UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

INTERPOL

Funded by
the European Union

Cybersecurity and New Technologies

Law Enforcement Capabilities Framework for New Technologies in Countering Terrorism

Disclaimer

The opinions, findings, conclusions, and recommendations expressed herein do not necessarily reflect the views of the United Nations, The International Criminal Police Organization (INTERPOL), the Governments of the Europe Union or any other national, regional, or global entities involved.

The designation employed and material presented in this publication does not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

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 the exploitation of new and emerging technologies for terrorist purposes and to leverage new and emerging technologies in the fight against terrorism as part of this effort, in full respect of human rights and the rule of law.

Our Offices stand ready to continue to support Member States and other partners to prevent and counter-terrorism in all its forms and manifestations and to take advantage of the positive effects of technology in countering terrorism.

Vladimir Voronkov
Under-Secretary-General, United Nations Office of Counter-Terrorism
Executive Director, United Nations Counter-Terrorism Centre

Stephen Kavanagh
Executive Director,
Police Services INTERPOL

Acknowledgements

This document has been developed through the contributions and reviewed by a wide range of stakeholders. Specifically, the United Nations Office of Counter-Terrorism (UNOCT) wish to acknowledge the contribution made by:

- **Ms. Nina Sunde** – Police Superintendent (PhD), Norwegian Police University College

Terms and Definitions

Accepted Data Protection Principles	Global frameworks that apply to collection and processing of personal data such as the OECD privacy principles, APEC privacy principles, Counsel of Europe Convention 108, African Union Convention in Cyber Security and Personal Data.
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.
Administrative Authorities	(1) Disruption of terrorist financing activity, through cooperation with Financial Intelligence Units and tax authorities. This activity could be challenged by new technologies that enable transfers, including cryptocurrencies. (2) Disruption of recruitment, incitement, and communication. Internet and social media enable reaching wide audiences and serves as a platform for communication, incitement, and recruitment. Disruption of such activity (and collection of information on actors) requires developing a framework for working with different Internet intermediaries. (3) Identification, tracing, freezing, seizure, and confiscation of proceeds of crime.
Advanced New Technologies LEA Authorities	(1) Ability to conduct operations on the Dark Web. (2) Remotely accessing a computer or other device and collecting information. (3) Remotely and covertly accessing a computer or other device and collecting information. (4) Stopping malicious use of infrastructures and websites to create computer-related risk or damage. (5) Stopping dissemination of clearly malicious terrorist speech such as incitement or recruitment through websites or platforms, by cooperation with private sector actors. (6) Ability to seize cryptocurrencies.
Ancillary Liability/ Material Support/ Accessory Offences	Offences that apply to actors that carry out some part of the illegal activity but not all of it. These offences apply to an 'attempt' to carry out the criminal activity, as well as aiding or abetting the offences. 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.

Artificial 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 corrections and rehabilitation.
Cybercrime Offences	Computer-related criminal offenses that prohibit activities which target the confidentiality, integrity, or availability of computers, networks, and data stored in them.
General Law Enforcement Authorities	Collection of information, summon witnesses, request for production of information or object, questioning, and detention for questioning.
Intelligence	The product resulting from collecting, developing, disseminating, analysing, and interpreting of information gathered from a wide range of sources, to inform decision makers for planning purposes to take decisions or actions – strategic, operational or tactical level. Intelligence should be collected, retained, used and shared in compliance with relevant Member State obligations under international human rights law
Criminal Investigations	The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support the prosecution in legal proceedings.
Investigations Management	Management of investigations using general law enforcement authorities, LEA new technologies digital authorities and advanced LEA new technologies digital authorities.
Law Enforcement Actions	Typically describes law enforcement actions, based on legal authority, taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e., content removal, asset seizures), etc.
Law Enforcement Agency Counter-Terrorism 'Value Chain'	Law Enforcement Agency counter-terrorism value chain describes core law enforcement operational capabilities which includes "general law enforcement authorities" and "unique counter-terrorist authorities"; law enforcement new technologies authorities; advanced law enforcement new technologies authorities; and law enforcement actions. It is complemented by a definition for "use of new technologies by law enforcement".[1]
New Technologies	While the New Technologies terminology covers a wide range of different technologies,[2] for the purpose of this document new technologies refer to the use and abuse of such new technologies as the Internet, social media, cryptocurrencies, facial recognition, and the darknet.[3]

1 As noted this definition should be revisited to ensure it is up to date with technological advances.

2 Artificial Intelligence, Internet of Things, block chain technologies, crypto-assets, drones and unmanned aerial systems, DNA, fingerprints, cyber technology, facial recognition, and 3D printing.

3 CT TECH Programme Document – Annex I Description of the Action.

New Technologies-Related Terrorist Risk[4]	Ransomware attacks / Production of malware / DDOS attacks / BGP hijacking / Use of encrypted communications/Activity on the "Dark Web" in general/Criminal abuse of cryptocurrencies/ Social engineering threats – phishing/smishing/vishing/Business email compromise/ "Grey infrastructure" – "bulletproof" hosting/Anonymization tools/Money muling/ Disinformation and misinformation / Use of 3D printing to produce weapons.
New Technologies LEA Authorities[5]	(1) Expeditious preservation of specified computer data, including traffic data. (2) Expedited preservation and partial disclosure of traffic data. (3) Order to produce digital evidence. (4) Search and seizure of stored computer data (5) Real-time collection of communication traffic data. (6) Interception of communication content data.
New Technologies Terrorist Offences	Terrorist criminal offences using new technology, including (1) Cyber-attacks against critical infrastructure; (2) Incitement using the Internet or social media; (3) Recruitment through the Internet or social media; (4) Spread of terrorist content or radicalization to terrorism on the Internet or social media; and (5) Terrorism financing.
Procedural Legal Safeguards	(1) Clear definition of circumstances and grounds justifying use of powers. (2) Limitation of the scope and duration of use of such powers. (3.) Consideration of the impact on rights, responsibilities, and legitimate interests of third parties. (4). Fair Process. (5) Requirement for judicial or other independent authorizing body, dependent on risk and context.
Rehabilitation	In a criminal justice context, the term 'rehabilitation' is used to refer to interventions managed by the corrections system with the aim to change the offender's views or behaviour to reduce the likelihood of re-offending and prepare and support the offender's reintegration back into society.
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.
Rule of Law	Exercise of functions and powers is based on clear provisions of law that exhaustively enumerate the powers in question. The exercise of such functions and powers may never violate peremptory 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.
Terrorism	Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism.[6]

4 Based on: Europol, Internet Organized Crime Threat Assessment (IOCTA), Strategic, policy and tactical updates on the fight against cybercrime, https://www.europol.europa.eu/publications-events/main-reports/iocta-report, and: ENISA, ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

