Operational Guidance

The EU's International Cooperation on Cyber Capacity Building

Second edition

PRINTED ON RECYCLED PAPER

Manuscript completed in 2023

Printed in Tallinn by EU CyberNet
Tallinn: Joon OÜ Printing House

This study was implemented by the EU Cyber Capacity Building Network (EU CyberNet) at the commission and under the supervision of the Service for Foreign Policy Instruments, Unit FPI.1 "Stability and Peace – Global and Transregional Threats and Challenges", and in cooperation with DG INTPA, DG NEAR, and EEAS. It is written by Nayia Barmpaliou and Patryk Pawlak, EU CyberNet experts.

This publication was funded by the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

EU CyberNet is a project funded by the European Union. It is implemented by the Estonian Information System Authority (RIA) in cooperation with German Federal Foreign Office and Luxembourg House of Cybersecurity. The purpose of EU CyberNet is to strengthen the global delivery, coordination and coherence of the European Union's external cyber capacity building actions and to reinforce the European Union's own capacity to provide technical assistance to third countries in the field of cybersecurity and cybercrime. EU CyberNet maintains and operates a Pool of Experts who are ready to contribute to capacity building initiatives and provide expertise to the EU's efforts in partner countries. The Expert Pool may be used by Commission services, Member States and all members of the EU CyberNet Stakeholder Community, including implementing partners of ongoing and future cyber capacity building actions at EU CyberNet's technical platform CynAct. More about EU CyberNet and its activities may be found at its website: www.eucybernet.eu.

Table of Contents

Acronyms

ADB	Asian Development Bank
AFRINIC	Regional Internet registry for Africa
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
ARF	ASEAN Regional Forum
ARIN	American Registry for Internet Numbers
ASEAN	Association of Southeast Asian Nations
AUC	African Union Commission
BSA	Software Alliance
CaaS	Crime-as-a-Service
CAIDA	Center for Applied Internet Data Analysis
CBMs	Confidence-Building Measures
CCB	Cyber Capacity Building
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-EU	EU Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CoE	Council of Europe
cPPP	Contractual Public-Private Partnership
C-PROC	Council of Europe's Cybercrime Programme Office
CSA	Cyber Solidarity Act
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
CSO	Civil Society Organisation
CSOC	Cyber Security Operations Centre
CT	Counterterrorism
CUSMA	Free trade agreement between Canada, Mexico, and the United States
Cyber-VAWG	Cyber-violence against women and girls
D4D	Digital for Development
DAC	Development Assistance Committee
DDP	Digital Development Partnership
DG INTPA	Directorate-General for International Partnerships
DG NEAR	Directorate-General for Neighbourhood and Enlargement Negotiations

DMA	Digital Markets Act
DORA	Digital Operational Resilience Act
DSA	Digital Services Act
DSM	Digital Single Market
EBRD	

HRBA	Human rights-based approach
HRVP	High Representative for Foreign Affairs and Security Policy / Vice President of the Commission
IADB	Inter-American Development Bank
ICANN	Internet Corporation for Assigned Names and Numbers
ICCP	Institute for Certification of Computing Professionals
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
IETF	Internet Engineer Task Force
IFI	International Financial Institution
IGF	Internet Governance Forum
IHL	International humanitarian law
IL	Intervention Logic
IMF	International Monetary Fund
IOT	Internet of Things
IPA	Instrument for Pre-accession Assistance
ISAC	Information and Intelligence Sharing Centre
ISO	International Standardisation Organisation
ISP	Internet Service Providers
ITU	International Telecommunications Union
ITU-D	International Telecommunication Union Development Sector
JICA	Japan International Cooperation Agency
LAC4	Latin America and Caribbean Cyber Competence Centre
LACNIC	Regional Internet registry for the Latin American and Caribbean regions
LE	Law enforcement
LEAs/IC	Law enforcement agencies / Intelligence community
LFA	Logical Framework Approach
M&E	Monitoring and evaluation
MIP	Multi-Annual Indicative Programme
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
NDICI	Neighbourhood, Development and International Cooperation Instrument
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

OCWAR-C	West African Response on Cybersecurity and Fight against Cybercrime
ODA	Official Development Assistance
OECD	Organisation for Economic Cooperation and Development
OG	Operational Guidance
OHCHR	Office of the United Nations High Commissioner for Human Rights
OSCE	Organisation for Security Cooperation in Europe
PESCO	Permanent Structured Cooperation
PI	Partnership Instrument
PIMS	Partnership Instrument Monitoring System
POA	Programme of Action
PoC	Point of Contact
PPMC	Project and Programme Management Cycle
PPP	Public-Private Partnership
PSIRT	Product Security Incident Response Team
R&D	Research and Development
RIA	Information System Authority of the Republic of Estonia
RIP	Regional Indicactive Programme
RIPE NCC	Regional Internet registry for Europe, the Middle East and parts of Central Asia
RIR	Regional Internet Registry
ROM	Result-Oriented Monitoring
SCADA	Supervisory Control and Data Acquisition
SCO	Shanghai Cooperation Organisation
SDGs	Sustainable Development Goals
SDG-Cs	Sustainable Development Goals Contracts
SPRCs	Sector Reform Performance Contracts
SRBCs	State and Resilience Building Contracts
STEM	Science, technology, engineering, and math
T-CY	Council of Europe 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
UNESCO	United Nations Education, Science and Culture Organisation
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
USAID	United States Agency for International Development
W3C	World Wide Web Consortium
WEF	World Economic Forum
WSIS+10	World Summit on Information Society
WTO	World Trade Organization

ABOUT THIS OPERATIONAL GUIDANCE

Rationale

In the era of digital interdependence, cybersecurity has evolved from a technical and technological issue to a societal need and a multifaceted discipline. The rise of digital authoritarianism and other policy approaches that run contrary to key EU values and policies for cyberspace – such as respecting human rights online and offline, promoting the multi-stakeholder Internet governance model, and applying international law in cyberspace – have increased the complexity of programming external actions in the digital age and challenged conventional methods and tools used for engaging with partner countries and organisations.

The promotion of digital transition and digital society as a key element of the EU's international cooperation and partnerships has also steadily increased the funding for such initiatives. The sustainability of the digital development outcomes and the safe transition to digital societies rely on the cybersecurity and cyber resilience of these processes. Therefore, a concerted effort is necessary to **consolidate lessons** from the EU's experience to date – particularly in bridging the development and technical communities – and articulate a **systematic methodology** that combines the various dimensions of cyber policy with development cooperation principles. This also impacts the type and approach of external actions taken in addressing cyber-related issues in the context of international cooperation.

Objectives

Cyber capacity building is a set of actions that strengthen the capacities of individuals, organisations, businesses, or governments and foster an enabling environment in support of a secure, safe, free, open and peaceful cyberspace for everyone, while respecting human rights and the rule of law. These actions typically focus on enhancing cyber resilience, strengthening capacities to fight cybercrime, or promote responsible state behaviour in cyberspace.

This *Operational Guidance*[1] provides a practical framework for designing and implementing the EU's external actions in **five main policy pillars**:

1. National strategic cyber framework,
2. Cyber crisis prevention and management,
3. Criminal justice in cyberspace,
4. Cybersecurity education and culture, and
5. Cyber diplomacy.

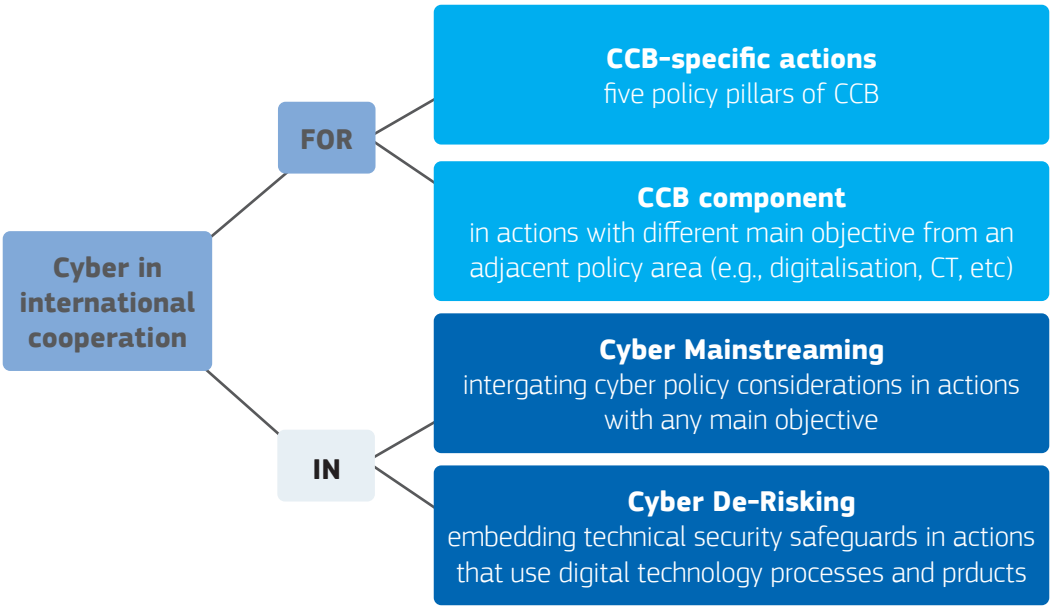
With streamlined content and revised tools, the document serves a resource for EU staff in headquarters and delegations, as well as for services of Member States and implementing partners involved in cyber capacity building. Its objectives are to:

- **Assist in designing appropriate, context-specific project actions**[2] for cyber capacity building in partner countries and regions, drawing from development best practices and lessons learnt.
- Offer **guidance on the implementation, monitoring and evaluation** of such actions.
- Serve as the **baseline material for training courses** on cyber capacity building organised by the EU.

The *Operational Guidance*[1] covers the entire intervention cycle – programming, identification, formulation, implementation (including monitoring and reporting), and evaluation[3]. It applies to **all management modes** (direct, shared, indirect) used in external action and is designed for **bilateral, regional or global actions** with a **cyber-specific focus**, as well as informing actions with **cyber components**. Therefore, it provides comprehensive knowledge for designing, delivering, and evaluating CCB projects and activities.[4]

1 It builds upon and replaces the 2018 Operational Guidance and Playbook for the EU's external cyber capacity building.
2 Throughout this document the use of the words 'action' or 'initiative' serve as the all-encompassing term for projects, programmes, interventions, initiatives.
3 The *Operational Guidance* is a cyber-specific complement to existing general project cycle management guides for the EU's external actions. These include the Project Cycle Management Guidelines, DG INTPA's Intervention Cycle Methodology Guide, and DG NEAR's Addressing capacity development in planning/programming, monitoring and evaluation together with its Guidelines on linking planning/programming, Monitoring and Evaluation.
4 While the *Operational Guidance* focuses on tailored advice for the project implementation modality, the principles and approaches it elaborates are also meant to inform the design of relevant actions in budget support and blending facilities.

Figure 1. Cyber approaches in external action



Scope

This Operational Guidance is designed to primarily support the EU's core cyber capacity building objectives in the areas of cyber resilience, cybercrime, cyber diplomacy, and/or any other **cyber-specific** issue. However, the specific tools and considerations presented in this document play a crucial role in various other scenarios:

- **Integrating a cyber-specific capacity building component** into actions addressing a broader challenge that contain a cyber dimension (e.g., cybercrime component in an organised crime action) or in an adjacent policy area with overlapping cyber aspects that requires the inclusion of cyber-specific activities (e.g., cyber component in initiatives focused on hybrid threats). The *Operational Guidance* supports the analysis on the policy context, as well as the identification of key stakeholders, capacity gaps and needs, as well as the main risks to be considered.
- **Mainstreaming** cyber-related policy considerations: This involves integrating cyber-related policy consideration as **a cross-cutting issue** into actions in other policy areas to ensure policy coherence across the EU's external action. For example, when working on actions focused on energy, transportation, or agriculture. The *Operational Guidance* provides an overview of the key issues and priorities that can be raised during the context analysis and the needs assessment.
- **De-risking** actions with a digital component: Actions that involve a digital component need to incorporate **cybersecurity technical safeguards** to mitigate digital risks against the action's investments and outcome. For instance, sections of the Operational Guidance devoted to cyber crisis prevention and management, or cybersecurity education and culture, offer valuable insights into adopting concrete standards or procedures to reduce exposure to risks and threats in cyberspace.

By considering these additional applications, the *Operational Guidance* becomes a comprehensive resource to support cyber capacity building across various policy domains, promoting policy coherence, and enhancing cybersecurity measures in digital-related actions.

I CAPACITY BUILDING IN CYBERSPACE

1. Basics of cyber capacity building

Digital growth and transformation cannot be achieved without addressing digital risks. This requires actions across several domains, including:

1. Cybersecurity: Involves ensuring the integrity and security of networks and infrastructure.
2. Cybercrime: Pertains to criminal activities committed online or using the Internet.
3. Cyber and digital diplomacy: Aims to promote international cooperation in the cyber domain.
4. Cyber defence: Refers to aspects necessary to protect military assets.

The post-pandemic focus on digital transformation as a pathway to recovery has highlighted the crucial link between 'cyber' and 'digital'. Achieving **sustainable digital transformation requires strengthening the cyber resilience of states and societies**.

Cyber capacity building is a set of actions that strengthen the capacities of individuals, organisations, businesses or governments and foster the enabling environment in support of a secure, safe, free, open and peaceful cyberspace for everyone, while respecting human rights and the rule of law. These actions typically focus on enhancing cyber resilience, strengthening capacities to fight cybercrime, or promoting responsible state behaviour in cyberspace. Since the 2010s, it has become the dominant term in the international discourse to describe efforts in improving the cybersecurity posture of organisations, nations, and regions and navigating the security challenges of a digitalised world. As a **catch-all umbrella term**, cyber capacity building[5] supports international cyber cooperation and partnerships.

BOX 1: CYBER-RELATED CONCEPTS & DEFINITIONS

Definitions of most terms used can be found in major EU legislative acts.

Capacity is often defined as the ability of people, organisations, and society to manage their affairs successfully (OECD DAC). The main purpose of **capacity building** is to enhance countries' ability to define and realise their goals effectively and stimulate change by developing or strengthening the capabilities and competencies of individuals, institutions, governments, and society at large (UN Economic and Social Council).

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, IBM Centre for the Business of Government).

Cyber threat means any potential circumstance, event, or action that could damage, disrupt, or otherwise adversely impact network and information systems, the users of such systems, or other persons (EU Cybersecurity Act). **Vulnerabilities** are defined as a weakness, susceptibility, or flaw of an asset, system, process, or control that can be exploited by a cyber threat (NIS 2 Directive).

Resilience means an ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover from an incident. **Incident** means an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, including when it affects the national systems that safeguard the rule of law (Resilience of Critical Entities Directive). **Risk** means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident (NIS 2 Directive).

Cybersecurity commonly refers to the safeguards and actions that can be used to protect network and information systems, the users of such systems, and other persons affected by cyber threats (EU Cybersecurity Act). **Security of network and information systems** means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the services offered by, or accessible via, those network and information systems (NIS 2 Directive).

5 This *Operational Guidance* uses the term 'cyber capacity building' in the broader meaning of 'cyber capacity development' since the former is more established as in international and EU cyber policy documents.

Cybersecurity initially emerged as a technical issue and later became a prominent topic on the global policy agenda, particularly in the context of national and international security discussions. Consequently, cyber capacity building was initially driven by practitioner communities with a focus on law enforcement and computer security incident response.[6] As a result, there are considerable disparities in the **conceptual and methodological approaches** to cyber capacity building among donors and implementing partners.[7]

To address these discrepancies and enhance the effectiveness of cyber capacity building, it is essential to draw upon the extensive experience of the development community in capacity building for poverty reduction and sustainable development. Leveraging the knowledge and expertise of the development community can help inform cyber capacity building methodologies and elevate the professionalism of the community's approaches.[8] By integrating the best practices from development capacity building, cyber capacity building efforts can be more comprehensive, effective, and tailored to specific needs.

BOX 2: WHY DOES CYBER CAPACITY BUILDING MATTER FOR THE EU?

1. It supports cyber resilience building in partner countries that contributes to an improved global digital ecosystem.
2. It fosters 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.
3. It encourages the creation of formal and informal cooperation frameworks between partner countries and regions and the EU and its Member States.
4. It promotes the EU's development commitments and the implementation of the 2030 Agenda for Sustainable Development.

2. Cyber capacity building in the EU

Acknowledging the significance of the **'security-development nexus'**, the EU has broadened its external action and development cooperation to encompass security-related areas, including cyber capacity building. The overarching goals of enhancing the resilience of partner countries and enabling them to harness the potential of the digital economy are central to the EU's endeavours in this domain. These efforts primarily address cybersecurity as a governance concern and cybercrime as a priority in the realm of criminal justice. As such, they correspond not only to the EU's development objectives but also fit well under its partnership priorities with neighbourhood countries and the reform agenda of the enlargement policy.

The EU's cyber capacity building initiatives also align closely with the **Sustainable Development Goals** (SDGs) that concern all countries at all levels of development. Of direct relevance are SDG 9 that emphasises industry, innovation, and infrastructure, and SDG 16, which focuses on peace, justice, and strong institutions. By addressing cybersecurity and cybercrime within this framework, the EU aims to contribute to the sustainable development of partner countries and facilitate their participation in the digital era while ensuring peace, security, and effective governance.

6 R. Collett and N. Barmpaliou, International Cyber Capacity Building: Global Trends and Scenarios, European Commission, Brussels, 2021, pp. 34-45.
7 P. Pawlak, Riding the digital wave – The impact of cyber capacity building on human development, EU Institute for Security Studies, Paris, 2014. pp. 61-71.
8 P. Pawlak and N. Barmpaliou, Politics of cybersecurity capacity building: conundrum and opportunity, Journal of Cyber Policy, 2017, pp. 14-18.

Figure 2. Goals of the EU's CCB engagement

The history of the EU's cyber capacity building efforts traces back to the 2010s. Starting already to finance relevant actions through pre-accession (IPA) and neighbourhood (ENI) financing instruments, the systematic impetus came from the first **EU Cybersecurity Strategy,** adopted in 2013, which advocated for utilising various EU aid instruments to support cybersecurity capacity building. Subsequently, the significance of cyber capacity building for fostering sustainable socioeconomic growth was emphasised in the 2015 **Council Conclusions on Cyber Diplomacy**. The 2017

BOX 3: COUNCIL CONCLUSIONS ON THE EU EXTERNAL CYBER CAPACITY BUILDING GUIDELINES (2018)

The EU agreed a set of core values and principles for cybersecurity to provide **a 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.**

3. EU financing for cyber capacity building

The European Union (EU) holds a prominent position as a global provider of Official Development Assistance (ODA) and maintains significant trading partnerships and foreign investments with countries worldwide. In recent years, the EU's approach to development cooperation has evolved to include consideration of its geopolitical goals, interests, and values, which play a crucial role in forming partnerships with ODA recipient countries. However, clear guidance on the eligibility of cybersecurity assistance and cyber defence capacity building for ODA (so-called DAC-ability) has not been fully established. Early discussions about the ODA Casebook had considered the inclusion of cyber defence but were eventually left out due to the dual-use nature of cyber tools, which poses challenges in preventing potential misuse of equipment or skills intended solely for defensive purposes.[9]

The EU's Multiannual Financial Framework (MFF) for 2021-2027 operates with two main external financial instruments: **the Neighbourhood, Development and International Cooperation Instrument** (NDICI-Global Europe) and the **Instrument for Pre-accession Assistance** (IPA III).

The NDICI consists of three main pillars that can all finance cyber-related actions:

1. **geographical** for the Neighbourhood, Sub-Saharan Africa, Asia and the Pacific, and the Americas and the Caribbean,
2. **thematic** for Human Rights and Democracy; Civil Society Organisations; Peace, Stability and Conflict Prevention; and Global Challenges, and
3. **a rapid response** mechanism to swiftly respond to crises, contribute to peace, stability, and conflict prevention, strengthen the resilience of states, societies, communities, and individuals, linking humanitarian aid and development action.

The NDICI **geographic programmes** (i.e., bilateral and regional) include CCB as an area of cooperation under the themes of:

- **prosperity,** that frames cybersecurity as an enabler to the digital economy and transition, in support of inclusive and sustainable economic growth and decent employment,[10] and
- **peace,** that focuses on the security dimensions and implications of cyber issues, in support of peace, stability and conflict prevention.[11]

9 OECD, DAC High Level Meeting Communiqué, Paris, 19 February 2016.
10 Regulation (EU) 2021/947 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI), 9 June 2021, Annex II, p. 60, point 5 (o).
11 Idem, Annex II, p. 62, point 6 (q).

The NDICI **thematic programme** for interventions related to peace, stability, and conflict prevention builds on previous

II. A FRAMEWORK FOR THE EU'S EXTERNAL CYBER CAPACITY BUILDING

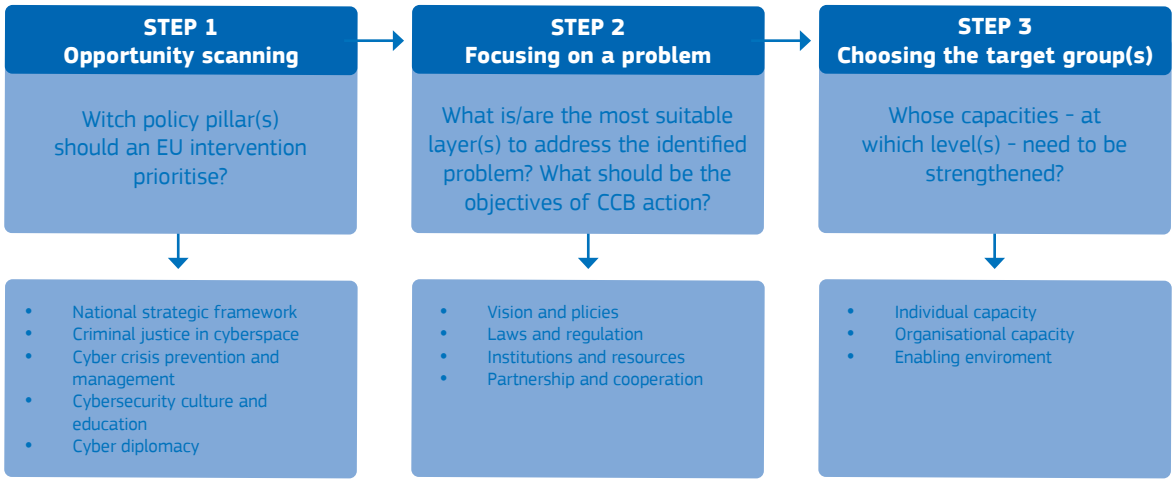
1. First steps into external cyber capacity building

The governance of cyberspace is a complex policy area with diverse and sometimes conflicting goals (for an overview of key policy issues, see Part IV). Addressing these complexities effectively and comprehensively requires significant resources and effort, potentially leading to capacity gaps and emerging needs for new capacities. Drawing from the existing practice of cyber capacity building, the *Operational Guidance* proposes a simplified three-step approach for those tasked with designing a cyber capacity building intervention:

- **Step 1: Scanning the opportunities for capacity building engagement:** The first step involves identifying the specific policy pillar(s) that an EU intervention should prioritise. It helps determine the focus of the intervention within the broader landscape of cyber capacity building.
- **Step 2: Focusing the intervention on a specific problem:** In this step, the intervention's objectives are clarified by pinpointing the challenge(s) it aims to address as well as identifying the most suitable layer (e.g., technical, institutional, legal) to tackle the problem effectively.
- **Step 3: Selecting a targeted group for capacity building:** This step involves deciding which entities or stakeholders' capacities need strengthening to achieve the desired objectives. The targeted groups may include individuals, organisations (e.g., within the executive, legislative, or judicial branches), or the broader enabling environment (e.g., civil society, regional organisations).

By following these three steps, the process of designing a cyber capacity building intervention gains a solid foundation.

Figure 3. Designing a cyber capacity building action



Important: This sequence is not rigid and may be subject to change based on specific circumstances. For instance, a partner country might express specific wishes and propose actions related to enhancing certain institutions or delivering concrete capacities (e.g., through training), which could influence the proposed approach. However, this does not negate the importance of conducting an independent analysis of needs and formulating appropriate responses, which is the primary goal of this framework. Additional tools and methods related to specific challenges within the project management cycle are addressed in Part III of this *Operational Guidance*.

1.1 Step 1: Selecting the policy area(s)

The first crucial decision in cyber capacity building is selecting the policy area where the intervention should be implemented. Typically, this initial decision is influenced by specific needs identified by the partner country or priorities for cooperation as identified by the EU. In line with the prevailing global practice in cyber capacity building and taking inspiration from approaches adopted by other organisations or countries, this *Operational Guidance* narrows its focus to five essential policy pillars:

- **National strategic cyber framework** to develop a comprehensive approach that reinforces state and societal cyber resilience in partner countries.
- **Criminal justice in cyberspace** to increase the quality and strengthen the capacity of the criminal justice system to adequately address cybercrime while ensuring the protection of fundamental rights and the rule of law.
- **Cyber crisis prevention and management** to strengthen state and societal capacity to manage cyber incidents and crises in a timely, effective, and efficient manner.
- **Cybersecurity education and culture** to strengthen state and societal resilience through education, awareness raising, skills development, and cyber hygiene.
- **Cyber diplomacy** to safeguard an open, global, free, and secure cyberspace by strengthening national capacities to engage in cyber diplomacy.

1.2 Step 2: Defining the objective(s)

Once the policy pillar has been determined, the next step involves narrowing down the scope of the intervention by identifying a specific problem that the action aims to address. This decision leads to definitions of concrete objectives that the intervention seeks to achieve:

- **Vision and policies** to strengthen the overall cyber policy framework (e.g., policy coordination mechanisms, an effective institutional framework that would deter potential malicious cyber actors),
- **Laws and regulations** to strengthen the legal and regulatory framework (e.g., aimed at protecting citizens and critical infrastructure from attacks, establishing procedures for incident reporting),
- **Institutions and resources** to strengthen the institutional framework and ensure proper resources for the implementation of policies and laws (e.g., creating a CERT/CSIRT, setting standards, conducting risk assessments, joint exercises),
- **Partnerships and cooperation** to reinforce whole-of-government and whole-of-society approach, including through cooperation with international partners, where necessary (e.g., public-private partnerships, 24/7 contact points).

By clearly defining these objectives, the intervention can proceed with a well-structured plan to achieve its goals and contribute to cyber capacity building in the designated policy area.

1.3 Step 3: Choosing the target(s)

Finally, the intervention must clarify the specific capacities it aims to reinforce, whether they are:

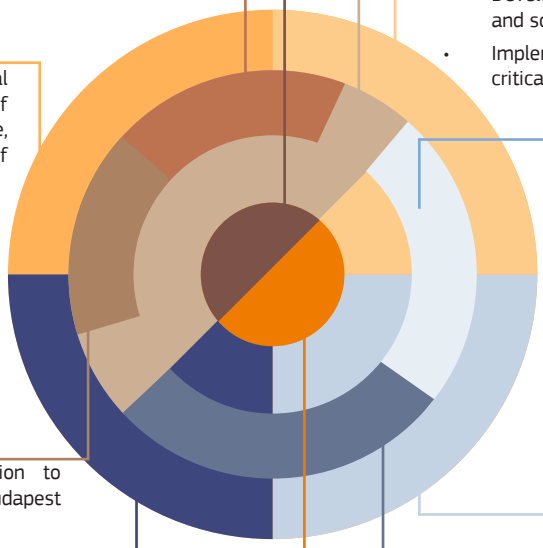
- **Individual capacities:** Focused on enhancing abilities, personal attitudes, skills and capabilities, and values of individuals concerning the cybersecurity or management of digital risks. This may include prosecutors, members of the digital forensic units, and diplomats.
- **Organisational capacities:** Focused on improving practices, roles, mandates, decision-making structures, and division of labour within organisations to contribute to strengthening cyber resilience at the level of individual organisations or structures. Strengthening organisational capacities often involves enhancing the individual capacities of employees within these organisations.
- **Enabling environment:** Focused on shaping the overall culture and tolerance for digital risks across society, establishing an adequate legal and institutional environment, and providing oversight and checks and balances to minimise the abuse of power. This level also aims to strengthen the overall commitment to the rules-based order in relation to cybersecurity.

Regardless of the level of intervention chosen, the capacity building actions should aim to strengthen national capabilities through a whole-of-government approach. For instance, this could involve strengthening national cyber resilience frameworks, providing law enforcement and judicial training, enhancing cybercrime or high-tech crime units, and developing computer forensic capabilities and CERT/CSIRT employees.

