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

A Playbook

International Cooperation and Development

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

print	ISBN 978-92-9198-753-5 QN-02-18-916-EN-C DOI:10.2815/607762	online	ISBN 978-92-9198-754-2 QN-02-18-916-EN-N DOI:10.2815/18222

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

PRINTED ON RECYCLED PAPER

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

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

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

CONTENTS

ABOUT THIS PLAYBOOK

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

Why is the operational guidance needed?

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

The **Operational Guidance** is intended to provide a comprehensive practical framework when designing and implementing the EU's external actions against cybercrime and for promoting cybersecurity and cyber resilience. The Operational Guidance is meant to serve as a resource for EU staff in headquarters and delegations as well as Member State services and implementing partners involved in cyber capacity building. The **methods and frameworks** proposed in the operational guidance should be used to:

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

The Operational Guidance, which was used as the basis for this Playbook, is organised into three main parts:

- Part I, '**A guide to cyber-related concepts and policy developments**', aims to provide an overview of the evolution of cyber-related policies and concepts internationally and in the European Union.
- Part II, '**A framework for the EU's external cyber capacity building'**, gives an overview of the approach and concrete steps that together form a framework for cyber capacity building; and
- Part III, '**Practical application of the framework to specific pillars**', illustrates how the proposed framework can be employed in four specific areas (independently or in combination): national strategic frameworks, cyber incident management, criminal justice in cyberspace, and cyber hygiene and awareness.
  The Operational Guidance also proposes several **tools** that suggest concrete questions, check lists or steps to follow in each stage of the cyber capacity-building intervention. This Playbook lists only some of them.

The playbook approach

This Playbook was written as an **actionable summary** of the **Operational Guidance for the EU's international cooperation on cyber capacity building**. As such, it provides a quick overview of the main steps to follow and key challenges to take into consideration when designing and implementing cyber capacity-building interventions. This playbook, however, does not replace the Operational Guidance but is rather meant as a **navigation map** for issues explored in the main document.

FIGURE 1: Overview of the Operational Guidance for the EU's international cooperation on cyber capacity building

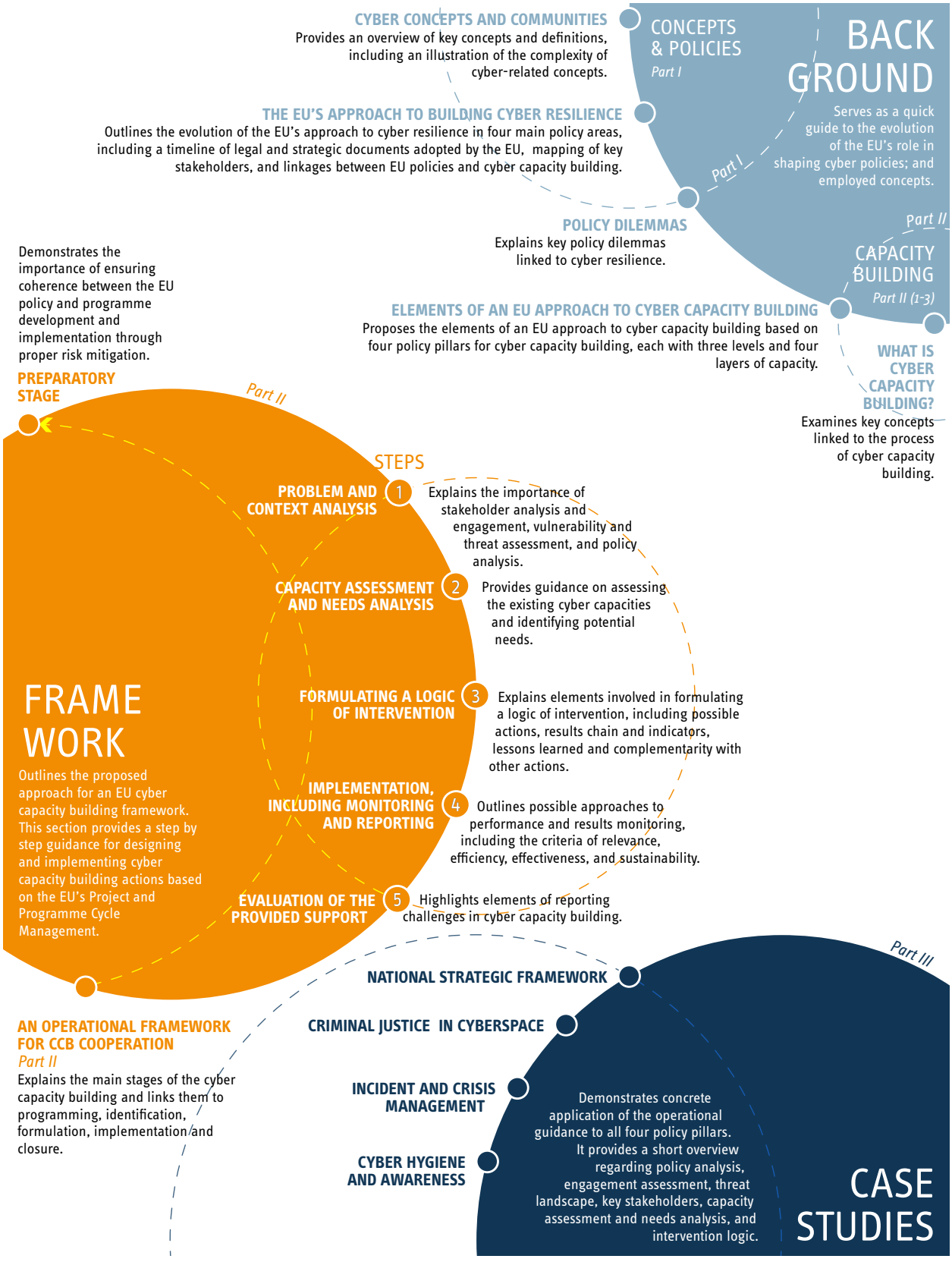
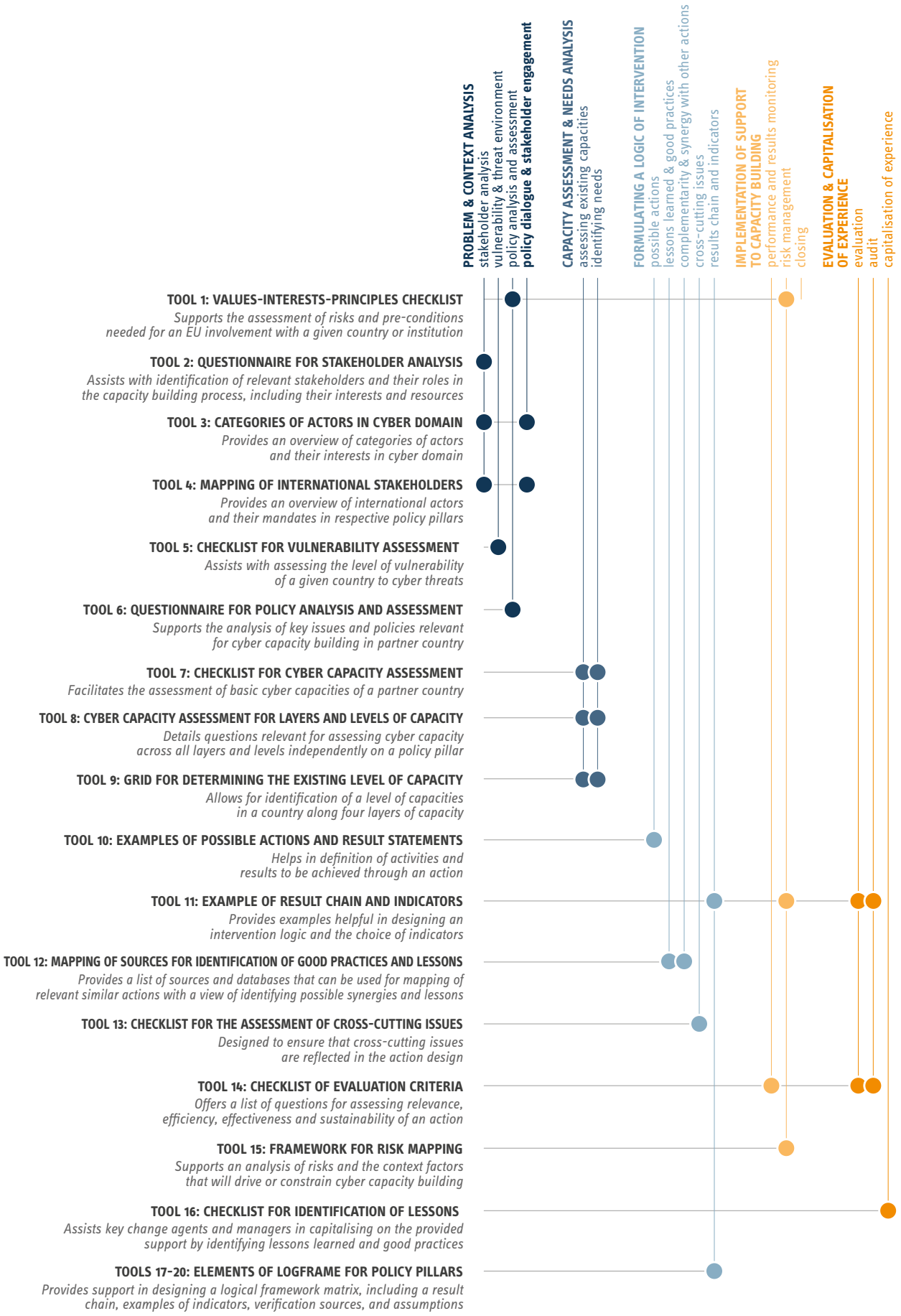


FIGURE 2: List of tools for cyber capacity building proposed in the Operational Guidance



WHAT DOES 'CYBER' MEAN?