5 Based on the Council Of Europe Convention on Cybercrime.

6 See S/RES/1566 (2004), para. 3.

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 defined legitimate aim, as permitted by international law. (2) Be proportionate to the benefit obtained in achieving the legitimate aim in question. (3) If the State is involved, as a party, in an ongoing armed conflict, the above provisions shall apply also to securing compliance with principles and provisions of international humanitarian law, without prejudice to the obligation to comply with international human rights and refugee law. (iv) If compelling reasons require the establishment of specific powers for certain authorities: (1) Such powers should be contained in stand-alone legislation capable of being recognized as a unique exception to customary legal constraint; (2) The provisions under which such powers are established should be subject to sunset clauses and regular review; and (3) The use of such powers for any purpose other than the combating of terrorism must be prohibited.
Unique Administrative Support	Legal powers to enable quick procurement, contracting with subject matter experts, and contracting within operational constraints.
Unique Counter-Terrorist Authorities	(1) Listing terrorist entities. (2) Filing secret evidence (3) Protection of human sources. (4) Special Investigation Techniques that include techniques used to gather information, such as electronic or other forms of surveillance and undercover operations, in such a way so as not to alert the target person(s) and for the purpose of detecting and investigating offences.[8]
Use of New Technologies by Law Enforcement	(1) Operational level use of new technologies that include mobile phones, body cameras, remote surveillance devices, tactical drones. (2) Biometric facial recognition in specific cases to improve identification and prevention. (3) Artificial intelligence (AI). (4) Big data analysis (5) Cryptography for dealing with ransomware and in accessing encrypted content. (6) Cryptocurrency analysis capabilities.
Zettabyte	One zettabyte is equal to one billon terabytes.

7 Based on UN Special Rapporteur on Counter-Terrorism and Human Rights on restrictions on rights and freedoms,

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/16/51), Practice XX, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/G1017898.pdf?OpenElement.

8 Council of Europe Committee of Ministers, Recommendation Rec(2005)10 on "special investigation techniques" in relation to serious crimes including acts of terrorism, Strasbourg, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da6f6.

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.

[1] 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 *"the use of the Internet and other information and communications technologies, including social media platforms, for terrorist purposes, including the continued spread of terrorist content"*, and requested the Office of Counter-Terrorism and other Global Counter-Terrorism Compact entities *"to jointly support innovative measures and approaches to build 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"*. 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**, in gathering digital data and evidence in cases related to terrorism.

In its 30th Report to the United Nations Security Council,[12] the Analytical Support and Sanctions Monitoring Team noted that *"Many Member States highlighted the evolving role of social media and other online technologies in the financing of terrorism and dissemination of propaganda"*, with platforms cited by Member States, which include Telegram, Rocket.Chat, Hoop, and TamTam, among others. **ISIL supporters using platforms on the Dark Web** for storing and accessing training materials that other sites decline to host as well as **for acquiring new technologies** were also cited in the Report.

Countering the use of new and emerging technologies for terrorist purposes was discussed at the dedicated special meeting of the United Nations Security Council's Counter-Terrorism Committee's (CTC), which took place on 28–29th October 2022 in New Delhi and resulted in the adoption of a non-binding document, known as the Delhi Declaration.[13]

The CTC noted "**with concern the increased use, in a globalized society, by terrorists and their supporters of the Internet and other information and communication technologies**, *including social media platforms, for terrorist purposes*" and acknowledged "**the need to balance fostering innovation and preventing and countering the use of new and emerging technologies, as their application expands, for terrorist purposes**", while emphasizing *"**the need to preserve global connectivity and the free and secure flow of information** facilitating economic development, communication, participation, and access to information"*.

9 The United Nations Global Counter-Terrorism Strategy: seventh review (A/RES/75/291), N2117570.pdf (un.org).

10 Security Resolution 2178 (2014), S/RES/2178%20(2014)(undocs.org).

11 Security Resolution 2396 (2017), http://undocs.org/S/RES/2396(2017).

12 Thirtieth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to Resolution 2610 (2021) concerning ISIL: (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities S/2022/547 (undocs.org).

13 The Delhi Declaration, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_outcome_document.pdf.

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 fight against terrorism.