Additionally, promoting the development of collective capabilities driven by a whole-of-society approach is crucial. This could include establishing mechanisms for public consultation and involving the private sector in cyber crisis management.

However, carrying out these tasks is not without challenges, as different organisational missions, objectives, working methods, and time frames may create complexities. Addressing cyber threats and retaining a skilled workforce in the public sector also presents additional challenges. Nevertheless, through a well-defined and focused approach to capacity building, the intervention can contribute to strengthening a partner country's cybersecurity ecosystem and ability to deal with cyber challenges effectively.

Figure 4. Complexity of cyber-related concepts



CRIME & SECURITY & DIPLOMACY

- Support strengthening capacities of partner countries and organisations in developing cyber resilience
- Design the adequate responses of foreign cyber operation (e.g. espionage, ransomware)

CRIME & SECURITY

- Develop criminal justice responses to cyber attacks
- Establish partnership between law enforcement and crisis management actors

CRIME

- Develop a legal and institutional framework to target all forms of cybercrime (including ransomware, online criminal markets, or use of internet by terrorists)

CRIME & DIPLOMACY

- Promote international cooperation to fights cybercrime (e.g. the Budapest Convention)
- Support the strengthening capacities of partner countries in the field of cubercrime (e.g. digital forensics, 24/7 Points of Contact)

DIPLOMACY

(incl. International Partnerships)

- Support cyber resilient digital transformation
- Promote norms of responsible state behaivour an application of existing international law
- Promote adherence to and comliance with the Declaration of the Furue of Internet

DIPLOMACY & SECURITY

- Support the implementation of cuber norms in national legislation (e.g. CERT-to-CERT cooperation)
- Promote international standards to reduce digital risks in the supply chain

SECURITY

- Design adequate legal and institutional framework to prevent, deter and respond to cyber attacks
- Develop a regulatory framework for strengthening state and societal cyber resilience
- Implement institutional and regulatory measures for critical information infrastructure protection

SECURITY & DEFENCE

- Develop channels for information sharing and cooperation between civilian and military operations

DEFENCE

- Prevent, deter and respond to cyber attacks on militarty infrastructure

DEFENCE & DIPLOMACY

- Develop and promote confidence-building measures in cyberspace
- Develop national cyber defence doctrine in compliance with international law

DEFENCE & DIPLOMACY & SECURITY & CRIME

- Support strengthering of capacities of partner countries to deal with the cyber operation (e.g. cyber and information operation)

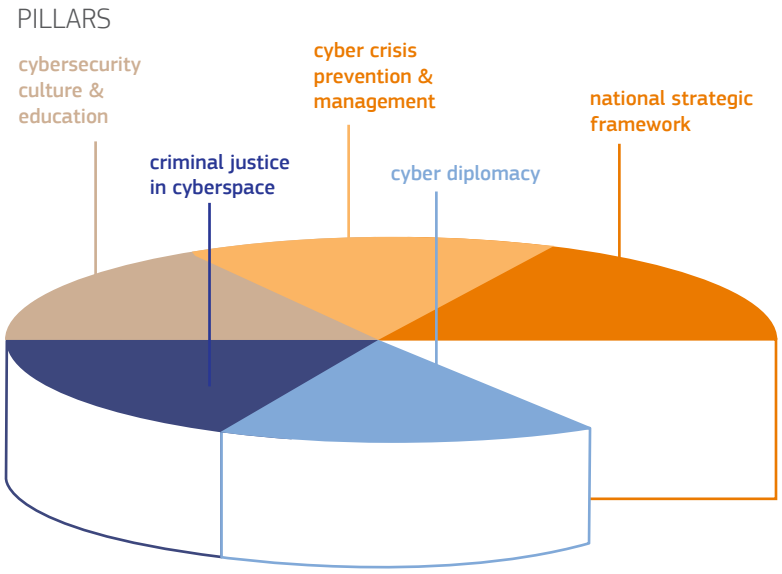
2. What policy priorities? Pillars of cyber capacity building

This *Operational Guidance* distinguishes five main policy pillars in which an intervention can take place:

1. National strategic cyber framework,
2. Cyber crisis prevention and management,
3. Criminal justice in cyberspace,
4. Cybersecurity education and culture,
5. Cyber diplomacy.

This list of cyber-related policy areas is not exhaustive, and there is a possibility of new policy areas emerging in the future, such as hybrid threats or disinformation. Additionally, the list is non-exclusionary, meaning that an intervention may involve multiple pillars simultaneously. In multinational or global programmes, the most common approach is to address a specific policy challenge within a particular policy area. However, country-specific actions may deal with challenges that cut across two or more policy areas. In such cases, a comprehensive and integrated approach is required to address the complex and interconnected cyber issues effectively.

Figure 5. Policy pillars in the external cyber capacity building



2.1. National strategic cyber framework

When a national strategic cyber framework is absent, it becomes the most obvious choice for engagement. However, if a country has already adopted such a framework, it becomes crucial to assess its implementation and relevance to the specific needs and security environment of the country. If this is not the case, the focus on implementation or revision of a strategic framework may be appropriate. Where strategies exist and are implemented, supporting the development of specific sectoral cyber strategies becomes a viable alternative.

The primary aim of the initiatives focused on cyber capacity building under the 'national strategic framework' pillar is **to contribute to developing a comprehensive strategic framework that reinforces state and societal cyber resilience in partner countries**. Creating a national strategic cyber framework (e.g., a cybersecurity strategy, a national cyber action plan) remains crucial for building cyber resilience and countering cyber threats. The process of developing a strategic framework has a multiplying effect, making it a central activity in cyber capacity building.

The 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 within a specific timeframe to mitigate cybersecurity risks. National strategic frameworks aim to address emerging cybersecurity challenges, such as critical infrastructure protection, cybercrime, and

skills gaps, in a comprehensive and coherent manner. On a broader scale, a national cyber strategic framework indicates the role a country aspires to play internationally, its priorities, and how it intends to achieve its objectives.

The drafting process offers countries an opportunity to self-assess vulnerabilities, define approaches to tackle them, and determine the existing capacity level and desired support to achieve pre-defined objectives. To be operational and relevant, a national strategic framework requires a clear identification of relevant stakeholders and their respective roles. Given the broad scope of the issues involved, critical infrastructure operators, law enforcement, judiciary, the ICT sector, and academic and research institutions are among the key stakeholders. However, bringing together actors with different priorities and interests, often due to limited trust between parties, can be challenging. Engaging trusted information-sharing communities may offer a solution to increase trust among stakeholders.

There is no one-size-fits-all solution for developing a national strategic cyber framework. The process itself is a capacity building exercise that requires mapping relevant stakeholders, navigating different missions and interests, and working towards a common understanding of a vision for cyberspace based on existing vulnerabilities and opportunities, among other factors. Lessons learnt from various countries provide valuable insights into what works and what doesn't when developing national strategic cyber frameworks

BOX 4: DEVELOPING A CYBERSECURITY STRATEGY

There are numerous resource materials available on how to develop a national cybersecurity strategy. Some of the notable examples include the manuals and guidance notes prepared by the International Telecommunications Union or the Organization of American States. The European Union Agency for Cybersecurity – ENISA published its first National Cyber Security Strategy Good Practice Guide in 2012 and has since delivered numerous guidance documents to support development of national cybersecurity strategies, national capabilities assessment framework, evaluation framework for cybersecurity strategies, and implementation guides.

The six **stages in the design and development of a strategy** are:

1. Identification of a lead authority and relevant stakeholders: establishment of a clear leadership, responsibility for the overall vision, and resource allocation, including decisions about the adoption process and format of the document.
2. Stocktaking and analysis: assessment of national cybersecurity landscape, critical processes and systems, vulnerabilities and risks. It includes identification of key digital assets and vulnerabilities, developing a common methodology for managing risks, sectoral cybersecurity profiles, etc.
3. Production of the strategy: set-up of clear governance structures, roles, responsibilities and accountability mechanisms, identification and engagement with relevant stakeholders, and establishment of trusted information-sharing mechanisms.
4. Implementation: development of a timeline with clearly defined priorities, resources and metrics.
5. Monitoring and evaluation: mechanisms for regular evaluation and revision, feedback loops.

The **most common objectives** for a strategy include:

- identification of stakeholders and their respective roles,
- development of national cyber contingency plans,
- protection of critical information infrastructure,
- organisation of cybersecurity exercises,
- establishment of baseline security measures,
- establishment of incident reporting mechanisms,
- awareness raising,
- training and educational programmes,
- development of incident response capability,
- countering cybercrime,
- development of international cooperation mechanisms,
- establishment of public-private partnerships,
- protection of human rights online, in particular data protection,
- research and development.

Some of the **best practices and lessons** include:

- A strategic cyber framework must **be flexible and actionable**, with periodic reviews that contribute to recalibrating the strategic outlook and addressing evolving threat landscapes. This translates into specific and time-bound action plans or roadmaps with concrete implementation steps. Such efforts are undertaken to enhance cyber resilience in critical sectors like energy, finance, health, and maritime.
- Developing a national cybersecurity strategy should adopt **whole-of-government and whole-of-society** approaches, allowing various stakeholders to contribute to defining national cybersecurity objectives. While the content of national strategies or frameworks may differ, the primary value lies in triggering strategic reflection, bringing different players to the same table, and encouraging different policy communities to work together towards a joint vision. In this sense, the process linked to the development of a national strategic framework is a de facto capacity building exercise.
- Strategies require constant **monitoring and adaptation**. Developing a set of near-term tasks and defining quick wins based on the existing capacities can be beneficial to avoid "implementation fatigue." However, it's important to recognise that periodic reviews are necessary to assess progress, check in with stakeholders, and confirm the validity of objectives.

2.2. Criminal justice in cyberspace

Engagement in criminal justice in cyberspace can encompass several aspects. The most obvious aspect is the development, adoption, and implementation of comprehensive domestic legislation on cybercrime. In terms of institutions, actions may focus on establishing specialised cybercrime units or enhancing forensic capabilities. Additionally, numerous existing cybercrime capacity building actions concentrate on strengthening the knowledge and skills of criminal justice organisations such as law enforcement agencies, prosecutors, or judges.

The primary purpose of initiatives aimed at cyber capacity building under the pillar 'criminal justice in cyberspace' is to **contribute to increasing the quality and strengthened capacity of the criminal justice system to adequately address cybercrime while ensuring the protection of fundamental rights and the rule of law**. Given that cybercrime has become a concern for many governments and considering their limited capacities to deal with this phenomenon, there is significant interest and commitment from partner countries towards such actions.

An effective criminal justice response is necessary to ensure the safety and security of citizens online as well as the economic viability of businesses while upholding respect for the rule of law and the rights of individuals in cyberspace. Differences in legal frameworks and ineffective international cooperation resulting from limited capacities may lead to the emergence of online criminal hotspots and safe havens where criminal investigations, prosecution, or evidence collection become difficult. Criminal justice action must be based on the law, and thus, the starting point of capacity building activities is most often the analysis of gaps and weaknesses in the national legal framework to provide adequate support for the development, adoption, and implementation of domestic legislation – both substantive (criminalising conduct) and procedural (powers to investigate cybercrime and other offences involving evidence on computer systems).

Cybercrime capacity building is probably the most advanced policy domain compared to others. The experience to date confirms that an effective response to cybercrime is conditioned on the states' capacity to:

1. **develop and implement legislation on cybercrime** and **access to evidence** in line with the existing international legal commitments and standards, and
2. effectively participate in **international networks** and

serious impediment to international criminal investigation and prosecution of cybercrime, primarily due to an incomplete transposition of international instruments to domestic legislation. Adaptation and alignment of these legal frameworks are difficult due to the rapid evolution of the cybercrime threat landscape, limited case law, as well as the limits of the existing operational processes such as Mutual Legal Assistance.

Certain instruments and tools are already available, and legislative reforms have been widely initiated or completed in recent years to address this complex issue. However, the strengthening of institutional capacities to ensure the completion of legal reforms (and the application of legislation to effectively investigate, prosecute, and adjudicate cases of cybercrime and other offences involving electronic evidence) appears to be a persistent challenge. Developing the necessary knowledge base and relevant training programmes for law enforcement and criminal justice authorities is therefore key. The Council of Europe Guide for developing law enforcement training strategies on cybercrime and electronic evidence offers a useful set of operational steps to facilitate such efforts.

Some of the best practices and lessons learnt include:

- In the absence of common definitions of cybercrime and considering different priorities set by individual partner countries, there is a risk that the requests for assistance may not always be aligned with the EU's interests and values. It is therefore important to **clarify any potential differences in language** and work towards similar understandings of the problem from the very beginning of the engagement process. Such discussions should focus primarily on cyber-related definitions contained in national legislation on cybercrime and electronic evidence, substantive criminal law provisions, or specific procedural powers to secure e-evidence. However, they should not overlook definitions in related policy areas such as counter-terrorism and preventing violent extremism (i.e., how a partner country defines terrorist acts) or countering foreign information operations (i.e., how a partner country defines disinformation).
- Evidence also shows that cooperation with the private sector is vital in combating cybercrime. Some of the most successful operations against cybercriminal networks resulted from **close cooperation between government agencies and the private sector**. In the absence of standardised rules of engagement with the industry, large multinational companies, or Internet Service Providers, many countries rely on informal arrangements. Since not all countries have defined such cooperation models, it is often difficult and time-consuming to establish which jurisdiction regulates the preservation and collection of evidence from online service providers.
- **Offences should be narrowly defined to avoid overcriminalisation and procedural powers should be limited by rule-of-law safeguards**. Legal acts containing provisions about criminalisation and sanctions need to be assessed against the principles of necessity and proportionality to limit any potential abuses of power. 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.
- **International cooperation needs to be reflected in cyber capacity building programmes**. Given that an effective fight against cybercrime requires cooperation across borders – for instance, to access electronic evidence located in multiple jurisdictions – it is critical to put in place adequate procedures and technological solutions (e.g., for the exchange of confidential information or handling personal information). 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 5: DEVELOPING CYBER CAPACITIES IN THE FIGHT AGAINST CYBERCRIME

The Council of Europe released a paper in 2013 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. The paper suggests that capacity building programmes for cybercrime prevention and criminal justice can address a large range of needs:

- cybercrime policies and strategies,
- development of domestic cybercrime legislation based on international standards: substantive law measures to criminalise offences against computer data and systems and by means of computers, procedural law tools for efficient investigations, safeguards and conditions for the use of investigative powers,
- cybercrime reporting: reporting channels for individuals and public and private sector organisations,
- prevention measures: public websites with information on cybercrime prevention, educational materials and courses,
- specialised high-tech crime/cybercrime units: police-type cybercrime and high-tech units, computer forensic capabilities, creation of specialised courts, cooperation channels with other police services or institutions (e.g., economic crime units, financial intelligence units, CERTs),
- law enforcement training,
- judicial training,
- access to electronic evidence,
- support for public/private cooperation: cooperation channels for law enforcement and ISPs, creation of information and intelligence sharing centres (ISACs) for various sectors, cybercrime reporting systems,
- support for enhanced international cooperation: strengthening domestic legislation, setting up 24/7 points of contact, training and networking of authorities for mutual legal assistance, ratification of or accession to international treaties or bilateral agreements,
- protection of children online,
- financial investigations and prevention of fraud and money laundering: implementation of international standards, cooperation between cybercrime, financial investigation and financial sector,
- prevention and control of terrorist use of ICT: strengthening interagency cooperation, implementing measures on terrorist financing.

The EU's involvement in cybercrime capacity building has been structured around a strategic partnership with the Council of Europe that implements several EU-funded actions, including GLACY+ aimed at strengthening the capacities of states worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation. The EU also supports region-specific cybercrime capacity building through OCWAR-C in West Africa or El PAcCTO in Latin America.

2.3. Cyber crisis prevention and management

Engagement in cyber crisis prevention and management may include numerous dimensions. One of the most critical aspects is the establishment of functioning and adequately resourced institutions: a national cybersecurity centre responsible for cyber policy and a Computer Emergency and Response Team at both national and sectoral levels. Where these institutions exist and are operational, the focus can shift towards enhancing their operational SSNRSSYTSSTRSI|TR through n|TR iuteonational n|TR cooperation, TR as n|TR telRSI|TR as n|TR promating n|TR

state and societal capacity to manage cyber incidents and crises in a timely, effective, and efficient manner. To achieve this, countries must establish an adequate institutional framework with clear responsibilities and processes for crisis management and cooperation among stakeholders. This may involve empowering existing institutions and providing them with relevant training and tools.

The smooth and secure functioning of critical infrastructure, including power plants, oil refineries, and transportation systems, is crucial for economic, social, and human development. With countries increasingly relying on ICT to optimise the operation of ports, energy grids, and manufacturing facilities, identifying vulnerabilities in these interconnected communication networks and information systems becomes paramount to prevent political or financial exploitation. The potential consequences of large-scale attacks on critical national infrastructure concern all governments. Countries can enhance their ability to monitor and manage such incidents in cyberspace through investments in technological and organisational measures. Setting up Computer Emergency Response Teams (CERT) and acquiring the right equipment while receiving specialised training are essential steps. The primary focus should be to define and protect **national critical information infrastructure**, supporting vital government and societal functions like health, energy, and transportation. According to the EU, critical infrastructure refers to 'an asset or system which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions'.

The initial focus under this pillar usually centres on establishing **CERTs/CSIRTs**. These teams gather and share information about potential threats or incidents, analyse incident reports, and improve cybersecurity awareness and practices among stakeholders. They may operate within a parent organisation, such as a university, government, or company, or be responsible for an entire country or parts of critical infrastructure, as seen with national and governmental CERTs/CSIRT.

T"#=+)#/++$+$T+$P+

- An effective response to cyber incidents and crisis management calls for developing a culture of **information sharing** between different stakeholders and across communities. However, the sensitive nature of shared information – including implications for personal data protection – brings many challenges. While different communities have developed their own structures and procedures for exchanging information, such as national or international CERT networks and networks of 24/7 points of contact for cybercrime, the task becomes more complicated among stakeholders with different missions, such as law enforcement, military, or cybersecurity agencies. The exchange of information with the military, intelligence agencies, and law enforcement is a particularly delicate issue due to the potential for abuses, necessitating the design of adequate oversight and checks-and-balances mechanisms.

- Finally, because the failure of critical information infrastructure may have catastrophic consequences for society, it is highly likely that actions under this policy pillar will enjoy **a high level of buy-in** from the partner country. However, given the sensitivity of the issues and their close link to national security, it is essential that action design pays particular attention to their supporting role and ensure the maximum degree of local ownership.

BOX 6: DEVELOPING CAPACITIES FOR CRITICAL INFRASTRUCTURE PROTECTION

Basic capacities for cyber crisis management have been defined by G8 Principles for Protecting Critical Information Infrastructures:

- emergency warning networks regarding cyber vulnerabilities, threats, and incidents,
- raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them,
- mechanisms for examination of infrastructures and identification of interdependencies among them, thereby enhancing the protection of such infrastructures,
- 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,
- crisis communication networks and procedures for testing them to ensure that they remain secure and stable in emergency situations,
- data availability policies taking into account the need to protect critical information infrastructures,
- mechanisms for tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries,
- training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack,
- adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention, and trained personnel to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries,
- international cooperation 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,
- national and international research and development,
- application of security technologies certified according to international standards.

2.4. Cybersecurity education and culture

The focus of engagement in cybersecurity education and culture lies in four main areas: developing a national cyber education system, strengthening cybersecurity culture, developing critical cybersecurity skills, and promoting cyber hygiene practices. Specific actions within this pillar may involve raising awareness about cybersecurity challenges, conducting cyber hygiene campaigns, or implementing more structured cyber education programmes and curricula. It is important to note that the cybersecurity education and culture pillar is distinct from the trainings and workshops offered under other pillars, as it primarily targets the broader goal of building a cyber-resilient society rather than individual capacity building.

Building a resilient society requires engaging diverse stakeholders with varying levels of awareness and expertise in cyber-related issues. Therefore, it is crucial to invest in improving cyber hygiene and awareness, which form the core components of a cybersecurity culture based on shared responsibility for cyber resilience among stakeholders at all levels. The primary objective of cyber capacity building initiatives focused on 'cybersecurity culture and education' is to **contribute to strengthening state and societal resilience through education, awareness raising, skills development, and cyber hygiene**. Elevating the level of cyber hygiene and awareness in countries can also positively impact trade and political relations, fostering mutual trust in each other's capacities and security standards. Cyber hygiene and awareness contribute significantly to the development of a cybersecurity culture, a key element in the enabling environment analysis. [15]

Building a robust **cybersecurity culture** entails a combination of approaches. First, it includes increasing and reinforcing **cybersecurity awareness** among the public, private sector, and government employees regarding risks, threats, and existing solutions and protective measures. Awareness-raising aims to make security a priority for targeted groups (e.g., end users, companies, institutions) in addressing cybersecurity concerns.[16] Various tools, such as brochures, newsletters, training and awareness courses, interactive cybersecurity training platforms, and viral marketing campaigns, are already in use. Complementing these efforts, **cyber hygiene** fosters automatic impulses that promote proactive thinking about cybersecurity aspects in online behaviour (e.g., using suitable products/tools, performing hygienic tasks correctly, establishing routines). One obstacle to broader investment in cyber hygiene and awareness is the perception that cybersecurity is expensive, necessitating costly tools, skilled professionals, and ISO 27001 certification on information security, potentially eroding company profits.

Second, enhancing **digital literacy** and promoting a cybersecurity mindset across governments and societies is essential to ensure that development interventions utilising digital technologies yield positive outcomes for all target groups. This can be achieved through increased investment in cybersecurity-related education and skills programmes, as well as general information security threat education for end users. Concrete initiatives may include developing dedicated cybersecurity curricula, educational and awareness materials, specific skills training, streamlined applicability of degrees, and mutual recognition of certifications. These initiatives can also help bridge the global cybersecurity skills gap.

Additionally, **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, thus enhancing cooperation, mutual understanding, and information exchange. Each critical sector requires some level of cybersecurity expertise: end-to-end network and systems security for telecommunications, defence against financial cybercrime and ID theft for banking/finance, digital forensics and e-crime investigation units for civil and military forces, and operational control networks for energy/water utilities. Public bodies, especially those providing essential services, should ensure that their staff are trained in cybersecurity-related areas to ensure a properly functioning of society and the credibility of state institutions.

15 See ENISA for an overview and concrete proposals regarding the design, implementation and result-based monitoring of cyber hygiene and awareness raising initiatives.

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

While the lessons from ongoing or completed capacity building actions under this pillar are somewhat limited, some **best practices** include:

- Increasing **involvement and establishing clear communication channels** with stakeholders at all levels facilitate information exchange and build safer communities online. For instance, the 'No More Ransom' initiative launched by the National High Tech Crime Unit of police in the Netherlands, Europol's European Cybercrime Centre, and cybersecurity companies helped users prevent ransomware infections and decrypt data if they were victims of an attack.

- Due to the fast pace of technology development, it is challenging to ensure that awareness-raising initiatives are up to date. **Broad coalitions and cooperation networks**, comprising various groups of actors, play a crucial role in ensuring that relevant and timely information is available and shared. Partnerships with the private sector are vital in strengthening the overall cybersecurity culture and skills, especially given the limited resources of the public sector. Overall, most programmes and initiatives focused on cyber hygiene and awareness involve identifying, prioritising, and responding to risks throughout five main spheres: perimeter, network, individual devices, the cloud, and the supply chain.

- Some of the main challenges to cyber hygiene and awareness-raising are linked to **changing or unlearning long-established behaviour patterns**. Cybersecurity is still too often approached as an afterthought rather than as a foundation for all processes within a company or society. To encourage employees to become 'human firewalls' against cyberattacks, organisations need to create a work environment that reinforces compliance with security policies as an integral part of their jobs.

- The development of a **sustainable supply of home-grown cyber expertise** both in terms of professionals and industry is a critical element in addressing the needs of an ever-increasing digital economy. One of the lessons from the evolution of policies and experiences in the cyber security profession around the world is the **need for a national strategic approach in addressing the cyber skills gap**. This includes the development of a national cyber skills strategy (e.g, the UK's Initial National Cyber Security Skills Strategy) and the adoption of a cyber skills framework based on existing international practices (e.g., the European Cybersecurity Skills Framework, the US National Initiative for Cybersecurity Education) to foster a shared understanding between the demand (workplace, recruitment) and supply (qualification, training) side of the cyber skills market that can accelerate collaboration, help policy-makers prioritise actions that address identified skills gaps, as well as promote harmonisation in cybersecurity education, training, workforce development and certification initiatives.

BOX 7: DEVELOPING INFORMATION SHARING PARTNERSHIPS

Effective cooperation and partnerships are not only necessary for addressing cyber risks but also a sign of a developing cybersecurity culture. Public-Private Partnerships (PPPs) and Information Sharing and Analysis Centres (ISACs) in different sectors constitute important capacities in that respect.

Partnerships between the public and private sectors are particularly relevant in the context of critical information infrastructure protection given that the private sector usually owns and operates national critical infrastructure. Partnerships that foster trust and effective coordination are essential for national cyber resilience. Concrete PPPs solutions for the exchange of threat information, coordination of risk reduction or other responses to other cyber-related challenges may include regular meetings between executive leaders and security experts. An example of a partnership between public and private cyber experts includes the Joint Cyber Defence Collaborative established by the US Cybersecurity and Infrastructure Security Agency to gather, analyse and share actionable cyber risk information to enable cybersecurity planning and response. Similarly, the European Public-Private Partnership for Resilience was the first attempt at Pan-European level to use a Public-Private Partnership (PPP) to address cross-border Security and Resilience concerns in the Telecom Sector. PPPs have been also developed in the fight against cybercrime, confidence-building measures, or cybersecurity skills development.

Information Sharing and Analysis Centers (ISACs) are non-profit organisations that provide a central resource for gathering information on cyber threats as well as allow two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis. ISACs may be established in specific sectors of critical infrastructure, including energy, railway, financial institutions or ISC/SCADA systems. While information sharing poses several challenges, numerous good practices may facilitate the process.

2.5. Cyber diplomacy

Actions in cyber diplomacy pillar are relatively new. Most states have limited capabilities to engage in international debates on cyber-related issues. In such a context, an action focused on improving their understanding of international cyber policies or strengthening their capacities to implement undertaken

actions. As a result, any such initiatives need to set realistic goals that consider the political realities and broader international context within which the partner country operates. In cyber diplomacy initiatives, conducting a thorough context analysis and risk assessment is crucial to avoid reputational damage or inefficient use of resources. This does not imply adopting a zero-risk policy, but rather emphasising the importance of risk anticipation and designing appropriate risk mitigation and response mechanisms should those risks materialise. This is especially vital for partner countries that have significant political or economic ties with countries that do not share the EU's vision of cyberspace. By taking these factors into account, cyber diplomacy capacity building initiatives can be more effective and better adapted to the specific circumstances of each partner country, ultimately fostering stronger and more constructive partnerships in the field of cyber diplomacy.

- **Regional organisations** play a crucial role in cyber diplomacy capacity building. They are important in setting the policy agenda and implementing capacity building efforts. Over the past decade, organisations like the EU, OAS, ASEAN, and OSCE have proven to be essential players in this area. Their unique understanding of member states, political sensitivities, and regional characteristics gives them a valuable perspective that external actors do not possess. They also hold institutional memory, enabling better identification of objectives, assumptions, and risks related to cyber diplomacy capacity building. Moreover, these organisations enjoy a high level of trust among their members, which makes them stand out from external actors. However, when working with regional organisations, it is essential to be aware of their mandates, tools, and decision-making procedures, as these factors may limit their capacity to deliver certain outcomes.

