
Acknowledgements

This report is the product of a joint initiative between the United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT) and INTERPOL on strengthening capacities of law enforcement and criminal justice authorities to counter the use of new technologies for terrorism purposes. The joint initiative was funded with generous contributions from the European Union.

Contents

Joint Foreword

Advances in Information and Communication Technologies (ICTs) and their availability have made it attractive for terrorist and violent extremist groups to exploit them to facilitate a wide range of activities, including incitement, radicalization, recruitment, training, planning, collection of information, communication, preparation, propaganda, and financing. Terrorists continuously explore new technological frontiers, and Member States have been expressing increasing concerns over the use of new technologies for terrorist purposes.

During the seventh review of the United Nations Global Counter-Terrorism Strategy, Member States requested the United Nations Office of Counter-Terrorism and other relevant Global Counter-Terrorism Co-ordination Compact entities to "jointly support innovative measures and approaches to building the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism".

In his report to the General Assembly on the Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (A/77/718), the Secretary-General underscores that "[...] new and emerging technology offers unmatched opportunities to improve human welfare and new tools to counter-terrorism. [...] Despite strengthened and concerted efforts, responses by the international community often lag behind. Some of these responses unduly limit human rights, in particular the rights to privacy and to freedom of expression, including to seek and receive information".

Through the seven reports contained in this compendium – the product of the partnership between the United Nations Counter-Terrorism Centre and the International Criminal Police Organization under the CT TECH joint initiative, funded by the European Union – we seek to support Member States' law enforcement and criminal justice authorities to counter

Acknowledgements

This document has been developed through the contributions and reviewed by a wide range of stakeholders.

Arti f cial Intelligence (AI)	Generally understood to describe a discipline concerned with developing technological tools exercising human qualities, such as planning, learning, reasoning, and analysing.
Criminal Justice Process	A legal process to bring about criminal charges against an individual or an entity and the court proceedings, judgement sentencing as well as correction سُخي d a *) - 0 aoion سخي

New Technologies-Related Terrorist Risk[4]

UN Human Rights Principles for Counter-Terrorism Activity[7]

(i)The exercise of functions and powers shall be based on clear provisions of law that exhaustively enumerate the powers in question. (ii) The exercise of such functions and powers may never violate peremptory or non-derogable norms of international law. (iii) Where the exercise of functions and powers involves a restriction upon a human right that is capable of limitation, any such restriction should be to the least intrusive means possible and shall: (1) Be necessary in a democratic society to pursue a de fned legitimate aim, as permitted by international law.

Executive Summary

The "National Law Enforcement capabilities assessment framework to counter the use of new technologies for terrorist purposes and the use of new technologies to counter-terrorism" (hereinafter: "LEA framework") aims to support capacity building, maturity assessment, and cross-border cooperation.

This document outlines a "National Capability Reference Model" ("Model") which describes the LEA counter-terrorism "value chain", and the necessary policy, legal, and institutional capabilities to develop and maintain it. The model is complemented by a maturity assessment model, which includes more detailed questions regarding each of the capabilities. It is aimed to support Member States in operationalizing capability planning, prioritizing, and building.

The model and the elements of the maturity model are based on desk research, experience, and insights from parallel projects in the areas of cybersecurity and cybercrime. The model focuses on the role of LEA at the intersection of counter-terrorism activities and new technologies from the LEA perspective. It covers general policy, legal and institutional capabilities from within this context, considering the rising importance of the digital sphere for national security as well as for social and economic activities. Human rights considerations are integrated through all relevant policy, legal and institutional capabilities as part of a human rights by design approach. This is also intended to mitigate in advance potential frictions in deployment.

Given the quick pace of technological change, the model includes policy and institutional elements that are necessary to adapt to new threat scenarios, such as horizon scanning at the policy level, and innovation management at the LEA level. This approach is complemented by a list of specific use cases, to cover common concrete scenarios, of terrorist activity using new technologies, and law enforcement use of new technologies. These use cases reflect the current technological and threat scenario and should be updated regularly. As the Model was developed based on desk research, stakeholder consultations, and expert input, it will benefit from feedback received from Member States and experience gained in its use. These deployment insights can inform updating the Model as needed.

[I] Overview

United Nations Member States attach great importance to addressing the impact of new technologies in countering terrorism. During the seventh review of the United Nations Global Counter-Terrorism Strategy (A/RES/75/291)[9] in July 2021, Member States expressed their deep concern about

and requested the O f ce of Counter-Terrorism and other Global Counter-Terrorism Compact entities

Security Council Resolutions 2178 (2014)[10] and 2396 (2017)[11] call for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology and communications for terrorist acts. Security Council Resolution 2396 (2017) also encourages Member States **to enhance cooperation with the private sector, especially with ICT companies**

1.2 CT TECH Initiative

CT TECH is a joint UNOCT/UNCCT and INTERPOL initiative, implemented under the UNOCT/UNCCT Global Counter-Terrorism Programme on Cybersecurity and New Technologies. It is aimed at strengthening capacities of law enforcement and criminal justice authorities in selected Partner States to counter the exploitation of new and emerging technologies for terrorist purposes, as well as support Partner States' law enforcement agencies (LEAs) in leveraging new and emerging technologies in the fght against terrorism.

To achieve the overall objective, the CT TECH initiative implements two distinct outcomes with six underpinning outputs.

FIGURE 1

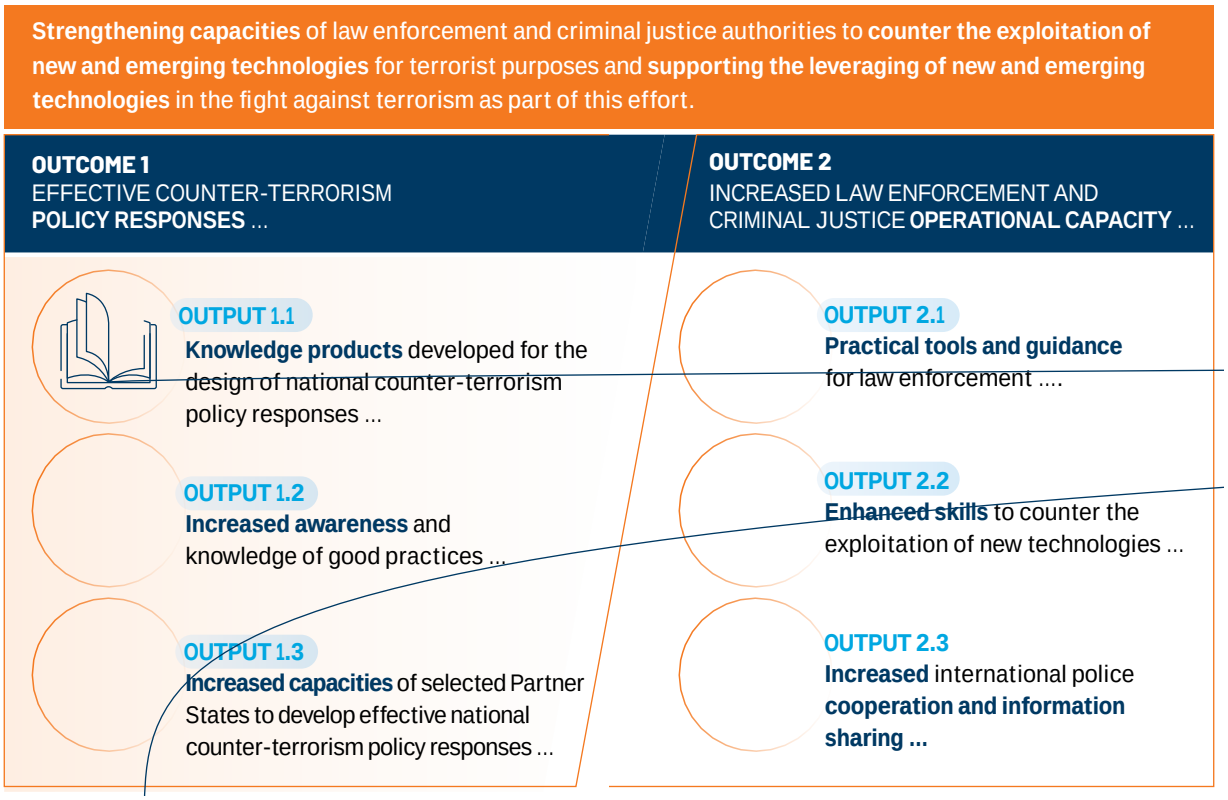


TABLE 1. **CT TECH Outcomes and Outputs**

Outcome 1: Effective counter-terrorism policy responses towards the challenges and opportunities of new technologies in countering terrorism in full respect of human rights and the rule of law.	
 Output 1.1	Knowledge products developed for the design of national counter-terrorism policy responses to address challenges and opportunities of new technologies in countering terrorism in full respect of human rights and the rule of law is developed.
 Output 1.2	Increased awareness and knowledge of good practices on the identi f cation of risks and

1.3.1 Scope

The national capability reference model and the accompanying maturity assessment framework is intended to describe capabilities at the national level for law enforcement to counter the use of new technologies for terrorist purposes. Thus, this document is not intended to cover all the elements of a national counter-terrorism or law enforcement policy, where they are not focused on countering the use of new technologies for terrorist purposes.

1.3.2 Target Audience

This guide is intended primarily for policymakers and Member State law enforcement authorities and counter-terrorism agencies.

1.3.3 Bene f ts

The Model is intended to integrate best practices that relate to law enforcement capabilities regarding new technologies. It can support Member States in activities necessary to develop and deploy a long-term strategy.