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

FIGURE 1

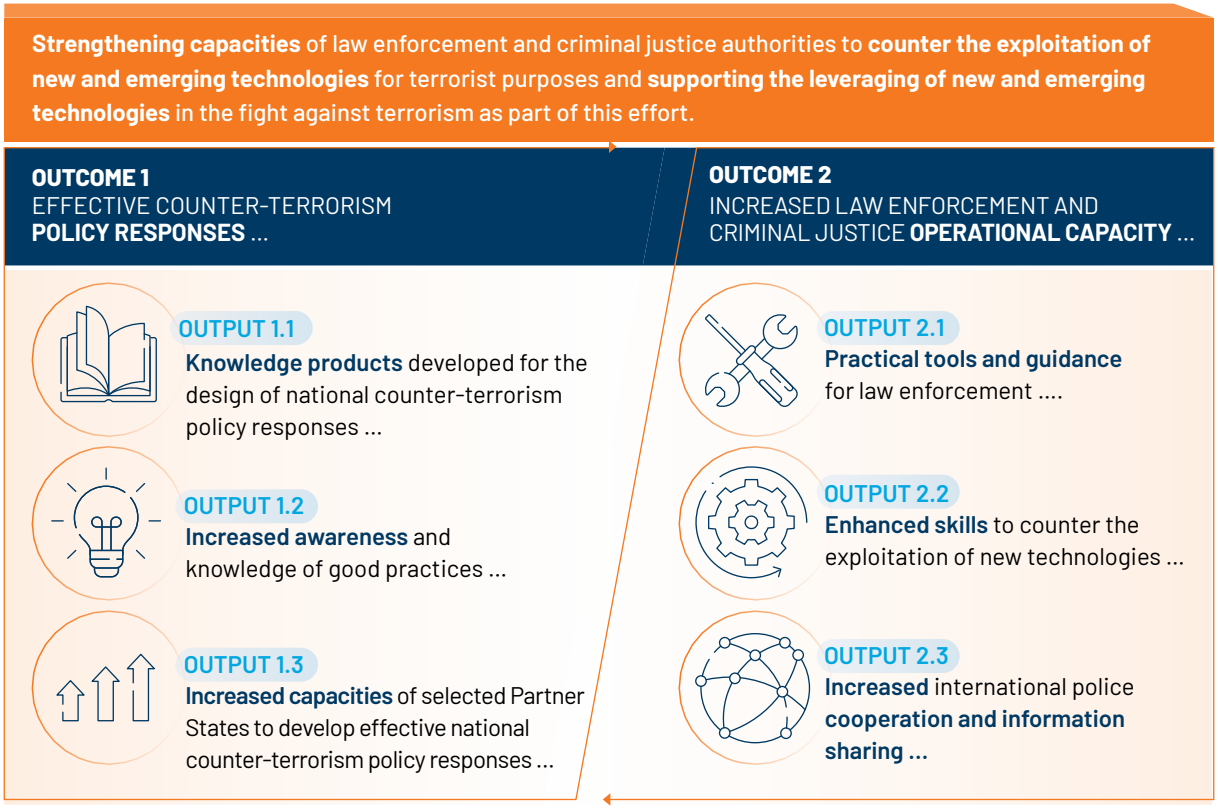


TABLE 1. **CT TECH Outcomes and Outputs**

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 identification of risks and benefits associated with new technologies and terrorism in full respect of human rights and the rule of law.
Output 1.3	Increased capacities of selected Partner States to develop effective national counter-terrorism policy responses towards countering terrorist use of new technologies and leveraging new technologies to counter-terrorism in full respect of human rights and the rule of law.
Outcome 2: Increased law enforcement and criminal justice operational capacity to counter the exploitation of new technologies for terrorist purposes and use of new technologies to prevent and counter-terrorism in full respect of human rights and the rule of law.	
Output 2.1	Practical tools and guidance for law enforcement on countering the exploitation of new technologies for terrorist purposes and use of new technologies to prevent and counter-terrorism in full respect of human rights and the rule of law is developed.
Output 2.2	Partner States' law enforcement and criminal justice institutions have enhanced skills to counter the exploitation of new technologies for terrorist purposes and use of new technologies to counter-terrorism in full respect of human rights and the rule of law.
Output 2.3	Increased international police cooperation and information sharing on countering terrorist use of new technologies and using new technologies to counter-terrorism.

1.3 Document Purpose and Use

This document serves as a comprehensive yet concise resource about Law Enforcement Capabilities necessary to counter the use of new technologies for terrorist purposes. It is intended to support Member States in developing and deploying these capabilities. The document includes a national capabilities model composed of three capability pillars: policy, legal, and institutional, and a capabilities assessment framework. The document aims to enable capability maturity measurement to support Member States in planning, management, and prioritization of capability-building efforts and use of resources.

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 Benefits

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 promote balanced use of law enforcement powers in this area. Cybercrime capacity-building programmes improve the rule of law and civil and human rights safeguards.[14] Cybercrime capacity-building programmes facilitate human development and improve governance.[15] The Model can also support each of these goals:[16]

- Oversight and accountability regarding necessary law enforcement measures;
- Protecting public safety and security while respecting fundamental rights;
- Identifying gaps and missing elements within law enforcement frameworks;
- Prioritizing investment in developing law enforcement capabilities;
- Supporting communication about law enforcement activities, manage expectations, and cooperation methods with the general public and relevant constituencies in the private sector;
- Supporting communication and collaboration with international partners; and
- Help anticipate the issues lying ahead.

1.3.4 Limitations

The capability model is focused on national law enforcement capabilities for counter-terrorism, specifically to counter the use of new technologies for terrorist purposes, whereas comprehensive counter-terrorism strategies require additional measures and capabilities. While the model covers some of these additional measures, it does not cover all of them. Such additional (out of scope) measures include, for example, improved social services to provide positive environments which reduce risks of radicalization.

---

14 World Bank, Combatting Cybercrime, Tools and Capacity Building for Emerging Economies, 2013 https://openknowledge.worldbank.org/entities/publication/fde78414-b14c-504b-af5d-78b5b21caaf3, (World Bank), p. 46.

15 World Bank, p. 46: "ICTs can be 'powerful tools for human development and poverty reduction', something that cybercrime capacity-building programmes might help societies realize. 7) Relatedly, strengthening confidence, trust, security, and reliability of ICT and of ICT systems will facilitate economic development and access to education and sharing of information. 8) Effective criminal justice systems enhance the physical security and health of individuals, for example, by protecting children against sexual exploitation and abuse, by preventing the distribution of counterfeit and substandard medicines, or by protecting people against crime in general. Increased adherence to the rule of law contributes to democratic governance and reduces undue interference in individual rights".

16 See: ENISA, National Capabilities Assessment Framework, December 2020, https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework, (ENISA), p. 19.

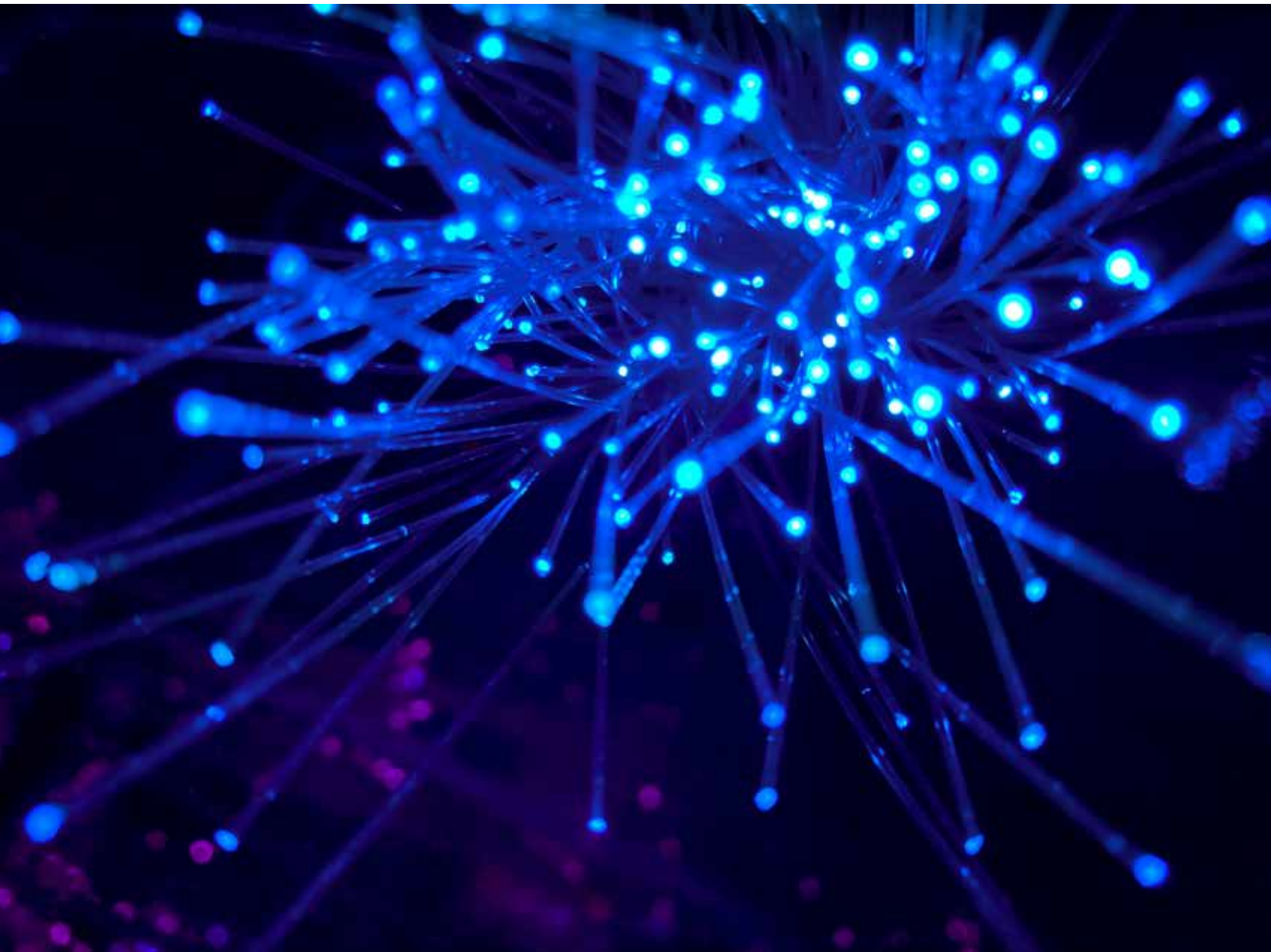
The Model is focused on LEAs' capabilities to deal with 'new technologies'. Yet these capabilities rely on LEAs having a basic level of general capabilities, such as established legal frameworks, enforcement procedures, and use of information technology.