- **Multistakeholder engagement** is essential for ensuring that cyber diplomacy discussions are inclusive and represent diverse perspectives on the development of norms and principles of responsible state behaviour in cyberspace. Civil society and the private sector have a crucial role to play in shaping both national and international cyber diplomacy discussions. Moreover, they serve as a valuable resource in cyber capacity building and enhancing expertise in the field of cyber diplomacy. Their participation at the national level can be particularly advantageous for countries with limited human resources or expertise, especially concerning international law or human rights. Civil society organisations have developed practical guides or toolkits to support the development of inclusive norms and have created human rights assessment guides for the application of international law. Additionally, they are actively involved in providing training and implementing capacity building initiatives. Their contributions are instrumental in fostering a collaborative and well-informed approach to cyber diplomacy and building a robust cyber ecosystem that promotes responsible state behaviour and respects human rights

BOX 8: DEVELOPING CAPACITIES FOR CYBER DIPLOMACY

The report by the UN Group of Governmental Experts has identified the following priorities for international cyber capacity building efforts in support of international peace and security:

a) developing and implementing national ICT policies, strategies, and programmes,

b) creating and enhancing the capacity of CERTs/CSIRTs and strengthening arrangements for CERT/CSIRT-to-CERT/CSIRT cooperation,

c) improving the security, resilience, and protection of critical infrastructure

d) building or enhancing the technical, legal, and policy capacities of States to detect, investigate, and resolve ICT incidents, including through investment in the development of human resources, institutions, resilient technology, and educational programmes,

e) deepening common understandings of how international law applies to the use of ICTs by States and promoting exchanges between States, including through discussions at the United Nations in this regard,

f) building or enhancing the technical, legal, and policy capacities of States to detect, investigate, and resolve ICT incidents, including through investment in the development of human resources, institutions, resilient technology, and educational programmes,

g) deepening common understandings of how international law applies to the use of ICTs by States and promoting exchanges between States, including through discussions at the United Nations in this regard,

h) enhancing the technical and legal capacities of all States to investigate and resolve serious ICT incidents,

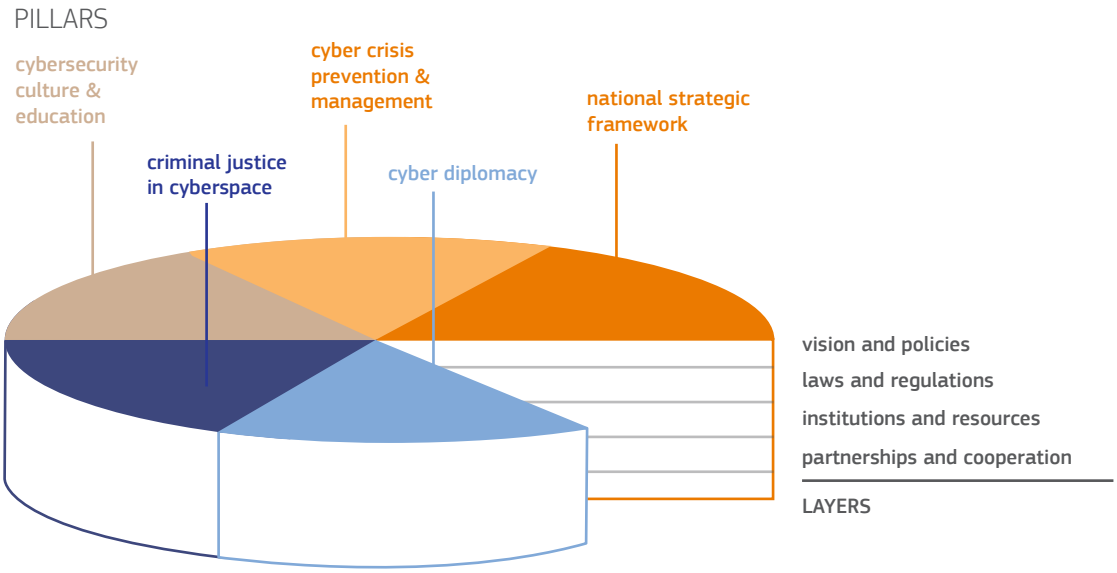
i) implementing agreed voluntary, non-binding norms of responsible State behaviour,

j) to this end, and as a means to assess their own priorities, needs, and resources, States are encouraged to use the voluntary Survey of National Implementation recommended by the United Nations OEWG.

3. What specific objectives? Layers of cyber capacity building

The experience of the development community with capacity building actions offers valuable guidance for defining the **primary layers** of cybersecurity capacity building that need consideration. Decisions regarding the layers of a cyber capacity building action are directly related to the focus and scope of a particular intervention. Capacity building actions conducted under a specific pillar may address one or several layers. This methodological approach helps identify and prioritise the gaps and needs of partner countries/regions to determine the necessary support.

Figure 6. Layers of cyber capacity



3.1. Vision and policies

Developing capacities to address vulnerabilities in cyberspace requires a clear identification of what needs protection and how. Strategic objectives may involve **strengthening state and societal resilience, protecting economic growth, ensuring national security, or supporting other developmental goals**. This vision is typically outlined in a general policy framework, such as a national security strategy or a cybersecurity strategy, which plays a crucial role in unifying stakeholders around a defined vision or policy. Ideally, the vision should be developed with the participation of a broad stakeholder community. Supporting partner countries in creating their own vision is essential, as it will likely influence the concrete policies they adopt. For example, a government with a more state-centric view on cyberspace governance may adopt more authoritarian digital policies, disregarding the perspectives of other stakeholders. Ultimately, **a vision and its associated policies should reflect a certain value system and contribute to the emergence of a unique cyber culture in society.**

Focusing on vision and policies in cyber capacity building provides an opportunity to showcase the benefits of policy solutions adopted in the EU and promote policy convergence between the EU and partner countries or regions. Specific actions may involve developing new policies (e.g., critical infrastructure resilience), enhancing linkages or coherence between different cyber policies to ensure their effectiveness, or strengthening the capacities of specific stakeholder groups to increase their involvement in cyber-related policy making (e.g., consumer organisations, ombudsman, specific ministries).

TABLE 1: VISION AND POLICIES	
If you decide to focus on pillar ...	then possible objectives include ...
National strategic framework	• Defining strategic objectives, priorities, and cyber governance framework • Identifying measures to strengthen preparedness, response, and recovery from cyber incidents • Developing, adopting, implementing or reviewing a national cybersecurity strategy • Adopting procedures for regular threat analysis and risk assessment • Setting up a comprehensive cyber governance mechanism
Crisis prevention and management	• Developing, adopting, and implementing national and/or sectoral cyber crisis management strategy or plan • Conducting regular cybersecurity exercises and recording lessons • Adopting a policy framework and tools for the identification of critical information infrastructure • Developing and implementing mechanisms for regular assessment of cyber vulnerabilities
Criminal justice in cyberspace	• Developing policies to fight against cybercrime • Adopting safeguards to ensure respect for human rights and the rule of law • Conducting a regular evaluation of the effectiveness of legislation and collection of statistical data on cases investigated, prosecuted, and adjudicated • Signing, ratifying, and implementing international standards on data protection in line with international (ETS 108), protection of children against sexual violence (Lanzarote Convention)
Cybersecurity education and culture	• Developing cybersecurity education, skills development and training programmes at all levels of education • Adopting policies around data breach notification and follow-up information campaigns
Cyber diplomacy	• Formulating an international cooperation strategy based on a clear vision for cyberspace (e.g., global, free, open, safe, secure) • Integrating international cyber policy in a coordinated national cybersecurity response system to prevent, detect, deter, and respond to cyber incidents • Implementing the framework for responsible state behaviour in cyberspace

3.2. Laws and regulations

Laws and regulations translate concepts, strategies, and principles into specific rules, rights, and obligations for all stakeholders within the cyber ecosystem – individuals, organisations, companies, and government entities. Simultaneously, they shape the context in which cyber capacity building takes place. Necessary legal measures may include defining and protecting protocols and standards for critical information infrastructure or information society services. However, **due to the complexity of Internet-related laws and regulations, many countries face challenges in adjusting their existing legal orders** to this rapidly changing technological environment. Coherently regulating different but overlapping policy areas, such as data protection, cybercrime, and network security, requires a good understanding of the legal dimensions of these cyber-related policy areas. This can be particularly challenging for countries with limited resources, placing a disproportionate burden on them. As a result, some countries might consider adopting model laws or adopting laws and regulations from other countries as a plausible alternative, despite the potential risks they may carry in the specific national context. Therefore, the adoption and implementation of legal and regulatory frameworks require strengthening capacities at all levels and across different branches of government. This includes enhancing individual legal skills, adjusting university curricula, raising awareness among parliamentarians, establishing cooperation mechanisms within the justice system, strengthening the organisational capacity to implement laws and regulations, and creating an enabling environment.

Focusing on laws and regulations in cyber capacity building provides an opportunity to showcase the benefits of legal and regulatory solutions adopted in the EU and promote regulatory convergence between the EU and partner countries or regions. Concrete actions may involve supporting a partner country in developing its own laws and regulations or adopting solutions like those in the EU. In the former case, particular attention must be given to a rights-based approach and ensuring that other legal instruments adopted in the country do not undermine or significantly alter the interpretations of cyber laws and regulations. At the regional level, it is essential to avoid developing laws that may hinder efforts towards interoperability and the harmonisation of practices at a global level. When initiatives focus on mirroring EU solutions, they must ensure that the proposed solutions are adapted to the local context, and the partner country has the capabilities to ensure their effective implementation.

TABLE 2: LAWS AND REGULATIONS

If you decide to focus on pillar ...	then possible objectives include ...
National strategic framework	• Developing mechanisms for the identification of gaps in laws and regulations • Promoting 'duty of care', 'security by design' and human-centric approaches through laws and regulations • Ensuring compliance with the existing international standards, including human rights online • Developing, adopting and implementing a coherent legal framework in support of a cybersecurity strategy and other policy pillars
Crisis prevention and management	•

Cybersecurity education and culture	• Developing standardisation, certification and/or labelling schemes to strengthen consumer protection against digital risks • Adopting cybersecurity standards for government and private sector, in line with existing international best practices (e.g., ISO) • Promoting basic cyber hygiene and awareness raising tools, including through service contracts and terms of use (e.g., password management policies, encryption)
Cyber diplomacy	• Developing a national position regarding the application of international law in cyberspace • Promoting implementation of the UN framework for responsible state behaviour in cyberspace in national legislation and policies

3.3. Institutions and resources

Institutions play a critical role in implementing policies and enforcing laws, especially in the following contexts:

- When implementing a national cybersecurity strategy.
- For preventing, detecting, and responding to potential cyberattacks, typically through a national level CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team).
- For conducting cybercrime investigations and digital forensics, often requiring the establishment of high-tech crime units.

Establishing a well-defined institutional structure with clear cybersecurity responsibilities is essential to eliminate uncertainties about roles and responsibilities at the national and international levels. The existence of specific institutions at the operational or technical level has become a benchmark for measuring a state's level of cyber maturity.

However, **there is no one-size-fits-all solution**, and the design of specific institutional arrangements should consider the nuances of national culture, history, law, and public administration methods. As countries adopt different models based on their cultural and political backgrounds (e.g., some set up such bodies within their Ministry of Defence, while others in the Ministry of Telecommunications), a thorough understanding of each specific domestic context is crucial. Elements such as leadership, relationship management, and accountability mechanisms are often decisive in ensuring the success of a project or undertaking. While involving different government entities is essential to achieve a whole-of-government approach, the ultimate coordinating role should be clearly assigned.

Addressing capacity needs at different layers also requires sufficient resources. This can be a challenge for developing countries where other priorities compete for funding, human resources, equipment, training, education, and awareness-raising efforts. Therefore, the capacity to plan, implement, manage, and evaluate projects and programmes is equally important. This includes the ability to prepare budgets, estimate capacity development costs, manage human and financial resources, engage in procurement, set indicators for monitoring progress, measure results, collect feedback for policy adjustments, codify lessons, promote learning, and ensure accountability to all relevant stakeholders.

Focusing on institutions and resources in cyber capacity building provides an opportunity to influence the stakeholder ecosystem and the power structure, as well as secure the human and financial resources necessary for the effective implementation of national policies, strategies, and laws. Concrete actions may focus on supporting a partner country in building or strengthening institutions such as a national cybersecurity coordination centre, national CSIRT, cybercrime units, or digital forensics labs. Additionally, improving coordination between various actors within the ecosystem, such as law enforcement and CSIRTs, and creating a network of cyber crisis incident responders are important aspects to consider. When strengthening institutions, it is crucial to ensure that a partner country commits human and financial resources to their proper functioning. In cases where this commitment is lacking, individual actions can support strengthening national capacities by providing funding, training, and other necessary resources.

TABLE 3: INSTITUTIONS AND RESOURCES	
If you decide to focus on pillar ...	**then possible objectives include ...**
National strategic framework	• Defining roles and responsibilities of governmental actors for national cyber policy • Setting up and equipping a national cybersecurity agency • Defining cybersecurity-related metrics for policy monitoring and evaluation • Strengthening inter-agency coordination mechanism in the cyber domain
Crisis prevention and management	• Developing incident monitoring and response capacity (e.g., CSIRT/CERT), including a focal point for managing cyber incidents/crises • Adopting a crisis management structure with a clearly defined command chain, SOPs • Improving mechanisms for information sharing (e.g., the establishment of Information Sharing and Analysis Centers – ISACs) • Regular training and exercises in cyber crisis management procedures and mechanisms • Developing mechanisms for early warning, alerts, or announcements • Defining clear procedures for capturing and sharing good practices and lessons
Criminal justice in cyberspace	• Establishment of national 24/7 points of contact • Training for staff and resources for complying with the MLAs commitments • Judicial oversight for compliance with principles of proportionality and necessity by LEAs • Setting up, training, and providing continuous support to digital forensics units, prosecution units, cybercrime units
Cybersecurity education and culture	• Developing the competence of consumer protection or ombudsman bodies in cyberspace • Adopting governmental support schemes for low-income citizens and businesses • Raising awareness about online abuse and gender-based violence • Developing modules and professional cybersecurity roles for CSO/CISO, network security specialists, digital forensics and incident response analysts, information security assessor, security architect, vulnerability analysts • Introducing electronic identification and trust services for citizens, businesses, and public administrations to access online services or manage electronic transactions • Promoting procedures for security accreditation and certification of skilled personnel • Establishing a one-stop-shop to help victims of cyberattacks, providing information on the latest threats and bringing together practical advice and cybersecurity tools
Cyber diplomacy	• Developing mechanisms for coordination of national positions within the government and with a broader multi-stakeholder community • Establishing a cyber diplomacy team, including a coordinator for cyber/digital issues • Defining roles of civilian and military actors in cyberspace, including procedures for civilian-military cooperation

3.4. Partnerships and cooperation

Developing robust domestic and international partnerships is key to effective policies across all pillars of cyber capacity building. At the national level, this involves ensuring collaboration between different government entities, such as ministries, national cybersecurity agencies, and prosecutors. Additionally, sustainable partnerships between the government and other stakeholders, including the private sector, civil society organisations, and research institutes, are essential. Cyber capacity building requires engaging resources at different levels, ideally through a whole-of-society approach. The increasing push for a more state-centric model of cyberspace governance promoted by certain governments

Criminal justice in cyberspace	• Developing mechanisms for identification and facilitation of good practices between specialised units at regional and international level • Adopting legal provisions facilitating public/private information sharing • Promoting international cooperation, including through the existing bi- and multilateral and regional arrangements such as the Cybercrime Convention Committee (T-CY) • Strengthening the culture of cooperation between LEA and ISPs and other private sector entities through MoUs • Establishing mechanisms for regular updates to directories of 24/7 Points of Contact and participation in 24/7 PoC Network
Cybersecurity education and culture	• Developing and implementing multi-sector and multi-stakeholder cybersecurity training and awareness programmes • Establishing mechanisms for multistakeholder cyberspace governance • Developing and implementing regular activities to raise awareness about cyber issues, including a national cybersecurity month
Cyber diplomacy	• Promoting and supporting participation in relevant regional and international initiatives on cyber diplomacy • Implementing international commitments in the cyber domain • Developing mechanisms for responding to international requests for assistance

4. Whose capacity? Levels of intervention

It is generally accepted that capacities in cyber capacity building are distributed across three main levels: individual, organisational, and enabling environment. Recognising that capacities at each level can either support or undermine the effectiveness of the other levels, comprehensive cyber capacity building actions must take into account, and ideally address, capacity gaps at all three levels.

Figure 7. Levels of cyber capacity

4.1. Individual capacity

Capacity building for individuals involves equipping them with the necessary understanding, skills, and access to information, knowledge, and training to perform effectively. It focuses on addressing needs, skills, capabilities, personal attitudes, motivations, values, etc. Monitoring the development of capacities at the individual level can be particularly challenging. Additionally, various risks need to be considered when designing capacity building actions. These risks range from difficulties in attracting and retaining skilled IT security personnel to a lack of understanding about the importance of investing in cybersecurity at the political level, and the risk of incompatibility with other donor activities. Ultimately, even the best equipment may prove ineffective if left unmanned, untested, not updated, or without a properly trained team in place.

The focus on strengthening individual capacities should be viewed as a long-term investment in developing interpersonal relationships that can become valuable resources in strengthening the EU's partnership and cooperation with a partner country or organisation. Concrete activities targeting this level may include trainings, workshops, seminars, fellowships, study visits, or exercises. However, it is essential to distinguish between efforts aimed at enhancing the capacities of individual employees of cyber-relevant institutions and organisations (which directly links to the institutions and resources layer and the organisational capacity level) and actions focused on improving the skills of individuals more broadly – such as STEM education or awareness raising – which connects to the enabling environment level and may overlap with the cybersecurity education and culture pillar.

TABLE 5: INDIVIDUAL CAPACITY

If you decide to focus on pillar ...	then possible objectives targeting individual capacities include ...
National strategic framework	• Improving awareness and knowledge of cyber-related issues among government officials at different levels • Strengthening knowledge and technical skills related to the development and/or implementation of a national cybersecurity strategy • Clearly defining the tasks for CSO/CISO, network security specialists, digital forensics and incident response analysts, information security assessor, security architect, vulnerability analysts
Crisis prevention and management	• Improving awareness, knowledge, and technical skills related to cyber crisis management for IT security experts, policymakers, and diplomats (e.g., through table-top exercises and trainings) • Strengthening operational skills in crisis management, implementation of cyber contingency plans, and communication with external stakeholders • Improving knowledge and/or development of standard operating procedures, guidance notes, manuals
Criminal justice	• Strengthening awareness, knowledge, and technical skills of judges, prosecutors, and law enforcement to effectively tackle cybercrime • Strengthening awareness, knowledge and technical skills of civil society organisations, journalists and data protection practitioners to strengthen monitoring and accountability of the security sector
Cybersecurity education and culture	• Developing educational and training curricula that include cyber components for schools (e.g., classes on cyber hygiene, lessons in coding, courses on online safety) and professional trainings (e.g., law schools, policy academies, diplomatic academies) • Promoting initiatives that strengthen the involvement of women in the cyber domain • Developing initiatives that improve the skills and knowledge of educators, teachers, and trainers • Conducting campaigns encouraging students to choose cyber-related professions • Developing awareness raising initiatives that strengthen the cybersecurity culture

Cyber diplomacy	• Improving awareness, knowledge, and technical skills of diplomats, educators working for foreign policy institutes and diplomatic schools • Improving awareness, knowledge and technical skills of non-governmental stakeholders and journalists on cyber diplomacy and foreign policy

4.2. Organisational capacity

Capacity building for organisations focuses on developing management structures, processes, and internal procedures, as well as managing relationships between different organisations and sectors (public, private, and community). It addresses practices, roles, mandates, decision-making structures, divisions of labour, sharing of responsibilities, methods of management, means of functioning, and the use of resources – intellectual, material, economic, and technological. Recognising the high level of interdependency between some organisations (e.g., hospitals relying on energy providers), it is essential to approach organisational capacities in a systemic way that addresses vulnerabilities of the entire cyber ecosystem and does not treat organisations in isolation. While many actions typically concentrate on creating new organisations, it is equally important to ensure that established institutions have sufficient resources to perform their tasks effectively.

The focus on organisational capacity represents an investment in the sustainability of any future EU cyber-related intervention and meaningful support to partner countries. Well-functioning, transparent, and accountable institutions help mitigate risks associated with political changes in a country and increase the possibility of continuous cooperation. Concrete actions targeting organisational capacities may involve establishing new institutions for cyber resilience, enhancing cooperation between different actors, and facilitating dialogue among various stakeholder groups.

For example, it is generally accepted that a functioning CERT/CSIRT is a bare minimum in developing a cyber crisis management system. Therefore, one of the first steps is to establish whether a country has a CERT and, if yes, identify its official mandate (e.g., the official national point of contact), external services provided to its constituency, and internal support services (e.g., requests for assistance, guidance for improving infrastructure, incident handling, and management). Additionally, cybersecurity exercises are particularly valuable tools as they enable competent authorities to target specific weaknesses, enhance cooperation across the critical information infrastructure sector, identify interdependencies, stimulate improvements in continuity planning, and foster a culture of cooperative effort to boost resilience in the cyber cooperation area. An exercise can be used to test various elements of the cybersecurity plan involving the technical, operational, and strategic levels.[17] Therefore, supporting cybersecurity exercises is one of the main objectives of cyber capacity building in the medium- to long-term.[18]

TABLE 6: ORGANISATIONAL CAPACITY	
If you decide to focus on pillar ...	**then possible objectives targeting organisation capacities include ...**
National strategic framework	• Establishing structures for the development and/or implementation of a national cybersecurity framework (e.g., task force, cybersecurity agency) • Developing a cybersecurity ecosystem with clearly prescribed mandates and responsibilities between different government agencies and stakeholder groups • Adopting action plans prescribing rights and duties of different stakeholder groups regarding the implementation of national cybersecurity strategy • Developing procedures for the operational implementation of the whole-of-society and whole-of-government approaches

17 ENISA, 'National and International Cyber Security Exercises: Survey, Analysis and Recommendations', Heraklion, 2012, 32p.
18 See: ENISA, 'National and International Cyber Security Exercises: Survey, Analysis and Recommendations', Heraklion, 2012; ENISA, 'Emergency Communications Stocktaking: A study into Emergency Communications Procedures', Heraklion, 2012; ENISA, '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.

Crisis prevention and management	• Developing a robust cyber crisis management ecosystem with clearly prescribed responsibilities, procedures, and resources • Identifying critical infrastructure entities, including mandates for their protection • Conducting cyber exercises in line with the whole-of-government approach • Establishing and appointing a 24/7 duty officer • Adopting internal procedures for breach notification and cyber incident reporting • Promoting the participation of CERTs/CSIRTs and other crisis management bodies in international networks (e.g., FIRST, AfricaCERT)
Criminal justice	• Establishing 24/7 points of contact • Establishing specialised prosecution units, digital forensics units, and specialised cybercrime units with clearly prescribed functions • Developing mechanisms for ensuring checks and balances, accountability
Cybersecurity education and culture	• Establishing schools and training institutions providing cyber-related training • Mainstreaming cyber-related issues into educational curricula (e.g., for judges, prosecutors, diplomats) • Raising awareness and training on cyber resilience across the education system • Developing and nurturing public-private partnerships for closing the skills gap • Establishing education and certification programmes for cyber personnel • Providing continuous training on cyber threats and security trends
Cyber diplomacy	• Setting up a cyber diplomacy team/unit • Appointing a coordinator/ambassador for cyber/digital issues • Developing procedures for attribution of cyberattacks and response mechanisms

4.3. Enabling environment

Creating an enabling environment involves establishing the right set of legal, regulatory, economic, and societal changes that support organisations, institutions, and agencies at all levels and in all sectors in enhancing their capacities. It can be seen as a set of pre-conditions necessary for undertaking actions. Assessing capacities at this level involves looking at society, laws, policies, procedures, norms, standards, power structures, systems, the environment, and culture.

Private sector development and fostering the right investment climate play a crucial role in achieving the Sustainable Development Goals (SDGs), particularly in the context of cybersecurity and digital transformation characterised by dependencies on a small group of technology providers. Building an enabling environment for domestic businesses and entrepreneurs to operate, as well as conditions facilitating international trade and private investment, is an essential element of cyber capacity building engagement. Such efforts may include business environment reform, which involves regulatory, legal, policy, and institutional reforms aimed at improving the business environment, as well as ensuring a stable and transparent political environment, good governance, an independent, impartial, and efficient national justice system, and anti-corruption measures. The European Commission's business environment reform guidelines could be useful in this regard.

The enabling environment is often overlooked in capacity building actions, yet it is the context within which they are conceived and implemented that ultimately determines their success or failure. No matter how well-designed, a cyber capacity building action will not deliver sustainable results without political support or if the legal tradition conflicts with the proposed solutions. Thus, it might be critical to initially focus on creating the right environment – for instance, through political dialogues and trade relations – before launching more targeted actions. Cyber-specific components of the enabling environment include a functioning open market economic environment, policies supporting research and development, digital literacy, and a skilled workforce. The enabling environment plays an important role in the context of growing strategic competition between traditional donors like the European Union, whose engagements are driven by rights-based approach methodologies, and new donors like China, which provides funding without any conditions attached.

The focus on the enabling environment in cyber capacity building provides an opportunity to create the right conditions for the implementation of cyber capacity actions and minimises the political risks of engaging with a particular partner country. Concrete initiatives may concentrate on strengthening legal or institutional frameworks that are not directly linked to cyber but are important for the implementation of a cyber-focused action. For instance, this could involve establishing robust data protection regulations, a commitment to the rule of law, and a system of institutional checks and balances. In that sense, interventions focusing on the enabling environment may require engagement across different policy areas or be part of a broader action focused on institutional, economic, or legal intervention in the partner country.

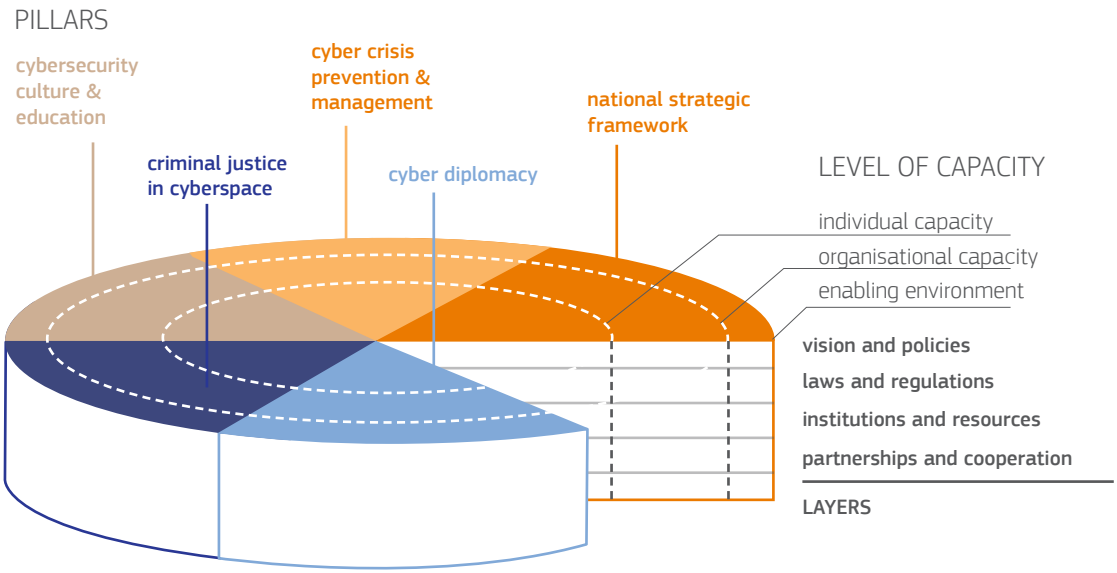
TABLE 7: ENABLING ENVIRONMENT

If you decide to focus on pillar ...	then possible objectives targeting enabling environment include ...
National strategic framework	• Promoting democratic institutions and commitment to human rights • Strengthening checks and balances, oversight and accountability mechanisms • Developing a monitoring and data collection culture • Supporting the development of a robust private sector, civil society and conditions for strengthening public-private partnerships • Adopting policies that provide incentives for investment in cybersecurity (e.g., industrial, taxation, trade) • Promoting commitment to 'data protection by design' and 'data protection by default'
Crisis prevention and management	• Development of laws, institutions and procedures for crisis management • Establishing information exchange channels for crisis management • Strengthening risk management culture
Criminal justice	• Strengthening independent judiciary • Adopting and implementing robust anti-corruption laws • Adopting and implementing adequate data protection regulation • Ensuring judicial oversight of intrusive powers • Ensuring respect for principles of proportionality and necessity by LEAs • Ensuring effective enforcement of the rule of law and human rights
Cybersecurity education and culture	• Ensuring universal access to education • Promoting and protecting freedom of the press and a robust media ecosystem • Promoting investment in STEMS education, in particular for girls
Cyber diplomacy	• Strengthening commitment to the UN Charter and international law • Supporting proper functioning of the foreign service • Developing peaceful relations and strengthening cooperation with neighbours

5. The EU's comprehensive approach to capacity building

At the end of the process, a framework for cyber capacity building actions emerges, requiring the **comprehensive and integrated approach** of tackling all three elements – pillars, levels, and layers of capacity. The proposed 'cake model' serves as a valuable methodological tool to deconstruct various concepts, organise issues, and design tailored and effective cyber capacity building engagements. It emphasises the significance of combining the right mix of ingredients for a successful capacity building action while allowing flexibility in determining the direction – the flavour – of the specific action.