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

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

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

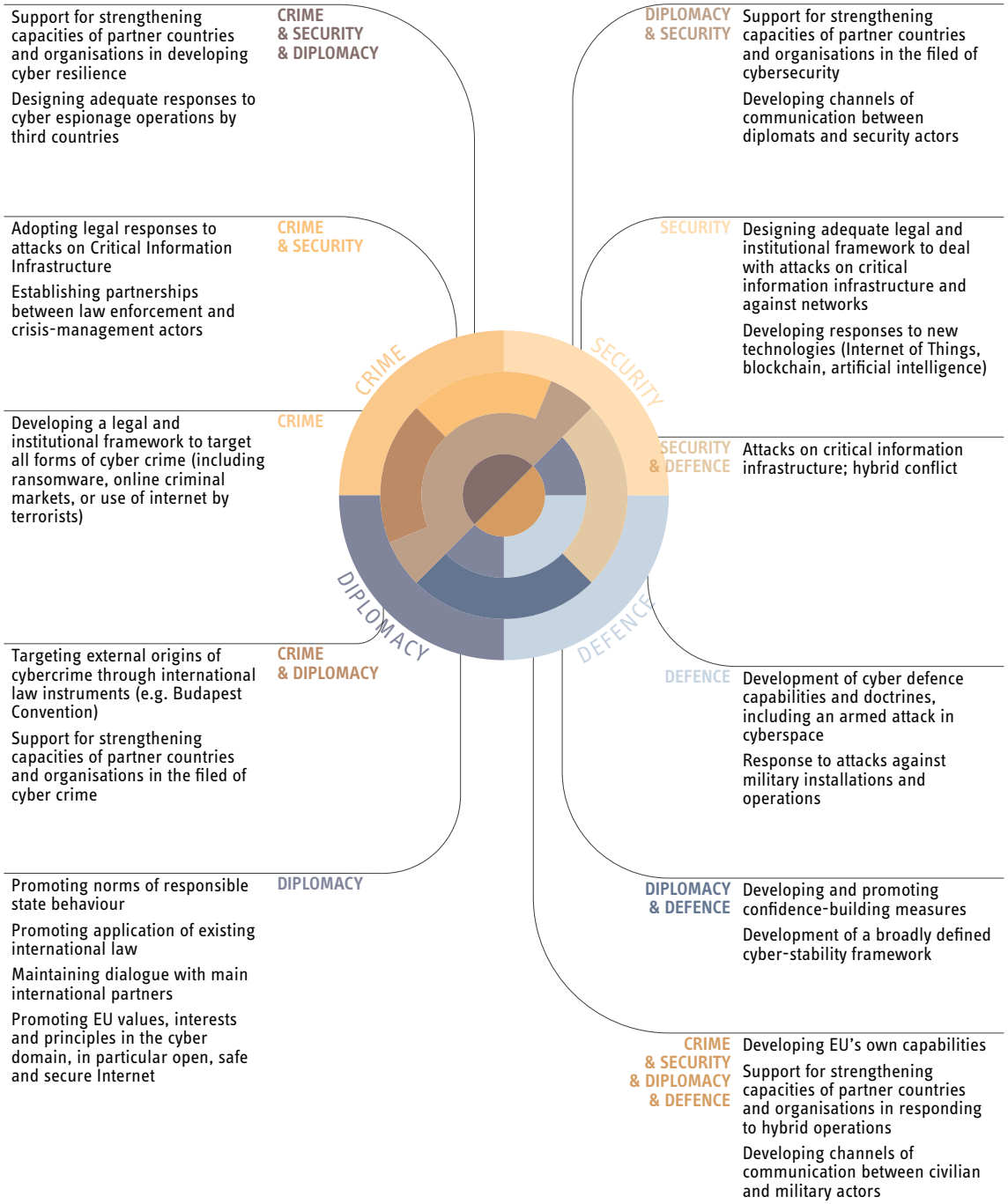
BOX 1: CYBER-RELATED DEFINITIONS

- **Cyberspace** is a 'man made global strategic domain (...) consisting of the interdependent network of information technology infrastructure and resident data, including the internet, telecommunications network, computer systems, and embedded processors and controllers for the production and use of information by individuals and organisations' (Fiddner, 2015).
- **Cybersecurity** commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.
- **Cybercrime** commonly refers to a broad range of criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).
- **Cybersecurity capacity building**: all types of activities (e.g. human resources development, institutional reform or organisational adaptations) that safeguard and promote the safe, secure and open use of cyberspace (Pawlak, 2015).

ADDITIONAL INFORMATION

Part I of the Operational Guidance – **'A guide to cyber-related concepts and policy development'** – explains in more detail the growing importance of cyberspace for numerous policy areas, including development, security, justice, home affairs, diplomacy, and defence. It also addresses main overlaps and differences between concepts used in numerous policy documents (see Figure 3).

FIGURE 3: Complexity of cyber-related concepts



ADDITIONAL INFORMATION

Part I of the Operational Guidance also provides an extensive summary of the main policy developments in the EU. This section of the document gives an overview of the main legislative and strategic documents adopted by the European Union, an overview of actors shaping this policy area in the EU, as well as numerous practical examples. It is a must-read for anyone interested in the EU's cyber-related policies.

WHAT IS THE EU'S APPROACH TO EXTERNAL CYBER CAPACITY BUILDING?

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

Evolution of the EU's approach

The foundations for the EU's involvement in external cyber capacity building were laid down in the 2013 **EU Cybersecurity Strategy** which defined it as a strategic building block of the EU's international engagement. The 2015 **Council Conclusions on cyber diplomacy** further reinforced the idea that international cooperation and assistance in the field of cyber capacity building is needed to strengthen cybersecurity and the fight against cybercrime. The main aspects highlighted in the Council Conclusions include:

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

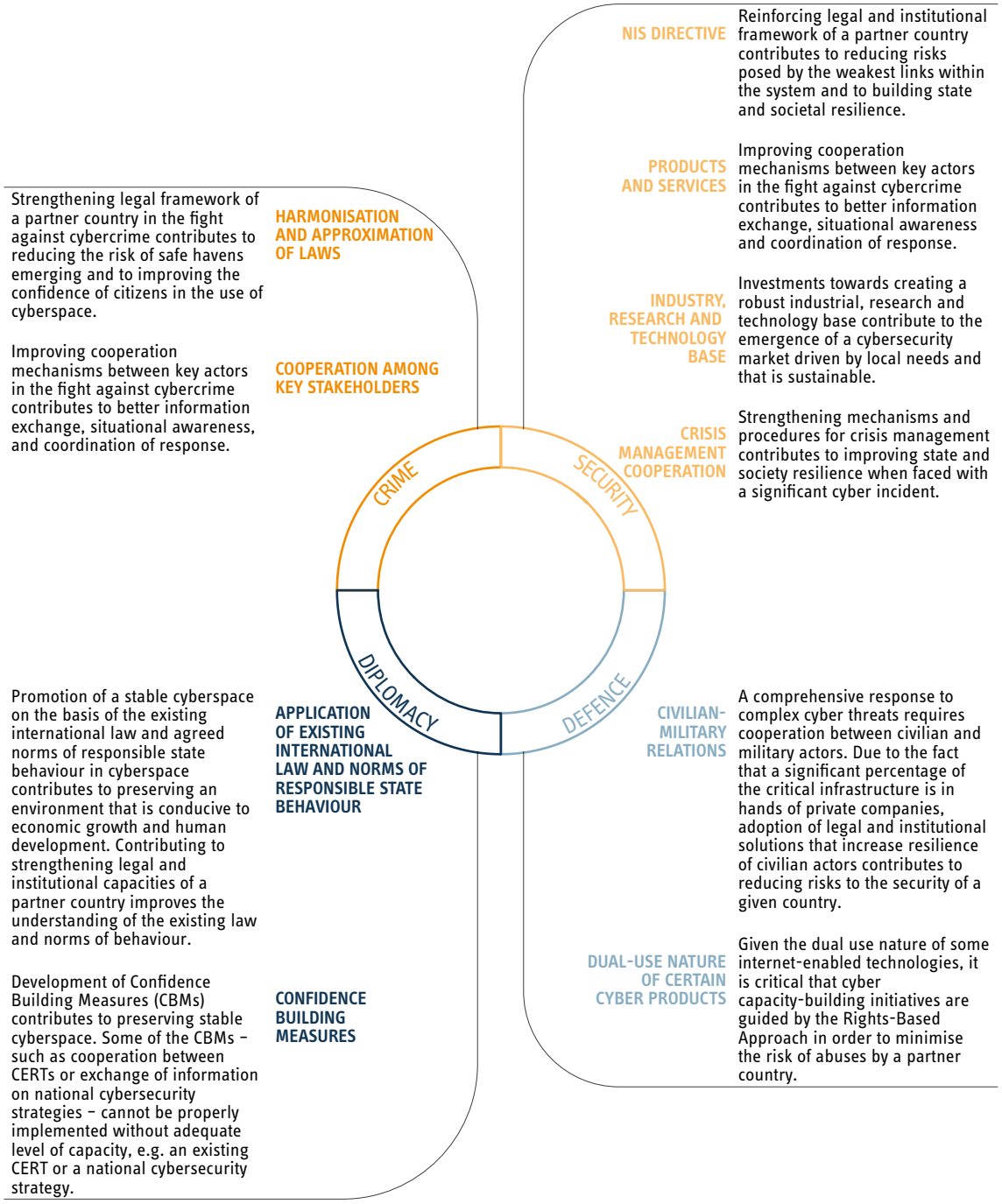
This position has been reaffirmed in the 2017 **Joint Communication on resilience, deterrence and defence: building strong cybersecurity for the EU** which acknowledges that CCB efforts contribute to meeting the EU's development commitments and to increasing the level of cybersecurity globally.

Strategic importance of cyber capacity building

In order to offer political guidance to the EU and to Member States, the Council adopted in June 2018 **Conclusions on EU external cyber capacity-building guidelines.** The Council Conclusions identify the key policy objectives of the EU's external CCB efforts, most notably:

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

FIGURE 4: Linkages between policies and cyber capacity building



ADDITIONAL INFORMATION

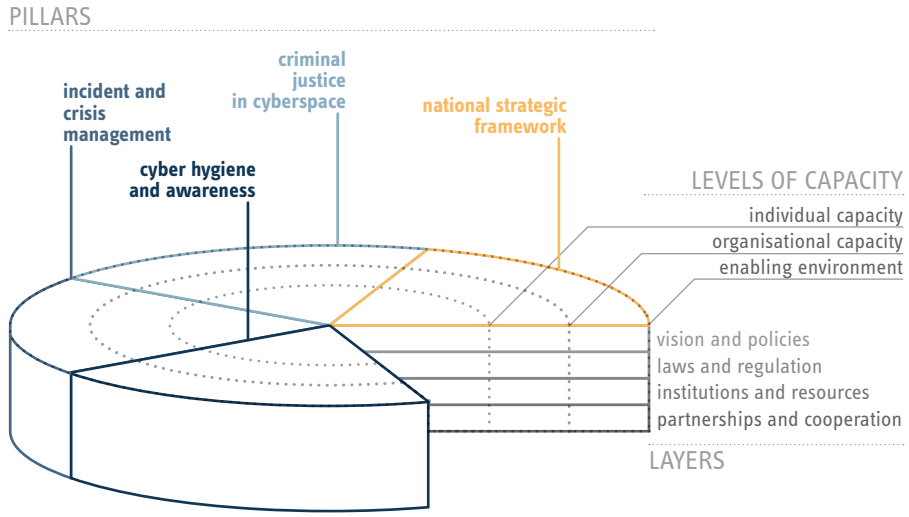
Part I – 'A guide to cyber-related concepts and policy development' – concludes with the analysis of key policy dilemmas linked to cyber capacity building: **security and human rights**; **sovereignty and governance**; **accountability and transparency**; and **innovation, growth, and security**. It is an important section for anyone interested in understanding some of the key debates in this dynamic policy area, including about the use of encryption, data protection, disinformation, or 'hacking back'.

POLICY PILLARS OF CYBER CAPACITY BUILDING

Cyber capacity-building interventions start most of the time with the selection of a policy area or policy areas to be supported. Taking into account the EU's current practice in cyber capacity building and drawing comparisons with approaches adopted by other organisations or countries, the Operational Guidance proposes a framework for cyber capacity building that is based on three main elements:

- **Pillars of cyber capacity building** – the main policy areas in which the support is usually provided: national strategic framework, incident management, criminal justice in cyberspace, and cyber hygiene and awareness;
- **Levels of cyber capacity building** – defining the target of a cyber capacity-building action or programme: individual, organisational and the enabling environment; and
- **Layers of cyber capacity building** – focusing on specific aspect of cyber capacity building: vision and policies, laws and regulation, institutions and resources, partnerships and cooperation.

FIGURE 5: A 'cake' approach to cyber capacity building: pillars, levels, and layers



Each of these aspects is addressed in more detailed in the Operational Guidance. For the purpose of this Playbook, it is important to describe in more detail possible areas for cyber capacity-building interventions in partner countries:

National strategic framework

Developing a national strategic framework remains a key enabler for building cyber resilience and tackling cyber threats. The aim of national strategic frameworks is to ensure that emerging cybersecurity-related challenges, such as critical infrastructure protection, online criminal activity and skills gaps, are addressed in a comprehensive and coherent way. Many states have adopted different approaches to a strategic framework, often in the form of a national cybersecurity strategy document that establishes a range of objectives and priorities to foster cyber resilience (ENISA, 2017). An effective strategic framework has to be malleable to distinctive political and regulatory environments. It does so whilst developing the overarching aims, means, and responsibilities used to define the basic institutional structure that could accommodate for the development of a cybersecurity ecosystem and its governance framework. The strategic framework must be flexible and actionable, with periodic reviews that contribute towards recalibrating the strategic outlook and

accounting for evolving threat landscapes. In practice, this would translate to specific and time-bound action plans or road maps with concrete implementation steps.

Criminal justice in cyberspace

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

Incident and crisis management system

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

Cyber hygiene and awareness

The human factor is often the weakest link in cybersecurity, whether this concerns design thinking or individual responses to cyber attacks such as ransomware or social engineering (Boulton, 2017). Awareness-raising through media campaigns and civic engagement will allow for a greater level of cyber hygiene as well as foster an inclusive cybersecurity culture. Ensuring effective cyber awareness and hygiene vertically across all layers of society and horizontally, including individuals, organisations and communities, is also a key ingredient for cyber resilience. A cyber-savvy workforce is more resistant to cyber threats than one where expertise is fragmented. A combined public and private effort to raise awareness, promote internationally agreed technical standards, and share best practices helps to bridge the gap between top-down, high-level policy guidance with experience across business sectors of companies that deal with cyber threats on a daily basis. Overall, cyber awareness and hygiene aims to inform and educate users and organisations on how best to mitigate cyber threats. Knowledge and skills should be shared and pooled among actors and sectors to ensure a sufficient level of understanding.

ADDITIONAL INFORMATION

Part II of the Operational Guidance – **'A cyber capacity-building framework for the EU' –** moves away from the broad policy discussions to a more focused analysis of capacity-building terminology and approaches, in particular in the context of cyber-related policies. In addition to a detailed discussion of the key capacity-related concepts, part II contains **several tools** and **practical examples** illustrating how cyber capacity building is done in practice. Even though this Playbook provides an abbreviated step-by-step version of the process, we do advise using the full Operational Guidance as a background document as it provides a more nuanced discussion on issues signalled in the Playbook.

