Cyber Diplomacy”, 6122/15, Brussels.
- Council of the European Union (2016) “Conclusions of the Council of the European Union on the European Judicial Cybercrime Network”, 10025/16, Brussels.
- Council of the European Union (2016) “Council Conclusions on ‘mainstreaming digital solutions and technologies in EU development policy’”, 14682/16, Brussels.
- Council of the European Union (2016) “Cyber capacity building: towards a strategic European approach”, 8732/1/16, Brussels.
- Council of the European Union (2015) “Joint paper by Europol and Eurojust on Common challenges in combating cybercrime”, 14812/15, Brussels.
- Council of the European Union (2018) “Council conclusions on malicious cyber activities”, 7925/18, Brussels.
- Council of the European Union (2018) “Council Conclusions on EU External Cyber Capacity Building Guidelines”, 10496/18, Brussels.
- Court of Justice of the European Union (2014) “Digital Rights Ireland and Seitlinger and Others, Joined cases” C-293/12 and C-594/12
- Davis, A. ; Lemma, T. and Wignaraja, K. (2009) “Capacity development. A UNDP primer”, United Nations Development Programme, New York.
- Dependability Development Support Initiative (2002) “Roadmap: Warning and Information Sharing.”
- Deutsche Gesellschaft für Internationale Zusammenarbeit (2012) “Capacity works: Success Stories”, Bonn.
- Dix, R. and Folk, C. (2015) “Driving Cybersecurity Awareness Home” AFCEA International Cyber Committee White paper Series.
- European Commission (2005) “Institutional Assessment and Capacity Development: why, what and how?”, *Tools and Methods series*, Reference doc n°1, Luxembourg.
- European Commission (2009) “Making Technical cooperation more effective”, *Tools and Methods series*, Guidelines n°3, Luxembourg.
- European Commission (2010) “Toolkit for Capacity Development 2010”, *Tools and Methods Series*, Reference Document no 6, Brussels.

- European Commission (2012) “Communication from the Commission to the European Parliament and the Council – The EU approach to resilience: Learning from food security crises”, COM(2012) 586 final, Brussels.
- European Commission (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, Brussels.
- European Commission (2013) “Commission Staff Working Document – Paving the way for an EU Development and Cooperation Results Framework”, SWD(2013) 530 final, Brussels.
- European Commission (2014) “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A stronger role of the Private Sector in Achieving Inclusive and Sustainable Growth in Developing Countries”, COM(2014) 263, Brussels.
- European Commission (2015) “Commission Staff Working Document – Launching the EU International Cooperation and Development Results Framework”, SWD(2015) 80 final, Brussels.
- European Commission (2015) “ROM Handbook: Instructions and guidance for ROM reviews and support to end-of-project results reporting for projects and programmes financed by the European Union within the framework of its external assistance”, DG DEVCO, Brussels.
- European Commission (2016) “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry”, COM(2016)410 final, Brussels.
- European Commission (2016) “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Proposal for a new European Consensus on Development our World, our Dignity, our Future”, COM(2016) 740 final, Brussels.
- European Commission (2016) “Guidelines on linking planning/programming, monitoring and evaluation”, DG NEAR, Brussels.
- European Commission (2016) “Integrating the environment and climate change into EU international cooperation and development. Towards sustainable development”, *Tool and Methods Series, Guidelines n°6*, Brussels.
- European Commission (2017) “Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises”, C(2017) 6100 final, Brussels.
- European Commission (2017) “Commission Staff Working Document – Digital4Development: mainstreaming digital technologies and services into EU Development Policy”, SWD(2017) 157 final, Brussels.
- European Commission (2017) “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the Implementation of the Digital Single Market Strategy: A connected digital single market for all”, COM(2017) 228 final, Brussels.
- European Commission (2017) “Cybersecurity in the European Digital Single Market”, Scientific Opinion No. 2/107, High Level Group of Scientific Advisors, Brussels.
- European Commission (2017) “Proposal for a Regulation of the European parliament and of the Council on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”)”, COM(2017) 477 final, Brussels
- European Commission (2018) “Flash Eurobarometer 464: Fake News and Disinformation Online”, Brussels
- European Commission (2018) “Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings”, COM(2018) 226 final, Brussels.
- European Commission (2018) “Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters”, COM(2018) 225 final, Brussels.
- European Commission (2018) “Tackling online disinformation: Commission proposes an EU-wide Code of Practice”, *Press Release*, Brussels.
- European Court of Human Rights (2008) “Case of K.U. v Finland” Application no. 2872/02, Strasbourg.
- European External Action Service (2018) “Permanent Structured Cooperation (PESCO) – Factsheet”, Brussels.
- European Parliament and Council of the European Union (2016) “Directive 2016/1148 concerning measures for a high common level of security of Network and Information Systems across the Union (NIS Directive)” *Official Journal of the European Union*, L194, pp. 1-29

- European Parliament and Council of the European Union (2016) “Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, *Official Journal of the European Union*, L 119, pp.1-88.