Figure 8. Policy pillars, layers, and levels in the external cyber capacity building



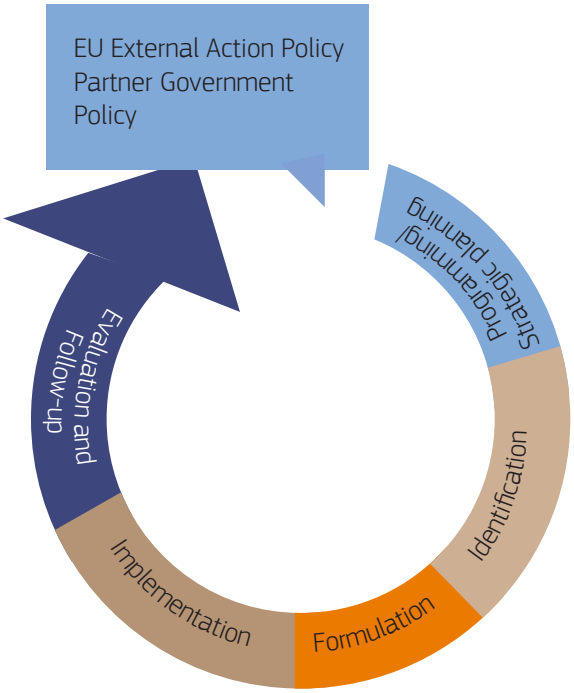
III. THE EU's EXTERNAL CYBER CAPACITY BUILDING IN PRACTICE

The increased funds for cyber issues under the EU external financing instruments raise challenges in ensuring policy coherence and optimal operational choices to promote a global, open, stable and secure cyberspace in a complex geopolitical environment. The interconnection between economic aspects of new technologies, internal security and foreign, security and defence policies requires a holistic understanding of policies and methodologies that support 'policy-first' and 'value-driven' cyber capacity building actions.

This chapter dives into the practical application of the CCB framework across the project cycle in a cyber-informed way to support a context-sensitive and demand-driven process of change. It covers the five stages of the EU's Intervention Cycle, namely:

- **Programming**: We consider if and how cyber issues can be embedded within the broader developmental context and contribute to development priorities set forth by the partner country/region. We articulate a cyber-related development goal or, if previously set, review and validate it.
- **Identification (design phase 1)**: Once a cyber-related developmental goal is mutually agreed upon with the partner, we identify the best options to achieve it within the specific context, assessing existing cyber capacities/ resources and identifying risks.
- **Formulation (design phase 2):** Building on the identified options, we expand the analysis on their feasibility and sustainability with the latest context, map a risk mitigation strategy, and design an intervention logic that is supported by a results chain to guide the change process towards the expected cyber outcomes.
- **Implementation:** Once the action starts, we focus on the efficient and effective execution of activities, monitor progress towards the cyber-related outcomes, manage risks, and make needed adjustments from inception to closure.
- **Evaluation and learning:** We assess the results of the action across the intended outputs, outcomes, and impact towards the cyber-relevant development goal, capture lessons learnt and inform decision-making for future cyber actions.

Figure 9. Intervention cycle stages



1. Values – Interests – Principles approach to CCB

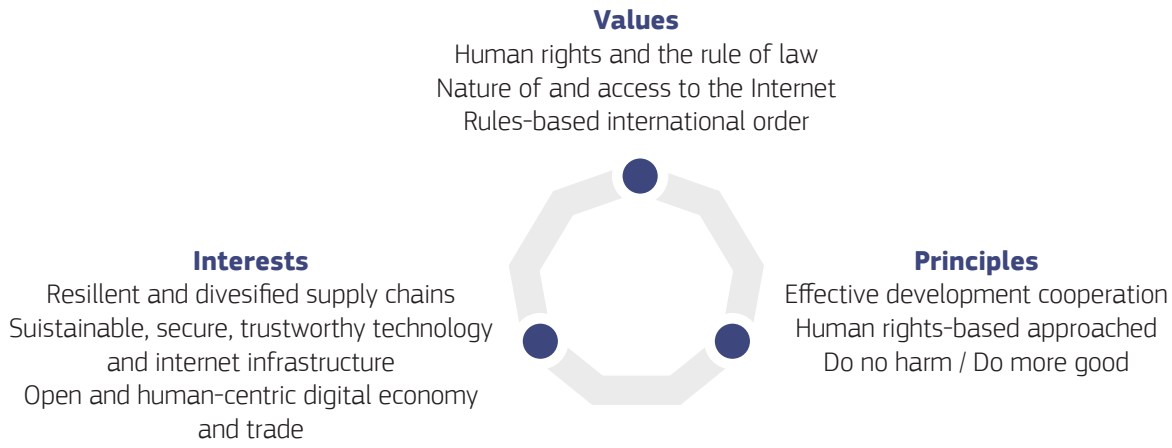
This V-I-P approach is meant to offer practitioners a simple and balanced framework to assess the most pertinent issues for the EU's engagement in a cyber capacity building action with a partner country or region, and support the risk monitoring across the intervention cycle.

The strategies to mitigate political, societal or institutional risks for the EU cyber capacity building actions need to be grounded in existing values, interests, and principles enshrined in international instruments, the EU Treaties and relevant cyber policies. This approach underlines the cyber dimension in the drivers of the EU's engagement while placing the partner country/region at the centre. Drawing from international instruments, EU Treaties, EU policy documents[19] and the

19 Notable examples to date include: the New European Consensus on Development (2017), the EU Cybersecurity Strategies (2013, 2017, 2020) and its legislation (see section IV), the Council Conclusions on the EU External Cyber Capacity Building Guidelines (2018) the NDICI-Global Europe Regulation (2021), Global Gateway Communication (2021), Trade Policy Communication (2021), as well as the European Economic Security Strategy (2023)

effective development cooperation body of work,[20] the V-I-P approach defined hereby aims to offer to EU staff a guiding framework for **a 'values-interests-principles'-informed EU cyber capacity building** that also serves as a risk monitoring and management framework.

Figure 10: Values – Interests – Principles approach to CCB



1.1. Promoting values

Any EU engagement with partner countries and regions needs to ensure the respect for and promotion of established universal values anchored in international instruments[21]. These serve also as a guide to CCB These values should guide the CCB action across the intervention cycle to assist practitioners in addressing challenges resulting from divergent or conflicting policy objectives in a dynamic political, societal, or institutional setting.

- **Human rights and the rule of law:** Cybersecurity efforts can be effective only if based on the respect for fundamental rights and freedoms. The same rights that exist offline also apply online. All CCB engagements must meet at least the minimum threshold of respecting, protecting, upholding, and enabling human rights as well as promoting peaceful coexistence in cyberspace as enshrined in the UN Conventions. They include respect for private and family life, home, and communications; freedom of expression and information; protection of personal data; media freedom and pluralism in the online environment. These can be assured within an environment of good governance with checks and balances, and accountability mechanisms. Increased global connectivity should not lead to online censorship, mass online surveillance, Internet shutdowns, or repression against civil society, academia, and citizens. CCB actions should integrate a human rights-based approach, systematically monitor human rights compliance, and assess their legality and legitimate aim, necessity and proportionality.[22]

- **The nature of and access to the Internet:** The Internet has been a key driver of innovation and economic development thanks to its free, open, plural, interoperable nature. This has been enabled by its multi-stakeholder governance model that is responsible for developing and implementing the principles, norms and decision-making processes that underpin the Internet's evolution and use. Conversely, authoritarian states promote a government-controlled model that could embed a system of centralised rule enforcement into the technical fabric of the Internet and cause its splintering. Therefore, CCB actions should promote Internet access that is open, safe, affordable, equally accessible, and non-discriminatory. Such approach shall all strengthen efforts to address Internet access disparities and tackle digital divides that manifest in multiple levels, including between women and men, urban and rural areas, more and less developed nations. To support an unhindered flow of information and equal access to the Internet, CCB actions should also include the 'analogue complements' that ensure competition among businesses, adaptability of workers' skills, accountable institutions, and access to knowledge.

20 Especially the efforts led by the OECD DAC Committee and the Global Partnership for Effective Development Cooperation.
21 In the EU context, the EU Cybersecurity Strategies elaborate on these values from a cyber perspective, while other key references with a relevant cyber accent are the Action Plan on Human Rights and Democracy 2020–2024 (2020), the EU Human Rights Guidelines on Freedom of Expression Online and Offline (2014), and the EU-supported Declaration for the Future of the Internet (2022).
22 The International Principles on the Application of Human Rights to Communications Surveillance are a good guidance framework for practitioners to understand how international human rights law applies in the current digital environment.

- **Rules-based international order:** The promotion of the rule of law in cyberspace, along with respect for norms of international rules and standards, form a United Nations acquis[23] that is aligned with the EU values for a rules-based international order. Building trust and confidence in ICT, mitigating cybersecurity threats, and promoting responsible State behaviour in cyberspace contribute to peace and stability. This means that CCB actions need to systematically assess and monitor the risk of potential misuse by a partner country of the provided support to harm its population or use it in ways contradictory to the peaceful use of cyberspace.

1.2. Protecting interests

While the premise of international development cooperation is the support for goals identified by partners, the EU's decisions about support are also driven by its own interests and priorities. In the case of cyber capacity actions, they can aim at reducing cybercrime or strengthening the protection of critical infrastructure in a partner country, which also serves the EU's own security. By the same token, the EU may decide not to engage if an action may undermine its political, economic, and strategic interests. While the EU interests may shift dynamically overtime, there are several core aspects to consider across the project cycle for a CCB action:

- **Resilient and diversified supply chains:** Supply chain disruptions may have a devastating impact. The ability to access a secure, diversified, affordable and sustainable supply of critical raw materials, essential products and technologies is a core EU interest. They are indispensable for a wide set of strategic sectors, including the twin green and digital transition. To enhance its economic resilience, the EU aims to mitigate the risks for supply chains stemming from its strategic dependencies, including in cybersecurity. Strategic partnerships with emerging markets and developing economies are a mutually beneficial method to support diversification and local value creation and to promote resilient, affordable, and sufficiently diversified value chains for the EU. Moreover, the EU has a stake in supporting its partners' resilience in the face of hybrid threats and the weaponisation of certain supply chain dependencies by adversaries and strategic competitors.

- **Sustainable, secure, trustworthy technology and internet infrastructure:** Investing in sustainable, trustworthy, and secure infrastructure, including next-generation networks, is a top EU priority. The global economy and supply chains increasingly rely on digital systems enabled by the deployment of digital networks and connectivity infrastructures – such as mobile, satellite and core networks, submarine cables, cloud, and data infrastructure. Enhancing the security and resiliency in critical infrastructure, particularly in the digital domain, is crucial and requires a rigorous evaluation using guidance such as the EU's 5G toolbox. Similarly, the EU's efforts to set regulatory cybersecurity requirements for products with digital elements aim to limit the vulnerabilities in hardware and software products entering the market. The EU's approach to new digital infrastructures and emerging technologies is underpinned by regulation that aims to promote technical standards and protocols enhancing security, resilience, and interoperability in a technology-neutral way, with a minimal environmental footprint. In the face of geopolitical rivalries, where creating technological dependencies is used as a tool to shape the global digital space, the EU can use its cyber capacity building actions to promote development of sustainable, secure and resilient internet infrastructure.

- **Open, human-centric digital economy and trade:** The EU promotes a human-centric vision for a fair and inclusive digital economy that leaves no one behind. It is committed to an open and rules-based global digital economy and advocates for international digital trade without unjustified barriers while maintaining high data protection standards. As such, the EU's regulatory model for communications networks and services emphasises robust privacy and personal data protection as a pre-condition for stable, secure, and competitive global commercial flows. This is the basis for enabling local businesses to benefit from the digital revolution and protecting people's privacy. Connected to the point on supply chains, it is also in the interest of the EU to support its partner countries' overall resilience against economic or trade coercion from certain international actors that seek to exploit economic vulnerabilities and dependencies.

23 As defined in the United Nations GGE and OEWG consensus reports – see section 'Cyberspace as a diplomatic arena'.

1.3. Implementing principles

A wealth of guiding principles based on decades of lessons from international and development cooperation[24] supports how the value- and interest-based approaches defined above are operationalised in practice. Key principles to guide CCB actions are grouped into the following:

- **Effective development and international cooperation:** While different motives drive cyber capacity building (e.g., development, security, economy), the development effectiveness body of work provides invaluable guidance for practitioners designing and implementing external cooperation programmes, including on digital and cyber issues. **Partner countries' ownership** is a pre-condition for the successful cyber cooperation and process of change that is aligned with national development. Also, CCB actions should **focus on results and sustainability** that create a shared obligation for the partner country and the EU to systematic monitoring and harmonised results reporting, including partner-country-level results frameworks where they exist. Moreover, effective cooperation relies on **inclusive, multistakeholder partnerships** acknowledging the diversity and complementarity of the different actors. In the context of cyber-related policies, this can be facilitated by a meaningful and regular policy dialogue that follows a whole-of-government and whole-of-society approaches critical for addressing the multi-faceted nature of cybersecurity. Cyber capacity building actions should be also implemented in a political, legal, and institutional environment that promotes **transparency and accountability** as primary conditions for building societal trust in digital solutions and cyber-related capabilities (e.g., on the handling of data by public authorities, service providers, and system developers).

- **Human rights-based approach (HRBA):** Throughout the project lifecycle, any flow-on human rights risks from the action need to be mitigated. The HRBA is a methodology used throughout the intervention cycle to incorporate human rights principles and standards as both **a means and a goal of cooperation**. It integrates the achievement and fulfilment of human rights into the design, implementation, monitoring, and evaluation of all policies and actions. The HRBA is a tool to help practitioners understand and address power imbalances, sources of discrimination and drivers of inequalities, and on that basis undertake due diligence measures, mitigation plans, and effective human rights impact assessment across the project cycle. The HRBA approach is also key to ensuring that **'no-one is left behind'**, regardless of ethnicity, gender, age, disability, religion or beliefs, sexual orientation and gender identity, migration status or other factors. In the context of cybersecurity, the assessment needs to consider privacy and data protection, freedom of expression, freedom of association, discrimination, fair trial, and access to information. The **'dual use' nature of cyber technologies** makes it also easier for some governments to abuse digital solutions for surveillance or repression. CCB actions should be assessed against the HRBA principles to identify risks that may negatively impact the exercise of human rights and map the risks that can be mitigated, tolerated, or those that are too high to justify engagement. Overall, in assessing the human rights context it is important to look at a government's current strategies, policies, and approaches to cyber resilience, how they are being implemented, whether they are upholding their commitments to the universal principles of human rights and the rule of law, and if/what impact these strategies and policies are having on human rights.

- **'Do no harm' and 'Do more good':** These twin principles are defined to avoid unintended negative consequences and maximise positive effects across humanitarian, development and peace actions. As such, they set the standards for any EU-funded action to ensure it does not cause human rights violations, exacerbate divisions between institutions and communities, fuel conflict, or worsen existing inequalities and grievances. In the context of the rapid uptake of digital development initiatives, these principles create new due diligence requirements for EU project managers: the roll-out of technological solutions in partner countries should embed security and resilience measures by design and not increase the country's cybersecurity vulnerabilities or create technological dependencies unfavourable to the partner country.

24 Milestones include the Paris Declaration on Aid Effectiveness of 2005, the Busan Partnership for Effective Development Co-operation of 2011, and the Global Partnership for Effective Development Co-operation Nairobi Outcome Document of 2016. The Global Forum on Cyber Expertise elaborated in 2017 the Delhi Communiqué on a Global Agenda for Cyber Capacity Building that endorses these development effectiveness principles for CCB. In 2021, in the final report of the 2019-2021 UN Open-ended working group on developments in the field of ICT in the context of international security a set of principles are defined to guide 'capacity-building in relation to State use of ICTs in the context of international security'.

TOOL 1: V-I-P FLOWCHART

VALUES	INTERESTS	PRINCIPLES
Human rights and the rule of law	Resillent and diversified supply chains	Effective development cooperation
Nature of acsess to the Internet	Sustainable, secure, trustworthy technology & internet infrastructure	Human right-based approach
Rules-based international order	Open and human-centric digital economy and trade	Do no harm, do more good

ASSESSMENT

Are the partner's (~~i.e.~~ country or region) policies, laws, and positions **compatible with these values?** Is there an **opportunity for the EU to influence** the partner's views and positions **to align more** with these values through a CCB engagement?	Are the partner's interests and overall direction **compatible with the EU interests?** Is the **an opportunity for the EU to promote its interests** with the partner through a CCB engagement?	Is the partner committed to engaging with the EU based on the principles of **effective development cooperation?** What are existing or potential **risks and unintended consequences** from the engagement and are they manageable/ mitigatable?

IF THE ASSESSMENT IS

Overall Positive	Overall Mixed	Overall Negative
Positive assessment of the policy alignement of the country's public policy with the EU values, interests, principles, and / or the policy credibility of the partner's good track record in cooperation and policy reforms, with **low or moderate risks** that can be managed/mitigated.	Mixed assessment of the partner's alignment or potential alignment with the EU's values, interests, principles. There are both weaknesses and opportunities in engaging (the most common scenario) with **moderate or substantial risks** that can be managed/mitigated.	The assessment points to weak or even conflicting existing policy alignement with the EU, and/or weak credible cooperation, with **high risk levels** (political, econimic, and reputational) that are unlikely to be managed/ mitigated and outweigh the benefits of a possible engagement.

THEN

The engagement could proceed following regluar procedures, including an analysis of the risks and assumptions linked to the overall objective(s) of the action at the next stage.	The engagement should be concidered if there is potential for the EU to have a credible policy influence by engaging with the partner counrty/region in this field, accompanied by a clear strategy fore responding to risks at all stages for responding to risks at all stages of the project cycle.	The engagement should be concidered only if there is a strong political motivation by the EU's institutional leadership despite the political, economic, and reputational risks. The key mitigating measure is to frame the engagement's scope and approach mainly at the trategic and legislative level (instead of operational capacities), with a clear risk response strategy at the core.

Key Question: What is the cost of not engaging?

Even if the national/regional context reises concerns over their human rights or rule of law record, the decision about non-engaging should engagement. This is particularly relevant in the case of a strong presence cases, there could still be room for a fexible, policy-first, value-driven engagement to promote EU norms and standards with strong monitoring mechanisms and a well rounded risk response strategy

2. Programming exercise

Objective: Define the strategic engagement areas of the EU's development cooperation and international partnerships with partner countries or regions in alignment with their priorities and interests. Identify entry points in the programming for engaging on cyber-related issues and sectors.

During the programming stage, we assess whether and how cyber capacity building should be considered for EU engagement in a specific country or region. This initial assessment considers whether it is strategically beneficial for the EU to engage in this field and whether there is strong interest and ownership from the partner government or regional organisation. Agreement for cooperation achieved during programming creates the **framework to consider cyber capacity building actions** at the next stage of the PCM.

Cyber-related cooperation has not been widely referenced in programming documents (Multi-Annual Indicative Programmes) of bilateral geographic envelopes until the 2021-2027 Multi-annual Financial Framework. It has been often mentioned or covered under good governance, public sector reform, criminal justice reform and digital transformation, while it was more commonly spelt out as a priority under regional programming. A shift in this approach can be seen due to the increased financing for digitalisation, while the programming document of the NDICI Thematic Programme on Peace, Stability and Conflict Prevention (2021-2027) sets distinct priorities for cybercrime and cybersecurity, based on the experience of previous instruments designed to address global and trans-regional threats.

2.1 Strategic context analysis

Programming documents under geographic envelopes typically identify broad priority areas of cooperation, such as good governance, public sector reform, justice and security sector reform, digital transformation, and hybrid threats. Within these areas, cyber capacity building may be included as a component or treated as a stand-alone priority, depending on the country/regional context and the EU's interests.

During programming, a **preliminary analysis of the political, financial, security, and digitalisation outlook** in the country or region will be conducted as a first step to identify opportunities for EU support. This involves reviewing recent political developments, assessing the possibility of pursuing a coherent and effective approach to cyber capacity building in the given context, and identifying any country or sector-level risks that could hinder the success of the potential action, the development of capacities, as well as the sustainability of the results. These risks may be related to the political climate, macroeconomic outlook, socio-economic situation, or governance structures.

2.2. Engagement through bilateral, regional, or global actions

The strategic programming documents (i.e., MIP and RIP) may not always provide details on cyber-related action priorities. In previous MFFs, **regional programmes were more frequently used** due to the availability of funds for cybercrime (e.g., Cybercrime@IPA, Cybercrime@EAP I, II, III, CyberEast, CyberSouth, etc.) and cybersecurity (e.g., OCWAR-C).

To be effective, regional programmes **require a similar level of maturity** in countries across the targeted region. For cyber issues, this has been difficult to pursue in most regions due to different levels of cyber capabilities. As a result, programmes often lose their regional orientation and shift their focus towards nationally-focused capacity building activities aimed at developing national cybersecurity strategies or cybercrime legislation instead of strengthening regional capabilities. This approach is suboptimal also from the national capacity building perspective as the regional actions usually lack the necessary resources (people, funding, time) to engage at depth with a partner country, especially with fly-in fly-out experts.

The general challenges of the **EU's internal coordination** on the development and implementation of regional or bilateral actions apply also to cyber capacity building. Under regional envelopes, the programming, design and management of actions are carried out either by headquarters or by multilateral/regional EU Delegations. Bilateral programming is aligned with national development strategies and includes actions that are designed and managed by EU Delegations in consultation with or upon initiative of the partner country. Because the decision-making cycles for regional and bilateral programmes are not aligned, the Commission's internal consultation and quality support process are critical.

Assessing the level of the cyber maturity of an individual country and its neighbours is an important first step in deciding between a bilateral or a regional CCB action (see Tool 2).

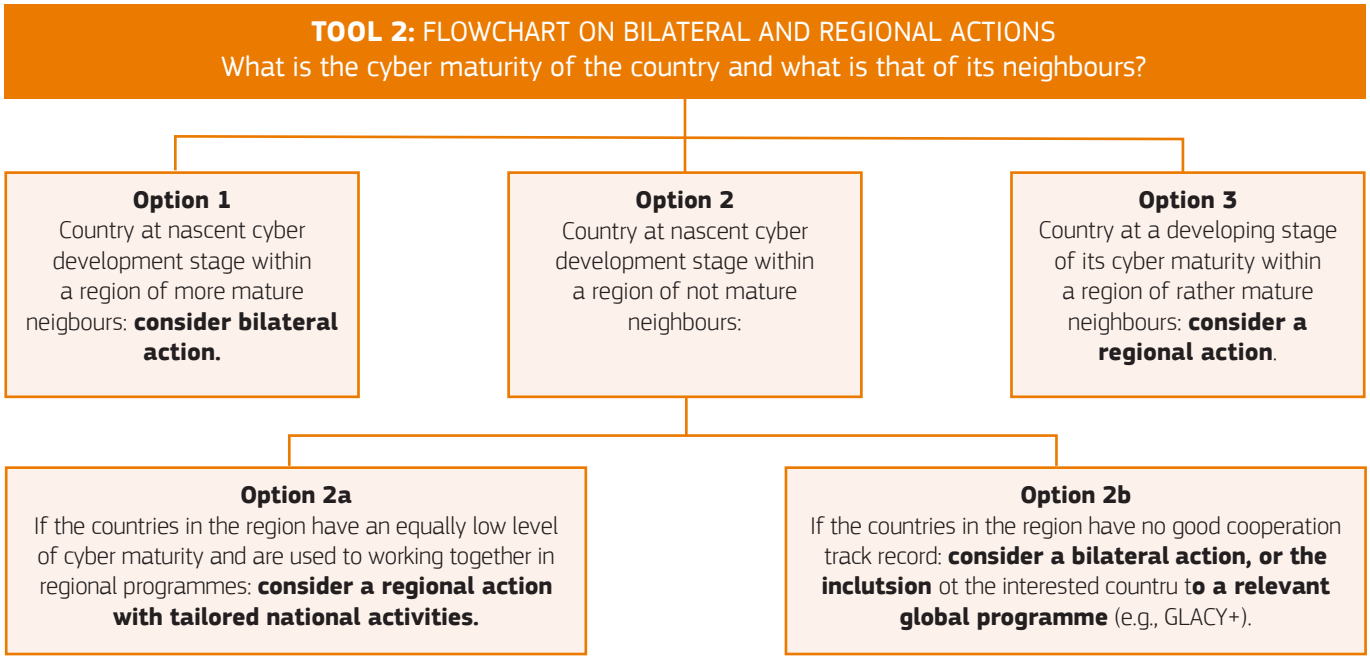
1. If the country is at **a nascent stage** in its cyber development **within a region of more mature neighbours**, a bilateral programme may be more adequate. This can be a stand-alone action or a component of a larger relevant action (e.g., on organised crime covering cybercrime; or on digitalisation covering cyber resilience). The bilateral engagement can concurrently support the national progress and a country's ability to engage more meaningfully in regional programmes.
2. If the country is at **a nascent stage** in its cyber development **within a region of not mature neighbours**, a more thorough assessment of the opportunity/cost paradigm allows for identification of additional options:
    a. If the countries in the region have an equally low level of cyber maturity and they are used to working together in regional programmes, a regional programme with tailored national activities should allow them all to work within a regionally driven cyber or digital development roadmaps. This option has lower transaction costs compared to multiple bilateral actions and embeds the regional cooperation dimension.
    b. If the countries in the region don't have a track record of cooperation, it is best to consider either a bilateral programme if the envelope exists, or the inclusion of the interested countries in any relevant global programme (e.g., GLACY+).
3. If the country is **at a developing stage** of cyber maturity **within a region of more or less mature neighbours**, a regional programme with the possibility of tailoring some bilateral activities to address some of its capacity gaps may be sufficient and more cost-effective.

Some of the lessons from the past projects are relevant for both regional and bilateral actions. Developing a national cybersecurity strategy in isolation from regional initiatives might be a missed opportunity to leverage regional or sub-regional expertise. Independently of the national or regional cyber capabilities, **regional or global actions can be used as entry points for cyber engagement** with national authorities when the EU has a clear interest to do so but a partner country does not consider cyber a priority.

Finally, it is essential to consider the added value of **global actions** managed by the headquarters:

- Actions with a cyber capacity building objective that can operate in any geographical context, fostering trans-regional cooperation dynamics and undertaking country-specific activities in priority countries (e.g., GLACY+, Cyber4Dev).
- Actions with a policy dialogue objective designed to facilitate cyber policy debates at national, regional and global levels to promote EU positions, standards, and policies, and also offer support to partners to engage in international cyber fora without undertaking in-depth capacity building activities (e.g., ESIWA).

The first case can create tension with bilateral and regional actions if there is no prior, meaningful consultation between HQ and EUDs on the identification of priority countries or a conscious effort to deconflict activities undertaken by different projects. Generally, global actions are a great resource. They can serve as **'facility' projects** that provide expertise in a flexible way when bilateral financing is unavailable. Additionally, they foster networking and triangular cooperation opportunities. The key issue for global actions is to ensure timely consultation with EU Delegations in selecting priority countries and in the implementation of activities on the ground. This ensures coherence and synergies with the bilateral dialogue and programmes they manage.



2.3. Political and policy dialogue

Dialogue with national and regional counterparts can be divided into two parts: the political and sectoral levels. To maximise impact, the links between the two need to be strong. Stakeholders participating in political dialogue meetings should be guided by sectoral-level inputs, and in turn, they must relay the outcomes of the political dialogue to policy officers and practitioners. This approach is vital to gaining government support and fostering cooperation in digitalisation, governance, justice, and security sectors that are priorities of EU international cooperation and partnerships. The political and policy dialogues create an enabling environment for a possible agreement to cooperate on cyber issues, including a possible future CCB action during the next PCM.

2.3.1. Political dialogue

Regular and in-depth dialogue between EU institutions, Member States, and political leaders in partner countries and regions is the starting point of engagement to explore issues of mutual importance. Political dialogue helps build shared understandings and **identify entry points** for financial and technical assistance to foster **government buy-in** for any intervention. Political dialogue also fosters the partner country's accountability outside the scope of financial assistance. Most often political dialogue covers multiple areas of cooperation and aims to reach a common understanding of the issues at stake from the outset. At this stage, political dialogue with national authorities should focus on the political, economic, social, and cultural **factors necessary for cyber cooperation**. The political dialogue will **inform the strategic choice** of whether to engage in cyber capacity building as it provides a preliminary understanding of the cyber threat landscape as perceived by the government or regional partners, as well as an indication of their current interest and ability to address challenges arising from cyber risks.