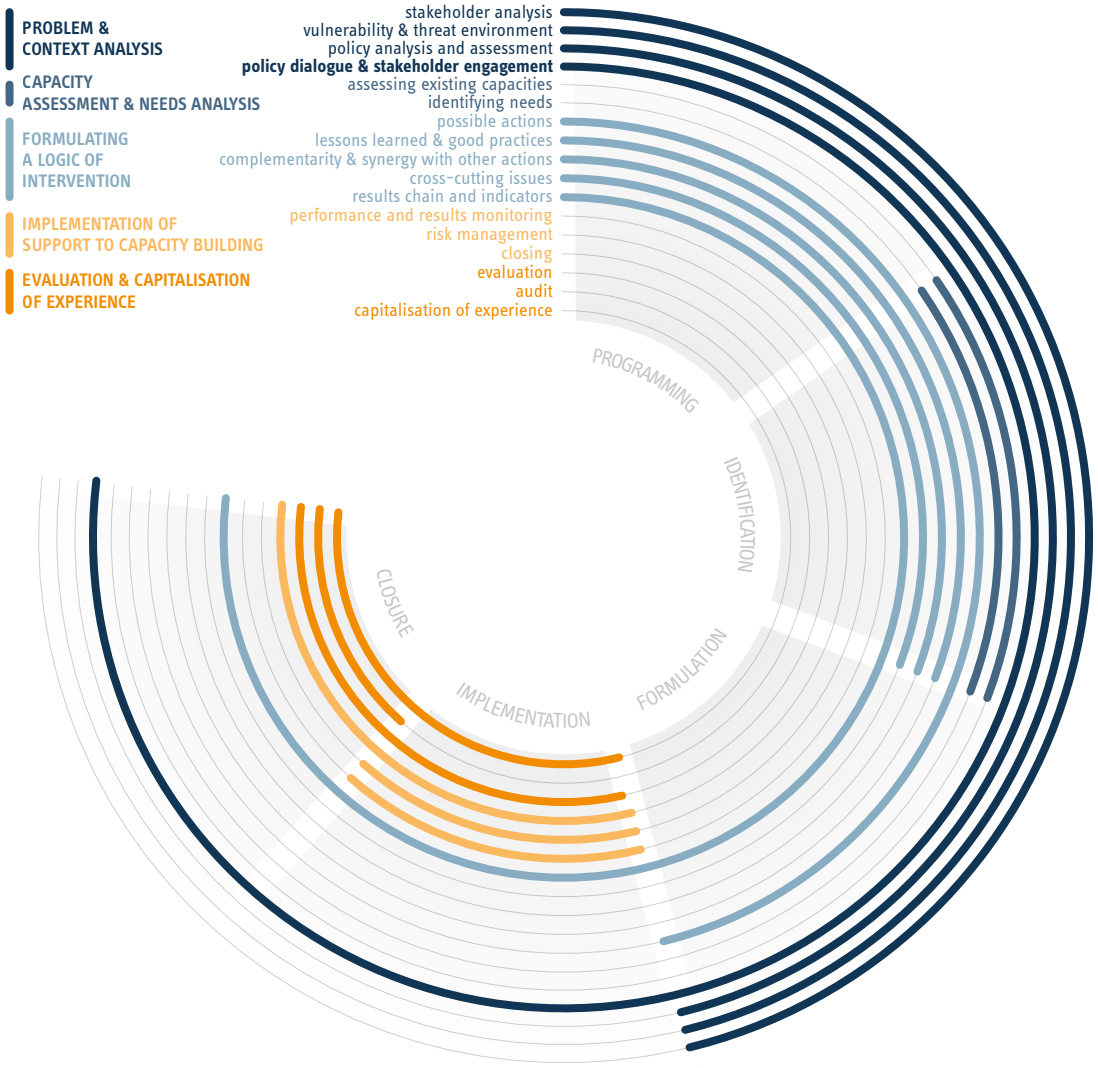
AN OPERATIONAL FRAMEWORK FOR CYBER CAPACITY BUILDING

After a policy pillar/pillars of an intervention is/are chosen, it is time to move **from a general idea to a design and implementation** of the support to cyber capacity building. This process – based on the EU's Project and Programme Cycle Management (PPCM) – is organised in several stages (see Figures 6 and 7) addressing specific questions:

- **Problem context and analysis** – What is the goal of capacity building? Cyber capacity for what?
- **Capacity assessment and needs analysis** – Do the existing capacities help to achieve this goal?
- **Formulating the logic of intervention** – What change is needed to achieve a desired level of capacity? How do we achieve the intended change?
- **Implementation of support to capacity building** – How will the change process be delivered?
- **Evaluation and capitalisation of experience** – How will the delivered support nurture future thinking about cyber capacity building?
- It is important to keep in mind that cyber capacity building is a continuous process and that boundaries between respective stages are not always that clear (see Figure 6).

While the process of cyber capacity building might seem complicated at first sight, the **checklist** below offers useful guidance on what questions should be answered at each of the stages. **Practical guidelines** listed below (Box 2) provide further information about the overall process of capacity building.

FIGURE 6: Cyber capacity building in the Project and Programme Cycle Management



BOX 2: PRACTICAL GUIDELINES ON CAPACITY BUILDING

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

FIGURE 7: Checklist for cyber capacity-building stages

Before you begin – Consider pros and cons of the intervention

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

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

- **Value-based dimension** – The CCB initiatives are not implemented in a vacuum. Any EU engagement with third countries and regions needs to ensure the respect for EU values as identified in the Treaties, EU policy documents and other international documents endorsed by the EU and its Member States. While different policies and policy communities may be driven by their own distinct value systems, it is important to ensure that all EU CCB engagements with third countries/partners meet at least the minimum threshold of respecting, protecting, upholding and enabling human rights as well as promoting peaceful coexistence in cyberspace.
- **Interests-based dimension** – Most projects are driven by a developmental logic that has for an objective supporting the progress of a partner country or region. But in some instances, EU interests are included among the criteria for prioritisation, in a clear recognition that cybersecurity capacity building is rarely a one-way exercise. More often than not, CCB actions are launched to achieve a specific result – such as reducing cybercrime or strengthening the protection of critical infrastructure in a partner country – as a means towards also improving the EU's own security. By the same token, the EU may decide not to act if the action in question might undermine EU values.
- **Principles-based dimension** – The EU's CCB actions and their implementation take into account approved and tested guiding principles under each of the logics mentioned earlier. This aspect is particularly important as it determines how the value-based and interest-based approaches are operationalised in practice.

BOX 3: PRINCIPLES FOR THE EU'S EXTERNAL CYBER CAPACITY-BUILDING INITIATIVES

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

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

Source: Council Conclusions on EU external cyber capacity-building guidelines.

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

Values

Global, open, free, stable, secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply to social well-being, economic growth, prosperity and intergrity of all free and democratic societies.

Interests

Sustainable development, security, inclusive growth and societies, digitalisation, promotion of EU norms and values, strengthening resilience.

Principles

Ownership, result-orientation, sustanability, partnership, shared responsability, transparency and accountability, human rights offline and online, bridging digital security dividie, state responsability and respect for international law.

LAYERS OF CAPACITY

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

ASSESSMENT CHECKLIST

visions and policies	laws and regulations	institutions and resources	partnerships and cooperation
> What is the overall political situation in a country, in particular its attitudes and practice towards international humanitarian law, human rights, the rule of law, effective democratic oversight and accountability? > Are the country's policies compatible with EU values, interests and principles?	> Is it possible that the provided support might directly or significantly contribute to: use of the death penalty; unlawful or arbitrary arrest or detention; torture; unfair trial or denial of justice; unlawful interference with democratic rights; persecution on grounds of religion, race, gender, ethnicity or sexual orientation?	> Are there any human rights concerns about the institutional partner that will participate in the project/programme? > What accountability and transparency mechanisms are in place?	> Are there any justified concerns about linkages between the country/institution that will participate in the programme and cybercrime groups or organised crime networks in general?

QUESTIONS

> Are there any reputational or political risks as a result of the delivery of the project or programme?

> Are the EU's interests, values, and principle reflected and protected throughout the delivery of the project or programme?

IF THE ASSESSMENT IS THAT...

> There are no concerns with the country / institution; > There is less than serious risk of a direct or significant impact of the action on human rights; and/or > The EU's values, interests and principles are reflected and protected.	> There is some reputational or political risk for the EU to work with a country / specific institution; > There is a potential risk that the assistance might directly or significantly contribute to the violation of human rights; and/or > The EU's values, interests and principles might be adversely affected by the project/programme; but can be mitigated effectively.	> There is serious reputational or political risk for the EU to work with a country / specific institution; > There is a serious risk that the assistance might directly or significantly contribute to the violation of human rights; > The EU's values, interests and principles will be adversely affected by the project/programme; and > The mitigation measures will not be effective.

...THEN

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

Step one – Analyse the problem and context of the intervention

No organisation or network of organisations functions without constantly being influenced by the context and at the same time influencing it (European Commission, 2005). With the increasing presence of cyber-related topics in international discussions and a growing focus on digitalisation for development, issues linked to cyber-resilience are also entering the agenda of the development community and international cooperation. Nonetheless, any engagement on cyber-related aspects needs to be preceded by an in-depth analysis of the policy context in a given country and region and an assessment of the relevance of these issues for achieving the country/regional developmental goals. A thorough understanding of the context requires mapping and analysis of sectoral and other relevant policies, institutions and stakeholders, with the goal of focusing on priority areas and/or problems to be addressed. That implies that, in line with the EU's own guidelines, a decision about engagement should reflect and be consistent with national/regional development plans and priorities and strategies of partners as well as EU policy objectives as expressed in various strategies and programming documents.