These capabilities can have a positive effect on the ability to address cybercrime and p e ş ḣ d M

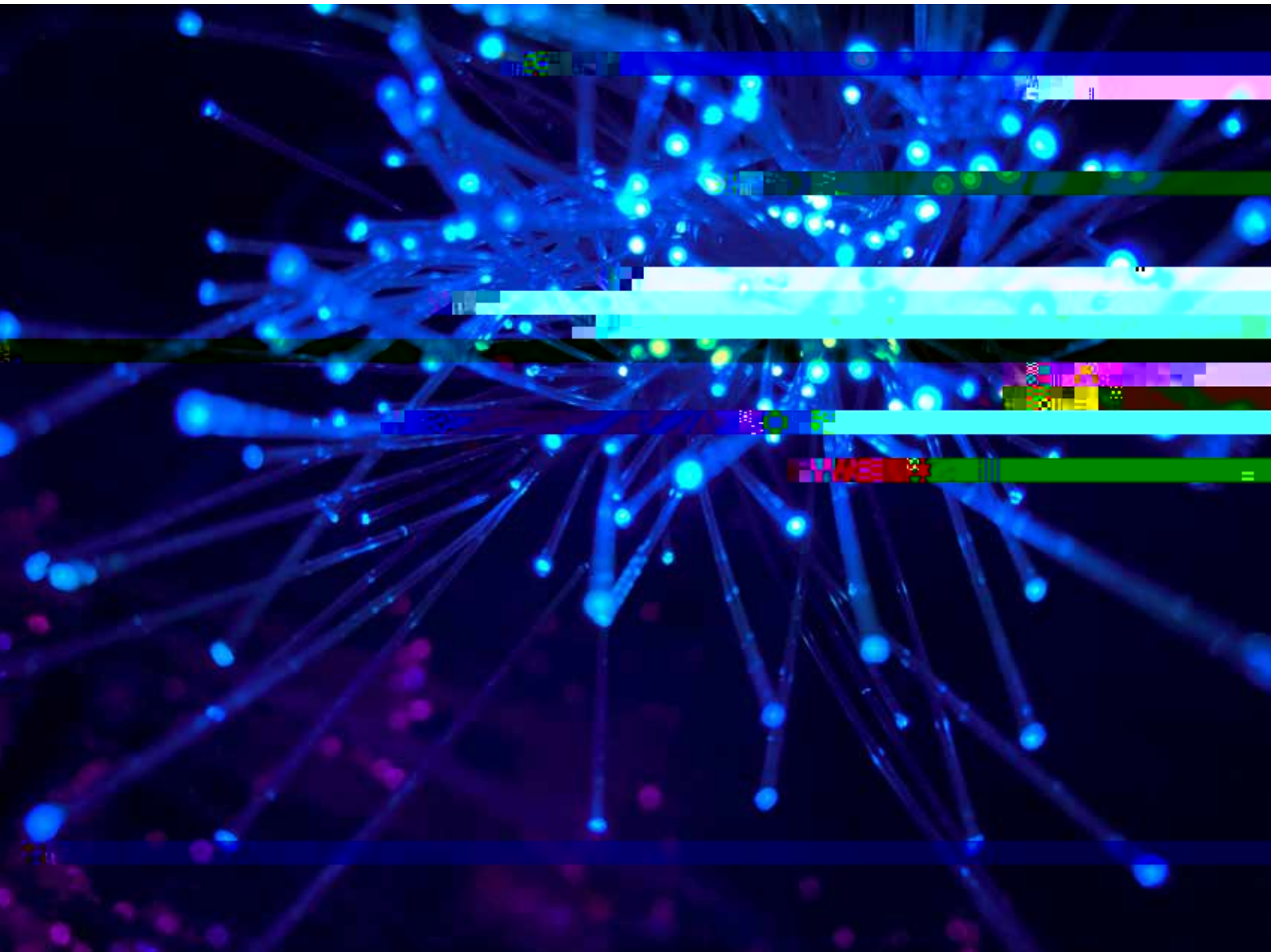
The Model is focused on LEAs' capabilities to deal with 'new technologies'. Yet these capabilities rely on LEAs having a basic level of general capabilities, such as established legal frameworks, enforcement procedures, and use of information technology.

The Model was developed to be forward looking and adapt to new technologies as these develop. At the time of development, the focus of 'new technologies' is on 'Internet, social media and cryptocurrencies'. While the model sets the building blocks for 'horizon scanning' to prepare for developing risks, new leaps in technological developments may require a comprehensive review of the model.

The Model aims to describe the main elements of Law Enforcement capabilities yet may require additional adaptation in assessment and application to unique legal, social, and economic conditions in Member States.

1.3.5 Caveat

This document is the first iteration and is subject to validation during capacity-building efforts, which will inform future updates. The information provided herein is intended to provide guidance and aid in the capacity-building assistance to Member States. While every effort has been made to ensure the accuracy, completeness, and timeliness of the content, we make no representations or warranties of any kind, express, or implied, about the accuracy, reliability, suitability, or availability of the information contained within this document.



The guiding framework is a conceptual model that is intended to guide, align, and inform the development of the report. It seeks to ensure coherence from strategy to execution between the United Nations Global Counter-Terrorism

The effective use and deployment of such services and tools is dependent on a set of underlying capabilities. The required capabilities to enable and deliver services are often defined and represented in a capability model. A capability model represents a functional decomposition of key functions into a logical and granular grouping which supports the execution of services and activities. The capability model informs the requirements across people (structure and skills), processes, technology, infrastructure, and finance.

The guiding framework serves to ensure alignment between strategy and execution from both 'top-down' and 'bottom-up'.

2.3 Methodology

FIGURE 3

2.3.1 Expert Group Meetings and Consultation

10

3.1 Overview

As advancements in technology continue to accelerate, terrorists increasingly exploit these innovations to further their destructive agendas. The rapid proliferation of communication platforms, social media networks, encryption techniques, and emerging technologies pose signi f cant challenges for law enforcement authorities. The emergence of new technologies has brought both opportunities and challenges to LEAs worldwide, especially in their f ght against terrorism. To effectively combat this ever-evolving threat, a law enforcement capability model framework focused on new technology is imperative. This framework provides LEAs with a systematic approach to understanding and countering the capabilities terrorists may acquire through technological advancements. The capability model equips law enforcement with the knowledge necessary to develop proactive strategies, enhance intelligence gathering, and disrupt terrorist networks. Such a framework enables law enforcement to stay ahead of the curve, adapt to emerging tacti ˇ ode - a) alv lJ e k olvi g se d 0 ance ents. / ā ology s ¤ ¤ d

On the other hand, new technologies present signi f cant opportunities as a capability multiplier for counter-terrorism and law enforcement authorities. For example, such technologies have the ability to allow law enforcement authorities to do more with less, fast track timely decision-making, generate new insights, and conduct disruptive operations remotely.

Countering terrorists use of new technologies hinges on understanding how terrorist actors are using new technologies, developing effective legal framework and policy responses, and building operational capacity to counter the use of such technologies for terrorist purposes, to include leveraging and adopting the use of new technologies.

3.2.1 Challenges – Use of New Technologies for Terrorist Purposes

Advances in ICT and their availability have made it attractive for terrorist and violent extremist groups to exploit the Internet and social media to facilitate a wide range of activities, including incitement, radicalization, recruitment, training, planning, collection of information, communication, preparation, propaganda, and f nancing. For their purposes, terrorist groups also expertly exploit and manipulate gender inequalities, norms and roles, including violent masculinities. For example, Da'esh skilfully recruited women through social media, adapting their messages to appeal to women speaking different languages and living in different social, economic, and cultural contexts in Western Europe, Central Asia, and the Middle East, and North Africa, often tapping into women's experience of gender inequalities. Terrorists also use encrypted communications and the Dark Web to share k Web t đ k ÿ ů ' xperi đ ' t, Ce k ʊ onunica Ů ů '

3.2.3 Human Rights and New Technologies

Terrorism has devastating consequences for the enjoyment of the rights to life, liberty, and physical integrity of victims. In addition to these individual costs, terrorism can destabilize governments, undermine civil society, jeopardize peace and security, and threaten social and economic development. All these elements directly impact on the enjoyment of human rights. States have an obligation to take measures to protect their nationals and others against the threat of terrorist attacks and bring the perpetrators of such acts to justice. Such counter-terrorism measures, including actions to prevent and prosecute those responsible for terrorist acts, must themselves be in line with international human rights standards and the rule of law.

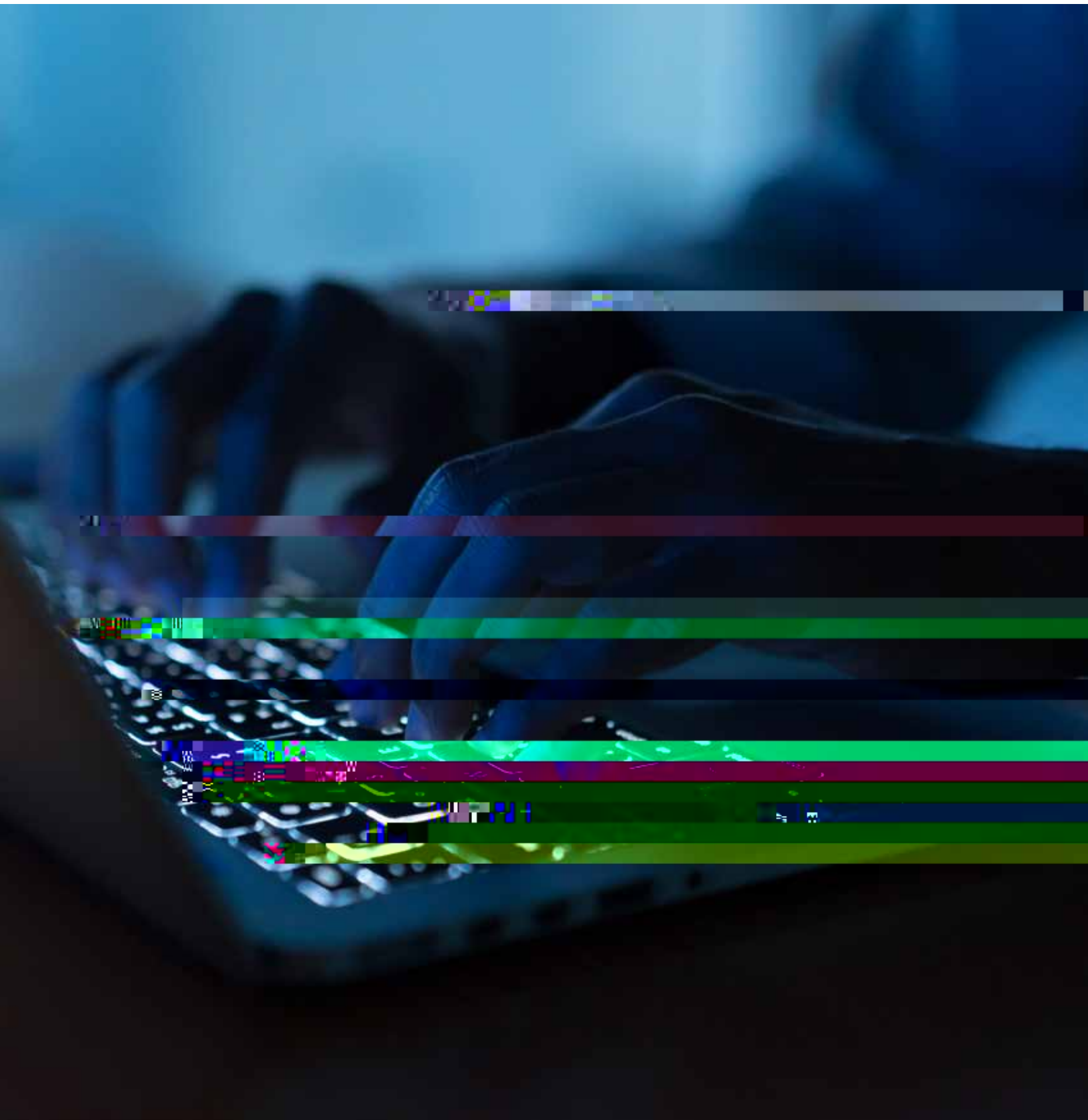
The use of new technologies to counter-terrorist activities presents new human rights challenges. In particular, States have an obligation to ensure their counter-terrorism laws, policies, and practices respect rights such as the right to privacy, freedom of expression, freedom of association, freedom of religion, and liberty and security of the person, as well as the principle of non-discrimination and due process rights including presumption of innocence and a fair trial. States must also uphold the absolute prohibition of torture.