2.3.2. Sector policy dialogue

Sector policy dialogue can investigate more specific aspects of the cybersecurity ambition of the country or region and explore concrete options for how the EU support could support its relevant priorities and/or action plans. A meaningful sector policy dialogue on cyber issues should be built on:

- A **whole-of-government approach**, bringing together government services and ministries. From the donor perspective, the experience shows that even in cases where one ministry or department is in the policy lead, the interconnectivity and linkages between cyber issues require broad support.
- A **whole-of-society approach**, engaging the private sector, civil society, academia, and research community in addition to the government. A whole-of-society dialogue led by the government strengthens its accountability

and brings insightful input into policy priorities, their relevance and credibility. It creates the foundation for support of the multi-stakeholder community in the implementation of cyber-related policy processes (e.g., national cybersecurity strategy, cybercrime legislation, cyber crisis prevention and management processes, cyber workforce and education initiatives). The EU should promote this approach and explain to partner governments the value added of such in dialogue at national and sectoral levels.

- A solid **national/regional and sector understanding** as a basis for efficient and credible dialogue built on the whole-of-government and whole-of-society approaches[25]. This should be aligned with **any existing country/sector coordination structure on digital, ICT and/or cyber issues** to reduce transaction costs and add weight to the dialogue. In case the country has a national cybersecurity strategy, a country-led (sector) policy dialogue and coordination is preferred, based on the priorities of the strategic framework.

- A **government-led, or regional organisation-led donor coordination dialogue on cyber issues** is another avenue for policy dialogue on cyber capacity building that could foster synergies and division of labour, pooling resources, and sharing of good practices among donors, development partners and the national or regional stakeholders.

Dialogue on both the political and sectoral levels must be **coherent, continuous and meaningful** to build political will and sectoral ownership of EU-financed initiatives. It cannot take place on a one-time basis but must be maintained, re-invigorated, and exercised through implementation and oversight mechanisms to keep initiatives on track and achieve meaningful results.[26]

BOX 9: PRACTICAL TIPS FOR PROGRAMMING

- ✓ Find out **what other donors are doing**. Even when not possible (or at times not advisable) to coordinate or cooperate at the programming stage, you could task implementers to coordinate at the working level. Check which donors have **cyber or digital attachés** with whom you could have informal or regular exchanges.

- ✓ In the policy dialogue with the government explore a possibility of holding a **government-chaired roundtable on cyber capacity building** with all donors to facilitate identification of potential priorities for each and coordination. It could be part of a broader thematic donor coordination effort (e.g., digitalisation).

3. Identifying gaps, needs and risks (design phase 1)

Objective: To understand the multi-level complexities of the national or regional digital and cyber ecosystem, identify the cyber capacity gaps and needs against the partners' existing capacities and define priority areas in alignment with the partners' development aims and plans.

A thorough, **evidence-based analysis** of the national or regional context and policy environment is the starting point of the design phase which is framed within the parameters of the partner's development plans and priorities as well as the EU's policy objectives set in the programming document priorities. Mapping and understanding the relevant **policies, institutions, and stakeholders** should guide the analysis to zoom in on priority areas and problems to be addressed through the intervention and lead to assessing different strategy options.

3.1. Context analysis

The context analysis for CCB should consider the cyber threat landscape, political and economic aspects relevant to cybersecurity (e.g., online surveillance, political commitments for the cybersecurity of national critical infrastructure) and assess its significance for EU interests.

25 Adapted from the Budget Support Guidelines, Annex 13, European Commission (2017).
26 Support to Justice and the Rule of Law, Tools and Methods Series Reference Document No. 15, European Commission (2012).

A starting point for the context analysis is to assess the **cyber threat landscape** in a partner country or region and its capability to handle these threats. Even if a country faces low cyber threats, intervention may be warranted if it poses cyber threats to the EU (e.g., cybercrime groups launching attacks from within the country). At this stage, we also evaluate broader political, economic, and social factors in the region that could impact the effectiveness of the EU's cyber engagement. These general elements, for instance, on political governance, macroeconomic outlook, public financial management, corruption, natural resource depletion, climate risks, etc., serve as the foundation for moving on to undertake a thorough **policy analysis** on the country's/region's state-of-play on cyber-related issues and determine what would be the most effective way of providing support to a partner country/region.

It is essential to ensure that cyber-related elements in development programmes align with the **overall national development plans and strategies** to ensure credibility, relevance, and sustainability. For example, improving law enforcement's competence in handling electronic evidence and addressing cybercrime may contribute to a country's online growth, but it should be integrated into broader developmental plans for good governance, the rule of law, and economic development.

TOOL 3: KEY QUESTIONS TO GUIDE CONTEXT ANALYSIS FOR CCB		
Vision & policies	**What are the main risks and threats in cyberspace that can affect the country's development?**	Understand to what extent **the level of digitalisation in a country creates vulnerabilities for the state and society.** This may include the analysis of the main cyber threats (e.g., DDoS, ransomware), type of threat actors (e.g., states, criminal groups), their motivations (e.g., political, financial, espionage), the key sectors impacted by cyber-attacks (e.g., banking, healthcare, research), or potential dependencies of the country/sector on external providers and suppliers of both software and hardware. Such information should be provided by government agencies but in reality it often comes from the private threat intelligence companies (e.g., Digital Defense Report by Microsoft, Cost of a Data Breach Report by IBM, the Data Breach Investigations Report by Verizon)
	Does the country's overall strategy adequately reflect the CCB needs?	**Understand the overall place of cyber- and digital-related issues in the country's national strategies for growth, development or security**. Cyber policies need to be driven by specific developmental, security and/or political objectives of the partner country. While some countries view developments in cyberspace as a catalyst towards economic and human development, others might place more focus on the security dimension. **Assess how relevant is the specific approach for addressing a given policy challenge**. That implies clarifying whether the policy is risk-informed, what concrete challenges it addresses, and **how compatible it is with relevant EU policies**.
Laws & regulations	**What is the existing legal framework and how relevant is it for addressing key cyber-related challenges?**	Analyse a broader regulatory framework for the digital domain and cyberspace to establish whether and **how policy goals are translated into legally binding rules that create concrete rights and obligations**. Regulation of cyberspace to fight cybercrime or to strengthen resilience has taken many new dimensions over the years and it is important to assess whether they are internally coherent, provide sufficient safeguards, and respect the rule of law.
	Does the existing policy framework guarantee compliance with international human rights / the rule of law commitments?	Assess cyber and digital policies for **compliance with international human rights commitments, the principles of the rule of law and good governance**. Laws and regulations should be assessed for their compatibility with the key commitments made at the international level, including at the UN, even if such commitments are of a voluntary and non-binding nature. Any doubts about the country's commitment to values promoted by the EU should be spelt out and the risks associated with a project in such an environment properly assessed.

Institutions & resources	**Are flagship national cybersecurity initiatives earmarked in the national budget?**	Verify if cybersecurity policy is implemented and supported with **adequate human resources and a credible budget** (e.g., the staffing levels and budgets that adequately reflect the tasks foreseen for the national CERT, a budget for the national cybersecurity agency). Policy assessment should investigate budgets and other documents that might indicate the government's commitment. Past experiences and lessons help to assess the effectiveness of policy implementation.
	What are the existing institutional capacities?	**Establish whether responsibilities for cyber-related policies are clearly defined**. Institutional capacity is needed to ensure the cyber policy formulation process, coherence, monitoring and evaluation, modes of cooperation between donors and the government and open/close processes for stakeholder engagement.
Partnerships & cooperation	**Is there a robust ecosystem to support CCB actions?**	Identify the **structural and institutional factors that shape present levels of cyber capacities and provide drivers as well as constraints to change**. The willingness or commitment of the partner government or region to engage meaningfully with the **private sector and civil society** should be clearly understood given their critical role in cyber resilience.
	Do sector coordination mechanisms exist?	Assess whether coordination mechanisms exist (e.g., for cyber crisis management or law enforcement) and whether they are used. Describer the government's approach to working with the CSOs and public-private partnerships. These mechanisms are critical for implementation of the **whole-of-government and whole-of-society approaches**. Adequate coordination mechanisms guarantee that the general cyber policy orientation adopted by a country is based on a broader consensus, with correspondingly higher chances of successful implementation.

3.2. Stakeholder analysis

Mapping of stakeholders who shape developments in cyber-related sectors, are affected, or might be affecting the change process is a key component for ensuring that the commitment to the **whole-of-society and whole-of-government approaches is implemented in practice**. The multi-stakeholder approach is widely accepted as the optimal way to make policy decisions for a globally distributed network.

Figure 11. Key stakeholder groups

Govermental actors & policy community

- Ministries of ICT/ Digitalisation, Interior/ Security, Foreign Affairs, Defence, Economic Development, Justice, ...
- Goverment agencies and bodies: prosecutors, law enforcements agencies, national cybersecurity agencies, intelligence service, ...
- Regional organisations: EU, ASEAN, ARF, APEC, SCO, AUC, OAS, ...
- UN: UNGA and SC, ITU, UNODC, UNIDIR

Development actors & financial institutions

- Development agencies and implementing bodies,: JICA, KOICA.
- Multilateral Development Banks: World Bank, Inter-American Development Bank, Asian Infrastructure Investment Bank, Asian Development Bank, African Development Bank, European Bank for Reconstruction and Development

Non-state actors

- Private sector: tech companies, ISPs, financial sector, industry
- Universities and research institutes
- Civil society organisations (privacy, access, right-centric focus)

Technical Community

- ITU
- Regulators and standardisation bodies: ISO, ETSI, W3C, IETF, IEEE
- CERTs (national, government, industry), and CERT networks: FIRST, APCERT, AfricaCert
- Critical infrastructure operators
- Regional Internet Registries

A properly conducted stakeholder analysis allows for a more accurate identification of the problem and how a specific action fits within national priorities, supports the identification of change agents, and potential resources and solutions already existing within the country. Below are a few **lessons learnt** to make this process efficient and successful:

1. **Avoid an overly complex analysis:** It might be more useful to limit the stakeholder analysis to a specific sector or policy objective rather than attempt to analyse the whole ecosystem of institutional arrangements, competencies, and roles. Consider ownership in this process and the capacity and legitimacy of the stakeholders to support the objectives of the action.
2. **Manage expectations from the very early stages:** Communicate the precise objectives and anticipated results of the projects and monitor changes in the attitudes of specific actors.
3. **Understand the existing power relations:** Capacity building is very likely to result in shifting power relations among stakeholders. To avoid undesired consequences resulting from situations of unbalanced power relations, it is important to understand the existing capacities of different stakeholder groups and how the intended action will affect them. Actors who are expected to benefit from the action may become **agents of change and change accelerators**, while others may be reluctant to support proposed solutions and act as **spoilers**. One of the main challenges working in a multi-stakeholder environment is identifying relevant institutions and organisations and designing adequate strategies to solicit their engagement.

TOOL 4: GUIDING QUESTIONS FOR STAKEHOLDER ANALYSIS	
Key actors	• Who are the main actors in the cyber ecosystem and what are their respective roles? • What are their main strengths and weaknesses, especially concerning the capacity to assume their mandates relevant to the cyber domain?
Multistakeholder approach	• Does the government recognise the role of the multi-stakeholder community in the governance of cyberspace? • Who are the key non-state active in the cyber domain and what are their relations with the government? • Does the private sector or civil society participate in the design, implementation and monitoring of cyber-related policies through consultations or other mechanisms? • What is the ownership structure of critical infrastructure: state, private or other form of arrangements? How are the operators of critical infrastructure involved?
Power structures	• What are the power structures within the cyber-related policy-making process? • Which agency or government body is primarily responsible for cyber-related policies? • How would changing the capacities of different stakeholders affect their positions within the power structure in the cyber ecosystem?
Coordination	• What are the coordination mechanisms in place for national stakeholders? • Are cross-sectorial consultations with other actors part of the process? • Are the whole-of-government and whole-of-society approaches implemented? • How are conflicts within the policy circles addressed?

3.3. Gaps and needs analysis

Part of the capacity assessment is identifying the capacity gap – the difference between existing capacities and those desired levels of capacities to achieve the identified objectives. Ideally, the capacity and needs assessment should be driven by the government or other domestic stakeholders. In cases where such assessments are unavailable, 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 the private sector may also provide valuable information. Since capacities and gaps in capacities change over time, their assessment cannot be a one-off exercise but needs to be a continuous process.

TOOL 5: CYBER CAPACITY GAPS AND NEEDS ASSESSMENT FOR CCB			
		If yes …	**If not …**
Vision & policies	Is there a comprehensive national cybersecurity strategy? Is there a legal/policy framework to deal with cybercrime and ensure the security of critical national infrastructure?	• Check if the strategy or legislation is implemented and focus on strengthening effective its effective implementation. • Check if the strategy or legislation still corresponds to the country's specific needs and consider suggesting an update or revision.	• Encourage and support the government in developing a national cybersecurity framework.
	Do the adopted strategies and policies contribute to the development of the culture of cyber resilience by creating incentives, motivation, etc.?	• Check if there are being properly implemented and provided with sufficient resources. • Check if there are policies and mechanisms in place to strengthen cyber competencies amongst the general population (e.g., availability of education and training programmes).	• Identify the main entry points or hooks for initiating discussion about the importance of cyber resilience in the national context, e.g., regarding cyber resilience of critical infrastructure or bridging the skills gap.
Laws & regulation	Is there existing legislation to protect, prevent, respond, and pursue the individuals and entities responsible for cyber-attacks on companies, institutions and individuals?	• Check if responsibilities for the implementation are clearly prescribed if the laws are implemented, and if institutions have sufficient resources. • Check if individuals responsible for the implementation have the skills required to put laws into practice, e.g., law enforcement agents, prosecutors, and judges.	• Encourage and support the government in developing adequate cybersecurity laws and regulations in specific pillars (e.g., cybercrime, cyber crisis management).
	Does the general organisation of the country provide guarantees for the rule of law and good governance needed to implement laws or regulatory frameworks in cyberspace?	• Check if the existing checks and balances and accountability mechanisms are adequate, especially regarding law enforcement and intelligence agencies.	• Focus on strengthening the overall enabling environment and include cyber-specific components, if needed.

Institutions & resources	Is there a national entity in charge of preventing, detecting, and responding to cyberattacks and/or a body responsible for the implementation of a national cybersecurity strategy?	• Check if the overall cybersecurity ecosystem is robust enough and supports better inter-institutional cooperation and information exchange. • Verify if there is a framework for certification of internationally recognised cybersecurity standards in the public sector or among critical infrastructure operators.	• Support the establishment of a national cybersecurity centre or another government agency with clear responsibilities and resources for cyber resilience. • Support the creation and proper functioning of national or sectoral CSIRTs.
	Are the roles of organisations and institutions in the field of cyber resilience clearly prescribed? Are they adequately resourced?	• If the institutional setting is adequate and properly resources, consider strengthening coordination and information exchange mechanisms across different cyber policy areas.	• Support the development of a broad cyber resilience ecosystem with clearly prescribed responsibilities and resources.
Partnerships & cooperation	Do the existing policy-making mechanisms follow the whole-of-government and whole-of-society approach?	• Assess the effectiveness of the existing mechanisms and their contribution to the policymaking process. • Verify if all stakeholders have similar capacities or whether some of them require strengthening (e.g., CSOs).	• Support developing or strengthening mechanisms for coordination between government agencies (e.g., joint task forces), public-private partnerships, or engagement with civil society.
	Does the country actively participate in and contribute to international debates on cyber issues, including at the UN?	• Assess whether country policies are aligned with the EU positions (e.g., on cybercrime, international law, norms of state behaviour) and promote their convergence.	• Assist with strengthening institutional and human capacities to strengthen international cooperation.

3.4. Risk identification

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. The European Commission defines risk management as 'a continuous, proactive and systematic process of identifying, assessing and managing risks in line with the accepted risk levels [...] to provide reasonable assurance as regards the achievement of the objectives'. Country and sector-level risks (e.g., 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.

The **Values-Interests-Principles approach** highlights the issues that EU operational managers and implementing partners need to consider from a cyber-perspective across the project cycle. Using the classification of risks defined in the Risk Management Framework of the Budget Support Guidelines, this Operational Guidance systematises them against the V-I-P and provides examples that are relevant for cyber-related risk assessment at each stage of the intervention cycle, starting with identification. All of these risk categories can create **reputational risks** for the EU if they are not appropriately mitigated or managed.

Aside from identifying the risks we also need to assess holistically at this stage (and continuously during the intervention cycle) both the **likelihood and the impact of each risk (low, moderate, substantial, high)** against the overall objectives of action.

TOOL 6: RISK STRATEGY - IDENTIFICATION	
RISKS RELATING TO	**KEY RISKS**
Values *Human rights and the rule of law* *Nature of and access to the Internet* *Rules-based international order*	Risks relating to the values dimension are **mainly political**. Overall, a key risk to identify is any backsliding of the rule of law and democratic standards. 1. Assess the partner's commitment and adherence to the fundamental values of human rights, democracy, the rule of law, as well as any risk of conflict and insecurity, including political and social destabilisation and regional tensions. 2. Assess whether the partner is committed to the multi-stakeholder approach to internet governance or is shifting towards the state-centric model, as well as assessing its track record on digital rights, from and online censorship and internet shutdowns, to the use of technology for unlawful surveillance of civilians, or the adoption of cybersecurity policies without human rights considerations.
Interests *Resilient and diversified supply chains* *Sustainable, secure, trustworthy infrastructure and technology* *Open and human-centric digital economy and trade*	Risks relating to the interests dimension are **mainly economic** and range from the partner's digital economy vision, its public finance management, as well as its economic security. 3. Assess the partner's commitment to a functioning market economy, notably in the digital realm, and identify any protectionist trends in its policy orientation, for example barriers to cross-border data flows. 4. Identify any risks in the government's overall financial regulatory framework, compliance and controls systems that could weaken its integration in the global economy and could jeopardise the effectiveness of the EU support. 5. Identify key economic security risks that the partner could face from external actors, most notably in relation to strategic dependencies in its supply chains, digital infrastructure and services, and technological products. These are all intrinsically connected to cybersecurity as it is the common thread that supports secure and trustworthy digital trade, infrastructure, and technologies.
Principles *Effective development and international cooperation* *Human rights-based approach* *'Do no harm' and 'Do more good'*	The principles dimension is primarily connected to **developmental risks** that can undermine the effectiveness of the intervention. A weak commitment to improving cyber resilience and not clearly demonstrated ownership of the process towards the relevant developmental goals is a risk. 6. Assess any risks in the partner's approach for the sustainability of the intervention and its results, as well as in its openness to engage in a whole-of-government and whole-of-society inclusive dialogue. Corruption and fraud can divert national resources for private gain and risks should also be assessed against the standards used for digital security products and solutions in public procurement. 7. Assess operational and resource-related risks to the intervention, such as competing claims of national stakeholders that could hamper effectiveness, failure of the partner to secure co-financing, or lack of the necessary staff to take the action forward. Applying the human-rights based approach and the 'do no harm' principle, assess any risks that the action further exacerbates or creates inequalities in relation to the digital divide and their access to cybersecurity resources (services, training, etc). 8. Assess if there is a plan and an enabling environment for ensuring the sustainability of the action, both on the human and technical side. Notably, how to address the action's potential contribution to brain drain if staff trained by the action look for work opportunities abroad especially as cybersecurity professionals are in high demand; as well as how to ensure that the action does not increase the digital security risks if the authorities are not able to sustain cybersecurity measures after the action (e.g., finance the cybersecurity software licences procured as part of the action).

3.5. Lessons learnt and mapping of CCB actions

The design of a new intervention should build on lessons, positive and negative, reflecting on previous experience in similar interventions and in relation to the sector and its adjacent sectors. General guiding questions in this reflective process are:

- what has and has not worked in the past?
- which were the enabling and limiting factors?
- how are these lessons considered in the current action?

For each policy pillar of cyber capacity building, this Operational Guidance listed **specific lessons in the previous chapter** (III. 2. Policy pillars for cyber capacity building). In addition:

- **Engage with other donors and development partners working on CCB**. It would be optimal to do so through **systematic participation in any sector policy dialogue and coordination on cyber or digital issues** that exists at a national level, or within a region convened by the mandated regional organisation. In practice, if the government does not have a strong reign or interest in cyber issues, bringing all the donors and implementers to the table might pose a challenge. In such cases, capturing macro-lessons or achieving complementarity between different cyber actions and projects is difficult.
- Use the existing cyber capacity building **mapping efforts** to deconflict, create synergies, and identify lessons. The **Global Forum on Cyber Expertise** is a global coordination platform on CCB that operates the Cybil portal as its repository of CCB initiatives, best practices, tools and resources. At the EU level, the **EU CyberNet** project is tasked with regular mapping of EU and EU Member State-funded CCB actions. It also provides short-term expertise to support EU Delegations in CCB actions.

BOX 10: UTILISING EU CYBERNET – EXPERTS POOL & PROJECT MAPPING

The EU's External Cyber Capacity Building Network is an EU-funded project with the aim to strengthen the global delivery, coordination and coherence of the EU external cyber capacity building actions. EU CyberNet has the following main functions:

- **An EU-wide Expert Pool** of cybersecurity experts covering a range of themes that can be mobilised for short term, targeted engagements to support EU institutions and services with technical assistance, including for the design and delivery of external cyber capacity building actions and activities. Member States stakeholders may also draw expertise from the Pool.
- **A Stakeholder Community** that brings together EU institutions and services, EU Member States national authorities, as well as an array of implementing partners from cybersecurity organisations, think tanks and academic institutions that are engaging in external cyber capacity building, to share their lessons learnt, updates on the implementation of their projects or research and strengthen their cooperation network.

The Stakeholder Community enables EU CyberNet to serve both as a **Coordination Hub** for the EU's external cyber capacity building engagement by bringing together the on-going CCB actions from the EU and EU Member States and improving awareness of the different actions (e.g., mapping exercise), and as a **Knowledge Hub** through the development of knowledge products and seminars (e.g., the EU CyberNet Club) for the stakeholders. EU CyberNet services and expert pool is available to EU institutions on FPI's prior coordination. The modalities of the deployment of experts will be agreed on a case-by-case basis. To inquire about the expertise, please contact FPI.1 or eucybernet@ria.ee

- **Engage in the multistakeholder policy dialogue from the outset** to help break cyber silos and mitigate the risks that the planned action is informed by lessons that are too narrow and do not reflect the views of the whole community. Considering that often the **cyber community is siloed within smaller thematic bubbles**, e.g., law enforcement, national security, intelligence, ICT and digitalisation, diplomacy, **as well as in functional ones**, e.g., technical experts, industry, academia, civil society, it can be particularly difficult to capture lessons in a holistic way that bring the different perspectives forward.
- If there is little to no previous engagement with the partner or cyber capacity building, it would be useful to **investigate adjacent sectors** such as good governance and the rule of law, security and justice sector reform, and digitalisation.

BOX 11: PRACTICAL TIPS FOR IDENTIFICATION

- ✓ **Get to conceptual clarity early on** through problem/context analysis and policy dialogue with the country. Use the 'cake' framework to untangle the issues and have a holistic understanding of the ecosystem.
- ✓ Consider whether certain elements / parts of the 'cake' would be better suited to be addressed under other, existing EU actions instead of the potential new action, to allow for a **clear scope definition and avoid overlaps later**.
- ✓ Reflect on the national multi-dimensional, multi-layer, multi-actor **cyber dynamics** also within the context of global cyber politics and EU cyber policy objectives.
- ✓ Strive for clarity in **stakeholders' mapping and capabilities identification,** e.g., whole-of-the-criminal-justice-chain understanding and approach for cybercrime and whole-of-government/whole-of-society approach for cyber resilience broadly. Identify the **'cyber brokers' or 'cyber champions'** in the national ecosystem to engage them throughout the project cycle.
- ✓ Check the **UNIDIR Cyber Policy Portal** that provides an **overview of cyber policies and partnerships** by national governments and regional organisations for a quick insight on the national/regional policy and regulatory state of play. For additional information on the national digital regulatory context, the joint ITU-World Bank **Digital Regulation Platform** provides an overview on the different elements of ICT regulation in light of the digital transformation (regulatory governance and independence; competition; access; data protection and trust; spectrum management; emerging technologies, etc.) and is accompanied by country metrics in the **ICT Regulatory Tracker**. Council of Europe provides a very useful Country wiki page with the latest updates on cybercrime legislation and state of play across the world.
- ✓ Check the **EU CyberNet Projects Mapping and the GFCE Cybil Knowledge Portal** for to see what other CCB actions were/are active in your country/region and if they have captured lessons learnt.

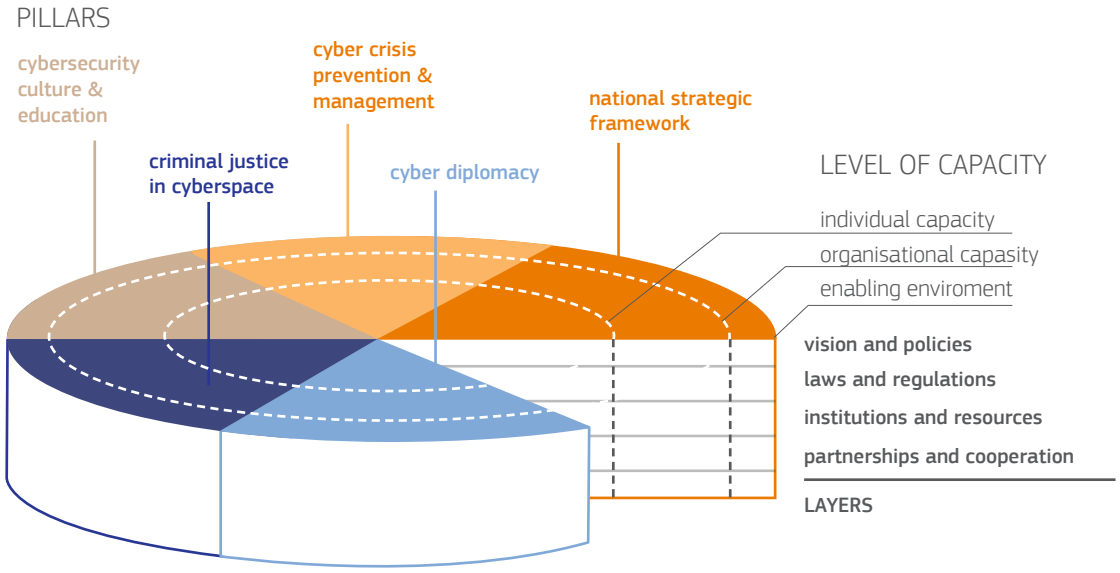
4. Formulating an action (design phase 2)

4.1. Intervention logic

The logic of intervention is a detailed and structured narrative that explains what changes the action wants to help bring about in a given context, how the associated change processes might happen and why.[27] On cyber capacity building, the 'cake model' offers clear guidance on how to consider, prioritise or combine the different CCB options per pillar and layer. A clear scope for the problem/challenge to be address is the starting point. Building on the theory of change (i.e. why and how change might happen) from the identification phase, with the intervention logic we move to the Theory of Action (i.e. what steps need to be taken to achieve the results).

27 Definitions provided in this section originate from DG INTPA's Results and Indicators for Development: Methodological Guidance (2022), the ROM Handbook 2020 (v.6.2), and the Glossary of Key Terms in Evaluation and Results Based Management (2nd edition), DAC Network on Development Evaluation (2022), OECD.

Figure 12: Policy pillars, layers, and levels in the external cyber capacity building



4.1.1 Logical Framework Approach

The Logical Framework Approach is used by the EU as a systematic process to build the intervention logic, making it explicit and using analytical and planning tools (such as context, public policy, stakeholder, and problem and risk analyses) that improve its design and allow for its relevant, feasible and effective outcome-focused management. Combining analytical and planning tools, the **Logical Framework Matrix (logframe)** summarises three interdependent pillars:

1. A results chain: It describes the action's hierarchy of expected results and the logical relationship among invested resources, implemented activities, and the expected changes or results (outputs, outcomes and impact). The starting point for the formulation of the results chain is the problem analysis.