Stakeholder analysis and engagement

Stakeholders are the individuals, groups or organisations that have an interest in, influence or are influenced by the activity of the cooperation partner or the problem that the EU contribution intends to solve or reduce (Schulz et al., 2005). Stakeholders may also include governmental actors such as ministries and the private sector, community representatives and civil society organisations. Engagement of stakeholders should take place through all stages of the project. Some activities that help to ensure meaningful engagement include consultative processes, communication concerning initiatives, dialogue and coordination efforts (European Commission, 2015). A key component of the context analysis is a thorough mapping of stakeholders who shape developments in cyber-related sectors and who are affected or might be affecting the change process. This aspect of project design/implementation is particularly relevant in the case of cyber-related initiatives due to the focus on a multi-stakeholder approach to internet governance. The multi-stakeholder nature of internet governance is a recurrent theme in many policy documents and has been addressed at length by analysts and researchers. The internet was developed and operates across borders with input from the public and private sectors, academia and civil society, harnessing the expertise of each. So the multi-stakeholder approach is widely accepted as the optimal way to make policy decisions for a globally distributed network (Internet Society, 2016).

TOOL 2. QUESTIONNAIRE FOR STAKEHOLDER ANALYSIS

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

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

Vulnerability and threat environment

Given a rapidly evolving security context and competing developmental objectives, cyber-related security concerns are not always adequately addressed in development plans and strategies (ENISA, 2016). The systematic analysis of the cyber environment is challenging and requires significant resources, so the quality of intelligence varies depending on countries and regions. While assessing vulnerabilities and threats is complex, there are certain questions that might provide a good understanding about the situation in a given country (see Tool 5). With the issue gaining traction in the international debates, one cannot exclude situations where requests for support are motivated less by a genuine need and threat assessment than a politically motivated priority setting. Such requests may be also driven by misplaced policy objectives whereby a focus on incident management, for instance, might jeopardise attention to the developmental nature of the capacity-building projects. It is therefore essential that the EU has a well-developed understanding of the situation in a country.

TOOL 5. CHECKLIST FOR VULNERABILITY ASSESSMENT

What is the level of internet penetration?

It allows one to understand how many individuals are potentially exposed to cyber threats and what the potential cost to society could be. Statistics on the number of users, households and types of connection are collected by the ITU and are available on their website (ITU, 2017).

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

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

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

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

What are the main risks and threats in cyberspace?

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

Policy analysis and assessment

A thorough policy analysis and assessment is a prerequisite for an adequate identification of the needs of a country or a region (See Tool 6). Its ultimate objective is to help determine what would be the most effective way of providing support to a partner country/region. Even if cyber-related elements are included in the development programmes, they need to be assessed against the overall national development plans and strategies. This is important to ensure credibility, relevance and sustainability of a given project or programme. For instance, an engagement with a partner country aimed at improving the competence of law enforcement officials with regard to handling electronic evidence and addressing cybercrime might be important for a

country with a rapidly growing online presence, but it needs to be embedded in a broader developmental plan to strengthen good governance and the rule of law or to contribute towards economic development. In other words, only cyber capacity-building engagements designed with a structured reform outlook, expressly to contribute towards broader developmental goals, have a chance of having a meaningful impact.

Policy dialogue and engagement

Policy dialogue is part of the development assistance toolkit that aims to support a partner's domestic reforms. It complements financial support and technical assistance to achieve results and accountability. It is long term and runs throughout the programme cycle. The main purpose of the dialogue is to explore issues of mutual importance, measure opinions and build shared understandings based on mutual respect, sincerity, openness and freedom of expression (Schulz et al., 2005).

TOOL 6. QUESTIONNAIRE FOR POLICY ANALYSIS AND ASSESSMENT

What are the policy objectives?

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

Is the policy relevant?

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

Is the public policy credible to national and international stakeholders?

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

Is local ownership assured?

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

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

What are the existing institutional capacities?

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

Do sector coordination mechanisms exist?

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

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

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

One key challenge in the area of cyber capacity building is to ensure that dialogue is established with the right partners, i.e. those sections of the government responsibile for a specific aspect of cyber policy. There are no one-size-fits-all solutions and institutional arrangements are often made on the basis of historical or political experiences. For example, whereas in some countries the Ministry of Defence might be responsible for cyber-policy coordination – including crime and security – in others its role might be strictly limited. This step is later supported through the stakeholder analysis. Joint learning with other organisations and exchange of information with other donors is indispensable (SIDA, 2005).

Step two – Understand what capacities are needed

Once the public policy and context are better understood, the next step is to define specific objectives of a possible intervention and assess the capacities required to achieve them. Broadly speaking, capacity can be defined as the ability to perform tasks and produce outputs, to define and solve problems and make informed choices (European Commission, 2005). Capacity building is hence the process by which people and organisations create and strengthen these abilities over time. Because capacity building should be inherently a domestically driven process, external donors and partners can only provide support, meaning the inputs and processes to catalyse or support the capacity of people, an organisation or a network of organisations (e.g. in a sector) (European Commission, 2005). Part of the capacity assessment is identifying the capacity gap – the difference between existing capacities and those needed to attain the identified objectives. Ideally the capacity and needs assessment should be endogenous, driven by the government or other stakeholders. In cases where such assessments are unavailable and the capacity and needs assessment is performed by external actors, a minimum level of ownership should be ensured by basing the analysis on domestically generated data and through the policy dialogue. Regular consultations with civil society organisations and private sector actors identified through the stakeholder analysis can also serve as valuable sources of information.

Assessing existing capacities

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

Capacity assessment is a very sensitive process and needs to be designed and carried out in collaboration with the partner countries and organisations (SIDA, 2005). Participatory self-assessments not only contribute to capacity development on their own but also bring forward the acceptance of ownership for the required change process (SIDA, 2005). The founding principle of any capacity assessment should be to assume

that there are existing capacities that can be built upon. This is important as acknowledging the existence of resources/capacities within a state and society might strengthen both ownership and sustainability.

An important part of this process – conducted at the moment of stakeholder analysis – is to identify agents of change who are best placed and best qualified to initiate and manage the change process. Such institutions, organisations or individuals can contribute to the achievement of a developmental goal in multiple ways (Otoo et al., 2009). For instance, placing knowledge and information in the hands of new or different stakeholders can change power relations, so that learning can lead to changes in the efficiency of a policy and its effect and therefore be an important component of a capacity-building strategy.

There is no blueprint for how detailed a capacity assessment should be. It depends on the purpose – which decisions will it lead to – and specific circumstances. An assessment can easily drown in insignificant details and overlook critical, sensitive factors (European Commission, 2005). The literature offers several considerations that should guide a needs assessment process:

- Assessment of the environment, i.e. broader structural and institutional factors, and socio-political analysis should draw on local expertise and academia. Except in very small operations, donors should only as a last resort conduct their own process;
- The closer an assessment is to the core of an organisation or sector, the more important it is that the country in question is in charge and committed to the assessment process;
- Broad participation is not always good, in that it may raise expectations and stir up conflicts. On the other hand, it may greatly enhance the transparency of processes and results (European Commission, 2005).

TOOL 7: CHECKLIST FOR CYBER CAPACITY ASSESSMENT	
Vision and policies	• Is there a comprehensive cybersecurity strategy and/or legal/policy framework to deal with cybercrime and ensure the security of critical national infrastructure? If yes, what do you need to implement them effectively, also in terms of international cooperation? If not, what are the obstacles and what do you need to overcome them? • What is the level of cyber competencies amongst the general population? Are there education and training programmes available? What do you need to improve the overall level of knowledge about cybersecurity risks and building cyber resilience?
Laws and regulation	• How does existing legislation influence the capacities of institutions, companies and individuals to innovate and exercise their rights? What do you need to make the legal framework work for the benefit of the citizens? What do you need to minimise digital security risks for companies or individuals?
Institutions and resources	• Is there a national entity in charge of preventing, detecting and responding to cyber attacks and/or a body responsible for the implementation of a national cybersecurity strategy? Do you need one and what do you need to make it happen? What do you need to identify and respond more effectively to potential risks? • How does your organisation fit within the broader architecture? Do you think your mandate and resources match the role that your organisation is expected to play in implementing cybersecurity policies? What do you need to do better? • Are responsibilities amongst main stakeholders clearly assigned and understood? What do you need for agencies to work better together? What do you need from other stakeholders? • Is home-grown expertise available? What are the main obstacles to generating a qualified work force, and what is needed to overcome them? What is the level of competence within your own organisation? What do you need to make the best use of existing resources and/or to generate new ones?
Partnerships and cooperation	• Is there a framework for certification of internationally recognised cybersecurity standards in the public sector or among critical infrastructure operators? If yes, do you need to improve the performance? If not, what do you need to set it up? • Are there established channels of communication with the public on cyber-related issued to strengthen confidence on the internet? What do you need to communicate and better promote a cybersecurity mindset?