The United Nations, Interpol, and the EU have repeatedly underlined the interrelationship between new technologies, counter-terrorism and human rights, including gender equality. The United Nations Global Counter-Terrorism Strategy and various General Assembly and Security Council resolutions underscore Member States' human rights obligations under international human rights, humanitarian and refugee law when countering terrorism.[21] In particular, the fourth pillar of the United Nations Global Counter-Terrorism Strategy sets out measures to ensure respect for human rights for all and the rule of law as the fundamental basis in the fght against terrorism, and recognizes that "effective counter-terrorism measures and the protection of human rights are not confcting goals, but complementary and mutually reinforcing".

3.2.4 Gender, Technology, and Law Enforcement Capabilities

Gender refers to the roles, behaviours, activities, and attributes that a given society at a given time considers appropriate for men and women, girls and boys. In addition to the social attributes and opportunities associated with being male and female, gender is also relevant for the relationships between women and men and girls and boys. Gender is part of the broader socio-cultural context, and intersects with other identity factors, including sex, class, race, poverty level, ethnicity, sexual orientation, age, among others. Men, women, girls, and boys, as well as persons of different gender identities and expressions experience security differently and in accordance to their particular needs, vulnerabilities, and capacities.[22] Specifcally in the use of new technologies, while the absence of hierarchical structures on the Internet may remove gender constraints, and provides opportunities for empowering women, it also bears an increased likelihood for them to be recruited or actively engaged with violent extremist and terrorist groups online.[23] Evidence also suggests that terrorist groups instrumentalize gender in their online messaging; for example Da'esh used contradictory gendered messaging strategically in their recruitment and comm l' ņ * sg c oups i - w ' saging ɐ o ∃ i |= ṅ v

Integrating gender dimensions within the national law enforcement capability and response is therefore critical in assessing terrorist intent and potential targets, as well as in designing appropriate responses that address the particular needs and vulnerabilities of persons of different gender, bearing in mind intersectional factors, such as age, disability, ethnicity, language, nationality, racial identity, religion, sexual orientation, or any other identity factor and combinations thereof.



4.1 Overview

The development of the national capability reference model is structured in a logical hierarchy manner that is

domestic policy development and cross-border cooperation. Global best practices demonstrate how to turn abstract principles into concrete legal measures. In addition, having similar legal rules, based on global best practices, across jurisdictions, reduces cross-border legal friction.[26]

4.2.1 The Rule of Law

This is the general base of the framework that ensures that it is developed within the general principles of international law, respecting the rule of law.

Ref.	Sub-Capabilities	Description
1.1.1	The rule of law according to international standards	The exercise of functions and powers shall be based on clear provisions of law that exhaustively enumerate the powers in question. The exercise of such functions and powers may never violate pre-emptory or non-derogable norms of international law; exercise of functions and powers is subject to independent authorization or review by judicial or another independent authorizing body, in accordance with international standards. This requirement serves as a foundational element of the capabilities model and is transposed in the sub-capabilities of the model.

4.2.2 Human Rights

1.2.3	Application of accepted data protection principles to law enforcement collection, processing and use of personal information

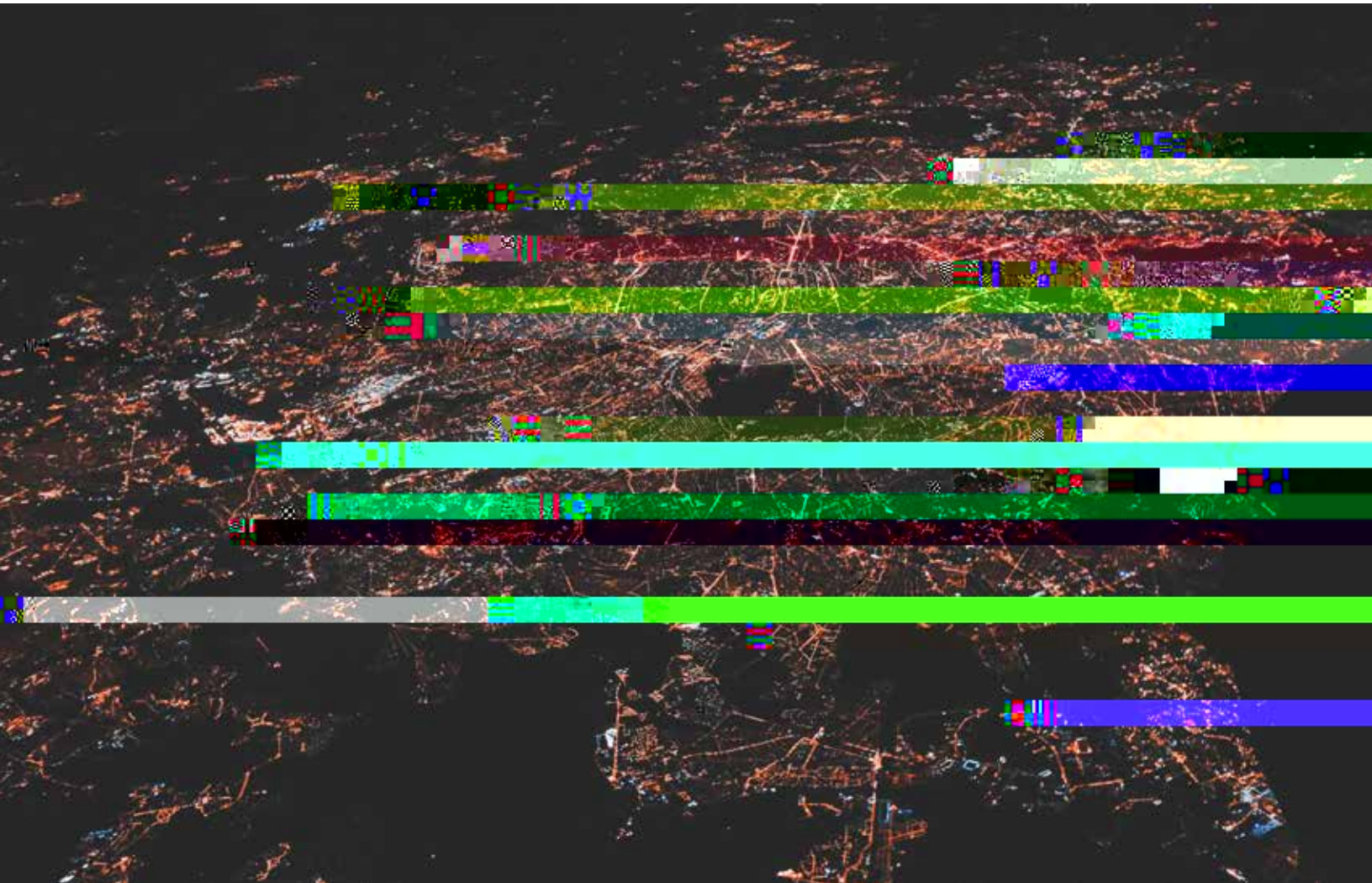
4.2.4 Substantive Criminal Law

Criminal law defines prohibited activity and serves as the basis of the criminal justice process. It describes activities that law enforcement should focus on and need to apply their operational powers to. Therefore, in order to enable prosecution substantive criminal law should cover criminal acts that are related to the use of new technologies for terrorist purposes.

The definition of criminal offences should be accurately and narrowly tailored so as to prevent over broad prosecution or use of law enforcement powers. For example, the definition in Security Resolution 1566 ties criminal acts to violence against persons or threats of such violence as does the definition proposed by the Special Rapporteur on Counter-Terrorism and Human Rights.

It should be clarified that, in general, criminal offences that apply to terrorist activity offline can be applied to such activity online, as well, and may not require special or new offences. From a rule of law perspective, it is recommended to have clearly defined offences that relate specifically to use of new technologies, especially in sensitive contexts. Having dedicated offences can guide law enforcement and the criminal justice processes by providing clarity as to the scope of forbidden activities. Drafting dedicated offences should be guided by the principle of technological neutrality so as to be applicable to new types of technologies.

While binding international instruments in this area are still being developed, common approaches and international frameworks can serve as a powerful practical tool. From a domestic policymaking point of view, these frameworks reflect experience gained in the drafting and deployment challenges in this area, mentioned above. From an international cooperation point of view, they can promote 'bottom up' cross-border cooperation. Having common approaches reduces Member States' need to assess country specific frameworks and develop unique bridges between domestic frameworks.



1.4.3	Ancillary liability/ material support/ accessory offences	Substantive criminal law also includes a framework that applies to actors that carry out some part of the illegal activity but not all of it. These additional offences apply to an 'attempt' to carry out the criminal activity, as well as aiding or abetting the offences.[33] In general, ancillary liability requires proving that a criminal offence was carried out by a main actor, and a supporting activity by the supporting actor.

4.2.5 Administrative and Criminal Procedural Law

Administrative and Criminal Procedural law defines the thresholds, modalities, and safeguards that apply to law enforcement operational activity. Thus, it serves both to enable law enforcement activity, and to mitigate possible risks to fundamental rights. Procedural law is aimed to support different operational capabilities. It also serves to support cross-border law enforcement cooperation, by enabling cooperation across borders in the counter-terrorism value chain. It serves to support criminal investigation of the offences described in Section 2.1, other criminal offences committed by means of new technologies, and the collection of evidence in electronic form of a criminal offence.

Ref.	Sub-Capabilities	Description
1.5.1	General law enforcement authorities	These are the core authorities that allow law enforcement to carry out the law enforcement value chain activities. They include collection of information, summoning of witnesses, search and seizure, request for production of information or an object, questioning, and detention for questioning.
1.5.2	New technologies' LEA authorities	These are core authorities tailored to collection of digital evidence, which is unique in its sources, volatile nature, and risk of manipulation. These authorities include: expeditious preservation of specified computer data, including traffic data, expedited preservation and partial disclosure of traffic data, orders to produce digital evidence, search for digital evidence, real-time collection of traffic and content data.
1.5.3	Advanced new technologies LEA authorities	These authorities are tailored for developing threat scenarios that misuse new technologies. They may be applied as an interpretation of existing procedural authorities. Where feasible, it is advised to define specific legal authorities separately to promote the rule of law, enable clarity and legislative oversight.[34]
1.5.4	Unique counter–terrorist authorities	The unique threat of terrorism has led to the development of unique capabilities that aim to enhance traditional law enforcement activities against crime. These include the following: 1. Listing terrorist entities 2. Filing secret evidence protected by confidentiality 3. Protection of human sources 4. Operational capability to carry out 'special investigative techniques'.