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.



[II]

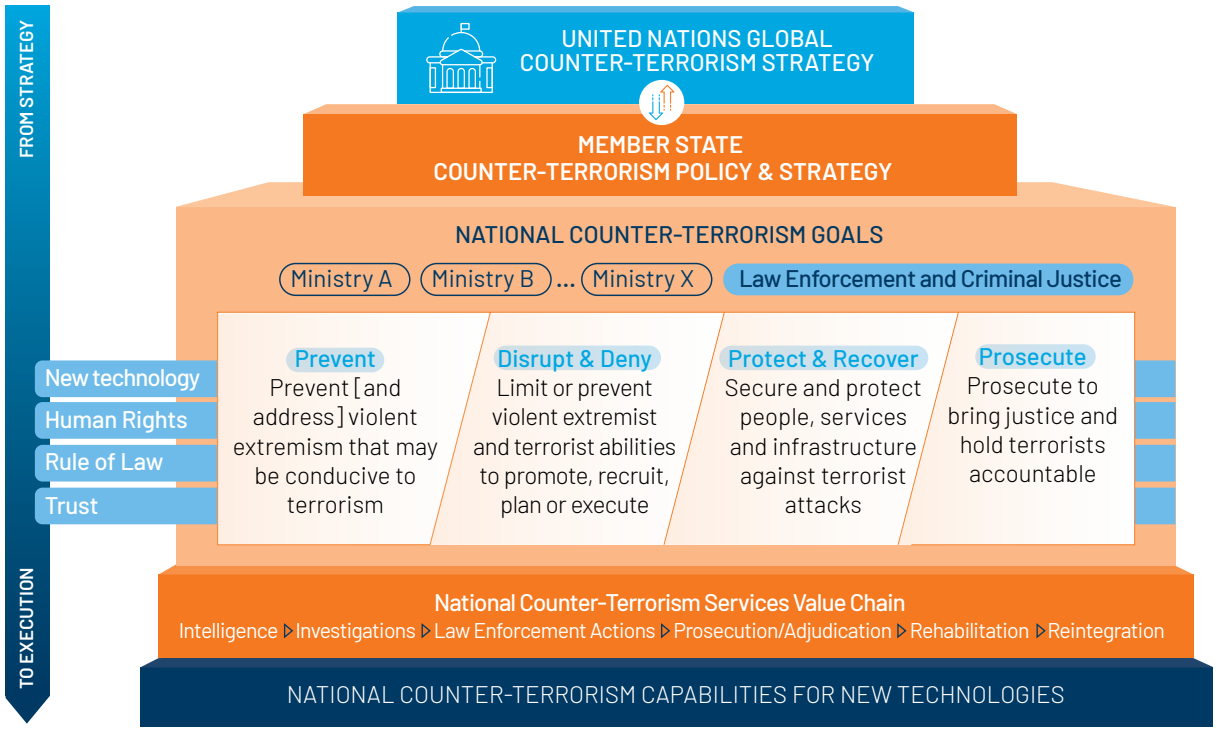
Approach

2.1 Overview

The report seeks to support and enable Member States to assess, identify gaps, and areas of enhancement with regards to current counter-terrorism law enforcement national capability in countering the use of new technologies for terrorist purposes, which are aligned to the United Nations Global Counter-Terrorism Strategy and in full respect of human rights and the rule of law.

2.2 Guiding Framework

FIGURE 2



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 Strategy (GCTS) and a Member State's National Counter-Terrorism Policy and Strategy goals and outcomes, services, and capabilities from a law enforcement and criminal justice perspective, regarding new technologies.

The United Nations GCTS, adopted by the General Assembly, sets out broad actions for Member States to address terrorism threat, which are set out across four key pillars:

Pillar I:	Measures to address the conditions conducive to the spread of terrorism
Pillar II:	Measures to prevent and combat terrorism
Pillar III:	Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard
Pillar IV:	Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism

Member States are encouraged to develop their respective national counter-terrorism legal and policy frameworks in alignment with the United Nations GCTS. They must ensure that their respective counter-terrorism laws, policies, strategies, and measures comply with their obligations under international law, including international human rights law, international refugee law, and international humanitarian law. A Member State's national counter-terrorism legal and policy framework should broadly seek to prevent and address violent extremism that may be conducive to terrorism, prevent or limit terrorist activities, take appropriate measures to protect persons within the State's jurisdiction, services, and infrastructure against reasonably foreseeable threats of terrorist attacks, and ensure that terrorists are held accountable for their actions.

To achieve the counter-terrorism outcomes and goals, Member States' national law enforcement and criminal justice authorities have a set of tools at their disposal. These include, but are not limited to the following:

TABLE 2. **High-Level National Law Enforcement and Criminal Justice Services for Counter-Terrorism**

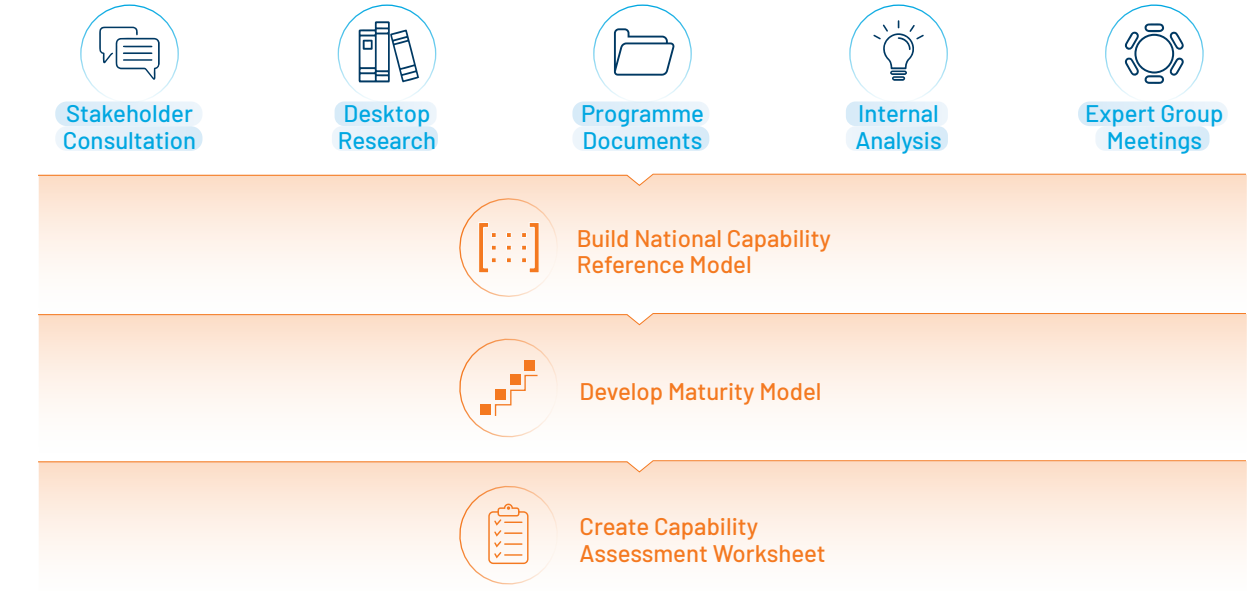
Services	Description
Criminal Justice Process	A legal process to bring about criminal charges against an individual or an entity and the court proceedings, judgement sentencing as well as corrections and rehabilitation.
Intelligence	The product resulting from collecting, developing, disseminating, analysing, and interpreting of information gathered from a wide range of sources, to inform decision makers for planning purposes to take decisions or actions – strategic, operational or tactical level. Intelligence should be collected, retained, used and shared in compliance with relevant Member State obligations under international human rights law.
Criminal Investigations	The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support criminal justice proceedings.
Law Enforcement Actions	Typically describes law enforcement actions taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e., content removal, asset seizures), etc.
Rehabilitation	In a criminal justice context, the term 'rehabilitation' is used to refer to interventions managed by the corrections system with the aim to change the offender's views or behaviour to reduce the likelihood of re-offending and prepare and support the offender's reintegration back into society.
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.