    - ***Impact or overall objective*** captures the intermediate to long-term desired change the action is expected to contribute to within the political, social, economic and/or environmental context, also in relation to the SDGs. It is a detectable improvement in the lives of people and can be only indirectly influenced by the intervention. For example: *citizens of the partner country enjoy an open, free, secure, resilient and peaceful cyberspace.*
    - ***Outcomes or specific objectives*** capture the medium-term changes in the political, social and economic areas targeted by the action and include changes in behaviours or relations of people and institutions (including policies or practices) that take place during or after the project implementation and their achievement is under the control of 'target groups' as well as of other actors. This means that EU-funded actions are expected to realise the stated outcomes even though they are outside of their direct control. For example: *the cyber resilience of the partner country is increased; cyber crisis prevention and management structures are operational; legislation on cybercrime and electronic evidence is aligned with existing international legal standards and implemented, etc.*
    - ***Outputs*** are the results (e.g., products, capital goods, services) expected to be delivered by the EU-funded action that are under control of this intervention and will influence the achievement of the stated outcome. For example: *Capacities of decision-makers to design and implement cybersecurity policies and strategies in line with international standards and good practices are strengthened; mechanisms for effective information sharing, consultation and coordination on cyber incidents between stakeholders (government bodies, private sector, civil society) are operational; protection of critical information infrastructure is enhanced, etc.*

2. **Assumptions:** They are external factors that are necessary for the success of action. They are evidence-based operational, behavioural, and political external conditions not under the control of the action. They should reflect a focused context and risk analysis that leads to a clear decision on how to deal with the identified risks and to the design of a risk management plan.
3. **A monitoring system:** It identifies the means to measure the action's achievements. It is designed at the formulation stage to summarise the intervention logic **based on indicators, baselines, targets, and sources of verification**

TOOL 7: Results chain sample (per CCB pillar and layer)

4.1.2. Designing a monitoring system

The **logframe is used as a monitoring tool** throughout the intervention's life cycle:

- **At formulation:** to summarise the intervention logic and support financing decisions.
- **During implementation:** to monitor changes in assumptions and assess progress towards targets for indicators.
- **At closure:** to assess the extent to which the intervention contributed to its desired outcomes and impact and whether risks affected achievement of objectives.

The **key principles** for designing a monitoring system are:

- to build on local systems wherever possible (harmonise with partner systems and align with those of other development partners)
- to keep users' information needs clearly in mind (amount, level of detail and aggregation of monitoring information)
- to plan sufficient time, resources and budget for monitoring and reporting already in the Action Document and in subsequent contractual documents.

4.2. Mainstreaming horizontal issues

Both the NDICI-Global Europe (Article 8.8) and the IPA II Regulations (Article 6.2) stipulate that programmes and actions financed under them shall 'mainstream the fight against climate change, environmental protection, human rights, democracy, and gender equality in order to promote integrated actions that create co-benefits and meet multiple objectives in a coherent way'. The following checklists help integrate these considerations across the design of a CCB action. They play an important role towards empowering specific communities (e.g., civil society organisations) or demographic groups (e.g., women and youth).[29]

4.2.1. Human rights

The human rights-based approach (HRBA) is a key **methodological tool** that should guide each stage of the intervention cycle. Its working principles entail (a) applying all human rights for all, (b) ensuring meaningful and inclusive participation and access to decision-making, (c) promoting non-discrimination and equality, (d) upholding accountability and the rule of law for all, and (e) promoting transparency and access to information supported by disaggregated data. It aims to assist partner countries' state actors (duty-bearers) in implementing their international human rights obligations and to support individuals and target groups (rights-holders) in knowing, claiming, and enjoying their rights.

At the formulation stage, we need to ensure appropriate consideration of human rights is integrated in the design of the action. To do so with a cyber lens, we need to **assess the state of:** freedom of expression and association, the right to privacy, the right to access to information, **the oversight and control of data-intensive public services,** the criminal substantive and procedural law provisions for cybercrime, as well as the meaningful and inclusive participation of rights holders in cyber policy making.

To support the analysis, we should **verify (and continue monitoring)** whether the government engages in practices such as internet shutdowns, online censorship, arbitrary digital surveillance of citizens, and repression against civil society and media. Also, if in cyber-related legislation there are restrictions to human rights that fail the test of legality, necessity, proportionality; as well as whether marginalised and vulnerable groups are discriminated against in their access to digital service delivery. Another alarming practice is the weaponisation of the information environment for misinformation, disinformation, and propaganda, as well as data localisation legislation using cybersecurity and data protection as pretext towards 'digital protectionism' that aims to exploit personal data to crack down on minorities, dissidents, etc.

Finally, it is important to also consider at this stage any **unintended flow-on risks** the action could have, such as misuse of dual-use capabilities.

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

TOOL 8: HUMAN RIGHTS-BASED APPROACH QUESTIONNAIRE

Context

- What is the overall human rights record in the country and which human rights are are denied or violated?
- What are the main issues regarding human rights linked to cyber capacity building?

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

- Does the overall objective orient towards the realisation of human rights, especially for women and men living in vulnerable situations?
- 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 and 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?
- Does the intervention promote meaningful and inclusive participation of rights holders?
- Do the intervention and corresponding activities respond to the interests, needs and capacity gaps of the rights-holders (especially women and groups in vulnerable situations) and duty-bearers (including oversight institutions, human rights institutions, and gender machinery) detected during the context analysis?
- Are there indicators measuring progress towards gender equality objectives and specifically addressing disparities? Which disparities were established in the context analysis?
- Are indicators included to measure progress in applying the HRBA working principles?

Adapted from the INTPA Intervention Cycle Methodology Guide

4.2.2. Gender

Cyber capacity building actions should promote women's and girls' participation to strengthen **equal access to cyberspace** and to close the gendered digital gap.[30] Another priority is addressing the **barriers that women face in entering the cybersecurity workforce**. Gender equality assessment for cyber-related projects should adequately reflect that **cyber-violence against women and girls (cyber-VAWG)** is an emerging global problem. Victims of cyber violence are often not aware of their rights and do not know how to get help, while law enforcement authorities are often not able to assist victims of cyber violence, which may not be considered as a law enforcement priority. For this reason, Cyber-VAWG is under-reported. This 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. Beyond women and girls, a **gendered-sensitive approach to CCB** would consider any issues affecting people of all gender identities and expressions given that gender is non-binary[31] and diverse.

Therefore, it is important to **assess and continue monitoring** the gender parity in the rates of internet access,

30 Useful resources on *cyber programme design and gender mainstreaming* include: Gender equality and cybercrime / cyber violence in the Gender Mainstreaming Toolkit for Co-operation Projects by the Council of Europe; a toolkit on Integrating gender in cybercrime capacity-building by Chatham House; a Framework for developing gender-responsive cybersecurity policy by the Association for Progressive Communications and The Intersectionality and Cybersecurity Toolkit by the Centre for Feminist Foreign Policy.

31 Non-binary is used here as a broad term to refer to gender identities that do not align with the male/female binary and does not imply a monolithic third option. See United Nations Free & Equal, 'Definitions'.

the efforts to empower women in joining the cyber workforce, whether there are any gender-sensitive responses to cybercrime and mechanisms to capture gender-disaggregated cybercrime data, the rates of cyber-violence against women and girls, as well as any systemic exclusion of women and girls from cyber policy initiatives. It is important to anticipate any unintended risks that the action would contribute to by perpetuating gender inequalities and barriers to full participation.

To date, there is slow uptake of systematic adoption of a gendered-sensitive approach in the intervention cycle, but there is an emergence of actions with a gender component focusing on the empowerment, mentoring, and networking of women in cybersecurity.[32] It is important to ensure CCB actions integrate a gender-sensitive approach across the intervention cycle in line with the priorities set in the EU's Action Plan on Gender Equality and Women's Empowerment in External Action (currently in its third iteration) that include ensuring freedom from all forms of gender-based violence; strengthening economic and social rights and the empowerment of girls and women; advancing equal participation and leadership; addressing challenges and harnessing the opportunities offered by the green transition and the digital transformation

TOOL 9: GENDER-SENSITIVE APPROACH QUESTIONNAIRE

Context

- What gender equality issues exist in the country?
- How do they relate to the proposed CCB 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 how can the proposed action contribute to it?
- Are gender issues considered/reflected in national cyber policies, strategies, and regulations?
- Are key gender policy priorities integrated in government cybersecurity programmes?
- Are gendered considerations integrated in the national cybersecurity strategy, if it exists?

Intervention

- Are gender-focused groups, grassroots women's rights organisations, national women's CSOs or gender units in partner organisations consulted in the action's design?
- How does the proposed action intent to tackle gender equality issues?
- Is at least one of the specific objectives/outcomes gender sensitive?
- Are indicators disaggregated by sex? Which gender-sensitive indicators does the proposed action intend to use to monitor progress?
- Are there resources foreseen in the action (budget/experts) to ensure activities and monitoring is done in a gender sensitive way and that data generated by the proposed action is disaggregated by sex and age?

To be used in conjunction with the Resource Package on Gender Mainstreaming in EU Development Cooperation

4.2.3. Environment and climate change

The EU's commitment to the Paris Agreement, while in the European Green Deal it recalls the principles of 'do no harm, 'leave no-one behind' and policy coherence in line with the Sustainable Development Goals, therefore also in its external action all sectors must contribute to the transition to environmental sustainability and climate neutrality. Yet, environmental and climate-related issues are usually not addressed rigorously in the assessment of cyber capacity building projects. The link between the environment and cybersecurity or ICT more broadly has not been fully explored. The European Commission guidelines on 'Integrating the environment and climate change into EU international cooperation and development' are useful in integrating environmental concerns into cyber-related policies.

32 For example, the Women and International Security in Cyberspace Fellowship, and the GFCE's Women in Cyber Capacity Building Network, and the UK-Gulf Women in Cybersecurity Fellowship.

At the design stage of the intervention, we need to verify whether environmental issues are considered in national cyber policies, strategies, regulations and programmes, and assess the overall impact of cyber-related policies on the country's environmental policies. It is important to identify any environmental and climate risks that would require more detailed analyses.

The 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.) or **environmental degradation resulting from digital infrastructure** projects.

But introduction of **new technologies and their secure use** might also have positive impact on the environment as pursued to 'do more good'. For instance, the use of censors 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.).

TOOL 10: ENVIRONMENT AND CLIMATE CHANGE-SENSITIVE APPROACH QUESTIONNAIRE

Context

- What are the main environmental issues in the country?
- How do they relate to the proposed cyber capacity building action?

Policy

- Is there a national environment/climate change strategy and how can the proposed action contribute to it?
- What is the overall impact of cyber-related policies on the country's environmental policies?
- Are environment issues considered/reflected in national cyber policies, strategies, regulations, and programmes?
- What are the main issues and/or opportunities regarding environment, biodiversity and climate change linked to cyber capacity building?

Intervention

- Is the action likely to have adverse impact on the environment or climate resilience, or generate significant greenhouse gas emissions? If so, what are the chosen mitigation measures to avoid or minimise the adverse impact and its carbon footprint?
- How does the proposed action intent to tackle environmental and climate-related issues?
- Are environment-focused groups (incl. grassroots organisations, civil society) or environment units in partner organisations consulted in the action's design?
- Which environment-sensitive indicators does the proposed action intend to use to monitor progress?

To be used in conjunction with the Guidelines 'Integrating the environment and climate change into EU international cooperation'.

4.3. Risk mitigation

The next step after the identification of risks and their assessment in terms of likelihood and impact, is to identify mitigating measures as part of a risk strategy. This is the most common risk response as a degree of risk is inevitable, and there is hardly ever a scenario of only low likelihood and low impact risks at play. Acceptance of a certain degree of risk that is considered acceptable within the specific context is necessary, especially as the risk of not engaging can cause higher risks as elaborated in the **V-I-P approach** that precisely is designed to help practitioners understand the main driving and disrupting forces in the national/regional context, which in turn can be used to define the action's risk mitigation strategy. In general, mitigation should be the most common risk response, but requires close monitoring and assurances in the implementation of mitigating measures.

TOOL 11: RISK STRATEGY - MITIGATION		
RISKS RELATING TO	**KEY RISKS**	**POSSIBLE MITIGATION MEASURES**
Values *Human rights and the rule of law* *Nature of and access to the Internet* *Rules-based international order*	Backsliding of the government's commitment and adherence to rule of law, human rights, and democratic standards as reflected in the digital realm (e.g., online censorship, internet shutdowns, use of technology for unlawful surveillance of civilians and targeting of vulnerable groups). Government shift towards supporting the multilateral, state-centric approach to internet governance instead of the multi-stakeholder model.	Set a clear scope for the intervention that focuses on legislative reform with procedural human rights safeguards and checks and balances oversight. Restrict types of support with high risk for abuse or unintended consequences. For example, decline requests for social media monitoring tools, and promote of a criminal justice response to cybercrime (instead of supporting the intelligence or security apparatus). Promote policy coherence with EU approaches to cyber issues both through continued policy dialogue with the government and other stakeholders, and by designing activities in the action that fully support it.
Interests *Resilient and diversified supply chains* *Sustainable, secure, trustworthy infrastructure and technology* *Open and human-centric digital economy and trade*	Backsliding of the government's commitment to a functioning market economy notably in the digital realm (e.g., barriers to cross-border data flows). Weak overall financial regulatory framework, public finance management, or compliance and controls systems that also trickle down to poor cyber hygiene of public sector systems. Increased economic security risks from external actors, and strategic dependencies in its supply chains, digital infrastructure and services, and technological products (e.g., higher risk of exploitation of cybersecurity vulnerabilities).	Articulate the value added of the EU approach and in the policy dialogue, and give examples from the EU experience, mobilising the Team Europe Approach where possible. Include requirements in the action for the implementation of specific controls and reforms that can address specific weaknesses and deal with substantial or high risks. For example, prioritise activities that support the development and adoption of legislative measures for independent oversight. Support the government to undertake further analyses to shed light on strategic dependencies that lead to substantial or high risks.

4.4. Implementation modalities and partners

The EU has mostly used the **project modality** for cyber capacity building to address the cyber-specific needs of partners. One of the **most challenging issues for cyber capacity building** is the identification of competent **implementing partners** that have the transversal expertise on cyber issues along with the operational capacity for the roll-out of activities at scale.

In the field of **cybercrime,** the EU has built a strong partnership with the Council of Europe. This has been possible chiefly thanks to the Council of Europe's own scaled-up capacity to implement projects since the establishment of its Cybercrime Programme Office (C-PROC) in Bucharest. Over time, the EU has also developed projects with the involvement of the EU agencies and bodies as partners in CCB where their respective mandates allow for such engagement, most notably EC3 at Europol and CEPOL.

In the field of **cybersecurity**, the EU's has relied primarily on consortia led by EU Member State entities to ensure alignment with the EU values and policies but also as a guarantee of the implementation capacity. Given the overall cyber skills shortage within the EU and the handful of EUMS implementers engaging in this field, there are significant constraints to this approach. It limits the EU's possible partner options and therefore hampers the ability to scale up funding and implementation of CCB. This is further

aggravated by the challenges that the implementers face in combining cyber policy/legal frameworks, technical knowledge, and development cooperation methodologies.

Lessons in addressing this challenge include:

- Create **local and regional ecosystems of expertise** to deliver more sustainable models. Options include the concept of the EU-funded LAC4 or the French-funded Cybersecurity Centers in Senegal and Montenegro.
- Design actions that aim at supporting **local public-private cybersecurity hubs and ecosystems**, with a focus on education, skills, and the development of a local cybersecurity security industry as an enabling environment.
- Embed **triangular and South-South cooperation modalities** in new actions. This is possible also within existing projects. For example, GLACY+ uses certain countries as **project regional hubs** that create local capacity at their police and judicial academies through a train-the-trainer scheme so that they can be mobilised as trainers for other countries. It is a phased-approach model whereby these countries/partners can encourage changes in and between their regions and eventually move from networking and information exchange to operational cooperation.
- **Consider more systematically partnerships with civil society organisations** as implementing partners or at least provide modalities for such organisations to be eligible for joining consortia of Member States' implementers.
- **Pursue also for cyber issues the Team Europe approach**, that is the backbone of NDICI-Global Europe and brings together the European Union and its Member States (including their implementing agencies and public development banks), as well as the European Investment Bank (EIB) and the European Bank for Reconstruction and Development (EBRD).
- Consider **budget support** as an implementation modality and integrate cyber-specific components in such actions. From the three types of budget support contracts, namely the Sustainable Development Goals Contracts (SDG-Cs), the State and Resilience Building Contracts (SRBCs), and the Sector Reform Performance Contracts (SRPCs), the latter is the most appropriate option for supporting cyber resilience efforts as part of digital transition.
- Explore utilising the **European Fund for Sustainable Development Plus (EFSD+)** as a modality for embedding cybersecurity and cyber resilience as components in the EU's external actions.
- Set an introductory training of implementing partners on the EU policies, interests and principles on cyber issues. The EU operational managers should request the **implementing partners to join the EU CyberNet stakeholder community** to take advantage of its coordination and knowledge sharing platform.

BOX 12: PRACTICAL TIPS FOR FORMULATION

- ✓ Use existing resources to help you with the intervention logic (OG, Capacity4Dev on cybersecurity) and pay attention to cross-cutting issues (esp. human rights) also as part of your risk analysis and mitigation design.
- ✓ Have selection criteria for the implementing partners that require them to showcase understanding of the EU's cyber diplomacy policies and objectives and how they will ensure all activities are coherent with these. Avoid a tech-only/ICT-focused pool of expertise.
- ✓ In defining expert profiles, foresee teams that bring together complementary knowledge on cyber policy, legislative and technical issues (with a focus on what is required by the action) with international cooperation expertise.
- ✓ Identify whether there are academic, civil society or private sector entities locally that could serve as local partners to implementers especially with a view to foster local capacities and expertise for the delivery of activities. Most CCB projects to date suffer from 'fly-in' expert practice. Consider designing actions that embed expertise in a long-term peer-to-peer setting (e.g., Twinning model).
- ✓ As there is often a notable time lapse between formulation and contract signature, include in the contract ToR/DoA the responsibility of the implementer to update during the inception phase the following tools:

- Update the risks and assumptions in a revised risk assessment and develop a **risk management plan** to anticipate unintended consequences

- Update the **human rights assessment** and elaborate a human rights **risk mitigation plan**

- Update or (if it does not exist) create a **gender sensitivity assessment and plan**

- Update or (if it does not exist) create an **environmental impact assessment and plan**

- Establish a **Monitoring & Reporting** system based on the logframe

- Include in the contracting documents **requirements for reporting how these plans are being implemented against the activities**, I order to supplement the overall reporting guidelines outlined in the GCs (which include inter alia reporting on results against indicators, update of logframe, etc.). Include a **'lessons learnt' section** in the progress and final report requirements. You can include these specific reporting requirements in the Special Conditions. Foresee **regular interim reviews** in the contract.

5. Implementing from inception to closure

Objective: Efficiently execute, manage, implement, and monitor the performance of a CCB intervention using appropriate mechanisms and tools.

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 and organisations feel a strong sense of ownership of initiatives when their own systems and procedures are used for implementing actions.[33]

5.1. Inception phase

The inception phase is critical, as is offers the opportunity to:

- confirm the validity of the analysis during the design stage, including if there are any context, public policy or stakeholder changes that impact the problem analysis and the intervention logic,
- review the logical framework matrix, and include indicators' targets (preferably set from the partner's policies, plans or strategies, consistent with internationally agreed SDG targets or other EU commitments),
- reassess the risk analysis and refine the risks framework,
- ensure local ownership, especially in cases of fluid political environments.

The implementing partner is in the lead of ensuring the analysis is updated and proposing any necessary adaptations to the EU operational manager, in consultation with the partner government.

TOOL 12: INCEPTION REPORT CHECKLIST

A checklist for the inception report detailing **the tasks that the implementing partner should undertake** during this phase will help set the expectations from the outset:

- ✓ A detailed assessment of the needs to inform the overall plan and resource allocation for the action and to produce a workplan for the first year on each component of the action. It should include an updated review of all national strategy, policy, and legislation documents related to cybersecurity/cybercrime and a comprehensive capability assessment.
- ✓ An overview of other on-going actions in the area of cybersecurity/cybercrime in the regions covered for de-confliction and also potential areas of cooperation with existing projects, and any strategic implications or dependencies other donors' actions may have in yours.
- ✓ A detailed proposed work plan (and approval by national authorities).
- ✓ An updated Logical Framework Matrix with baseline figures, and proposals for any necessary intervention/ theory of change revisions and validation of risks/assumptions, to be approved by the Contracting Authority by the end of the inception phase.

33 Capacity development: A UNDP primer, United Nations Development Programme, New York, 2009.

A human rights compliance and risk assessment/mitigation strategy for the action that anticipates also mitigation of unintended consequences.

- ✓ A gender mainstreaming plan (updating and elaborating any assessments done during formulation and contracting).
- ✓ An environment impact assessment/mainstreaming plan (updating and elaborating any assessments done during formulation and contracting).
- ✓ Detailed elaboration of the communication and visibility strategy.
- ✓ The inception report will also provide updates on the management structure of the project clearly describing the responsibilities of the main players (incl. input by different entities/sub-contractors) as well as the decision-making process and information flow among the project participants.
- ✓ If strong reluctances and/or divergences arise from this phase (e.g., in the ownership/buy-in of national authorities), including against the foreseen assumptions, the inception report should include contingency proposals to align the foreseen implementation activities to the findings of the Inception Phase, as long as they do not deviate from the overall objective and purpose of the action.

5.2. Continued policy dialogue and stakeholder engagement

During the implementation stage, it will be necessary to re-engage all the stakeholders identified and engaged during formulation. At the policy level, it is important to maintain the engagement of government at the national (and possibly subnational) level. The commitment of host governments to address these sensitive issues in practice may vary enormously according to the context. Project outcomes may be seriously compromised without regular dialogue.

The project management team should consult and coordinate with all relevant stakeholders and project beneficiaries that participated in the identification phase by attending briefings and discussion meetings on a bilateral or multilateral basis. This promotes transparency and accountability, facilitates an understanding of the institutional landscape and available capacities, and ensures an updated diagnosis of the specific issues to be addressed.

Flexibility in the conduct of the consultation is required to adapt to rapidly changing situations, to identify new **'cyber champions'** across government and society, and to prepare for the potentially necessary changes. The stakeholder coordination process facilitates increased exchanges on cyber-specific issues between the different institutions that perform at the national and regional levels, which are often lacking on cyber-related issues. It can also serve as a platform for donor coordination led by the partner country.

5.3. Communication and visibility strategy

An efficient and comprehensive communication and visibility strategy should inform local, national, regional, and international audiences, and communicate the action's results. In addition, a communications package or presentation about the programme can help generate support from other partners or donors for similar activities or create an opportunity to share lessons learnt.

The following strategic communication principles should guide the process:

- Ensure consistency, coherency, and clarity of the project's communication in line with EU communication standards and orientations.
- Regularly assess and adapt communication to the various target groups' perception of the project to ensure proper ownership of the project's results by its stakeholders (local, national, regional, and international).
- Adapt communication to respect the need for confidentiality/security of specific sensitive information and data.

- Ensure the visibility of concrete actions/events illustrating progress and results achieved throughout the project.
- Favour digital communication to facilitate the circulation and dissemination of data and information.

The CCB action should have a clear communication line on the added value of working with the EU on cyber issues. It should also have a strategy for limiting communication activities if it would attract undue attention to implementers and engaged partners that would risk making them potential targets of cyberattacks (e.g., if the action entails support to enhance the digital safety skills of vulnerable groups or the organisational cyber resilience of civil society organisations critical to the government).

5.4. Monitoring and reporting

Project monitoring is a continuing function that uses systematic collection of data on specified indicators to provide management and the main stakeholders of an on-going intervention with indications of the extent of progress and achievement of objectives and progress in the use of allocated funds.

Internal monitoring is implemented both by implementing partners (such as the agency's staff, government personnel, other donors, non-state actors e.g., private sector companies, NGOs, etc.) and by EU staff that collect and analyse data to inform progress against planned results. It feeds into decision-making processes and gives details on the use of resources.

External monitoring of EU external actions is implemented through Results Oriented Monitoring (ROM). It has been introduced by the European Commission to get an independent view on action's performance.

Most CCB actions foresee as outcomes a change in public policy, for example through the introduction and application of national cybercrime or cybersecurity legislation; the adoption and implementation of a national cybersecurity strategy; or the creation of cyber crisis management coordination policies and procedures. However, the **monitoring and evaluation (M&E) of public policies** are often the weakest phases of the policy cycle.

The **logframe is the main management tool for monitoring and reporting** during implementation. EU-funded actions should, as much as possible, use and build on **existing national monitoring systems and sources** to support institutional strengthening and avoid the creation of parallel, stand-alone information systems that would not be kept outside the life cycle of the project. Improving countries' M&E systems also helps to respond to difficulties during policy implementation. Where weaknesses in the country's M&E systems are identified during the contract design, governments should be supported to improve them.

Acknowledging the **limited budgets** that are generally available to monitoring activities, it is valuable to foresee necessary resources in the action to ensure the project can monitor and collect relevant data at a large scale to measure the long-term effects in the country or countries where the action has been delivered, in a way that the country's own monitoring capacity is also enhanced.

5.5. Risk response

Risk management[34] goes hand in hand with monitoring during implementation. Risks and their mitigating measures are monitored on a periodical basis in order to:

- check that identified risks are being adequately managed,
- assess the implementation progress of the mitigating measures,
- identify any new risks or changes in circumstances.

The development of a sound risk management framework based on the project design stages creates the structure for vigilant monitoring that then enables the implementing partners and the EU to anticipate risks, mitigate them, and manage unintended consequences that may arise.

The risk management framework should be updated at least once a year, except when new circumstances lead to deterioration in at least one of the risk categories to substantial or high. Most monitoring of the identified risks can be done as an inherent part of good management of the action by the implementing partners, Delegations and HQ, while the development of close relationships with partner governments, civil society organisations, and other cooperation partners in the country (e.g., EU Member States and IFIs), will allow for a natural flow of information on new or aggravating risks.

34 Adapted from the European Commission Budget Support Guidelines (Annex 13), 2017.

TOOL 13: RISK STRATEGY - RESPONSE		
RISKS RELATING TO	**KEY RISKS**	**POSSIBLE RESPONSE MEASURES**
Values • *Human rights and the rule of law* • *Nature of and access to the Internet* • *Rules-based international order*	Backsliding of the government's commitment and adherence to rule of law, human rights, and democratic standards as reflected in the digital realm (e.g., online censorship, internet shutdowns, use of technology for unlawful surveillance of civilians and targeting of vulnerable groups). Government shift towards supporting the multilateral, state-centric approach to internet governance instead of the multi-stakeholder model.	Regular update on the status of the mitigating measures undertaken by the implementing partner on the activities and related developments in the policy and legislative sphere. Policy dialogue with the government to raise concerns in case of deteriorating situation. It is an opportunity to convey clear messages on the implications for further assistance in this field, or for the overall assistance of the EU should the materialised risk is very serious. Coordinated demarches with like-minded partners (donors, development partners) to exert political pressure for reverting the risk situation. Enhanced support to the multistakeholder community and civil society in particular to strengthen bottom-up capacities, promote reforms, and increase their cyber resilience, especially if their rights are restricted or they are targeted by unlawful digital surveillance practices. Consideration of shifting the action's focus, or limiting activities, or suspending the action depending on the level of deterioration of a risk category from a previously lower assessment to substantial or high.
Interests • *Resilient and diversified supply chains* • *Sustainable, secure, trustworthy infrastructure and technology* • *Open and human-centric digital economy and trade*	Backsliding of the government's commitment to a functioning market economy notably in the digital realm (e.g., barriers to cross-border data flows). Weak overall financial regulatory framework, public finance management, or compliance and controls systems that also trickle down to poor cyber hygiene of public sector systems. Increased economic security risks from external actors, and strategic dependencies in its supply chains, digital infrastructure and services, and technological products (e.g., higher risk of exploitation of cybersecurity vulnerabilities).	
Principles • *Effective development and international cooperation* • *Human rights-based approach* • *'Do no harm' and 'Do more good'*	Weak ownership for cyber policies and reforms, and lack of commitment to inclusive dialogue and approaches to cyber resilience Corruption and fraud that could divert resources meant for cyber issues. Exacerbation of existing inequalities in relation to the digital divide and their access to cybersecurity resources (services, training, etc). Sustainability risks for human and technical aspects (e.g., cybersecurity software licences; brain-drain of cybersecurity-trained staff).	

5.6. Closure

An important aspect of capacity building programmes is negotiating from the beginning **clear exit strategies and timeframes** and making sure that they are included in any formal arrangement. As a result, the external actor's role is framed from the beginning as supporting the partner until a certain capacity level is achieved, to ensure that the partner country assumes ownership of the process early on. Actions 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 to make sure that the phasing out of external expertise and systems is done in a professional and mutually beneficial manner, with minimum disruption.