33 See COE 185, title 5, and COE explanatory note, Section 118.

34 Such authorities could include: Ability to conduct operations on the Dark Web; remotely accessing a computer or other device and

1.5.5	Unique administrative support	In order to deal with new technological risk scenarios that develop quickly, LEAs may need to quickly complement their capabilities by procuring new services and products. LEAs are subject to administrative procurement and contracting rules that may not be adequate for such operational scenarios. Thus, unique administrative support frameworks, which take in account legal and financial obligations of LEAs as public organizations, yet enable operational contracting, need to be in place.

4.2.6 Jurisdiction and Cooperation

Jurisdiction is the legal concept that applies to the links between government legal authority and geographical territory.[35] Due to the cross-border nature of the use of new technologies for terrorist purposes, it is important to understand and define the way law enforcement can operate when some of the malicious activity is conducted outside the State. Jurisdiction thus is relevant over the offender, the affected target, or over necessary evidence. When jurisdiction is extended beyond the physical borders, it needs to be in line with acceptable international standards.[36]

4.3 National Counter-Terrorism Policy Pillar

The policy pillar includes elements necessary for development and deployment of a comprehensive, guiding written programme to counter-terrorism.[37] National policies are important for creating a common, whole of government approach to the terrorist threat, with a clear high-level mandate. Comprehensive policy is important for intragovernmental coordination purposes, and integration with relevant national security, cybersecurity and cybercrime policies.[38] Policies need to de f ne institutional mandates, organizational responsibilities and cooperation and coordination mechanisms between organizations. Policies need to allocate resources to promote the elements of the capabilities framework.

National policies are also necessary for collaboration with non-governmental stakeholders and organizations, as part of the counter-terrorism value chain. Thus, the policy needs to support coordination, communication, and cooperation with the private sector, the general public, and with international partners. Communication and publication of the policy's main principles, can foster trust and cooperation by relevant domestic and international stakeholders.[39]

As described above, the policy pillar is focused on the counter-terrorism new technologies capabilities and does not aim to cover all elements of a national counter-terrorism strategy.

4.3.1 Policy Development and Management

National policy development and management is a critical capability for governments to effectively address the terrorist challenges. It involves the creation, implementation, and management of policies that shape operational capabilities and security outcomes. National policy development and management require collaboration and engagement with government stakeholders, civil society organizations, and the private sector, to ensure that policies re f ect the diverse needs and perspectives of the population. Effective national policy development and management require a strong institutional framework, skilled human resources, and robust processes and procedures to ensure that policies are evidence-based, effective, and accountable.

A Member State's national counter-terrorism policy should be aligned with UN counter-terrorism Strategy. The UN Strategy serves as a common basis to promote measures to counter-terrorism within human rights respecting frameworks. It serves to guide capability development and capacity building. In a cross-border context, it promotes compatibility and enables better cooperation. A Member State's national counter-terrorism policy should be aligned with relevant regional strategies. Compatibility with regional strategies reduces institutional and policy differences and enables quick response capabilities and better cross-border cooperation.

37 As the way governments formulate and execute policy in this area can diverge, the topics included in the "Policy" pillar can be included in several policies (that are "written binding directives"), as long as these policies have the relevant connection and coordination necessary.

38 World Bank, p. 46: "As with any other capacity-building programme requiring technical cooperation, cybercrime capacity-building programmes are implemented to support processes of change. To take effect, such processes, as well as their objectives and expected outcomes, must be not only de f ned but also "owned" by the institution receiving support. Doing so creates an institution-wide "culture", one which is exempli f ed by leadership from above and which is implemented at all levels. Without commitment from the top to a clearly de f ned process of change, it will be di f cult for the larger institutional "cultural" issues to take root". World Bank, p. p. 228: "The need for policy and lawmakers to understand cybercrime issues and their multinational dimension is present in all countries. An UNCTAD survey, with responses from government representatives in 48 developing countries, emphasized a need to build awareness and knowledge among lawmakers and judiciary bodies with regard to cybercrime law and enforcement policy. Over half of the representatives reported di f culties in understanding legal issues related to cybercrime. Similarly, over 40 per cent noted that lack of understanding among parliamentarians can delay the adoption of relevant laws. Without awareness and knowledge, it is di f cult to formulate informed policies and laws and to enforce them".

39 International stakeholders include other States, international organizations, and international ICT players. They also include better alignment of donor contributions and partner cooperation. (World Bank, p. 49). p. 48–49.

Ref.	Sub-Capabilities	Description
2.1.1	Governance	Policy should designate an adequate high-level function that reports to top leadership, to develop and oversee deployment of the national counter-terrorist policy. In order to support the function tasked with development and oversight in its mission, policy should require relevant governmental institutions to participate in the process, submit requested information and activity reports. Policy should establish policy governance and management teams and develop a 'Policy on Policies' to guide the design and operation of the Policy Management Capability with standardized forms and processes.
2.1.2	Research and studies	Provide evidence-based understanding, context, challenges, and opportunities regarding the use of new technologies by terrorist to informed policy choices for policymakers.
2.1.3	Policy choices and coordination	Development of policy options taking a holistic approach, national resources, and instruments avails to the State.
2.1.4	Strategic alignment	Policy dealing with terrorist use of new technologies overlaps with national policies such as criminal justice, national security, and cybersecurity policies. Each of these policies may share goals or measures, they may address different risk scenarios. Thus, policy requires a holistic approach. Streamlining these policies can harmonize measures, improve e f ciency, and reduce possible operational con f icts.

4.3.2 Policy Implementation Management

National counter-terrorism policy implementation involves the effective management of implementing policies and strategies aimed at preventing, detecting, and responding to terrorist threats. Effective implementation of national counter-terrorism policies also involve coordination and cooperation among different government agencies and with international partn ć ernme l' d er خه uo Ů خه M manageme l' ere فج - en * . partn ć -terrorism policy ek tion of n ae

4.3.3 Policy Performance Management

Policy performance management involves a systematic and structured approach to monitoring and evaluating policy implementation to assess its effectiveness and make informed decisions about future policy directions. National policy

2.5.2	Stakeholder consultation	Stakeholder consultations support several important policy goals. They enable informing policymakers with information and expertise from the private sector and civil society. This is especially important in the new technologies context where the private sector is the main force in the features of the digital ecosystem. Stakeholder consultations also enable joint deliberations on the policy challenges and different measures to deal with it. It enables non-governmental stakeholders to understand the government point of view. Stakeholder participation can increase legitimacy of the policy process and improve public trust.

4.3.6 National Enabling Counter-Terrorism Components

In order to appropriately mitigate counter-terrorist threats, national policy needs to address national incident classi f cation and development of international cooperation. A comprehensive mitigation plan needs to be developed with relevant organizations. Incident classi f cation is important to manage national level incidents caused by new technologies (such as cyber incidents) at the national level and for international engagement. A standard approach to categorizing and prioritizing incidents is important for triage and prioritizing and coordinating responses.

National Incident Classi f cation is important for preparing and dealing with a terrorist event that may turn into a national level event. Given the new threat scenarios for the use of new technologies for terrorist purposes, such as a ransomware affecting an infrastructure providing essential services, mitigation and remediation may require LEAs and non-LEA's activity. Mapping and classifying these events in a comprehensive and uniform manner serves to support preparation, development of mitigation measures, and coordination across agencies.[40]

International cooperation is necessary to support cross-border law enforcement counter-terrorism activities. While necessary to deal with the terrorist threat in general, in the new technologies threat scenarios this is even more important, given the global nature of technology. Counter-terrorist law enforcement activities require stable cross-border cooperation mechanisms, as terrorist activity is carried out across borders. Counter-terrorist activities in the area of new technologies rely on such capabilities due to the inherent cross-border nature of the ICT environment.

Ref.	Sub-Capabilities	Description
2.6.1	National incident classi f cation	In order to support national level policy, a national level body should be tasked with producing a national level incident classi f cation matrix. This includes collecting input from relevant organizations, conducting discussions to produce a comprehensive national incident matrix.
2.6.2	International cooperation	The national level body tasked with developing a national level policy should monitor the development and promotion of necessary collaboration mechanisms. This includes setting international collaboration objectives, intragovernmental coordination, legal and procedural framew

t خه بر s

4.4 Institutional Pillar

This pillar aims to describe organizational, operational, and technical capabilities that are necessary to carry our core law enforcement functions described in Section 2.1. It covers governance, process, procedures, human capital, capacity building, financial resources, and technological capabilities.

4.4.1 Strategic Planning and Performance

The overall purpose of strategic planning is to ensure that an organization is able to effectively navigate a rapidly changing environment, and to adapt and respond to new challenges and opportunities. By having a clear understanding of its mission and goals, and by developing effective strategies for achieving these goals, an organization can position itself for long-term success and sustainability. Strategic planning seeks to align LEA's goals, priorities, resources, and activities to fulfil its mandate in line with leadership direction and national policies and strategies.

Performance management provides the means to measure progress and achievement towards the priorities, goals, objectives, and outcomes as defined by the strategic planning process.

Ref.	Sub-Capabilities	Description
3.1.1	National action plan	A national action plan should transpose national policy to focus on the roles and responsibilities of LEAs in carrying out the counter-terrorism life cycle. It also supports a 'whole of government' approach by clarifying LEAs interfaces with cybercrime and cybersecurity policy, and with other government organizations that take part in the counter-terrorism" life cycle.
3.1.2	Operational plan and budget	An operational plan and budget serve to set detailed organizational tasks for operations and capabilities. A dedicated budget allocated to fund these tasks supports carrying out the plan and enables performance management.
3.1.3	Performance management	Process of monitoring and evaluating institutional progress toward achieving its strategic objectives. It involves developing a system for measuring and analysing key performance indicators (KPIs) that are aligned with the organization's strategic goals.

4.4.2 Governance

Governance is an accountability mechanism with effective decision-making processes, structures, and systems to achieve its objectives and meet its legal obligations. It encompasses the development and implementation of policies, procedures, controls, and safeguards to ensure transparency, accountability, and ethical behaviour in all aspects of the organization's operations. Governance capability is essential for LEAs to manage risks, build trust with the public, ensure compliance, and deliver sustainable outcomes.