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



This document was developed and informed by a wide range of inputs which include CT TECH project documents, stakeholder consultation, internal analysis, desktop research, Expert Group Meetings (EGM), co-ordination with the United Nations Global Counter-Terrorism Co-ordination Compact entities, and the guiding framework as described above in Section 2.2. The content of the model builds upon prior knowledge developed for national cybercrime capabilities, national cybersecurity capabilities, and national counter-terrorism strategies.

The document aims to both provide a general framework yet focuses on LEA Counter-Terrorism activity regarding new technologies and provide practical and relevant information. This approach is supported by terms and definitions that apply throughout the document to clarify the capability model and the maturity assessment questions. These terms and definitions describe law enforcement activity as well as law enforcement's use of new technologies.

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. In addition, to enable updating, it is suggested that terms and definitions that are more time sensitive (such as those including 'new technologies') be updated periodically.

2.3.1 Expert Group Meetings and Consultation

This guide has been developed with input by experts through the EGM sessions as well as individual consultations and review. The EGM brought together a group of experts and practitioners from counter-terrorism and LEAs, human rights, private sector, academia and civil society to discuss how to counter use of new technologies for terrorist purposes and use new technologies as part of this effort, identify good practices in this regard, and also discuss risks, challenges, and not so good practices that require attention and caution. The guide was further refined through engagement with the United Nations Global Counter-Terrorism Coordination Compact and its Working Group on Emerging Threats and Critical Infrastructure Protection, which promotes coordination and coherence to support the efforts of Member States to prevent and respond to emerging terrorist threats, with respect for human rights and the rule of law as the fundamental basis, in line with international law, including human rights, humanitarian and refugee laws.

2.3.2 Reference Document Review

The development of this guide was informed by, took into consideration, built upon, and complemented existing research, guidelines, and publications – which includes the following:

TABLE 3. **References**

1 Interpol, National Cybercrime Strategy Guidebook, 2021, [https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf]

2 Global Cyber Security Capacity Center, Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 edition, [https://gcscc.ox.ac.uk/cmm-2021-edition]

3 ENISA, National Capabilities Assessment Framework, December 2020, [https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework]

4 World Bank, Combatting Cybercrime, Tools and Capacity Building for Emerging Economies, [https://openknowledge.worldbank.org/entities/publication/fde78414-b14c-504b-af5d-78b5b21caaf3]

5 Counsel of Europe, European Union, Specialised Cybercrime Units – good practice study, 2011, [https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33]

6 Council of Europe/Cybercrime Programme Office [EN], Global State of Cybercrime Legislation 2013-2023: A Cursory Overview, 31 December 2022

7 Europol, Internet Organized Crime Threat Assessment (IOCTA), Strategic, policy and tactical updates on the fight against cybercrime, https://www.europol.europa.eu/publications-events/main-reports/iocta-report

8 United Nations Office on Drugs and Crime, Criminal Intelligence, Manual for Front-line Law Enforcement, UN, NY, 2010

9 Counsel of Europe, Consultative Committee of the convention for the Protection of Individuals with regards to automatic processing of personal data, Practical guide on the use of personal data in the police sector, T-PD (2018), [https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5]

10 United Nations Office on Drugs and Crime, United Nations Security Council, Counter-Terrorism Committee Executive Directorate, Data Disclosure Framework (DDF) General Practices developed by International Service Providers in Responding to Overseas Government Requests for Data, United Nations, 2021, [https://sherloc.unodc.org/cld/en/st/evidence/ddf.html]

11 Rick Muir and Stephen Walcott, Unleashing the Value of Digital Forensics, The Police Foundation, 2021, [https://www.police-foundation.org.uk/publication/unleashing-the-value-of-digital-forensics/]

12 Council of Europe Committee of Ministers, Recommendation Rec(2005)10 on "special investigation techniques" in relation to serious crimes including acts of terrorism, Strasbourg, 20 April 2005, Chapter 1, https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=COE

13 Tech against Terrorism, State of Play – Trends in Terrorist and Violent Extremist Use of the Internet, 2022, [https://www.techagainstterrorism.org/2023/01/19/state-of-play-trends-in-terrorist-and-violent-extremist-use-of-the-Internet-2022/]

14 EUROPOL, Europol spotlight, Cryptocurrencies: Tracing the Evolution of Criminal Finances, 26.01.22, https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances#downloads

15 OSCE, Cyber Incident Classification: A report on emerging practices within the OSCE region, 2022, https://www.osce.org/secretariat/530293

16 OSCE Guidebook Intelligence-Led Policing, 2017, [https://www.osce.org/chairmanship/327476]

17 UN Special Rapporteur on Counter-Terrorism and Human Rights on restrictions on rights and freedoms, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/16/51), Practice XX, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/G1017898.pdf?OpenElement

18 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

19 OSCE, ODIHR, Human rights in counter terrorism investigations, A Practical Manual for Law Enforcement officers, 2013, [https://www.osce.org/files/f/documents/5/f/108930.pdf]

20 ENISA, ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[III]

Introduction

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 significant challenges for law enforcement authorities. The emergence of new technologies has brought both opportunities and challenges to LEAs worldwide, especially in their fight 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 tactics, and protect society from the evolving challenges posed by terrorist organizations exploiting new technology.