- European Union Agency for Network and Information Security (ENISA) (2010) “The new users’ guide: How to raise information security awareness”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2011), “A flair for sharing – encouraging information exchange between CERTs. A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2012), “Emergency Communications Stocktaking: A study into Emergency Communications Procedures”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2012), “Introduction to Return on Security Investment: Helping CERTs assessing the cost of (lack of) security”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2012), “National and International Cyber Security Exercises: Survey, Analysis and Recommendations”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2014), “An evaluation Framework for National Cyber Security Strategies”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2014), “Technical Guideline on Incident Reporting: Technical guidance on the incident reporting in article 13a”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2014), “Report on Cyber Crisis Cooperation and Management: Comparative study on the cyber crisis management and the general crisis management”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2015), “CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2016) “NCSS Good Practice Guide. Designing and implementing National Cyber Security Strategies”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2016), “Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity”, Heraklion.
- European Union Agency for Network and Information Society (ENISA) (2016) “ENISA’s Opinion paper on encryption. Strong Encryption Safeguards our Digital Identity”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2016), “Strategies for Incident Response and Cyber Crisis Cooperation”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2017) “Review of Cyber Hygiene practices”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2018), “Public Private Partnerships (PPP) – Cooperative models”, Heraklion.
- European Union Agency for Network and Information Security (ENISA) (2018) “Cyber Security Culture in organisations”, Heraklion.
- Europol (2016) “Avalanche network dismantled in international cyber operation”, *Press Release*
- Europol (2017) “Andromeda botnet dismantled in international cyber operation”, *Press Release*
- Europol (2017) “Internet Organized Crime Threat Assessment (IOCTA)”.
- Fiddner, D. (2015) “Defining a Framework for decision making in cyberspace”, IBM Centre for the Business of Government.
- Forum of Incident Response and Security Teams (FIRST) (2017) “Draft PSIRT Services Framework”.
- G8 Summit (1998) “Drugs and International Crime”, Birmingham Summit.
- Gill, L.; Israel, T. and Parsons, C. (2018) “Shining a Light on the Encryption Debate: A Canadian Field Guide” *The Citizen Lab*.
- Global Forum on Cyber Expertise (GFCE) (2017) “Global Agenda for Cyber Capacity Building: Putting Principles into Practice”, The Hague.
- Global Forum on Cyber Expertise (GFCE) (2017) “Global Good Practices: National Computer Security Incident Response Teams”, The Hague.
- Global Forum on Cyber Expertise (GFCE) (2017), “Global Good practices identified by the GFCE community”, The Hague.
- Gustafsson, I.; Iles, E. and Schulz, K. (2007) “Manual for Capacity Development”, SIDA, Stockholm.
- Hathaway, M. (2015) Cyber Readiness Index 2.0, Potomac Institute.

- International Organisation for Standardisation (ISO) (2012) "Information technology – Security techniques – Guidelines for cybersecurity", ISO/IEC27032.
- International Telecommunication Union (ITU) (2017) "ICT Facts and Figures 2017".
- International Telecommunication Union (ITU) "Our Mandate, Mission and Strategy".
- International Telecommunication Union (ITU) "CIRT Programme".
- Internet Governance Forum (2014), "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security", Istanbul.
- Internet Society (2016) "Internet Governance: Why the Multistakeholder Approach Works".
- Kelly, S. et al. (2017) "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy", Freedom House.
- Lawson, S. (2012) "Putting the 'war' in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States", *First Monday*, vol.17, n°.7.
- Lucas, B. (2013) "Current thinking on capacity development", GSDRC Helpdesk Research report No. 960, Birmingham.
- Luijff, E.; Van Schie, T. and Van Ruijven, T. (2017) "Companion Document to the GFCE-Meridian Process Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers", GFCE-MERIDIAN.
- Malik, K. (2013) "Human Development Report 2013 – The Rise of the South: Human progress in a Diverse World", United Nations Development Programme, New York.
- Morgan, S. (2015) "Cybersecurity job market to suffer severe workforce shortage" CSO
- National Institute of Standards and Technology (NIST) (1998) Information technology security training requirements: A role- and performance-based model, Computer Security Resource Center — SP 800-16, USA.
- Organisation for Economic Cooperation and Development (OECD) (1992) "OECD Guidelines for the Security of Information Systems", Paris.
- Organisation for Economic Cooperation and Development (OECD) (2006), "The Challenge of Capacity Development. Working towards good practice", Paris.
- Organisation for Economic Cooperation and Development (OECD) (2014) "Mainstreaming cross-cutting issues – 7 Lessons from DAC Peer Reviews", Paris.
- Organisation for Economic Cooperation and Development (OECD)(2015) "Digital Security Risk Management for Economic and Social Prosperity", Paris.
- Organisation for Economic Cooperation and Development (OECD) (2016), "Communiqué: DAC High Level Meeting", Paris.
- Organisation for Security Co-Operation in Europe (2013) "Permanent Council Decision No. 1106 on the initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies", Vienna.