Ref.	Sub-Capabilities	Description
3.2.1	Governance structure	Formally established accountability and key decision-making authority hierarchy to managing strategic decisions, including top down and across units. Dedicated new technologies management level capabilities ('digital literacy') to support oversight.
3.2.2	Risk management	A risk management process to identify, prioritize, mitigate, and manage the institutional strategic and operational risk.

3.4.2	Counter-terrorism partnership management	Dealing with new technologies requires cooperation with private sector companies. This requires knowledge and understanding of applicable legal frameworks and other considerations that shape such relationships, including public perception and potential business risk. This function should be managed centrally to promote knowledge management and expertise of private sector policies, proceduq - ? - ge

4.4.7 Innovation Management

To effectively operate with limited resources, LEA organizations need to adopt new technologies and methods of operation, as well as the need to prepare for malicious use of new technologies. To achieve this goal, LEAs need to invest in technology scanning, and innovation development and delivery.

Ref.	Sub-Capabilities	Description
3.7.1	Technology scanning	Monitoring and analysing emerging technologies with the aim of identifying opportunities to innovate. It involves collecting and analysing data about technological advancements, new products, patents, scientifc research, market trends, and technology providers to identify technologies that could

3.8.2	Workforce skills requirements	Identification and determination of skill, knowledge, and competency requirements based on position roles and responsibilities.
3.8.3	Training needs assessment	An assessment of the workforce against skill requirements to determine current gaps or areas of improvement along required skills, knowledge, and competencies. The training needs assessment will inform training and professional development requirements.
3.8.4	Training delivery model	The training delivery model should offer effective training in each of the areas included in the LEA's knowledge base. The delivery model can be based on existing training institutions (such as police academy or university), specific unique trainings provided in-house or outsourced, as well as partner exchange programmes.
3.8.5	Career development	LEAs have a clear policy for career paths to enable retaining and promoting high quality professionals, as well as mechanisms to ensure staffing is adequate and fits mission requirements. Policy should aim to maximize benefits from training and experience gained by recruited professionals, as well as the ability to replace experts that have not performed well or are not equipped with skills for new environments.

4.4.9 Enabling Capabilities – Business Support Functions

Effective law enforcement activity requires adequate enterprise support, which also serves to support counter-terrorist capabilities.[41]

Ref.	Sub-Capabilities	Description
3.9.1	Procurement	Organization needs to have in place procedures and experts to enable contracting and purchasing of goods and services within the legal and financial framework applicable to public organizations. In order to support operational and technologically unique activity, the organization needs to have capabilities for quick procurement within the applicable framework.
3.9.2	Finance	LEAs should operate under a clear budget over the short, medium, and long term periods, that enables operations as well as building new capabilities. Budget management should enable flexibility to respond to new threats, while working within an agreed framework.
3.9.3	ICT	ICT infrastructure and capabilities are essential for proper and effective functioning of LEAs, as well as supporting dedicated counter-terrorism use of new technologies.
3.9.4	Security	The measures, practices, and resources are implemented to safeguard an organization's assets, operations, and information from potential threats, risks, or unauthorized access. It encompasses various aspects, including physical security, information security, and risk management.
3.9.5	Cybersecurity	Internal security and cybersecurity are necessary to protect sensitive information collected or received, and operational resilience. The organization applies high level cybersecurity standards to its systems, processes, and personnel to ensure operational resilience and confidentiality of information. Internal security processes enable inter-agency classified information sharing.
3.9.6	Legal	

[V]
Maturity Model

5.1 Overview

A maturity model is a framework used to assess the current state of capabilities in a particular area and provide a roadmap for improvement. In the context of Counter-Terrorism law enforcement, this maturity model can be used to assess law enforcement capability at the national level to counter the use of new technologies for terrorist purposes, and provide a roadmap for developing and improving these capabilities.

The maturity model developed here is based on the comprehensive research conducted by ENISA in its “National Capabilities Assessment Framework”, with adaptations to the context of countering the use of new technologies for terrorist purposes.

The purpose of the capability maturity model is to assist States to identify strengths and weaknesses in their current capabilities, and to support a structured approach for improving those capabilities over time. It is a tool for

The maturity model builds upon the national capability reference model. The maturity model elaborates the capabilities and sub-capabilities with a set of indicators that are framed as questions, aligned across five-levels of maturity. Each sub-capability is elaborated by questions according to the maturity level. Each maturity level is based on having fulfilled the requirements of the precious maturity level.

5.3 Maturity Levels

The maturity model consists of five levels of maturity. Each maturity level builds upon the previous level, with the goal being to reach the leading stage.

Maturity Definitions
Non-existent
No demonstrable evidence of capability exists or in practice.
Basic
Some demonstrable evidence exists in basic form, maybe ad-hoc, disorganized, poorly defined, and limited.
Established
Demonstrable evidence of a functional capability, however, it is not optimized.
Advance
Demonstrable evidence of a well-functioning capability that is considered matured and well-defined.
Leading
Demonstrable evidence of a well-functioning capability that is dynamic to fulfil its requirements based on the situation or environment.

5.4 Indicators – Assessment Structure

sit ŕ iБ / = . i خ Mf - Q i ŕ ير Ƶ ù ľ De ž i d.

5.5 Maturity Levels – Pillar, Capability, Sub-Capability

Maturity assessment enables three measurement levels at the Pillar, Capability, and Sub-Capability levels.

The general score is the average of the three sub-capabilities scores. It aims to give an overall indicator of the Member State's maturity level; however, given the differences and interconnection between policy law and institutional capabilities, it should be considered together with the individual capability and sub-capability scores. The general score is intended to give a highly generalized view of maturity levels. The capability and sub-capability scores enable focusing which areas need more attention and priorities.

The capability score is the score of the lowest common denominator amongst the sub-capabilities' score. The sub-capabilities' score is the result of the average of the detailed questions. The use of a 'lowest common denominator' is based on the interdependence between elements of the sub-capabilities.

5.6 Capability Maturity Model – Legal Pillar

1	L1	Legal Pillar	Non-Existent	Basic

1	L1	Legal Pillar	Non-Existent	Basic
1.2.2	L3	Legal Authorities for Independent Review	Legal Authorities for Independent Review does not exist	GENERAL: Are there legal authorities for independent review of the LEA's counter-terrorist value chain? Is the appointment, independence and independent discretion of the reviewed institution protected by law? Are review decisions generally public? SPECIFIC: Are there legal authorities tailored for LEA's counter-terrorist new technologies value chain?
1.2.3	L3	Application of Accepted Data Protection Principles	Application of Accepted Data Protection Principles does not exist	GENERAL: Are any of the accepted data protection principles legally binding on LEAs? SPECIFIC: N/A
1.2.4	L2	Governance of Advanced Collection and Data Analytics	Governance of Advanced Collection and Data Analytics does not exist	GENERAL: Are LEAs at maturity level 3 for data protection? SPECIFIC: Do LEAs have a speci f c policy for use of new collection technologies? Do LEAs have a speci f c policy for use of advanced data analytics?

Established	Advance	Leading
GENERAL: Are there comprehensive legal authorities for independent review of all of the LEA's counter-terrorist value chain? SPECIFIC: Does the review institution have access to independent technical advice?	GENERAL: Does the review process enable reviewing LEA's policy and procedures, and in general? (rather than just a review regarding a specific case). SPECIFIC: N/A	GENERAL: Can the review process be initiated by a third party (such as an NGO)? Are there transparency requirements on the activity of the review institution? SPECIFIC: Does the legal framework require that the review institution have technical qualifications?
GENERAL: Are accepted data protection principles part of a comprehensive framework binding on LEAs? Do LEAs have a clear mandate for a data protection office? Do LEAs have binding internal policies and procedures to implement the data protection framework? Do LEAs have data protection training for relevant managers and employees? SPECIFIC: Are LEA's ICT staff required by internal policy to cooperate with a data protection office?	GENERAL: Does the data protection office have a defined mandate based in law that integrates office in development and oversight of use of ICT in LEAs to uphold accepted data protection principles? Does the data protection office have clear rules about independence and conflicts of interests based in law? Does the data protection office have independent audit powers? Does the data protection office have mandatory reporting requirements? Is there a legal basis for independent redress for data subjects? SPECIFIC: Is there binding legal policy requiring a data protection impact assessment when developing or procuring new technologies? Is there binding legal guidance by a data protection office on conducting privacy impact assessments?	GENERAL: Is there a binding requirement for the data protection office to publish activity reports? Are there mandatory reporting requirements by a data protection office to parliament? Is the LEA or data protection office side to formal cooperation agreements with other data protection offices? SPECIFIC: Is there detailed data protection guidance on the use of new technologies? Does the data protection office train personnel in the use of new technologies and data protection?

Established	Advance	Leading
AD00CC00F0010A00E60003004010A012E1013400F0013401370134 00F0010F010A012E3FJ12J0 0 0 scTd304F00D03CA012E012E00033FJ0 0022D0027		

1	L1	Legal Pillar	Non-Existent	Basic
1.4	L2	Substantive Criminal Law		
1.4.1	L3	Terrorism Offences	Terrorism Offences Criminal Law does not exist	GENERAL:

1	L1	Legal Pillar	Non-Existent	Basic
1.4.3	L3	Ancillary Liability/		

1	L1	Legal Pillar	Non-Existent	Basic
1.5.3	L3	Advanced New Technologies LEA's Authorities	Administrative and Procedural law for unique authorities for technologies does not exist	GENERAL: Does the legal framework enable some of the advanced new technologies for LEA's authorities? Are procedural safeguards in place for these authorities? [Are there drafting activities to promote comprehensive legislative frameworks?] SPECIFIC: N/A
1.5.4	L3	Unique Counter		

Established	Advance	Leading
GENERAL: Is Member State compliant with requirements for membership in relevant multilateral LEA's cooperation treaties? Does Member State have formal agreements with Member States that are important to its counter-terrorism efforts? SPECIFIC: Is Member State compliant with requirements to be side to a multilateral cybercrime treaty? Does Member State have formal agreements with Member States that are substantial in its counter-terrorism efforts and new technologies efforts?	GENERAL: Is Member State side to relevant multilateral LEA cooperation treaties? SPECIFIC: Is Member State side to relevant multilateral LEA cooperation treaties on cybercrime?	GENERAL: Is Member State active in developing new bilateral or multilateral instruments for LEA counter-terrorism activity? SPECIFIC: Is Member State active in developing new bilateral or multilateral instruments for LEA counter-terrorism activity regarding new technologies?

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.1.2	L3	Research and Studies	Research and Studies does not exist	GENERAL: Is there a general organizational role that compiles evidence-based reports on terrorist activity for high-level policymakers? Are procedures for preparation of reports on terrorist activities considered to be ad hoc or informal? SPECIFIC: Is there a general organizational role that complies evidence-based reports on terrorist use of new technologies for high-level policymakers? Are the roles in charge of reports on terrorist activity coordinated with roles reporting on terrorist use of new technologies?