3.2 New Technologies and Counter-Terrorism

Today, the advancements of digital technologies, data, and the Internet have led to a hyperconnected world in which information is accessed, shared, and received nearly instantaneously. As of 2022, nearly 70 per cent of the global population uses the Internet,[17] of which over 93 per cent are social media users.[18] Globally, it is estimated that in 2022 over 97 zettabytes[19] of information was generated.[20] Whilst such technology advancements provide the opportunity to transform society for the greater good, terrorist actors are taking advantage of the same technology for their own nefarious purposes. The use of new technologies for terrorist purposes poses significant challenges to Member States in countering terrorism – in particular – the use technologies that allow for anonymity and the ability to coordinate and operate remotely.

17 ITU Global Connectivity Report 2022, https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/.

18 Domo Data Never Sleeps, Data Never Sleeps 10.0 | Domo.

19 One zettabyte equals to one billion terabytes.

20 Statista, Total data volume worldwide 2010-2025 | Statista.

On the other hand, new technologies present significant 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 financing. 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 terrorist content, expertise, such as designs of improvised explosive devices and attack strategies, as well as to coordinate and facilitate attacks and procure weapons and counterfeit documents. Meanwhile, developments in the fields of artificial intelligence, machine learning, 5G telecommunications, robotics, big data, algorithmic filters, biotechnology, self-driving cars and drones may suggest that once these technologies become commercially available, affordable, and convenient to use, they could also be misused by terrorists to expand the range and lethality of their attacks.

3.2.2 Opportunities – Counter-Terrorism Law Enforcement

New technologies present endless opportunities for LEAs to effectively counter-terrorism while upholding responsible practices with respect to international human rights law. Law enforcement can harness new technologies to detect, investigate, prosecute, and adjudicate terrorist activities in new and more effective ways.

Open-source intelligence enables quick collection of information about targets of interests, which can make law enforcement activities more effective. Advanced data analytics and artificial intelligence (AI) capabilities allow for the processing and analysis of vast amounts of information, enabling law enforcement to identify patterns, detect potential threats, and pre-emptively respond to terrorist activities. Advanced surveillance systems, including facial recognition and biometric technologies, aid in the identification and tracking of suspects, enhancing the efficiency of investigations, preventing potential attacks, and prosecuting terrorists. Furthermore, digital forensics tools assist in extracting critical evidence from electronic devices, enabling law enforcement to uncover hidden connections, disrupt terrorist networks, and prosecute terrorists.

Leveraging new technologies can help prioritize limited law enforcement resources in a more effective way. However, it is crucial that these technologies are employed ethically and with strict adherence to privacy, human rights, and the rule of law. Transparency and accountability measures must be in place to ensure responsible use and prevent any potential misuse of these powerful tools. Additionally, comprehensive training programmes should be implemented to equip law enforcement personnel with the necessary skills to leverage new technologies effectively and within the boundaries of legal and ethical frameworks. By leveraging new technology responsibly, law enforcement can significantly enhance their counter-terrorism efforts and safeguard the security and safety of communities.

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 fight against terrorism, and recognizes that "effective counter-terrorism measures and the protection of human rights are not conflicting 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] Specifically 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 communications, shifting their discourse according to their target group.[24] Another critical aspect regarding gender and new technologies refers to the digital gender divide, whereby globally, women's access to the Internet is estimated to be at 85 per cent that of men with an approximate number of 1.7 billion women in the Global South lacking access. This disparity poses a human rights concern underlying all dimensions of cybersecurity, including the potential exposure, insecurity, or participation in governance.[25]

21 A/RES/60/288, GA resolution 60/158, Security Council resolutions 1456 (2003), 1624 (2005), 1805 (2008), 2129 (2013), 2178 (2014), 395 (2017) and 2396 (2017).

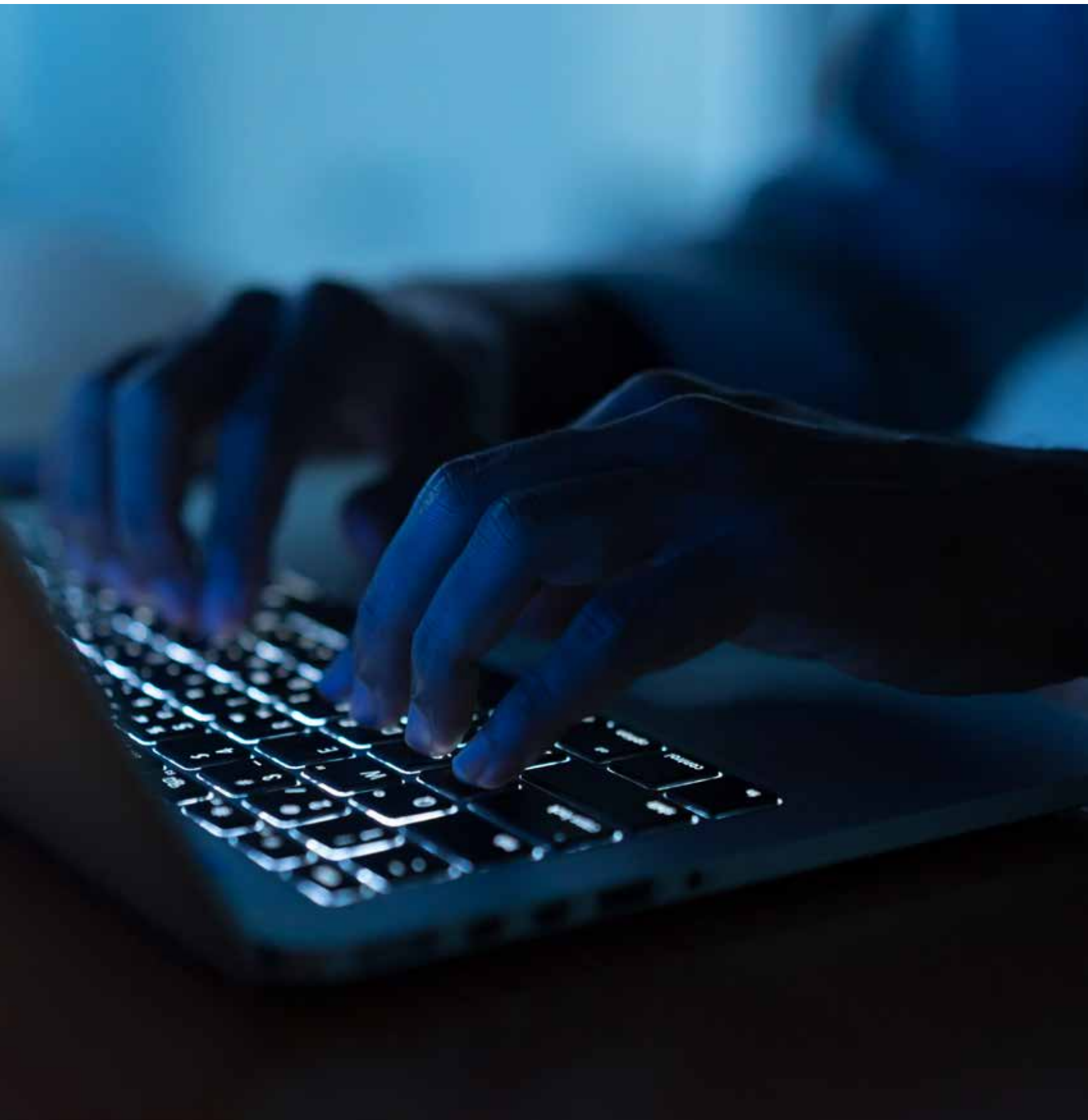
22 DCAF, OSCE/ODIHR, and UN Women, Gender and Security Sector Reform Toolkit (Geneva: DCAF, 2008). https://www.dcaf.ch/gender-and-security-toolkit.