TOOL 14: CLOSING PHASE CHECKLIST

Require from the **implementing partner** to:

- ✓ Finalise an 'exit strategy' proposal for the action with concrete proposals and plan for sustainability.
- ✓ Ensure that the final report has a strong results focus, including lessons learnt and a detailed explanation of results delivered at the output level and the intervention's contribution to the desired outcomes and impact. It should include any known external factors that affected the intervention's performance. Moreover, it should also capture ideas and recommendations for upcoming interventions in the same area. The information obtained through final reports and evaluations should also help operational managers plan for the continuation of an intervention (e.g., in the next annual action plan or Action Document).
- ✓ Compile an overview of the action's results including an analytical view of the cybersecurity state-of-play in beneficiary countries and its evolution during the implementation of the action.
- ✓ Collate products and reports developed by the action and prepare a systematic presentation of the action's results that should be published and disseminated.
- ✓ Complete an official hand-over of all material produced by the action to beneficiary institutions (e.g., remaining training material, manuals, equipment).
- ✓ Organise a final conference involving senior officials and decision-makers, (national, regional, and international) partners and organisations to showcase progress made during the action and concrete results attained, to highlight partnerships developed, showcase lessons learnt and recommendations for further action to be taken by the government(s) and other organisations, and to foster agreement on strategic priorities for the future.

BOX 13: PRACTICAL TIPS FOR IMPLEMENTATION

- ✓ Be cognisant of the importance in sequencing of CCB planning. For example, if there is no legislative framework or no human rights safeguards in the existing one, it may be a risk to support specialised LE trainings.
- ✓ Consistently use the monitoring tools you have incorporated into the project to have a good overview of progress and risks. This entails requesting the implementing partner for regular (e.g., quarterly) updates of the risk management plan and the M&E system. Ensure that the strong reporting requirements you have foreseen on the contract are followed.
- ✓ Request the implementing partner to share regular updates on the cyber policy landscape developments in the country/region and flag immediately any issues of concern (for example the discussion of a new legislation on cyber or adjacent issues that is not in line with international standards, or the use of Internet shutdowns, etc.) and be ready to adapt the activities.
- ✓ Engage with EU Agencies to identify open-source resources that could be used as part of the intervention (e.g., ENISA, EC3, CEPOL). Also, the EU has been financing the **ECTEG project** for the creation of courses for EU LEAs that could also be used, under conditions, by external projects.
- ✓ Flag to **EU CyberNet** whether you are managing a project with a cyber-specific scope, or a cyber-relevant component so that the implementing partners are invited to the coordination and lessons learnt meetings hosted by EU CyberNet and the project is included in the EU's on-going mapping efforts.
- ✓ Foresee a communication expert in the project design (i.e. part-time expert) to ensure consistent and coherent messaging, in line with the Communication and Visibility Manual for EU external actions.
- ✓ Put mechanisms in place for implementers to:
- Capture lessons learnt in progress reports to create opportunities for feedback loops throughout the project life cycle for integrating improvements/lessons and inform the next programming cycle after the action's end.
- Engage local civil society (as partners and/or as participants) in the project activities.
- Join the EU CyberNet stakeholder community that offers a platform for sharing knowledge and lessons amongst implementers and other CCB actors.

6. Evaluating and learning

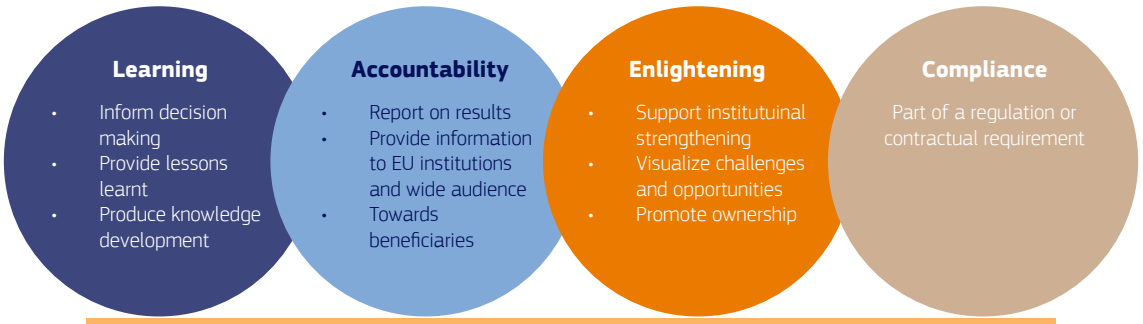
Objective: Assess the relevance, coherence, effectiveness, efficiency, impact, sustainability, and EU added value of CCB actions, and create feedback loops by capturing lessons learnt and integrating them in on-going and future actions to improve their effectiveness.

The purpose of the last stage of the intervention cycle is to assess how successful the action has been in meeting its stated objectives, reflect upon the coherence and relevance of activities, identify lessons learnt in terms of impact, sustainability, effectiveness, and efficiency, and systematise these lessons to guide future work in this area of intervention. This is an inclusive process that requires the involvement of all the main stakeholders engaged in the implementation and outcome of the intervention's activities. As such, evaluation is a dual tool: on the one hand it is meant to **support decision-making** by providing information and identifying lessons that can be used to improve policies and future interventions; and on the other hand it can **improve accountability** given that its findings can be used to demonstrate results towards stakeholders at all levels (i.e. EU, Member States, partner countries, taxpayers, civil society, etc.).

Given the **inherent difficulty in measuring cyber resilience**, the CCB community has struggled to date to make concrete evidence-based analyses on how cyber capacity building programmes have contributed at the impact level, with most interventions being able to demonstrate results at output levels and some at the outcome. Evaluation is a useful tool for CCB practitioners who need to pay strong attention to the actions' performance not only to justify their budgets but also to enhance the collective understanding of what works in the CCB field.

Figure 13: Evaluation purposes

Evaluation gives evidence of **WHY intended changes are or are not being achieved.** It seeks to address issues of causality. It has multiple purposes.



Source: DG NEAR Wiki

6.1. Evaluating for results

Evaluation is the systematic and objective assessment of an on-going or completed intervention, its design, implementation, and results. As elaborated by the OECD Development Assistance Committee, the aim is to determine the **relevance, coherence (including complementarity and synergies), effectiveness, efficiency, impact, and sustainability** to provide information that is credible and useful, enabling the incorporation of lessons learnt into decision-making processes. The EU's Better Regulation Toolbox sets five mandatory criteria for each evaluation: relevance, efficiency, effectiveness, coherence, and **EU added value.** The OECD criteria together with the EU Better Regulation guidelines set a comprehensive set of **seven criteria** that can be used for EU external actions. They also align with the evaluation criteria set in the Regulations governing external action (see for the period 2021-2027 NDICI-

Global Europe, Art. 42, and IPA III Art 13) that also put forward **'the scope for simplification'** as an element to examine. While some of the evaluation criteria by nature assess the entire results chain, others focus on individual result levels (i.e., impact and effectiveness revolve around the outcomes).

The timing of evaluations is important as it serves different objectives:

- Final evaluations aim to contribute to accountability and lessons learnt and therefore take place a few months before the operational closure of an action. They provide an assessment of the results achieved, including an understanding of the factors that facilitated or hindered the achievement of results, as well as an identification of lessons that can improve future interventions.

- Ex-post evaluations focus on the impact (expected and unexpected) and sustainability of the action, therefore are planned one to two years after the action's operational closure. They are designed to draw conclusions on what achievements the intervention contributed to and how it did so, or why it did not contribute as expected.

At the impact level, it is valuable to collect and exploit data on a large scale and gauge the long-term effects in the country or countries where the programme has been delivered. Given the difficulty in crediting changes to the intervention at the impact level, it is important that implementing partners allocate sufficient resources to implement the monitoring system and collect data that can be then useful for an evaluation. While specific CCB actions usually form single elements within a broader ecosystem of security and/or digitalisation reforms within countries or regions, it is often a challenge

to use indicators linked to such system-wide efforts rather than individual actions. However, the **use of existing cyber metrics and indices** could be a partial solution, even if their methodologies vary and do not provide a holistic view.

Examples of **quantitative cyber metrics** include Cyber Green, Center for Applied Internet Data Analysis (CAIDA), Shadowserver Foundation, etc. In addition, one can look into **reports** of incident numbers, ransomware rates, botnet attacks, and any data on organisational patching cadence, security audit compliance and third-party risk and compliance. Moreover, there are **several relevant indices**, such as the Cyber Readiness Index 2.0 (CRI), the Global Cybersecurity Index (GCI), the National Cyber Security Index (NCSI), the National Cyber Power Index (Harvard University), and the UN E-Government Development Index (EGDI).

6.2. Deciding to follow-up

During the closing phase, or earlier, a follow-up action comes under consideration, for example, to expand on achieved results, and to scale successful interventions to a larger stakeholder group or a bigger geographical scope. Designing a second phase of an intervention is inspired by what is observed from the first phase, including lessons identified in past evaluation reports, ROM reports, records of meetings, and data collected through internal monitoring systems.

TOOL 15: QUESTIONNAIRE ASSESSING FOLLOW-UP ACTIONS

The questions below can help guide EU operational managers in their assessment of a follow-up action

Results

- Has the action contributed to increasing local capacities according to the action's indicators?
- Has the action influenced policy positions in the partner countries in alignment with EU ones?
- Does the action have policy implications for the region?
- Is the action's sustained impact guaranteed with specific measures?

Follow-up

- Does the action require a follow-up intervention or continued activities to meet its objectives?
- Can the action's results be scaled up through a new phase?
- Can lessons learnt be shared?
- Is there a (locally-led) management system in place to continue activities?

Financing

- Did the action perform according to its financial performance targets?
- If follow-up programming is recommended, is the same source of funding the best option?
- Could a follow-up action transition to an alternative EU financing envelope (e.g., from regional to bilateral or vice versa), or other donor sources (EU Member States or others)? Is that a better fit?

Implementation

- Does the implementing partner of the action have the requisite expertise (cyber-specific and PCM) for a scaled-up action?
- Did the action empower local entities that can serve as implementing partners going forward?

6.3. Learning

The identification of lessons is important to ensure that the outcomes and experiences associated with the intervention feed into future policies and practices, and capture approaches that had particularly good outcomes. Such information includes lessons from the management of risks, methods for engaging key stakeholders, outsourcing or contractor issues, work plans or time management issues, etc.

A good example of systematically capturing lessons is the practice of the Council of Europe's Cybercrime Programme Office (C-PROC) which publishes periodical reports with results and lessons from its actions.

TOOL 16: IDENTIFICATION OF LESSONS QUESTIONNAIR

Sharing this questionnaire with the implementing partner from the start of the intervention will help guide them in capturing lessons:

- What was learnt about the intervention, i.e., what has and has not worked?
- Which were the enabling factors for the intervention achievements?
- Which were the limiting factors or hurdles that impacted the intervention?
- Were risks identified and mitigated? If not, why?
- What was learnt about project management? Was the schedule met? If not, why? Did the project management methodology work? If not, why?
- What was learnt about communication? What changes would assist in speeding up future interventions while increasing communication?
- What was learnt about budgeting? Were costs/budgets met? If not, why?
- What was learnt about stakeholders? Have the relevant groups of actors been involved? Which elements of the stakeholder analysis contributed to this outcome?
- What was learnt about what needs to change? What can be done in future actions to facilitate success?
- How will/was this (be) incorporated into the intervention? What procedures should be implemented in future actions?

Compilation based on DG NEAR Programming M&E Wiki, and the Lessons Learnt guide developed by the Centers for Disease Control and Prevention (CDC).

BOX 14: PRACTICAL TIPS FOR EVALUATION & LEARNING

- ✓ Foresee a separate budget for evaluations in the Commission Decision.
- ✓ Request the implementing partner to have sufficient budget and staff for using and feeding into the agreed monitoring system to allow for systematic data collection that can be used also for the evaluations.
- ✓ The timing of evaluations is critical for their usefulness: try to commission them when implementing partners can provide their draft final report and before the start of the next identification/formulation phase.
- ✓ Ensure that the evaluators incorporate gender sensitivity in their analysis.
- ✓ Request implementing partners to allocate requisite resources to document lessons learnt throughout the intervention's life cycle. The relevant briefs should:
  - Include information about the action and contact information, a clear statement of the lesson, a background of how the lesson was learnt, benefits of using the lesson and suggestions on how the lesson may be used in the future.
  - Capture not only positive, but also negative lessons from failed activities, or interventions that did not bring desired outcomes, as they form the basis of corrective measures.
  - Reflect on the usefulness and usability of specific cybersecurity indicators from the logframe.
  - Group and prioritise lessons to understand key potential improvement areas.
  - Have a plan on how to disseminate these lessons.

IV. CYBER-RELATED POLICIES AND CONCEPTS

Internet connectivity has significantly changed not only how people live, work, and communicate but also redefined how different communities define and pursue their strategic objectives in cyberspace. The multiplicity of objectives that the Internet serves, makes the governance of a broadly defined cyberspace a complicated task even within the same policy communities. This chapter offers an understanding of the cyber dimension in different policy areas, highlighting the EU approach.

1. Cyberspace as an arena for sustainable development

Cyberspace serves as the fundamental platform for the development and dissemination of transformative digital technologies, offering numerous human, economic, and social benefits. In 2016, the World Development Report on

BOX 14: PRACTICAL TIPS FOR EVALUATION & LEARNING

The EU considers an open, free, stable, and secure cyberspace along with its uncensored and non-discriminatory use as essential for fostering open societies and enabling economic growth and social development globally. The shift towards 'Geopolitical Commission' has redefined the EU's approach to international partnerships. In 2020, the EU presented the **Global Gateway Strategy** which sets several concrete goals regarding the link between digital, cyber, and international partnerships policies:

- reducing the environmental footprint of digital infrastructure;
- supporting network security and resilience, interoperability, and an open, plural, and secure Internet by using the EU toolbox for the cybersecurity of 5G networks to guide investments in digital infrastructure and promoting cybersecurity standards;
- promoting access to the Open Internet as a key driver of innovation, socio-political, economic, and cultural development;
- offering digital economy packages that combine infrastructure investments with country-level assistance on ensuring the protection of personal data, cybersecurity and the right to privacy, trustworthy AI, as well as fair and open digital markets.

The EU established new digital partnerships as an instrument to boost digital and cyber cooperation and connectivity with partners in a flexible way but focused on concrete deliverables. In addition, to promote a human-centric approach to digital transformation and align the EU's digital initiatives for an increased impact through the Team Europe approach, the EU launched the Digital for Development (D4D) Hub. This strategic multi-stakeholder platform promotes new international partnerships on digital transformation between the European Union and partner countries in Africa, Asia, Latin America, the Caribbean, and EU Eastern Neighbourhood. The cybersecurity thematic working group established under the umbrella of D4D Hub deals with issues related to cybersecurity and cyber capacity building.

Figure 14: Selected legal and strategic documents adopted by the EU

Overall strategic framework

Strategic Compass for Security and Defence (2022)
2030 Digital Compass (2021)
European Cybersecurity Strategy for the Digital Age (2020)
EU Security Union Strategy 2020-2025 (2020)

Sustainable development
- Global Gateway Strategy (2021)
- Council conclusions on EU external cyber capacity building guidelines (2018)
- Council conclusions on Digital for Development (2017)

Digital transformation
- Gigabit Infrastructure Act (2023)
- Europe's Digital Decade (2022) and Path to the Digital Decade (2022)
- European Data Governance Act (2022)
- 2030 Digital Compass (2021)
- eGovernance regulation, including on digital identity and Digital Identity Wallets (2020)

Internet governance
- Next Generation Internet initiative (2023)
- Declaration for the Future of the Internet (2022)
- Council conclusions on digital diplomacy (2022)
- 2030 Digital Compass (2021)
- Open Internet Regulation (2016)

Marketplace
- European Economic Security Strategy (2023)
- Critical Raw Materials Act (2023)
- European Chips Act (2022)
- European Data Governance Act (2022)
- Digital Services Act and Digital Markets Act (2022)
- 2030 Digital Compass (2021)
- Artificial Intelligence Act (Proposal in 2021)

Security
- Cyber Solidarity Act (2023)
- NIS 2 Directive (2022)
- Digital Operational Resilience Act (2022)
- EU Cyber Resilience Act (Proposal in 2022)
- Critical Entities Resilience Directive (2022)
- EU Toolbox for 5G Security (2021)
- Cybersecurity Act (2019)

Crime
- Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse (Proposal in 2020)
- Directive on non-cash payments (2019)
- Regulation and Directive facilitating cross-border access to electronic evidence for criminal investigations (Proposal in 2018)
- Directive on attacks against information systems (2013)
- Council of Europe Convention on Cybercrime (Budapest Convention) (2004)

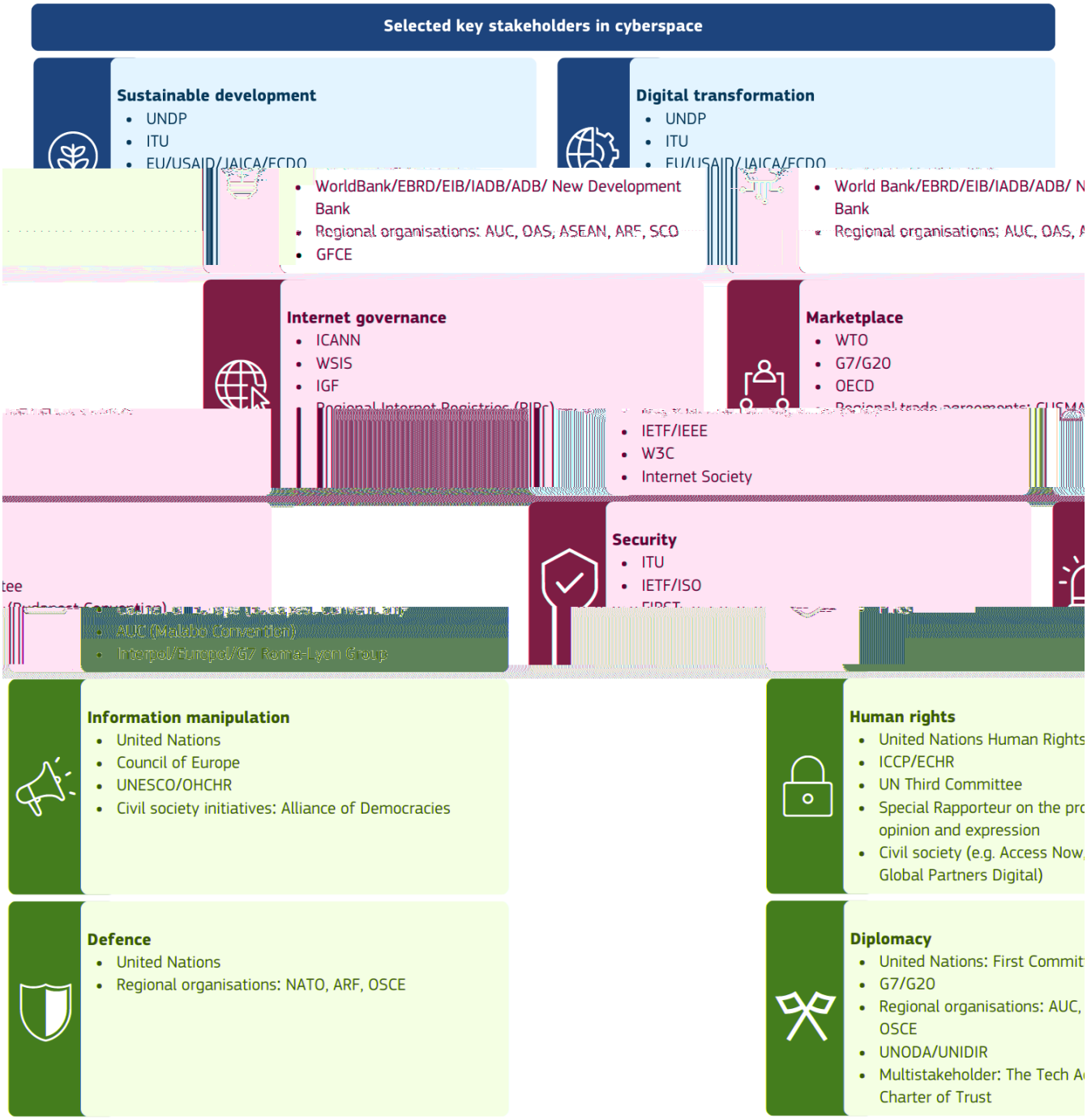
Human rights
- European declaration on digital rights and principles for the digital decade (2022)
- Global Human Rights Sanctions regime (2020)
- EU Human Rights Guidelines on Freedom of Expression Online and Offline (2014)

Information manipulation
- Code of Practice on Disinformation (2022)
- Council Conclusions on foreign information manipulation and interference (FIMI) (2022)
- Compendium on cybersecurity of election technology (2018)

Diplomacy
- Council conclusions on digital diplomacy (2023)
- Council conclusions on the development of the European Union's cyber posture (2022)
- Council conclusions on digital diplomacy (2022)
- Declaration for the Future of the Internet (2022)
- EU Cyber Sanctions regime (2019)
- Council conclusions on malicious activities in cyberspace (2018)
- Joint EU diplomatic response to malicious cyber activities (Cyber Diplomacy Toolbox), including declarations by HRVP (2017)
- Council conclusion on cyber diplomacy (2015)

Defence
- Framework for a coordinated EU response to hybrid campaigns and EU Hybrid Toolbox (2022)
- Council conclusions on the EU Policy on Cyber Defence (2022)
- Joint Framework on Countering Hybrid Threats (2016)
- EU-NATO Joint Declaration (2016)

Figure 15: Selected key stakeholders across cyber policy areas



2. Cyberspace as a field for digital transformation

Digital technologies and data present new opportunities and transform the relationships between individuals, institutions, and governments. Robotics, Artificial Intelligence, big data, blockchain technologies, and the Internet of Things are reshaping production and distribution processes, with the potential to significantly impact democratic processes, government institutions, and work dynamics. However, they also raise critical concerns about privacy, equality, consumer rights, and safety. The goal of connecting everyone to the Internet is to ensure accessible, affordable, inclusive, secure, and safe access through trusted networks to an open Internet. Achieving this requires digital transformation at governmental, organisational, and societal levels, founded on multi-stakeholder cooperation that places citizens at the

heart of these processes and promotes trustworthy technology, creating opportunities for individuals and businesses while fostering democratic and accountable forms of governance.

Digital transformation unlocks growth potential and enhances the accessibility and efficiency of public services, making it a crucial tool for achieving sustainable development. Various technologies, such as sensors and geospatial technologies, assist farmers in resource and production management and accessing markets along the agriculture value chain. Smart cities utilise new technologies and Internet of Things devices to improve operational efficiency and offer better quality services in areas such as transportation, water supply, and energy. Blockchain technology is being adopted to facilitate transparent, decentralised, and efficient transactions, reducing power imbalances between farmers and intermediaries. In addition, digitalisation across public services and the adoption of e-governance solutions, including in the judicial system, legislative branch, e-voting systems, and voter registration, contribute to enhanced efficiency, improved management, transparency, and government legitimacy. Measures like introducing electronic identification can reduce administrative burdens and promote cross-border trade. A 'mobile first' approach should guide digital transformation, enabling citizens to interact digitally with public authorities and providing universal access and the choice to use e-government services.

While Internet connectivity can accelerate these processes, it necessitates access to affordable and secure broadband, appropriate policy and regulatory frameworks, tools for technology transfer and adaptation, and the development of digital skills and cooperation among stakeholders. International partnerships focus on enhancing the regulatory environment, investing in digital infrastructure and the digital start-up ecosystem, promoting digital skills and entrepreneurship, developing digitally enabled public and private services (e-services), and addressing digital risks. Given that barriers to internet access are often related to digital skills, digital transformation processes should ensure that all individuals become well-informed and responsible digital citizens, fully and equally participating in all aspects of the digital economy, society, and political life.

BOX 16: ESSENTIALS OF THE EU APPROACH

The EU is committed to a future for an **Internet that is open, stable, free, inclusive, global, interoperable, reliable, secure, and green** and puts humans and their rights at the centre of digital transformation. The **Europe's Digital Decade** is a comprehensive framework established to guide all actions related to digital. The framework for the Digital Decade includes the Digital Decade Policy Programme, the Digital Decade targets, the objectives, the multi-country projects and the Digital Decade rights and principles. The Digital Decade Policy Programme 2030 revolves around four cardinal points: skills, digital transformation of businesses, secure and sustainable digital infrastructure, and digitalisation of public services.

The EU's approach puts **people at the centre of the digital transformation**, at home and globally. Through its policies, the EU aims to ensure that digital transformation leaves no one behind, strengthen the democratic framework for digital transformation, ensure the protection of and respect for human rights online and offline, foster responsible and diligent action by all stakeholders, support local data and technological ownership as well technological capacity building for a safe and secure digital environment.

The EU's international partnerships promote human-centred digital agenda and aim to promote alignment or convergence with EU norms and standards, including through designing digital economy packages and setting a toolbox combining regulatory cooperation, addressing capacity building and skills, investment in international cooperation and research partnerships. The EU's approach includes several dimensions:

Connectivity: The main goal for connectivity in the Digital Decade is for every European household to have access to high-speed Internet coverage by 2025 and gigabit connectivity by 2030. In 2023, the European Commission proposed the Gigabit Infrastructure Act which aims to facilitate and stimulate the roll-out of very high-capacity networks by promoting the joint use of existing physical infrastructure and by enabling a more efficient deployment of new physical infrastructure. The European Electronic Communications Code comprises essential pro-investment rules, both in spectrum management and access regulation. For instance, the EU offers support to developing regional roaming agreements and technical assistance and expertise.

3. Cyberspace as an Internet governance domain

The Internet is designed as a single, global, decentralised network of networks. All stakeholders work towards ensuring

issues. In particular, the possible **fragmentation of Internet governance** due to the divergent values of commercial, economic, and legal interests raises growing concerns. To counter such trends, it is essential to ensure that digital markets are open, fair, and contestable; provide affordable, inclusive, and reliable access to the Internet; and support the promotion and protection of human rights online.

BOX 17: ESSENTIALS OF THE EU APPROACH

The EU advocates 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 and the provider. For instance, in 2016, the EU adopted the **open Internet regulation** which grants users the right to access and distribute lawful content and services of their choice via their Internet access service. It ensures that Internet traffic is treated without discrimination, blocking, throttling, or prioritisation. The EU also launched the **Next Generation Internet initiative** to put in place the key technological building blocks of the future Internet as an interoperable platform ecosystem that ensures openness, inclusivity, transparency, privacy, cooperation, and protection of data. The goal is to empower users with the freedom of choice among a range of open-source decentralised digital solutions.

The EU's vision for a digitally transformed Europe in line with European values is enshrined in the **2030 Digital Compass** and the **Path to the Digital Decade** which sets up an annual cooperation cycle to achieve the EU's targets. The overall idea is to make digital transformation the engine of sustainable economic growth and social well-being in Europe. Some of the tools to achieve that include extending high-performance broadband access for all citizens, building up digital skills and competencies for, digitalising businesses and public services, and making the latter more efficient. The EU also recognises that secure cyberspace creates greater trust among people in digital tools and services, which allows to preserve freedom of expression and information, including media freedom and pluralism.

To promote a human-centric digital transformation, the EU and its member states are committed to promoting **Declaration for the Future of the Internet** which sets out the vision and principles of a trusted Internet, including: the protection and promotion of human rights and fundamental freedoms; ensuring universal connectivity to the Internet through increased access, affordability, and digital skills; strengthening trust in the safety and the confidentiality of the digital technologies among individuals and businesses; safeguarding a fair and competitive ecosystem for businesses of all sizes to innovate, compete and thrive; designing secure, interoperable, reliable, and sustainable infrastructure; and using technology to promote pluralism and freedom of expression, sustainability, inclusive economic growth, and the fight against global climate change.

The EU's vision of the Internet is also pursued through the mechanisms and tools offered by the **EU's digital diplomacy** that aims to actively promote the EU's positions on digital issues, including advancing a human-centric and human rights-based approach to digital technologies in relevant multilateral fora and other platforms; as well as influencing the shaping of ethical, safe and inclusive international technology standards based on human rights and fundamental freedoms through international bodies and organisations such as the International Telecommunications Union (ITU), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE).

Figure 16: Layers of governance in cyberspace

4. Cyberspace as a marketplace

Many countries aim to become fully-fledged digital societies, where digital technologies facilitate the growth of businesses and individuals. The digital economy currently constitutes 15.5 % of the global GDP, growing two and a half times faster than the overall global GDP in the last 15 years. In Africa, a mere 10 % increase in mobile broadband penetration could lead to a 2.5 % rise in GDP per capita.

However, achieving this goal often involves dependency on products, services, and infrastructure provided by others, raising concerns about risks, including national security risks, and lack of ownership. To address these issues, the concept of **digital sovereignty** emerged as a potential solution to recalibrate certain types of dependencies. Simultaneously, the rise of technological solutions offered by China on global markets and the risk of spreading a **digital authoritarian** model have intensified strategic competition with the United States and the European Union.