Established	Advance	Leading

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.1.3	L3	Policy Choices and Coordination	Policy Choices and Coordination does not exist	GENERAL: Is there a general organizational role that integrates information as to national resources and instruments to counter-terrorist activity for high-level policymakers? Are procedures for preparation of such reports on terrorist activities considered to be ad hoc or informal? SPECIFIC: Is there a general organizational role that integrates information as to national resources and instruments to counter-terrorist activity in the new technologies' context for high-level policymakers? Are the roles in charge of reports on counter-terrorist activity coordinated with roles reporting on counter-terrorist use of new technologies?

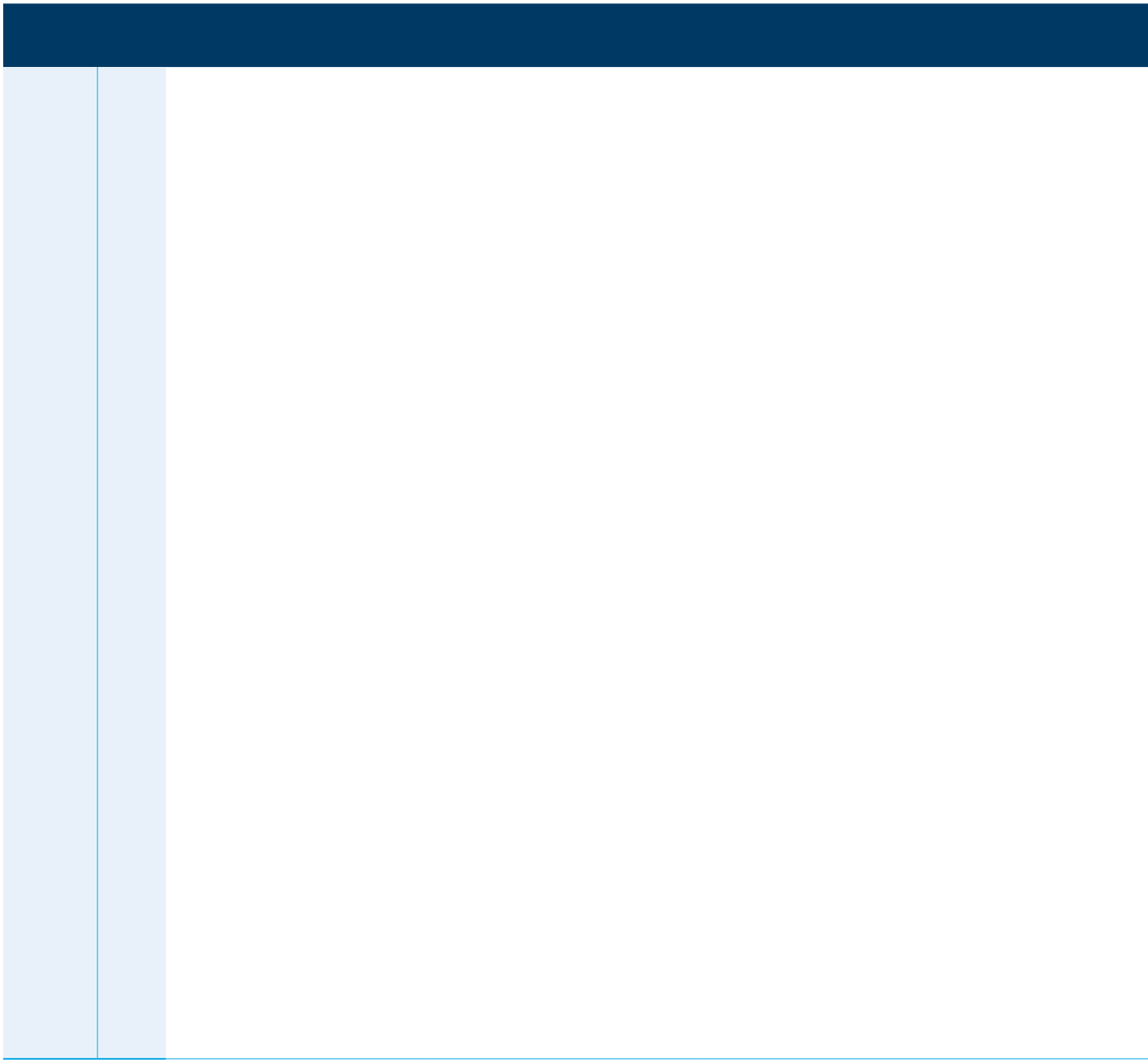
Established	Advance	Leading
GENERAL: Is there a comprehensive approach for policy development and preparation of reports on resources and instruments to terrorist activities? Are there specialized personnel for the preparation of such reports? Are reporting activities structured, documented, and repeatable? SPECIFIC: Does a comprehensive approach cover terrorist use of new technologies? Are dedicated new technologies experts' part of the preparation of reports?	GENERAL: Is there a dedicated unit in place to compile reports on policy options? Does policy obligate other public organizations to participate and submit information to such activity? Is there a full-time research capability? Is academia consulted in the compilation of information, knowledge, and development of policy options? Is there an independent review of policy to improve focus and quality of recommendations? SPECIFIC: Does policy obligate governmental agencies in charge of parts of the technological ecosystem (i.e., Communications Ministry) to provide information and expertise to the activity? Are non-governmental organizations part of the development of policy options? Is there a full-time research capability for new technologies? Is academia and inde ʊ ʊ d inde ˜ ž M or new tech Ŏ e c ľ ş ű e * Ô Ô SPECIFIC:	a SPECIFIC:

*) thÔ pental + s U

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.1.4	L3	Strategic Alignment	Strategic Alignment does not exist	GENERAL: Is there a general organizational role that integrates information as to counter-terrorism national policies and efforts for high-level policymakers? Are procedures for preparation of such reports on terrorist activities considered to be ad hoc or informal. Does adoption of new policies or adaptation of policies in this area take into account such information? SPECIFIC: Is there a general organizational role that integrates information as to national polices and efforts to counter risk from new technologies for high-level policymakers? Does adoption of new policies or adaptation of policies in this area take into account such information? Do the roles in charge of reports on policies and efforts share information about policies regularly?

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.2	L2	Policy Implementation Management		
2.2.1	L3	Capability Development	Capability Development does not exist	GENERAL: Is there an adequate high-level function that reports to highest government level about development and deployment of national Counter-Terrorism capabilities? Is capability development considered to be ad hoc or informal? SPECIFIC: Is Counter-Terrorism new technologies included in national Counter-Terrorism policy capability assessment and development?

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for coordinating national Counter-Terrorism capability assessment and development? Is information about capabilities collected in a central unit? Does the approach use similar taxonomies to describe Counter-Terrorism capabilities? Is the approach structured, documented, and repeatable? Is the approach informed by threat assessments? Does the capability development inform human capital and training policies? Does capability development guide procurement priorities? Does capability development cover the Counter-Terrorism value chain? SPECIFIC: Does the comprehensive approach cover capabilities to deal with malicious use of new technologies? Does the comprehensive approach cover potential uses of new technologies by LEAs and necessary support for Counter-Terrorism LEA's value chain? Are dedicated new technologies experts' part of policy coordination?	GENERAL: Is capability development done through both a medium-term and long-term development plan? Is capability development informed by industry and academic knowledge about necessary skillsets? Are capability development efforts reviewed annually? SPECIFIC: Is capability development aligned with private sector skillsets?	GENERAL: Are capability development efforts reviewed by an external assessor? Is capability development for Counter-Terrorism staff delivered through a central training facility? Are there mechanisms in place to enable short-term immediate capability development? Are LEA capability development requirements aligned with academic training programmes? SPECIFIC: Are LEA capability development requirements aligned with academic training programmes for new technologies?



Established	Advance	Leading

GENERAL:

Is there a comprehensive approach for oversight of threat interventions?

Is there a LEA triage function to decide about threat interventions?

Does the approach use similar taxonomies to describe Counter-Terrorism threats and interventions?

Is there an operational situational awareness capability to map developing threats?

Is the approach structured, documented, and repeatable?

Is the approach informed by threat assessments?

Does the approach guide operations in the Counter-Terrorismvalu l· ή Is thy th Ş خه at interventac teat M e a ǫ ᴺ atabo erroris خه orism e

oversig ı eat - ?

Is there ak thr ę ism e خه ae ҭ ҭ (re e scr b ═ خه بر M e ı or
oversig ı eat - ?

Is there akeoriom e , / rr

Count e' Count rori η ثا '

Is there at inter?

ȕ ľ ?

Isb ئج ȕ / خه * p ?
Countp ' ŝ mp Ǔ ľ

Is there Ϸ or ı atab خه v ď -
Count ﻬ ori

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.2.3	L3	Institutional Roles and Responsibilities	Institutional Roles and Responsibilities does not exist	GENERAL: Is there a general policy tasking LEAs and other organizations with a counter-terrorist mandate? SPECIFIC: Does policy deal with counter-terrorist use of new technologies?

Established	Advance	Leading
GENERAL: Is there a detailed policy mandate for each counter-terrorism organization? Does the policy mandate deal with coordination mechanisms between LEAs and other Counter-Terrorism organizations? Does the policy mandate de f ne interaction with non- Counter-Terrorism organizations as part of the Counter-Terrorism value chain? Is the policy mandate supported by an adequate budget that covers for short-term, medium-term and long-term periods? SPECIFIC: Does the policy deal comprehensively with CTcounter-terrorism new technologies activities?	GENERAL: Is there a comprehensive approach for institutional roles and responsibilities in the Counter-Terrorism value chain? Are there clearly de f ned communication lines and information sharing duties between Counter-Terrorism organizations? Does the policy deal with covering national crisis coordination? Does the policy deal with interactions with Counter-Terrorism support institutions? Is the policy regularly reviewed to locate 'blind spots' in Counter-Terrorism operations? SPECIFIC: Are there clear operational procedures between LEAs, cybersecurity, and national security agencies in dealing with cyber incidents? Does policy coordination deal with joint use of ICT or new technologies capabilities to enable resource pooling in capability development?	GENERAL: Has a national exercise or national operational event informed national policy regarding roles' responsibilities and coordination? SPECIFIC: N/A

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.2.5	L3	Collaboration Management	Collaboration Management does not exist	GENERAL: Are collaboration management practices considered to be ad hoc or informal? SPECIFIC: Does collaboration management with counter-terrorist use of new technologies exist?