23 CTED, 'Gender Dimensions of The Response to Returning Foreign Terrorist Fighters - Research Perspectives', February 2019.

24 Nelly Lahoud, 'Empowerment or Subjugation: An Analysis of ISIL's Gendered Messaging' (UN Women, June 2018).

25 DCAF, 'Gender Equality, Cybersecurity, and Security Sector Governance – Understanding the role of gender in cybersecurity governance'. January 2023.

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.



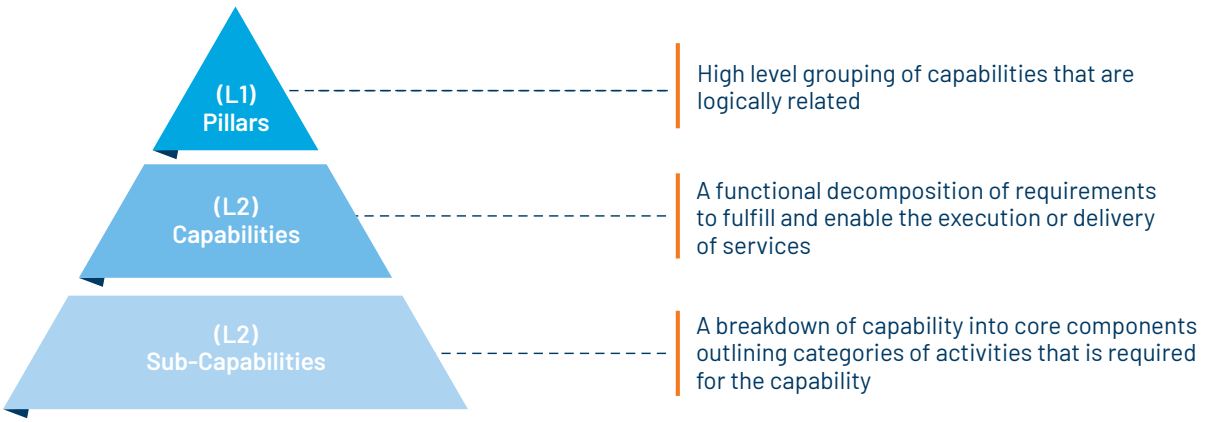
[IV] National Capability Reference Model

4.1 Overview

The national capability reference model serves as a national blueprint that maps out required national capabilities to counter the use of new technologies for terrorist purposes as well as leveraging new technologies to counter-terrorism. It allows Member States to assess current national capabilities against the national capability reference model to identify key gaps and opportunities for further enhancement and development. The proposed model framework builds on the unique elements of the intersection of law enforcement, terrorist activity, and protection of fundamental rights, as its starting point. It builds upon accepted legal and policy principles in this area, with the aim of enabling effective law enforcement operations with an accepted fundamental rights' protection framework.

4.1.1 Framework Overview

FIGURE 4



The development of the national capability reference model is structured in a logical hierarchy manner that is functionally decomposed into granular grouping.

Level 1 – Pillars	*The national capability reference model is structured across Legal, National Policy, and Institutional Pillars.*
Level 2 – Capabilities	*Each of the Pillars are broken down by a set of core capabilities. In total **21** core capabilities have been defined.*
Level 3 – Sub-Capabilities	*Each core capabilities are further broken down and defined as sub-capabilities. In total **77** sub-capabilities have been defined.*

4.1.2 Policy Pillar

The policy pillar aims to review the policy elements necessary for development and deployment of a comprehensive use of new technologies, guiding written programmes to counter-terrorism. The complexity of dealing with the use of new technologies for terrorist purposes requires a policy or policies at the national level, with the backing of top-level policymakers.

The policy is important for intragovernmental coordination purposes, and to integrate with relevant national security, cybersecurity, and cybercrime policies. The communication and publication of the policy is important for external government relations, to foster trust and cooperation by relevant domestic and international stakeholders.

4.1.3 Legal Pillar

The legal pillar describes the necessary laws and regulations that are needed to enable and support the law enforcement counter-terrorism value chain. With social and technical developments in cyberspace, law needs to develop innovative public policy and legal approaches to deal with new challenges, balancing security with human rights requirements. These frameworks need to be known to the public to maintain public trust.

The model aims to guide the development of law and regulations in accordance with international law and considering global best practices. It includes general legal elements that apply to law enforcement activity, protection of human rights, criminal law, procedural law and authorities, and international cooperation.

4.1.4 Institutional Pillar

This pillar aims to describe necessary organizational, operational, and technical capabilities that are necessary to carry our core law enforcement functions that are part of the law enforcement counter-terrorism value chain, specifically concerning the new technologies. It covers governance, process, procedures, human capital and capacity building, financial resources, and technological capabilities.

4.2 Legal Pillar

The legal pillar describes the necessary laws and regulations that are needed to enable and support the law enforcement counter-terrorism value chain.

The legal pillar aims to guide development of law and regulations in accordance with international law, taking into account global best practices. Global best practices, while not necessarily legally binding in the UN context, can support

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

Any measures impacting on or restricting human rights must be established by law, necessary, and proportionate. Protection of human rights is embedded in the framework through three legal contexts. The first is core requirements of the rule of law systems is protection of human rights, which serves as the minimum basis for the use of law enforcement power. The second is a dedicated framework for data protection. The third are substantive and procedural elements that are part of the specific rules such for the requirement for judicial approval.

Ref.	Sub-Capabilities	Description
1.2.1	**Adherence/compatibility with UN guidance on respecting human rights**	International legal instruments protecting human rights create a general framework for developing law enforcement capabilities. Thus, these frameworks serve to complement specific human rights' protections, and promote human rights within the development of new frameworks. The UN guidance in this area serves as the baseline.[27] These requirements are transposed in the model where relevant.
1.2.2	**Legal authorities for independent review or redress of human rights' risk or violations**	To protect human rights, the legal framework needs to include legal powers for review and redress which is independent from the LEAs.

26 See: World Bank, p. 228.

27 UN Special Rapporteur on Counter-Terrorism and Human Rights on restrictions on rights and freedoms, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/16/51), Practice XX, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/G1017898.pdf?OpenElement.