The progress of digital societies hinges on their infrastructure and technological foundation, leading to policy debates on controlling and setting standards for Internet infrastructure and developing new technological capabilities. Concerns about **supply chain security**, due to reliance on high-risk vendors, have sparked discussions about legitimate ways for states to impose market access restrictions to safeguard national security. The rapid development of digital technologies has also brought the question of **international standards** in areas like AI, cloud computing, quantum computing, and quantum communication to the forefront. This aspect has become especially crucial, given some countries' attempts to use international standardisation bodies to advance their political and ideological agendas. Additionally, cyberspace has become an arena for competition in digital technologies and cybersecurity across the **digital supply chain**, including data and cloud services, next-generation processor technologies, ultra-secure connectivity, and 6G networks.

The proliferation of **cyber-surveillance technologies**, with potential misuse threatening safe and open cyberspace, is a significant concern. While surveillance activities for criminal justice purposes are generally accepted if conducted with adherence to the principles of legality, necessity, and proportionality, there have been numerous reports of cyber-surveillance technologies being misused, especially when exported to repressive regimes. In response, trade in cyber-surveillance technologies has become subject to export controls similar to those applied for other **dual-use goods** covered by the Wassenaar Arrangements

BOX 18: ESSENTIALS OF THE EU APPROACH

The general direction for the EU's policy aimed at establishing a **Digital Single Market** date back to 2015. It is grounded in the conviction that co-regulation of the digital space should serve to reinforce the rule of law that is essential to well-functioning democracies and markets. The EU is taking a systemic approach to set global standards for regulating online activities through the regulatory package composed of the Digital Services Act (DSA) and the Digital Markets Act (DMA) and the AI Act. The strategy for **Shaping Europe's Digital Future** and a **Digital Compass** translated the digital ambitions of the EU for 2030 into concrete targets. The Digital Compass identifies four main goals: 1) a digitally skilled population and highly skilled digital professionals; 2) secure and sustainable digital infrastructures; 3) digital transformation of businesses; and 4) digitalisation of public services. The EU has also translated the policy objectives linked to digital economy and digital sovereignty into concrete regulatory frameworks, including:

- **Data Governance Act** seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data. It will also support the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration, and skills.

- **Digital Services Act** aims to enhance freedom of expression online, make marketplaces safer and address illegal (and non-illegal, but harmful) content to the benefit of both consumers and companies. The objective of the regulation is to ensure that citizens have access to safe Internet while at the same time ensuring the protection of their freedom of expression online.
- **Digital Markets Act** aims to tackle unfair practices and lack of market contestability. It establishes a set of narrowly defined objective criteria for qualifying a large online platform as a so-called 'gatekeeper' and puts in place rules that give consumers and companies the freedom to make decisions and compete on fair terms. This allows the DMA to remain well-targeted to the problem that it aims to tackle as regards large, systemic online platforms.
- **European Chips Act** to bolster Europe's competitiveness and resilience in semiconductor technologies and applications and help achieve both the digital and green transition.
- **European AI Strategy** aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy. The Commission aims to address the risks generated by specific uses of AI through a set of complementary, proportionate and flexible rules. The legal framework for AI proposes a clear, easy to understand approach, based on four different levels of risk: unacceptable risk, high risk, limited risk, and minimal risk.

In 2021, the EU upgraded its legislation on export controls applicable to sensitive dual-use goods and technologies such as cyber-surveillance tools. Furthermore, in June 2023, the EU presented a Joint Communication on a **European Economic Security Strategy** which aims to address risks to the Union's economic security in four main areas: resilience of supply chains, physical and cyber security of critical infrastructure, technology security and technology leakage, and weaponisation of economic dependencies or economic coercion.

5. Cyberspace as a security domain

Cybersecurity lapses or vulnerabilities impose significant costs on the global economy and erode trust in digital transformation as a catalyst for growth. As businesses and services increasingly rely on Information and Communication Technologies (ICTs), the risks of disruptions that negatively impact the economy, democracy, and society also escalate. The utilisation of Internet-connected platforms for delivering public services and the evolving threat landscape have underscored the need to address the security aspect of digital transformation and connectivity, commonly known as cybersecurity or cyber resilience.

The focus on cybersecurity encompasses policies, laws, and institutions with the primary objective of addressing risks arising from the use of ICTs and safeguarding citizens and infrastructure from cyber threats. To avoid an excessive securitisation of economic and societal development, certain policy communities have preferred references to digital security risk management, which denotes a coordinated set of actions aimed at minimising risks and maximising opportunities in the digital environment. The central goal associated with cybersecurity is the protection of network and information systems. Achieving this involves implementing policies that reduce vulnerabilities in hardware and software through standards and certification, as well as establishing relevant policies and tools to facilitate cooperation among stakeholders. For instance, standardisation bodies like the International Standardization Organization (ISO) focus on Internet security to preserve the confidentiality, integrity, and availability of information in cyberspace. In response to the increasing frequency, sophistication, and impact of cyberattacks in recent years, cybersecurity has gradually been integrated into national and international crisis management efforts, resulting in the development of specific terminology and a more streamlined approach across various policy domains.

BOX 19: ESSENTIALS OF THE EU APPROACH

The **Digital Single Market Strategy for Europe** (2015) created a broad framework for enhancing the EU's position as a world leader in the digital economy and highlighted the need to address potential vulnerabilities that could be exploited illicitly resulting in financial losses, breaches of personal data or the subversion of democratic processes. The **EU Cybersecurity Strategy** adopted in 2020 took further steps to strengthen the EU's resilience to cyber threats and to ensure a global and open Internet with strong safeguards where there are risks to security and fundamental rights. It highlights three specific areas of EU action: 1) resilience, technological sovereignty, and leadership; 2) operational capacity to prevent, deter, and respond to cyberattacks; and 3) cooperation to advance a global and open cyberspace.

In the past years, the EU put in place a robust policy and regulatory framework focused on various dimensions of the EU's cyber resilience that might serve as inspiration for other countries. These include, among others:

- **Network and Information Security Directive** (NIS 2) is a comprehensive, EU-wide cybersecurity legislation to enhance cybersecurity across the EU. The successor to the NIS Directive, it broadens the scope of the regulation to new sectors designated as critical infrastructure.
- **EU Cybersecurity Act** introduces an EU-wide cybersecurity certification framework for ICT products, services and processes and strengthens the EU Agency for Cybersecurity (ENISA).
- **Digital Operational Resilience Act** (DORA) creates a regulatory framework (a regulation and a directive) on digital operational resilience and sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT-related services to them, such as cloud platforms or data analytics services.
- **Cyber Resilience Act**: the proposal for a regulation on cybersecurity requirements for products with digital elements bolsters cybersecurity rules to ensure more secure hardware and software products. The Act aims, among others, to create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle.
- **Cyber Solidarity Act** (CSA): the proposal for a regulation aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. It foresees the creation of a European Cybersecurity Shield composed of Security Operations Centers (SOCs) across the EU as well as developing the EU's Cyber Emergency Mechanism built on three pillars: supporting preparedness through testing entities in crucial sectors, creating an EU Cybersecurity Reserve, and elaborating principles for the mutual assistance to a member States affected by a cybersecurity incident.

Another important pillar of the EU approach is strengthening cyber crisis prevention and management mechanisms. The so-called **Blueprint** adopted in 2017 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 has been strengthened with the establishment of new structures at the strategic (NIS Cooperation Group), operational (CyCLONe) and technical (CSIRT Network) levels. The EU also conducts regular cybersecurity exercises at technical, operational and strategic levels.

6. Cyberspace as a crime scene

As the nature of crime in the digital space evolves and cybercrime groups exploit 'safe havens', policy responses must address various areas, including privacy and data protection, content-related offences, economic crimes, unauthorised access, and intellectual property violations. However, there is no universally accepted definition of criminal activities in cyberspace, which can create obstacles to cooperation between states. In many national legislations, cybercrime is not strictly defined. Generally, cybercrime refers to criminal activities involving computers and information systems either as primary tools or primary targets. The decisions on which actions are criminalised in national laws and what system

of safeguards to put in place (e.g., legality, proportionality, necessity, and respect for human rights) may lead to tensions between different national legal frameworks, such as disagreements over the references and definition of terms like **'cyber terrorism'**.

Nearly all types of crime nowadays leave **digital footprints** that can serve as evidence in court proceedings, often serving as the primary leads law enforcement authorities and prosecutors can gather. However, this evidence is often stored on servers in foreign jurisdictions. Obtaining such data requires judicial cooperation and mutual legal assistance, but the process is presently slow and cumbersome. Almost two-thirds of crimes involving **electronic evidence** held in another country cannot be adequately investigated or prosecuted due to the time-consuming nature of gathering evidence or the fragmentation of legal frameworks concerning data availability and retention rules for communication service providers. Consequently, **cross-border access to data** for investigatory purposes has become a contested issue as it raises sovereignty concerns for individual states.

Encryption is another crucial aspect of criminal justice in cyberspace. While regarded as an effective means of ensuring cybersecurity, data protection, and privacy, it also poses challenges in criminal investigations. Strong encryption tools are essential for the safety of human rights defenders, journalists, opposition leaders, and civil society organisations, whose activities are often subject to online surveillance and spyware by government agencies. However, research on cryptography has shown that *'cryptography backdoors'* and exceptional access for law enforcement create opportunities for malicious intruders[35], undermine the privacy of communications, erode citizens' trust,[36] and open doors for criminal and malicious non-state actors.[37] Balancing the use of encryption while ensuring effective criminal investigations and protecting individual rights becomes a critical and complex challenge in cyberspace.

BOX 20: ESSENTIALS OF THE EU APPROACH

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'. The EU law criminalises any illegal access to information systems, system interference, data interference and illegal interception. According to the EU, cybercrime can be classified into three broad definitions:

- crimes specific to the Internet, such as attacks against information systems or phishing (e.g., fake bank websites to solicit passwords enabling access to victims' bank accounts);
- online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam, and malicious code;
- illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism, and xenophobia.

To facilitate cross-border access to e-evidence, the European Commission proposed new rules to guarantee strong protection of fundamental rights, oblige service providers to designate a legal representative in the EU and provide legal certainty for businesses and service providers. The proposed regulation on production and preservation orders establishes two new tools:

- **European Production Order** will allow a judicial authority in one EU country to obtain electronic evidence (such as emails, text or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider, or its legal representative, in another EU country.
- **European Preservation Order** will allow a judicial authority in one EU country to request that a service provider, or its legal representative, in another EU country, preserves specific data in view of a subsequent request to produce this data via mutual legal assistance, a European Investigation Order or a European Production Order.

35 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, p. 70.
36 European Union Agency for Network and Information Society (ENISA), 'ENISA's Opinion paper on encryption. Strong Encryption Safeguards our Digital Identity', Heraklion, 2016, p. 17.
37 H. Abelson et al., 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', *Massachusetts Institute of Technology*, Cambridge, 2015, p. 34.

To support law enforcement authorities dealing with the challenges of encryption and provide for the necessary human rights safeguards, the European Commission proposed a set of non-legislative measures such as strengthening the technical capabilities of Europol's Cyber Crime Centre (EC3) to deal with encryption or establishing a toolbox of legal and technical instruments. The EU also promotes the adoption of legal standards enshrined in the Budapest Convention on Cybercrime, including through cyber capacity building projects implemented by the Council of Europe with EU funding.

In an effort to counter the removal of terrorist content online and limit the spread of terrorist propaganda, instructions facilitating and directing terrorist activities, or recruitment the EU adopted the Terrorist Content Online Regulation. This law regulates the duties of care to be applied by hosting service providers (HSPs) and the measures to be adopted by the EU Member States to identify and ensure the quick removal of terrorist content online and facilitate cooperation between Member States and Europol.

7. Cyberspace as a rights-enabling field

The Internet has gradually become a crucial platform for individuals and groups to access information, express their views, and organise social, political, or religious movements, highlighting the significance of cyberspace as an enabling domain for rights. In an era where some governments consistently restrict online access and relevant rights – even shutting down the Internet – it is essential to proactively work towards ensuring that the same civil, political, economic, social, and cultural rights that people enjoy offline are also protected online. For human rights defenders, political opposition, or social movements in authoritarian regimes, anonymity online remains the only means to avoid prosecution and imprisonment. This aspect of cyberspace gains particular importance in the face of the rise of digital authoritarianism and the shrinking space for civil society engagement. Additionally, the expansion of social platforms and rapid developments in new digital technologies, such as AI, bring forth new questions regarding the promotion and protection of human rights, emphasising the importance of a human-rights based approach throughout the entire life-cycle of digital technologies (i.e., design, development, deployment, evaluation, and use).

The use of national security arguments to curb Internet freedoms has highlighted the importance of protecting human rights online. The notion of security that states prioritise does not always align with the personal safety and security of their citizens. It is therefore crucial to ensure that the use of cyberspace and digital technologies is human-centric and compliant with human rights. Legitimate actions aimed at strengthening the state's security (e.g., through new legislation or increased competencies for government agencies) may not adequately address – or in some cases, 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). The European Court of Human Rights has emphasised that governments have an obligation to protect individuals online, including through criminal law, as outlined in the Budapest Convention on Cybercrime.[38]

The protection of human rights online is closely linked to the **right to privacy and data protection**. Personal data should be safeguarded to prevent or limit adverse effects that improper or unlawful use could have on individuals, including physical, material (financial loss), or non-material (reputation, profiling) harm, or infringement on other rights (e.g., freedom of association). Privacy allows for the autonomous development of a person, both individually and socially, which is vital for democracy. Consequently, data protection and privacy are entitlements recognised and protected by domestic law, regional and international conventions, and soft law instruments (such as the Council of Europe Convention for the Protection of Individuals regarding Automatic Processing of Personal Data, the EU Charter of Fundamental Rights, and the OECD Privacy Guidelines).

38 Case of K.U. v Finland, 2 March 2009.

BOX 21: ESSENTIALS OF THE EU APPROACH

The **EU Cybersecurity Strategy** states clearly that the EU should continue to lead in the protection and promotion of human rights and fundamental freedoms online. Already in 2014, the EU adopted the **EU Human Rights Guidelines on Freedom of Expression Online and Offline** which state 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'.

The **2020–2024 EU Action Plan on Human Rights and Democracy** also includes several commitments in this field, stressing the importance of ensuring that digital technologies are human-centred and human rights compliant. To this effect, the Action Plan proposes several concrete actions focused on capacity building and effective monitoring and promoting human rights and democracy in the use of digital technologies. The EU also addresses the challenges posed by new and emerging technologies like AI or quantum by stressing the need for a **human-centric and trustworthy** innovation. To implement this vision, the EU proposed the first-ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally.

In line with the EU Action Plan on Human Rights and Democracy 2020–2024, promoting human rights and democracy in the use of digital technologies, including artificial intelligence, is one of the main priorities of EU external human rights policy. The EU efforts focus on promoting the rights to privacy and data protection and fighting mass surveillance, Internet shutdowns, online censorship, hate speech online, online gender-based violence, information manipulation and interference, including disinformation and cybercrime. The EU also supports human rights defenders (HRDs) through funding for trainings in cybersecurity and a safe digital environment.

In 2022, the EU signed the **European Declaration on digital rights and principles for the digital decade**. The document covers key rights and principles for the digital transformation, such as placing people and their rights at its centre, supporting solidarity and inclusion, ensuring the freedom of choice online, fostering participation in the digital public space, increasing safety, security and empowerment of individuals, and promoting the sustainability of the digital future.

The EU data governance framework addressing personal and other types of data aims to ensure the protection of the right to privacy in all matters related to access, collection, sharing, use and governance of data, including those related to non-personal data. Protection of personal data in the digital domain in the EU is governed by the **EU General Data Protection Regulation** (GDPR) while other types of data are regulated by the proposal for an **EU Data Act** that introduces mandatory safeguards to protect non-personal data of EU customers held on cloud infrastructures against unlawful access by non-EU/EEA authorities. The EU also remains committed to the concept of 'data free flow with trust' as the driver of innovation and business opportunities. The EU legal framework also provides protection for the data of EU citizens and companies in case of transborder data flows. For instance, the EU Data Act will introduce mandatory safeguards to protect non-personal data of EU customers held on cloud infrastructures against unlawful access by non-EU/EEAS authorities.

8. Cyberspace as an information manipulation venue

Digital information ecosystems necessitate transparency and accountability to ensure the free flow and availability of high-quality, pluralistic information. Transparency regarding the origin of information and the way it is produced, sponsored, used, disseminated, and targeted can empower citizens against information manipulation and interference, including disinformation, discrimination, online gender-based violence and harassment, and misleading content online.

The growth of online platforms with limited content controls and anonymity has made them a tool for organisations and governments pursuing specific interests, including through various forms of information manipulation (e.g., misinformation, disinformation). Such practices gained particular attention following reports of online platforms being used to manipulate domestic audiences for political gains (e.g., the Cambridge Analytica scandal) or by foreign governments to interfere in national democratic processes (e.g., presidential elections in the United States and France). Large-scale disinformation campaigns, especially when orchestrated by foreign governments, pose a significant risk to societies by polarising debates or endangering people's health or security. As a result, foreign information manipulation and interference have become crucial topics in international debates.

However, some methods adopted by governments to limit potential harm caused by disinformation may harm freedom of expression and other fundamental rights online. Some governments exploit the fight against disinformation as

an excuse to suppress political opposition, effectively limiting freedom of expression online. Instances abound of governments using disinformation as a pretext to crack down on political opponents or restrict freedom of expression online through Internet shutdowns, website blocking, or arrests for Internet activity. Moreover, the complexity and scope of challenges posed by disinformation, coupled with the responsibility for content management increasingly shifting towards the private sector, have demonstrated the need for new forms of information governance. This has led to the development of soft modes of governance (e.g., codes of conduct) or laws to address these issues.

BOX 22: ESSENTIALS OF THE EU APPROACH

The EU distinguishes between dis- and misinformation. **Disinformation** is false or misleading content that is spread with the intention to deceive or secure economic or political gain, and which may cause public harm. **Misinformation**, on the other hand, is false or misleading content shared without harmful intent though the effects can be still harmful. The aim of the EU policies in this domain is twofold. On one hand, it aims to strengthen multilateral and multi-stakeholder engagement to eliminate any content of discriminatory, false or misleading nature at all levels. On the other hand, it promotes transparent and accountable content governance models that protect freedom of expression and enhance the availability of accurate and reliable information in the public sphere with full respect for human rights.

In 2018, the European Commission presented the **Communication on tackling online disinformation** which outlines the key overarching principles and objectives to tackle this phenomenon effectively. Among others, the Communication provides concrete recommendations to improve transparency regarding the origin of information and the way it is produced, sponsored, and disseminated, as well as ways to promote diversity of information and foster its credibility.

The 2018 **Action Plan Against Disinformation** provides a set of initiatives to build up capabilities and strengthen cooperation between Member States and EU institutions to proactively address disinformation. It focuses on 1) improving detection, analysis and exposure of disinformation; 2) stronger cooperation and joint responses to disinformation; 3) mobilising the private sector to tackle disinformation; and 4) raising awareness and improving societal resilience. In 2022, major online platforms, emerging and specialised platforms, and other stakeholder groups (e.g., players in the advertising industry, fact-checkers, research and civil society organisations) delivered a strengthened **Code of Practice on Disinformation**.

Finally, to address more effectively the challenge of accountability online for illegal and harmful content, the EU adopted the **Digital Services Act (DSA)** that rebalances the rights and responsibilities of users, online intermediaries (including online platforms), and public authorities. The DSA contains EU-wide due diligence obligation that applies to all digital services that connect consumers to goods, services, or content. It proposes new procedures for faster removal of illegal content and comprehensive protection for users' fundamental rights online.

Regarding the role of disinformation in the EU's foreign and security policy, the 2022 **Council Conclusions on foreign information manipulation and interference (FIMI**) address the misuse of the Internet by foreign actors to destabilise the EU's democratic societies, create or exploit societal frictions, or negatively affect the EU's ability to conduct foreign and security policy.

9. Cyberspace as a diplomatic arena

The increasing number of countries interested in shaping Internet governance has given rise to different, sometimes conflicting, visions of cyberspace. While all countries generally agree on promoting open, global, free, safe, and secure cyberspace in principle, their interpretations of these terms may not always align in practice, often influenced by national sovereignty concerns. This divergence is evident in international debates on the future of cyberspace, particularly in UN processes such as the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG) and the UN Global Digital Compact. As the malicious use of cyberspace by state and non-state

actors poses risks of miscalculation and conflict, the need to prevent conflicts through the responsible use of ICTs and strengthen accountability mechanisms for non-compliant actors has become apparent. Consequently, cyber and digital diplomacy have emerged as crucial components of foreign and security policies.

Cyber diplomacy's primary focus has been on developing and reinforcing the framework for responsible state behaviour in cyberspace. Since 1998, the United Nations has served as the main platform for discussions, leading to the adoption of several reports that established four pillars of the framework:

1. **Application of existing international law in cyberspace**: While there is a consensus that existing international law, including the UN Charter, applies in cyberspace, countries still disagree on how it applies and the parameters to be used. One significant debate concerns the application of International Humanitarian Law in cyberspace, with some countries viewing it as an attempt to normalise the militarisation of cyberspace. Legal scholars involved in initiatives like the Tallinn Manual, or the Oxford Process aim to provide more clarity on these issues.

2. **Voluntary and non-binding norms, rules, and principles**: This set of 11 norms, agreed upon by states, provides overarching guidance for responsible state behaviour in cyberspace. The norms are either cooperative or prohibitive in nature, and cover areas such as threats to critical infrastructure or cooperation among Computer Emergency Response Teams (CERTs). Their voluntary and non-binding nature is seen as a limitation on the framework's effectiveness, leading countries to develop alternative arrangements, including targeted sanction regimes.

3. **Confidence-Building Measures (CBMs)**: CBMs are transparency, cooperation, and stability measures that can contribute to preventing conflicts, avoiding misperceptions and misunderstandings, and reducing tensions resulting from activities in cyberspace. While CBMs cannot fully prevent or mitigate intentional conflicts among states, they are expected to help states avoid conflicts arising from misunderstandings or unintentional activities. Examples of CBMs include establishing points of contact networks, exchanging information about the designation of critical infrastructure and national cybersecurity strategies, or creating mechanisms for cooperation among CERTs.

4. **Capacity building**: This pillar aims to close existing capacity gaps and support states in implementing the framework for responsible state behaviour in cyberspace. It involves various activities to help countries develop the skills, human resources, policies, and institutions necessary to enhance their cyber resilience and security, thus enabling them to fully benefit from digital technologies. The recent focus on cyber diplomacy capacity building responds to the need for strengthening states' capacities to adhere to international law and implement norms and CBMs for the peaceful use of cyberspace.

Until 2025, discussions about the framework continue in the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG). However, in November 2022, the UN adopted a resolution on the **Programme of Action** (PoA) to advance responsible state behaviour in the use of ICTs in the context of international security. The aim is to establish the PoA as a single, long-term, inclusive permanent UN forum with a progress-oriented format.

BOX 23: ESSENTIALS OF THE EU APPROACH

The primary objective of the EU's cyber diplomacy 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.

The scope of the EU's cyber diplomacy is outlined in the **Council Conclusions on Cyber Diplomacy** adopted in 2015, 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 and strategic engagement with key partners and international organisations.

The 2020 **EU Cybersecurity Strategy** mentions cyber diplomacy as one of the approaches to prevent, deter, and respond to cyberattacks, including through the 2017 framework for a joint EU diplomatic response to malicious cyber activities, the **Cyber Diplomacy Toolbox.** The existing options for action include statements by the Council and High Representative, formal Council Conclusions, formal requests for technical assistance through diplomatic channels, diplomatic demarches, signalling through dialogues and restrictive measures, among others. These measures should encourage cooperation, help mitigate threats and deter potential aggressors in the long term. The Strategy also acknowledges that the EU should develop and implement a coherent and holistic international cyber policy. A step in this direction was taken in 2022 with the adoption of the **Council Conclusions on the development of the European Union's cyber posture** by enhancing the EU's ability to prevent cyberattacks through capacity building, capability development, training, exercises, enhanced resilience and by responding firmly to cyberattacks against the EU and its Member States using all available EU tools.

Recognising the growing importance of technology and digital transformation as part of geopolitical competition within the international system, the EU adopted in 2022 **Council Conclusions on digital diplomacy**. The document stresses the need for a more concerted effort to promote technological solutions and regulatory frameworks that respect democratic values and human rights, including through capacity building. The EU will actively promote universal human rights and fundamental freedoms, the rule of law and democratic principles in the digital space and advance a human-centric approach to digital technologies in relevant multilateral fora and other platforms.

10. Cyberspace as a battlefield

Malicious behaviour in cyberspace, carried out by state actors or their proxies, poses a threat to the rules-based international order, effectively turning cyberspace into another contested domain, alongside land, sea, air, and space. The rise in cyberattacks targeting military actors and civilian critical infrastructure, with the potential for destructive effects and human cost, has elevated cyber defence as a crucial aspect of cyber policies, along with considerations related to economy, crime, development, and diplomacy.

While the term "cyber defence" is often used broadly to describe efforts aimed at strengthening preparedness and responding to cyber incidents, both public and private, it is essential to recognise that its strict interpretation pertains exclusively to the protection of military assets and a state's territorial integrity, primarily through military means. In practice, making this distinction becomes more complex, particularly as military infrastructure often relies on off-the-shelf solutions from the private sector and civilian networks (e.g., energy, transportation, telecommunication). Consequently, clarifying the nature of **civil-military relations** in cyberspace is crucial. It necessitates further analysis of a state's right to store vulnerabilities (commonly referred to as "cyber weapons") that could be used against other states or non-state actors and the resulting obligations in case of damage caused.

The discussion about cyber defence is closely tied to the concept of **stability in cyberspace**, particularly concerning the rights and obligations of states as outlined in the UN Charter. These include the right to self-defence in the event of an armed attack (Article 51) and the obligation to refrain from the threat or use of force against the territorial integrity or

political independence of any state (Article 2). One of the most contentious issues in this realm has been the application of **international humanitarian law** (IHL), which dictates rules for protecting civilians, civilian infrastructure, and civilian data against cyber harm.

In addition to cyber defence, the concept of **hybrid threats and warfare** comes into play when malicious activities occur below the threshold of armed conflict and exploit grey areas in existing international norms and laws. These hybrid threats involve a combination of conventional and unconventional, military and non-military, overt and covert actions orchestrated by state or non-state actors to achieve specific objectives while avoiding formal declaration of warfare. Foreign Information Manipulation and Interference (FIMI) and cyberattacks are often employed in this context.

BOX 24: ESSENTIALS OF THE EU APPROACH

Russia's unjustified and unprovoked military aggression against Ukraine – including using offensive cyber operations – has reemphasised the need for a common EU approach to cyber defence. The **Strategic Compass for Security and Defence** approved by the Council in March 2022 recognised such a need and the new **EU Policy on Cyber Defence** was presented in November 2022. The approach adopted by the EU is built around four pillars aimed to support the EU and Member States in detecting, deterring, and defending against cyberattacks. These pillars are: 1) acting together for a stronger EU cyber defence; 2) securing the defence ecosystem; 3) investing in cyber defence capabilities; and 4) partnering to address common challenges. Better cooperation between the military and civilian actors is the common thread running across all these pillars

Cyber defence was also integrated into the **Capability Development Plan** by the European Defence Agency, with several projects launched to this end. 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 others. In March 2018, the Council adopted 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.

In the context of cyber defence, cooperation between the **EU and NATO** is particularly important. A joint EU-NATO Declaration signed in January 2023 reinstated the commitment to cooperation on cyber defence. The ongoing work focuses on the implementation of proposals put forward following the 2016 Warsaw Summit, including the exchange of concepts on the integration of cyber defence aspects into the planning and conduct of missions and operations. The EU and NATO staff maintained regular contact and information exchanges on respective cyber activities, including policy developments. Both sides also increased cooperation on cyber exercises and continued to implement the **Technical Arrangement on Cyber Defence** between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU).

Insofar as countering hybrid threats relates to national security and defence, the primary responsibility lies with the Member States, as most national vulnerabilities are country-specific. However, in the Strategic Compass for Security and Defence, Member States agreed to establish an EU Hybrid Toolbox, which comprises preventive, cooperative, stability-building, restrictive and support measures. As an overall framework, the Hybrid Toolbox brings together other relevant response mechanisms and instruments, such as the Cyber Diplomacy Toolbox and the Foreign Information Manipulation and Interference (FIMI) Toolbox. These developments built on the 2016 **Joint Framework on Countering Hybrid Threats** and the 2018 **Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats**. The EU's response is based on four main pillars: developing situational awareness to enhance common strategic culture; strengthening resilience to hybrid operations; Response options can range from diplomatic engagement, CSDP and crisis response mechanisms, to rapid response teams and restrictive measures; cooperation with international partners and organisations as well as with other stakeholders from civil society.