- Organisation for Security Co-Operation in Europe (2016) "Permanent Council Decision No. 1202 on the OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies", Vienna.
- Organisation for Security and Co-operation in Europe (OSCE) (2016) "Decision No.5/16 - OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Vienna.
- Organisation for Security and Co-operation in Europe (OSCE) (2017) "Decision No.5/17 - Enhancing OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Vienna.
- Otoo, S.; Agapitova, N. and Behren, J. (2009) The Capacity Development Results Framework: A strategic and results-oriented approach to learning for capacity development, World Bank Institute, New York.
- Pawlak, P. (2014) Riding the digital wave – The impact of cyber capacity building on human development, EU Institute for Security Studies, Paris.
- Pawlak, P. (2016) "Confidence-Building Measures in Cyberspace: Current Debates and Trends" in Osula, A-M and Rõigas, H. (Eds.), *International Cyber Norms: Legal, Policy and Industry Perspectives*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence Publications, pp.129-153.
- Pawlak, P. (2017) "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", *EU Institute for Security Studies*, Brief n° 24, Brussels.
- Pawlak, P. and P.-N. Barmaliou (2017) "Politics of cybersecurity capacity building: conundrum and opportunity", *Journal of Cyber Policy*, Vol. 2, Issue 1, pp. 123-144.

- Porcedda, M. G. and Wall, D.S. (2018) "Data Science, Data Crime and the Law" in Berlee, A.; Mak, V. and Tjong Tjin Tai, E. (Eds), *Research handbook on Data Science and Law*, London.
- Porcedda, M.G. (2018) "Patching the patchwork: appraising the EU regulatory framework on cyber security breaches", *Computer Law and Security Review : The International Journal of Technology Law and Practice*.
- Robinson, N. and Horvath, V.(2013) "Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts", Report prepared for the European Parliament.
- Snowdon, C. (2017) "Managing a Cyber Crisis: What is the most effective way to prepare leadership for a high tech threat?", *Register Larkin*.
- The Royal Society (2016) "Progress and research in cyber security. Supporting a resilient and trustworthy system for the UK", *The Royal Society Science Policy Centre*, London.
- Trevors, M. (2017) "Cyber Hygiene: 11 essential practices" *Insider Threat Blog*, Carnegie Mellon University.
- United Nations (2001) "Resolution 55/63 on combatting criminal misuse of information technologies", New York.
- United Nations (2002) "Resolution 56/121 on combatting criminal misuse of information technologies", New York.
- United Nations (2003) "Resolution 57/239 on the creation of a global culture of cyber security", New York.
- United Nations (2004) "Resolution 58/199 on the creation of a global culture of cyber security and the protection of critical information infrastructure", New York.
- United Nations (2013) "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security", New York.
- United Nations (2015) "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security", New York.
- United Nations Conference on Environment and Development (1992) "Agenda 21: Chapter 37 National Mechanisms and International Cooperation for Capacity-Building in Developing Countries", Rio de Janeiro.
- United Nations Congress on Crime Prevention and Criminal Justice (2015) "Report on the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice", Doha
- United Nations Development Programme (2002) "Report of the UN Inter-Agency Workshop on Capacity Development", Geneva.
- United Nations Development Programme (2003) "Development Effectiveness Report: Partnerships for Results", New York.
- United Nations Development Programme (2008) "Capacity Development: Practice Note", New York.
- United Nations Development Programme (2008) "Capacity Assessment Methodology", New York.
- United Nations Development Programme (2009) "Handbook on monitoring and evaluating for results", New York.
- United Nations Economic and Social Council (2002) "United Nations System Support for Capacity-Building" E/2002/58, New York.
- United Nations Economic and Social Council (2004) "Effectiveness of the EU development system and its operational activities: capacity of the system to provide country level support and develop national capacities", New York.
- United Nations Educational, Scientific, and Cultural Organization (UNESCO) (2011) "Capacity Development for Education for All – Translating Theory into Practice", Paris.
- United Nations Office on Drugs and Cybercrime (2017), Expert Group to Conduct a Comprehensive Study on Cybercrime, Conference Room Paper 2 "Capacity-building on cybercrime and e-evidence. The experience of EU/ Council of Europe joint projects 2013-2017" (doc. UNODC/CCPCJ/EG.4/2017/CRP.2), 6 April 2017, Vienna.
- Wall, D. S. (2007)"Cybercrime. The transformation of crime in the information age", Polity.
- Wetzling, T. (2017) "Options for more effective intelligence oversight", Discussion paper, *Stiftung Neue Verantwortung*.
- World Bank (2016) *World Development Report: Digital Dividends*, Washington D. C.
- World Economic Forum (2016) "Recommendations for Public-Private Partnership against Cybercrime", Geneva.
- World Economic Forum (2017), "Cyber Resilience Playbook for Public Private Collaboration", Geneva.
- World Summit on the Information Society (2005) "The Tunis Agenda for the Information Society" WSIS-05/TUNIS/DOC/6(Rev. 1)-E, Tunis.