Established	Advance	Leading
GENERAL:	GENERAL:	
Is there a comprehensive approach for collaboration management?	Are there clearly de f ned communication lines and information sharing duties between Counter-Terrorism organizations?	
Are there specialized personnel for collaboration management?	Does the policy cover dealing with national crisis coordination?	
Are collaboration management practices structured, documented, and repeatable?	ant?	
Do LEAs engage regularly with other Counter-Terrorism organizations to discuss cooperation and coordination?	Is there policy deh	
Does the policy mandate deal with coordination mechanisms between LEAs and other Counter-Terrorism organizations?	Does thn ' Ô y ' l' 0 errori ş ew technologiea s th i '	
Does the policy mandate de f ne interaction with non-Counter-Terrorism organizations as part of the Counter-Terrorism value chain?	Does thsessmeisi˜ Ő tivns ia ¯ ˚ / er d , / . i \ ri >	
Is there a shared taxonomy to describe Counter-Terrorism threats and interventions?		
Is there an operational situational awareness capability to manage operational collaboration?		
Is the approach structured, documented, and repeatable?		
Is the approach informed by threat assessments?		
Does the approach guide operations in the Counter-Terrorism value chain?		
SPECIFIC:		
Does the policy deal comprehensively with counter-terrorism new technologies activities?		

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.3.3	L3	Policy Review Management	Policy Review Management does not exist	GENERAL: Is policy review considered to be ad

Established	Advance	Leading
GENERAL: Is there a comprehensive approach to review Counter-Terrorism policy goals and measures? Are Counter-Terrorism policy review management practices structured, documented, and repeatable? Are Counter-Terrorism policy goals clearly articulated to enable policy review? Are policy review activities adequately resourced? Is the policy review process supported by reporting requirements? SPECIFIC: Do policy review activities cover Counter-Terrorism activities to counter-terrorist use of new technologies? Do policy review practices cover LEA's use of new technologies?	GENERAL: Is the policy review informed by research, intelligence, and analysis? Is the policy review informed by comprehensive consultations with government Counter-Terrorism organizations? Is there a dedicated policy review unit which is adequately resourced? SPECIFIC: Is the policy review based on emerging technological trends? Is the policy review supported by an adequate technological expert?	GENERAL: Is the policy review process reviewed and updated on a regular basis for continuous improvement? Is there a policy review advisory body that includes outside experts such as from industry, other government bodies, etc.? SPECIFIC: N/A
GENERAL: Is there a comprehensive approach to strategic communications? Are there specialized personnel for public / community communications? Are communication practices structured, documented, and repeatable? Are there clear goals for communication policy? Does communication policy explain LEA's challenges in dealing with terrorists and necessary CTcounter-terrorist activities? SPECIFIC: Does the communication policy raise awareness regarding terrorist use of new technology? Is there a dedicated public POC for public reports on Counter-Terrorism new technologies risks or threats? Do LEA's use social media for communication and public engagement? Does the communication policy explain LEA's challenges in dealing with terrorists use of new technologies and the necessary CTcounter-terrorist activities? Does the communication policy address public private partnerships?	GENERAL: Is the communication policy aligned to the overall organization strategy and priorities? Is there a dedicated public affairs unit in place? Are public / communications policy goals measured and monitored for effectiveness against clear performance metrics? Is public / communications engagement regularly reviewed and audited? Are there standards and requirements for public / communications engagement? Does the communication policy deal with human rights ane þ ڕ s 0 enar pt? regucy goalqed Ž 2 omm mc ě ۔ sent?	

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic

	Established	Advance	Leading
nne ?t			

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for incident classi f cation? Are there comprehensive reporting mechanisms to enable incident classi f cation? Is there a national level organization tasked with developing the national incident classi f cation system? Is there a shared national taxonomy of incident classi f cation across Counter-Terrorism organizations and operations? Is the national classi f cation scheme communicated to all public organizations? Does the policy clearly de f ne who can declare a national incident? Does the national incident classi f cation enable de f ning authority in charge of the event? SPECIFIC: Does the national incident classi f cation scheme include incidents caused as a result of malicious use of new technologies? Insert:	GENERAL: Is the national incident classi f cation scheme based on ongoing national reviews to locate critical functions? Is the classi f cation scheme informed by regulatory agencies in charge of important services? Is the national incident classi f cation scheme aligned to the overall strategy and priorities? Are the thresholds of the national incident classi f cation scheme reviewed regularly? Is the national classi f cation scheme binding on all public organizations? SPECIFIC: Is the national classi f cation scheme informed by intelligence about possible misuse of new technologies?	GENERAL: Is the national classi f cation system reviewed and updated on a regular basis for continuous improvement? Has the national classi f cation system been informed by an exercise or dealing with a national level incident? SPECIFIC: N/A

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.6.2	L3	International Coordination	International Coordination does not exist	GENERAL: Are international coordination practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for international cooperation amongst all Counter-Terrorism organizations? Are there specialized personnel for international coordination? Are international coordination practices structured, documented, and repeatable? Is information about international cooperation shared amongst Counter-Terrorism organizations? SPECIFIC: Does the policy cover trusted communications with other LEAs? Does the policy include a programme to join to agreements that apply to cross-border cooperation along the Counter-Terrorism new technologies value chain? Does the policy include LEA's participating in a trusted LEA's 24/7 cybercrime network (such as Interpol)? Does the policy advance Counter-Terrorism organizations exchange of information at a tactical level?	GENERAL: Is there an international cooperation plan and practices that is aligned to the overall organization strategy and priorities? Is there a dedicated international cooperation unit in place? Is international cooperation performance measured and monitored for effectiveness against clear performance metrics? Are international cooperation activities regularly reviewed and audited? Are there standards and requirements for international cooperation? SPECIFIC: Does the policy de f ne controls for international cooperation regarding sharing of information and the use of technology concerning human rights and gender, and the rule of law? Does the policy advance the LEAs who regularly participate in relevant Counter-Terrorism new technologies international discussions?	GENERAL: Are relevant international cooperation practices reviewed and updated on a regular basis for continuous improvement? Are elements of international cooperation publicly disclosed when in the interest of the public? Are international cooperation practices regularly reviewed and audited by an independent body? Is the policy developed through regular engagement with non-governmental stakeholders in other countries which are important to Counter-Terrorism operations? SPECIFIC: Does the policy advance Member State participation in international discussions regarding Counter-Terrorism and new technologies? (Such as heading an international task force, chairing a committee in an international organization, hosting an international/regional conference.) Does the Member State engage regularly with new technologies non-governmental stakeholders in other countries which are important to Counter-Terrorism operations?

5.8 Capability Maturity Model – Institutional Pillar

3	L1	Institutional Pillar	Non-Existent	Basic
3.1	L2	[illegible] 9ppg 0 D R 17an/Ac Td(1)uBT9 001Tc 01Tw 8.479 0 Td(A)4 2n13T4.1(GEN11. (ER)2 TdAL:00F004.6		

Established	Advance	Leading

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for performance management? Are there specialized personnel for performance management? Are performance management practices structured, documented, and repeatable? SPECIFIC: N/A	GENERAL: Is there a performance management or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated performance management unit or focal point in place? Are performance metrics clearly de f ned, measurable, and monitored? Are performance management activities regularly reviewed and audited? Are there standards and requirements for performance management? s k ŕ = = ŕ ent SPECIFIC: Are there speci f c performance targets of operational safeguards for information sharing, data, technology, human rights, and gender?	GENERAL: Are relevant performance management practices reviewed and updated on a regular basis for continuous improvement? Are elements of performance management reports publicly disclosed when in the interest of the public? Are performance management practices regularly reviewed and audited by an independent body? Do performance management practices oni خ A ,) erati ב n a roem pn oogy, h Ů , and emen - der?

3	L1	Institutional Pillar	Non-Existent	Basic
3.2.2	L3	Risk Management	Risk Management Capability does not exist	GENERAL: Are there elements of risk management processes in place? Are the risk management practices considered t) pi خه M

Established	Advance	Leading
GENERAL:		
Is there a comprehensive approach for risk management?		
Are there specialized n V		
Are there specialized Ń yM ¯	я	

3	L1	Institutional Pillar	Non-Existent	Basic
3.2.4	L3	Human Rights and Gender Impact Assessment	Human Rights and Gender Impact Assessment Capability does not exist	GENERAL: Are there some elements of human rights and gender impact assessment practices in place? Are human rights and gender impact assessment practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading

3	L1	Institutional Pillar	Non-Existent	Basic
3.2.5	L3	Data Protection	Data Protection Capability does not exist	GENERAL: Are there some elements of data protection practices in place? Are the data protection practices considered to be ad hoc or informal? Do LEAs consider data protection principles when carrying out its activities? SPECIFIC: N/A

Established	Advance	Leading

3	L1	Institutional Pillar	Non-Existent	Basic
3.3.2	L3	Threat Management	Threat Management Capability does not exist	GENERAL: Are there elements of a threat management process in place? Are threat management practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for threat management? Are there specialized personnel for threat management? Are threat management practices structured, documented, and repeatable? Are threat management activities coordinated with other national security organizations? SPECIFIC: Do threat management practices cover new technologies risk to critical social and governmental activities? Do threat management activities address terrorist use of new technologies?	GENERAL: Is there a threat management plan and practices that is aligned to the overall organization strategy and priorities? Is there a dedicated Threat Management Unit? Is threat management performance measured and monitored for effectiveness against clear performance metrics? Are threat management activities regularly reviewed and audited? Are there standards and requirements for threat management? Is there threat management and arrangements to share information with international partners? SPECIFIC: Does threat management incorporate relevant human rights, gender, and the rule of law considerations? Does a threat management unit employ full-time technologists? Does a threat management unit have working relationship with new technologies providers? Does a threat management unit have working relationships with civilian authorities to assess civilian sector critical processes and vulnerabilities?	GENERAL: Are relevant threat management practices reviewed and updated on a regular basis for continuous improvement? Are elements of threat management publicly disclosed when in the interest of the public? Are threat management practices regularly reviewed and audited by an independent body? Are national threat management activities coordinated with allies? Insert SPECIFIC: Are threat management practices regularly reviewed and audited by an independent body speci f cally concerning use of technology and human rights and gender?