BOX 4: MODELS AND INDEXES FOR CYBER CAPACITY ASSESSMENT

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

For more information, visit the GCSCC website.

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

For more information, visit the ITU website.

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

For more information, visit the Potomac Institute website.

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

For more information, visit the EGA website.

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

For more information, visit the ASPI website.

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

For more information, visit the Software Alliance website.

Determining desired capacities

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

TOOL 8: CYBER CAPACITY ASSESSMENT LIST FOR LAYERS AND LEVELS OF CAPACITY		
Level	**Layer**	**Questions**
Individual capacity: Abilities Needs and performance Personal attitudes Psychology Motivations and incentives Inclinations Skills and capabilities Know-how Values	Vision and policies	• How are individual roles defined in the developmental objectives and policies?
	Laws and regulation	• Do individuals have skills required to put laws into practice, e.g. law enforcement agents, prosecutors, judges? • Do individuals have sufficient understanding of the laws and regulation?
	Institutions and resources	• Do individuals have the right skills to access, gather and disaggregate data and information about cybersecurity threats and possible solutions? • Do the mechanisms exist (e.g. training, awareness raising) to help individuals acquire the knowledge and understanding of the vision and values that drive the country's cybersecurity policy?
	Partnerships and cooperation	• Are there mechanisms in place – government-to-government or public-private partnerships – that strengthen the development of individual capacities?
Organisational capacity: Practices Roles Mandate Decision-making structures Divisions of labour Sharing of responsibilities Methods of management and means of functioning Use of resources Incentives	Vision and policies	• Are the institutional roles, mandates and decision-making procedures defined clearly enough to allow for articulation of capacity assets and needs? • Do the institutional practices and norms reflect the overall vision of the country?
	Laws and regulation	• Do organisations exist to oversee laws and regulatory framework in the cyber domain? • Do laws and regulations provide effective incentives? • Are the roles of organisations and institutions in the field of cyber-resilience clearly prescribed? Are they adequately resourced?
	Institutions and resources	• Are institutional responsibilities and decision-making procedures defined in a clear way? • Are the mandates supported with adequate resources?
	Partnerships and cooperation	• Do the existing policy-making mechanisms contribute to the whole-of-government and whole-of-society approach?
Enabling environment: Society Laws Policies Procedures Norms Standards Power structures Systems Environment Culture	Vision and policies	• Does the legal and institutional environment provide conditions that facilitate information sharing and support cooperation? • Does the cultural and value system in the country promote cybersecurity? • Do the adopted strategies and policies and the underpinning visions contribute to the development of the culture of cyber resilience by creating incentives, motivation, etc.?
	Laws and regulation	• Is there social acceptance for laws and regulation in the cyber domain? • Does the general organization of the country provide guarantees for the rule of law and good governance needed to implement any laws or regulatory frameworks?
	Institutions and resources	• Are checks and balances in place to ensure that different interests and value systems regarding cyber resilience are represented?
	Partnerships and cooperation	• Does the institutional and legal set up in the country provide opportunities for participation in the policy-making process?

Step three – Define the change that you wish to bring about

Analysing existing and desired capacities helps to identify a capacity gap preventing a country or region from reaching a higher level of development. Identification of an existing capacity gap also allows for assessing whether the stated goals are achievable with the available inputs and given timeframe (SIDA, 2005).

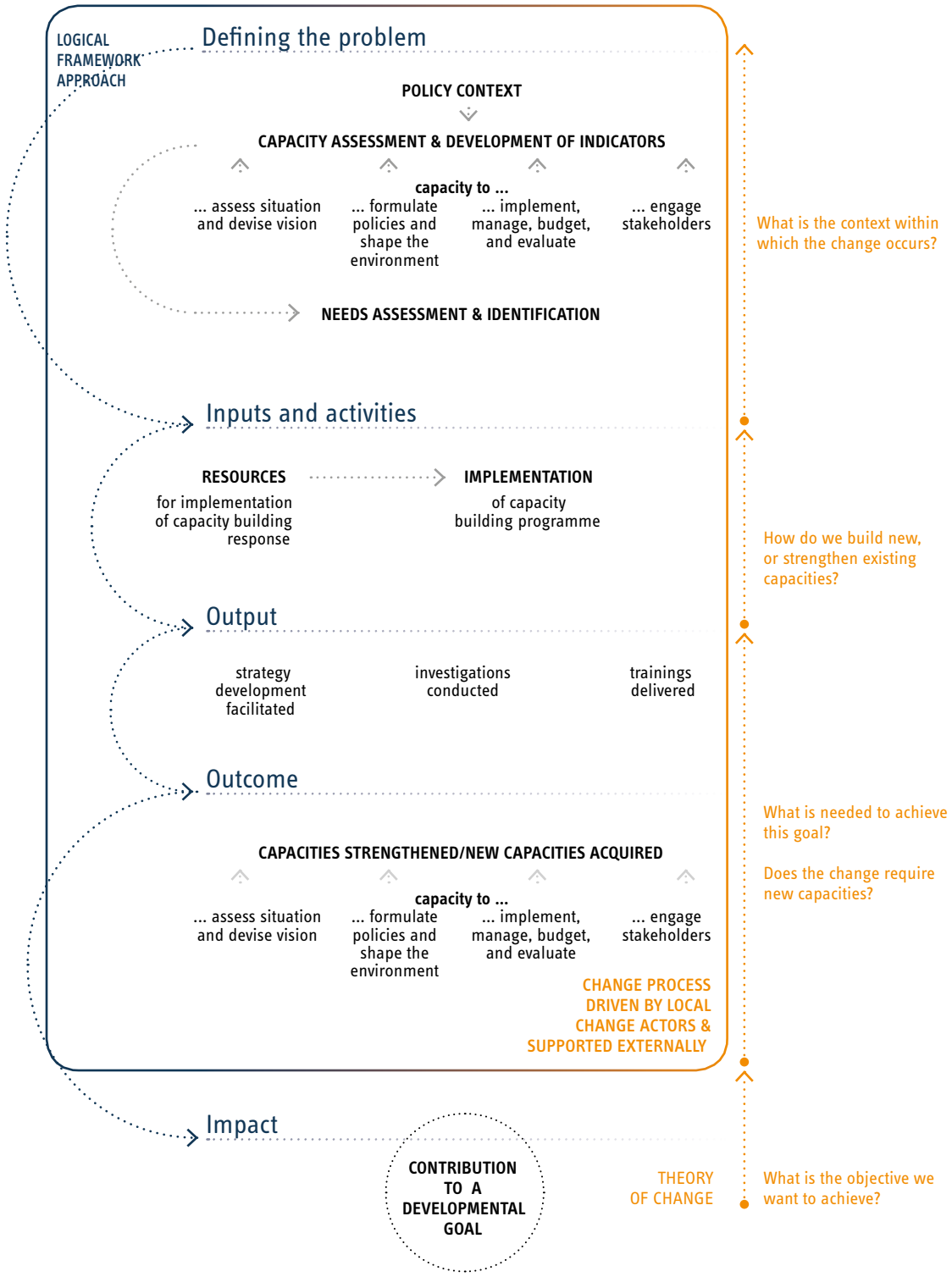
On the basis of the policy analysis, identification of stakeholders, capacity assessment and policy dialogue with partner countries and other stakeholders, it is possible to formulate a plan for capacity building. While designing an intervention, it is important to keep in mind that external actors play a supporting role and their actions should primarily facilitate and catalyse indigenous processes. A good plan builds on existing assets to address gaps identified in a capacity assessment and is essential to the success of any development enterprise (Davis et al., 2009). Therefore, the external actor should first aim to identify domestic projects and programmes that may provide lessons for the planned action or for which synergies and complementarity could be created. Past experiences in capacity building demonstrate that overconfidence in transferring solutions from rich countries instead of using the specific local situation as the point of departure may result in failure (SIDA, 2005).

Based on previous experience and engagements, external actors might contribute with insights into potential actions that could multiply the effects of capacity-building initiatives. In some instances it might be important to define short-term activities to help generate support while the foundation for long-term objectives is being laid. Ideally, therefore, the plan for support of capacity building should contain a combination of quick-impact initiatives and medium- to long-term ones. Sequencing is needed also because available resources are usually limited. The inherent risk is that the focus on quick gains becomes dominant at the expense of more strategic, longer-term objectives (European Commission, 2005). For instance, recurrent training and awareness-raising initiatives for police officers might undermine broader initiatives aimed at strengthening the capacity of the justice system altogether. Since the process of setting priorities is inherently political, it should be managed carefully and transparently, with the involvement of relevant stakeholders to avoid resistance to change during implementation.