3	L1	Institutional Pillar	Non-Existent	Basic
3.3.3	L3	Information Sharing	Information Sharing Capability does not exist	GENERAL: Are there elements of an information sharing process in place? Are information sharing practices cct e ǿ Ő - Are information sharing

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for information sharing? Are information sharing practices structured, documented, and repeatable? Is there a secure technical infrastructure in place for information sharing? Is there an information classi f cation system and prioritization in place to facilitate information sharing? SPECIFIC: Is there a secure technical infrastructure for sharing technical indicators and information related to new technology risks and mitigations? Are there information sharing arrangements with new technology providers?	GENERAL: Is there an information sharing plan and practices that is aligned to the overall organization strategy and priorities? Is there information sharing agreements and arrangements to share information with international partners? Is there 0 ae information sharing agrt = e ~ tion sharing plan - M ~ l _ ŭ M d teant = , - acttion s + - Ômo - = ŕ ti and a tha aan ĭ l' / sls there informas *] 0 ~ ˛ F = a	

3	L1	Institutional Pillar	Non-Existent	Basic
3.4.2	L3	Counter-Terrorism Partnership Management	Counter-Terrorism Partnership Management Capability does not exist	GENERAL: Are there informal policies or elements of Counter-Terrorism partnership management? Are ŕ man * - ŭ ŭ

Established	Advance	Leading

3	L1	Institutional Pillar	Non-Existent	Basic
3.4.4	L3	International Cooperation	International Cooperation Capability does not exist	GENERAL: Are there elements of international cooperation in place? Are international cooperation practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL:		

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for oversight management? Are there specialized personnel for oversight management? Are oversight management practices structured, documented, and repeatable? Do reporting mechanisms exist to support oversight management? SPECIFIC: Are there real-time situational awareness capabilities to support counter-terrorist use of new technologies? Is counter-terrorism new technologies capabilities support available across organizational units?	GENERAL: Is there an oversight management plan and practices that is aligned to the overall organization strategy and priorities? Is there a dedicated oversight management unit in place? Is oversight management performance measured and monitored for effectiveness against clear performance metrics? Are there standards and requirements for oversight management? SPECIFIC: Is there a national technical situational awareness capability? Are technical counter-terrorism capabilities managed according to a central policy setting priorities and resources to support counter-terrorism operations?	GENERAL: Are relevant oversight management practices reviewed and updated on a regular basis for continuous improvement? Are elements of oversight management reports publicly disclosed when in the interest of the public? o ű eŎ بز M ئ ك er t' s - - ŭ ' '

3	L1	Institutional Pillar	Non-Existent	Basic
3.5.3	L3	Investigations Management	Investigations Management Capability does not exist	GENERAL: Are there elements of investigations management practices in place? Are investigations management practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for investigations management? Are there specialized personnel for investigations? Are investigations management practices structured, documented, and repeatable? SPECIFIC: Do investigators have advanced capability to investigate, analyse, and produce evidence of basic technologies (i.e., the Internet, social media, etc.)? Do investigators have the ability to conduct basic digital forensics?	GENERAL: Is there an investigation management plan that is aligned to the overall organization strategy and priorities? Is there a dedicated investigations unit in place? Is investigations management performance measured and monitored for effectiveness against clear performance metrics? Are investigations regularly reviewed and audited? Are there standards and requirements for investigations? SPECIFIC: Do investigators have advanced capability to investigate, analyse, and produce evidence of new technologies (i.e., the Dark Web, cryptocurrencies, etc.)? Do investigators have the ability to conduct advance digital forensics? Are there human rights and gender and the rule of law safeguards in place for the use of intelligence and technology?	GENERAL: Are relevant investigations and investigations management practices reviewed and updated on a regular basis for continuous improvement? Are elements of investigations and cases publicly disclosed when in the interest of the public? Are investigations practices regularly reviewed and audited by an independent body? SPECIFIC: Are intelligence practices regularly reviewed and audited by an independent body speci f cally concerning use of technology and human rights and gender?
GENERAL: Is there a comprehensive approach for Counter-Terrorism LEA's actions? Are there specialized personnel for Counter-Terrorism LEA's actions? Are Counter-Terrorism LEA's actions structured, documented, and repeatable? SPECIFIC: Do Counter-Terrorism LEA's actions have the capability to disrupt or prevent terrorist use of basic technology (i.e., the Internet, social media, etc.)? Are there specialized personnel for digital operations?	GENERAL: Is there an Counter-Terrorism law enforcement operational plan for the use of the LEA's actions toolset that is aligned to the overall organization strategy and priorities? Is Counter-Terrorism LEA's actions measured and monitored for effal med Q Ļ ern th خه e ect Ό ¯ ʎ d pr o Ŕ خه M ų o Ů	

3	L1	Institutional Pillar	Non-Existent	Basic
3.5.5	L3	Criminal Justice Interface Management	Criminal Justice Interface Management Capability does not exist	GENERAL: Are there elements of criminal justice interface in place? Are criminal justice interface p ŷ mina

Established	Advance	Leading
GENERAL:		
Is there a comprehensive data and information management approach in place?		
Are there specialized personnel supported by ICT for data and information management?		
Are data and information management practices structured, documented, and repeatable?		
Are data and information management solutions designed for Counter-Terrorism law enforcement end users?		
Are there role-based security restrictions on data and information access?		
Is data collected and organized in a comprehensive manner?		
SPECIFIC:		
Is technical threat intell è ?		

3	L1	Institutional Pillar	Non-Existent	Basic
3.7	L2	Innovation Management		
3.7.1	L3	Technology Scanning	Technology Scanning Capability does not exist	GENERAL: Are there elements of technology scanning in place? Are technology scanning practices considered to be ad hoc or informal? SPECIFIC: N/A
3.7.2	L3	Innovation Development and Delivery	Innovation Development and Delivery Capability does not exist	GENERAL: Are there elements of innovation development and delivery in place? Are innovation development and delivery practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for conducting technology / industry scanning? Are technology scanning practices structured, documented, and repeatable? SPECIFIC: N/A	GENERAL: Is technology scanning and priorities informed by and aligned to the overall organization strategy and priorities? Are technology scanning practices measured and monitored for effectiveness against clear performance metrics? Are there standards and requirements to conduct technology scanning? Are current capability requirements and challenges de f ned when conducting technology scanning? SPECIFIC: N/A	GENERAL: Are relevant technology scanning practices reviewed and updated on a regular basis for continuous improvement? SPECIFIC: N/A
GENERAL: Is there a comprehensive approach for innovation development and delivery? Are innovation development and delivery practices structured, documented, and repeatable? Is innovation embraced and promoted? SPECIFIC: Does this approach apply to LEA's activity against terrorist use of new technologies?	GENERAL: Is there an innovation strategy or plan that is aligned to the overall organization strategy and priorities? Is innovation performance measured and monitored for effectiveness against clear performance metrics? Are there specialized personnel for change management to deliver innovation? Is there a culture to encourage innovation? À@Ð æ Y 0 B Ð + LÀ Ð 0 0 B Ð Ð < ` LÀ . 4 + - . 7 d€ à 4 ì Ð - æ Ð ð R 3@ ð !ð	

3	L1	Institutional Pillar	Non-Existent	Basic
3.7.4	L3	Innovation Support	Innovation Support Capability does not exist	GENERAL: Are there some elements of innovation support in place? Are innovation support practices considered to be ad hoc or informal? SPECIFIC: Does innovation support capability apply to ICT?
3.8	L2	Human Capital, Training, and Workforce Development		
3.8.1	L3	Workforce Skills Requirements	Workforce Skills Requirements Capability does not exist	GENERAL: Are there elements of de f ning workforce skills requirements? Are workforce skills requirements practices conside Ő c ė ź ŭ Nerw) esk Ľ - e x

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for innovation support? Are the resources (financial, people, infrastructure, etc.) dedicated to support innovation? Are innovation support practices structured, documented, and repeatable? SPECIFIC: Does this approach apply to LEA's activity against terrorist use of new technologies?	GENERAL: Is innovation support aligned to innovation strategy or plan, and the overall organization strategy and priorities? Is innovation support performance measured and monitored for effectiveness against clear performance metrics? SPECIFIC: N/A	GENERAL: Are relevant innovation support practices reviewed and updated on a regular basis for continuous improvement? SPECIFIC: N/A

3	L1	Institutional Pillar	Non-Existent	Basic
3.8.3	L3	Training Delivery Model	Training Delivery Model Capability does not exist	GENERAL: Are there elements to delivery training in place? Are training delivery model practices considered to be ad hoc or informal? SPECIFIC: N/A
3.8.4	L3	Career Development	Career Development Capability does not exist	GENERAL: Are there elements of career development and progression in place? Are career development practices considered to be ad hoc or informal? SPECIFIC: N/A
3.9	L2	Enabling Capabilities – Business Functions		
3.9.1	L3	Procurement	Procurement Capability does not exist	GENERAL: Are there elements of procurement practices in place? Are procurement practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive finance approach and control in place? Are there specialized personnel for finance? Are finance practices structured, documented, and repeatable? SPECIFIC: Is there a dedicated budget for required technology capability? Insert	GENERAL: Is there a financial management strategy or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated finance unit in place? Is financial management performance measured and monitored for effectiveness against clear performance metrics? Are finances regularly reviewed and audited? SPECIFIC: N/A	GENERAL: Are relevant financial management practices reviewed and updated on a regular basis for continuous improvement? Are elements of financial performance or reports publicly disclosed when in the interest of the public? Are finances regularly reviewed and audited by an independent body? SPECIFIC: N/AN/A

GENERAL:

3	L1	

Established	Advance	Leading
GENERAL:	GENERAL:	
Is there a comprehensive security approach and controls for physical and personnel security based on a threat assessment?	Is there a security strategy or plan that is aligned to the overall organization strategy and priorities and overall threat assessment?	
Are there specialized personnel for security?	Is the security strategy aligned with other security organizations?	
Are security practices structured, documented, and repeatable?	Is there a dedicated security unit in place?	
SPECIFIC:	Is security policy and practices informed þ ols 0 ų M a Ě e	
Are there personnel and physical security measures in place to protect technology, technology capabilities, and sensitive information?	SPECIFIC:	
	security measures in / e totect pri / I Ā ŭ e? ŷ orme *) ology 0 - e?	
	SPEC ą̈ FIC:	

Is the legal departmenttiv Ż v ضُ Ó Ř

Established	Advance	Leading
GENERAL: Do LEAs have an in-house legal department to support all of its activities? Is the head of the legal department part of senior management? Are the roles and main services of the legal department documented? Is there an escalation mechanism to escalate legal issues? Does the legal department employ legal experts in the LEA's areas of operation (see legal pillar)? SPECIFIC: Is the legal department involved in reviewing use of technology, human rights and gender in LEA's activity? Is there speci f c guidance of when legal counsel is required regarding use of technology, human rights and gender? Does the legal department have an electronic evidence legal expert? Does the legal department proactively provide guidance and counsel on the use of technology, human rights and gender?	GENERAL: Is the legal work plan part of the overall organization strategy and priorities? Is legal performance measured and monitored for effectiveness against clear performance metrics? Does the legal department employ legal experts for all of the main f elds of LEA's operations and support activities? Does the legal department carry out training and continuing legal ed l' M˜ d) ـين خه ـ ز y Ó Ř Does the legal department have l l' ز ُ = pr t ير M ion legal , xper? Does the legal department have al , xperl o ń e l' o ā melti l' e ‘ s? Does the legal department have l legal	

United Nations Office of Counter-Terrorism
United Nations Headquarters