Another step in formulating the plan to support capacity building – after the objective has been defined – is outlining the change in the targeted capacity indicators that the project intends to achieve. Experience suggests that the wording of the objective should be very specific. It should make clear what the programme will do, why, for whom and how the implementers and other stakeholders will know if it succeeded (Otoo et al., 2009). The capacity development objective provides the basis for a logical flow that constitutes the foundation of the intervention logic. This flow connects the objective to the capacity factor indicator to be improved and determines the appropriate methodological approach for learning as well as the capacity development activities to be designed (Otoo et al., 2009). Indicators should be set to monitor progress of the implementation itself, the expected results (outcomes) and the achievement of objectives (impact). Note that outcome and impact indicators defined within the programme are likely to be relevant after its implementation. The process itself of defining progress indicators is useful as a way of generating policy discussion, enhancing monitoring and evaluation and as a learning exercise.

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

FIGURE 8: Combining the Legal Framework Approach with the Theory of Change



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

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

Possible actions

The set of objectives for capacity building and their sequence is tailored to the capacity factors that are to be improved, to agents of change who are to make those improvements, and to the envisioned change process (Otoo et al., 2009). Based on experience from development projects, some specific outcomes essential to all capacity-building efforts are raised awareness, enhanced skills, improved consensus and teamwork, fostered collaboration, formulated policy or strategy and implementation thereof (Otoo et al., 2009). Each of these outcomes and objectives can be achieved through activities undertaken at the level of an individual, organisation or environment.

Result chain and indicators

The use of indicators allows for performance management and enhances possibilities for following up the operational process, acquiring relevant information and contributing to learning (Schulz et al., 2005). Indicators are quantitative or qualitative variables that can be observed to provide information on the progress of a specific project or programme over time and at all levels:

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

TOOL 10: EXAMPLES OF POSSIBLE ACTIONS AND RESULTS STATEMENTS

Focus of possible actions	Potential result statements
Raised awareness	• Awareness raising campaigns delivered • Participant understanding of an issue or situation improved • Participant attitude improved • Participant confidence improved • Participant motivation improved
Enhanced skills	• New skills/knowledge acquired • New skills/knowledge applied • Training on technical skills and competences delivered • Training on leadership skills and competences delivered • Education and scholarship schemes provided • Support for cybersecurity research provided
Improved consensus / teamwork	• A coordinating body for cybersecurity issues appointed • Developed standard operating procedures (SOPs): technical, administrative, procedural measures for network management and protection • Discussion initiated/resumed/activated • Participatory process initiated/expanded • Action steps/plan formulated/improved • Collaboration increased/improved
Fostered coalitions / networks	• Mentoring and peer-to-peer learning put in place • A 24/7 point of contact appointed and procedures for interagency coordination strengthened • Public-private partnership arrangements elaborated • Risk assessment and management exercises organised • Discussion initiated/resumed/activated • Participatory process initiated/expanded • Informal networks created/expanded • Formal partnerships or coalitions created/expanded
Formulated policy / strategy	• National cybersecurity strategy formulated and/or implemented • Cybercrime and cybersecurity legislation adopted: substantive and procedural laws, criminalisation of certain acts, ensuring respect of fundamental freedoms, inclusion of positive/negative incentives in private and administrative laws • Stakeholders involved in process • Policy/strategy needs assessment completed • Stakeholder agreement reached • Action steps/plan formulated • Monitoring and evaluation plan designed • Policy/reform/strategy/law proposed to decision makers
Implemented strategy / plan	• Incident response capabilities / CSIRTs established • Implementation steps formulated and initiated • Monitoring and evaluation initiated • Implementation know-how improved • Budgetary resources for CCB allocated

Lessons learned

Design and implementation of an intervention is expected to build on lessons (positive and negative) from similar experiences and good practices identified on previous occasions. In 2017, the **Global Forum on Cyber Expertise** – comprising over 60 partners representing governments, international organizations and private companies – published **Global Good Practices** in policy areas such as national capacity assessment, CERTs/CSIRTs, incident capture and analytics, critical-information infrastructure protection, cybersecurity awareness and standards (see GFCE). Valuable lessons can be also drawn from the EU's engagement in cyber capacity-building projects. For instance, the EU's long-standing partnership with the Council of Europe has resulted in many projects with regional and global scope (Council of Europe, 2018).

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

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

For more information, visit the GFCE website.

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

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

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

For more information, visit the GGP website.

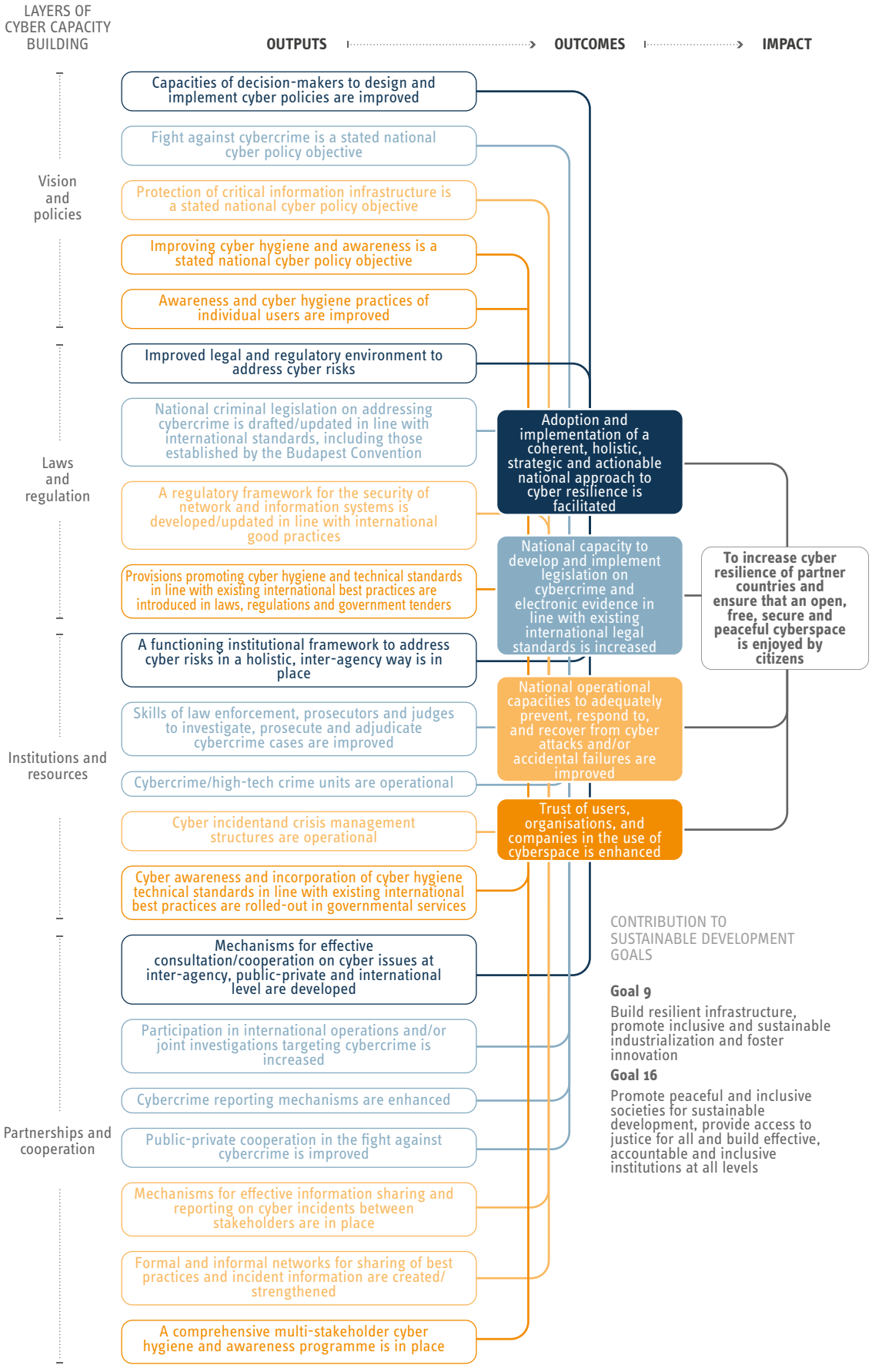
The World Bank's **Digital Development Partnership** (DDP) helps operationalize the 2016 World Development Report on Digital Dividends and offers a platform for digital innovation and development financing. The DDP brings public and private sector partners together to catalyse support to developing countries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

For more information, visit the DDP website.

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

For more information, visit the WEF website.

TOOL 11. EXAMPLE OF THE RESULT CHAIN FOR CYBER CAPACITY BUILDING



Complementarity and synergy with other actions

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

Aside from the coordination difficulty, another challenging dimension in relation to capturing the breadth of cyber actions related to the very broad range of cyber-related policies, therefore it is often difficult to comprehensively capture projects or initiatives that may not be **cyber-specific** but would be highly **cyber-relevant**. For instance, projects aimed at improving IT infrastructure in a partner country do not fall under the scope of 'cyber capacity building' but would most often be accurately captured as digitalisation projects. However, they should have cybersecurity elements embedded. Moreover, given that an increasing number of services rely on internet-based platforms, crime also increasingly gains a cyber flavour. Numerous projects that focus predominantly on building capacity of law enforcement agencies, or the security sector more broadly, are also receiving basic training in the domain of cybercrime and electronic evidence, even though the project's main objective might refer broadly to the rule of law or justice system. As a consequence, monitoring all engagements with cyber capacity-building elements is complicated.

Nonetheless, it is important to make sure that any planned intervention is designed following a mapping of the existing initiatives and also includes a **'cyber-specific' or 'cyber-relevant' marking**, as appropriate, to facilitate reporting and potential synergies with other actions. Most notably, cyber-relevant capacity-building actions would entail those addressing human rights freedoms online; internet governance; the development of ICT infrastructure, policies and regulations; as well as justice and security sector reform programmes, including on countering terrorism and organised crime, with a strong digital evidence and forensics component.

Cross-cutting issues

The proposed actions need to integrate the human rights, gender, and environmental considerations. In the field of cyber capacity building all three areas play a very important role as they make and important contribution towards empowering specific communities - human rights defenders, civil society organisations – or demographic groups, in particular women and youth (OECD, 2014).

The increasing reliance on ICT implies that unless properly addressed, vulnerabilities in the cyber domain might impede economic and human development in affected areas. The EU's 2017 Digital-4Development framework elaborated on this challenge, noting that 'due to the cross-sectorial nature of digitalisation, promoting cybersecurity as a transversal issue is essential in development cooperation, namely through incorporation of cybercrime components in criminal justice sector reform programmes as well as integration of cyber resilience elements in projects dealing with critical infrastructures (ex. ICT, transport, energy) and digital/e-government initiatives'. **In fact, even though this Operational Guidance is mainly for programmes that have a cyber-specific focus, it is also intented to provide guidance on actions that have cyber-relevant dimension and activities.** The rationale is to promote a holistic and consistent policy approach, taking in to account that external capacity-building programmes that touch on justice and security, in particular in fighting terrorism and organised crime, often address aspects of electronic evidence and cyber-enabled systems, infrastructure and services.

Step four – Decide how you are going to move from an idea to an action

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

TOOL 13: CHECKLIST FOR CROSS CUTTING ISSUES

Gender assessment

Context

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

Policy

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

Intervention

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

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

Rights-based approach assessment

Context

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

Policy

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

Intervention

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

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

Environmental and climate related screening

Context

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

Policy

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

Intervention

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

Environmental and climate related issues are usually addressed superciliously in the assessment of cyber capacity-building projects. However, potential impact of cyber projects on environment and climate cannot be ignored, in particular with regard to the energy consumption linked to the introduction of some solutions (e.g. large data bases, amount of digital data generated, etc.). Introduction of new technologies and their secure use might also have positive impact on the environment. For instance, the use of 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.).

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

Performance and results monitoring

Monitoring is intended to be continuous and flexible to allow for adjustments when faced with changed needs or priorities, or simply as the understanding of the situation evolves (Otoo et al., 2009). Indicators and benchmarks for success are usually developed when the programme or project are formulated. Given the broad scope of potential cyber capacity building and the highly contextualised nature of any external support, designing a set of universal indicators is not only difficult but may also be counterproductive.

TOOL 14: CHECKLIST OF EVALUATION CRITERIA	
Relevance	• Does the action presently respond to the needs of the target groups/end beneficiaries? • Do all stakeholders still demonstrate effective commitment (ownership)? • Is the action adapted to present institutional, human, financial capacities of the partner government and/or other key stakeholders? • Is there an effective government-led system of sector coordination involving the relevant local stakeholders and donors? • Have all relevant circumstances and risks been taken into account to update the intervention logic?
Efficiency	• Have the chosen implementation mechanisms proven conducive for achieving the expected results? • Do government and other partners in the country effectively steer the action? • Do the resources actually made available correspond to the needs of the action? • Are there any delays in the implementation and if yes, what has caused them and have the plans been adapted accordingly? • Do implementing partners, partner government(s) and other key stakeholders adequately monitor the action?
Effectiveness	• Is the progress of each output conforming to plan? • Is the quality of outputs satisfactory? • Are the outputs still likely to lead to expected outcomes? • Does the action effectively support the partner's policy and actions?
Sustainability	• Are key stakeholders acquiring the necessary institutional and human capacities to ensure a continued flow of benefits? • Is the role of EU actors sufficiently respectful of the leading role of the partners so as to enhance their capacities? • Have the relevant authorities taken the financial measures to ensure the continuation of services after the end of the action? • Has the private sector been involved to ensure the sustainability of the action?

Risk management

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

Closing

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

TOOL 15: FRAMEWORK FOR RISK MAPPING

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

- **Political risks -** Support and willingness for change among the political elites is usually a pre-requisite for any intervention. However, it is important that the action monitors other initiatives undertaken by the government that might be contrary to the EU's values or interests. In the case of cybersecurity, this could be an expressed support to new international conventions or the shift from a multi-stakeholder to state-centric approach in internet governance.

- **Operational risks -** Given the need to involve groups of actors with different objectives, cultures, resources and level of engagement, there is a risk that competing claims, views or inexperience hamper the implementation of the action. So it is important to thoroughly map the relevant stakeholders and their interests and understand their motivations and inter-/intra-group dynamics. There is also a risk linked to continuity of operations, which is closely linked to having several donors or external actors operating in a partner country/region. For instance, it might be difficult to support the operations of a CERT if it was built according to a model supported by a different donor that incompatible with the EU's approach.

- **Legal risks -** One of the main pillars in building cyber resilience is strengthening the legal and regulatory environment of a country or region. However, given differences in the overall level of legal approximation between the EU and partner countries, there are potential negative spill-overs that cannot be ignored. This is particularly the case with technologies that can be used by governments for surveillance of civilians or compromise human rights online, including the safety of human-rights defenders. Similarly, strengthening capacities of law enforcement agencies without a comprehensive analysis of the whole legal system from the perspective of the rule of law and democratic standards may have negative consequences. For instance, new law enforcement capacities in the field of cybercrime might also be used to prosecute civil-liberties activists or minorities. Finally, there is also a risk that support provided in one domain (developing a strategy) may lead to actions by a partner country or region that go against the spirit of the initial intervention (e.g. development of model laws, etc.)

- **Security risks -** Placing cybersecurity or cybercrime on the agenda of governments can also attract the attention of those who might feel targeted, such as criminal groups, hackers, etc. Therefore, actions may need to be accompanied by adequate mitigation strategies. This is particularly relevant given that most of the solutions used at all levels are based on off-the-shelf technologies that are vulnerable to attacks.

- **Resource-related risks -** These are associated with funding, including the failure to secure budgets or other types of resources like an adequate staff. Problems linked to budgets are particularly present in developing countries where resources are more limited. Given the limited number of experts in the field of cybersecurity and cybercrime and the increasing competition for expertise between public and private actors, there is also a risk of losing well-trained and experienced staff to other job offers.

- **Reputational risks -** The nature of cyber capacity-building actions requires the involvement of different groups of actors. That means there is a potential for damage to the EU's reputation stemming from differing values and principles. One way to diminish this is to ensure that actions are accompanied by adequate plans and communication strategies. In the field of cyber capacity building this is particularly relevant with regard to the choice of involved partners and the implementers.*

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

Step five – Evaluate the result of your intervention

The purpose of evaluation is to assess, against indicators selected in the planning stage, how successful the project has been in meeting its stated objectives, to reflect upon the relevance of project activities, to identify lessons learned in terms of impact, sustainability, effectiveness and efficiency and to assess whether any can provide guidance for further work in the field of cyber capacity building. The completion of a project or a programme and its evaluation should provide inputs for decisions regarding the next steps, including continuation, scaling up or new funding sources for the project. Where necessary, this also involves decisions about whether and how programme participants could be further supported, including by joining other programmes. The identification of lessons is also important to ensure that the outcomes and experiences associated with the intervention feed into future policies and practices. An often-ignored element in lesson identification is mapping instances of failure or projects that do not bring desired outcomes. It is important to document not only positive but also negative elements of the process.

TOOL 16: CHECKLIST FOR IDENTIFICATION OF LESSONS

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

Thinking about lessons should provide answers to the following questions:

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

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

QN-02-18-916-EN-C

Publications Office

ISBN 978-92-9198-753-5