1.2.3	**Application of accepted data protection principles to law enforcement collection, processing and use of personal information**	Much of law enforcement activity includes collection and processing of personal information, utilizing computing, storage and processing powers. These activities are essential for effective law enforcement activity, yet they create risk of misuse by internal and external actors, and loss of trust by domestic and international stakeholders. Any measures impacting on, or restricting human rights, must be necessary and proportionate. Applying an internationally acceptable framework, to these activities can lower these risks and promote public trust.[28]
1.2.4	**Governance of advanced data collection and analytics**	Advanced data collection and analytics, such as CCTV or 'big data' capabilities enable more effective law enforcement activities. Yet this activity creates risks of collection of excessive information accuracy, or bias, and therefore, risk assessments should be conducted and measures taken to mitigate risk adopted, including to reduce any risk of discrimination. Specifically, collection, processing and retention should be based on relevant criteria, and should not be excessive or discriminatory.

4.2.3 Institutional Mandates

According to the principle of the rule of law, executive agency powers need to be grounded in legislation that defines these powers purposes and scope. This legal requirement applies both to the institutions taking part in the counter-terrorism value chain, and the actions they may take. It is complemented by the next sections that describe the legal basis for law enforcement activities in the counter-terrorism value chain.

Dealing with terrorist activities using new technologies can challenge institutional mandates, such as a terrorist cyberattack that may involve the cybersecurity agency or CSIRT, law enforcement and national security organizations. This stresses the importance of complementing the legal institutional mandate with policy mandates and coordination between institutions.

Ref.	Sub-Capabilities	Description
1.3.1	**Defining counter-terrorism leading institutions**	The counter-terrorism task should be clearly grounded in law, and include dealing with terrorist use of new technologies. This element serves to provide clarity as to relevant roles, authorities, and required resources in the counter-terrorist value chain, and also focuses on the need for adequate attention to new technologies risk. It also serves to clearly designate organizations that can use counter-terrorist measures. It thus serves to promote accountability and reduce risks to human rights in the use of these measures.
1.3.2	**Defining counter-terrorism support institutions**	Law or a policy grounded in law, describes the roles of support organizations that may not be tasked with counter-terrorist operations, but support the counter-terrorism value chain.
1.3.3	**Defining coordination mechanisms (interfaces)**	Law, or a policy grounded in law, describes how counter-terrorism organizations (if more than one) and other organizations coordinate their activities within the counter-terrorism value chain. This is especially important for new technologies risk scenarios, which require a comprehensive counter-terrorist response.

28 Examples of such frameworks include The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487. The pragmatic benefit of the OECD declaration is that it is both high level, yet tailored to law enforcement use, and was accepted by jurisdictions with different privacy and data protection frameworks, such as the US, EU, and APEC countries. See also: Kenneth Propp, Gentlemen's Rules for Reading Each Other's Mail: The New OECD Principles on Government Access to Personal Data Held by Private Sector Entities, Lawfare, 10.01.2023, https://www.lawfareblog.com/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held.

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.

Ref.	Sub-Capabilities	Description
1.4.1	Terrorism offences	Criminal law should prohibit acts of terrorism. Security Resolution 1566 defines these acts.[29] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, has elaborated this definition.[30] Criminal law should apply to computer-related crime when conducted knowingly by a terrorist group for terrorist purposes. These prohibited activities could include a cyberattack on a critical infrastructure, or the development of a ransomware tool. Use of the Internet or social networks to incite or distribute illegal terrorist content should also be prohibited.[31] Offences should be narrowly tailored such that they do not limit legitimate speech, including political speech. While these activities may be illegal according to counter-terrorist sanctions or cyber-crime, tailoring specific offences enables adapting these offences to this context and promotes domestic and cross-border clarity. Thus, Terrorism offences should include all 'new technologies terrorist offences'.
1.4.2	Cybercrime – computers	Computer-related criminal offences prohibit activities which target the confidentiality, integrity, or availability of computers, networks and data stored in them.[32] These criminal offences serve as the basis for law enforcement activity against malicious cyber activity. They provide a normative baseline to counter malicious terrorist cyber activity. Accepted (while not universal) international frameworks for cybercrime provide a solid drafting reference as well as real-world knowledge of their application. They also serve as a baseline for cross-border cooperation and interoperability. A general cybercrime framework also supports prevention of cyber-related terrorist activity. This is because terrorist and criminal activity often overlap. It can be challenging to discern criminal activity related to computers from terrorist activity.

29 United Nations Security Council Resolution 1566 (2004), adopted by the Security Council at its 5,053rd meeting on 8 October 2004, S/RES/1566 (2004). https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1566(2004)&Language=E&DeviceType=Desktop&LangRequested=False.

30 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 2010, A/HRC/16/51, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/G1017898.pdf?OpenElement.

31 United Nations Security Council Resolution 1624 calls on States to enact laws prohibiting incitement to terrorism but does not define incitement. The Special Rapporteur on counter-terrorism and human rights has suggested the following model definition: It is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed. European Regulation 2021/784 defines terrorist content as the following:"1) solicits someone to commit or to contribute to terrorist offences, or to participate in activities of a terrorist group; (2) incites or advocates terrorist offences, such as by glorification of terrorist acts; and (3) provides instruction on how to conduct attacks". Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of content online, Article 2 (7): Terrorist content means…: "(a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3 (1) of EU Directive 2017/541, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed; (b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541; (c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541; (d) provides instruction on the making or use of explosives, firearms, or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541". Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32021R0784.

32 Computer related crime as defined in COE 185 includes these categories: (1) Offences against the confidentiality, integrity, and availability of computer data and systems – illegal access, illegal interception, data interference, system interference, and misuse of devices; (2) Computer-related offences – computer-related forgery, computer-related fraud; (3) Content-related offences – child pornography; (4) Offences related to infringements of copyright and related rights; and (5) Ancillary liability and sanctions – attempt and aiding or abetting, corporate liability.

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 collect information; remotely and covertly accessing a computer or other device and collecting information; stopping malicious use of infrastructures and websites to create computer-related risk or damage; stopping dissemination of clearly malicious terrorist speech such as incitement or recruitment through websites or platforms, by cooperation with private sector actors; and the ability to seize cryptocurrencies.

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] When a State cannot act outside its physical borders, it needs to have adequate legal frameworks to enable cooperation with relevant States.

Ref.	Sub-Capabilities	Description
1.6.1	Clear jurisdictional legal policy	A policy regarding jurisdictional scope of online activities, within international best practices, is important to guide law enforcement. It serves to support activities that are part of the counter-terrorism value chain. It also guides the role of cross-border assistance arrangements. Given the evolving nature of this field, not all of these elements need to be grounded in legislation but can rather be described in binding policy.
1.6.2	Formal legal arrangements to support cross-border cooperation	Bilateral and multilateral legal arrangements serve as a firm legal basis for cross-border law enforcement cooperation. Such arrangements, such as the Counsel of Europe Convention on cybercrime enable cross-border assistance, including, mutual legal assistance, law enforcement cooperation and joint investigations.
1.6.3	Legal ecosystem that enables informal cooperation	Some law enforcement cross-border cooperation activities depend on voluntary, non-binding, arrangements. These arrangements, while informal may be useful to complement other measures in the cross-border context. To enable such cooperation, legal cooperation should be enabled, and the legal ecosystem should not hinder such cooperation. For instance, having a clear data protection framework can support such cooperation as it addresses human rights' concerns.

35 World Bank, p. 121: Fundamentally, a State's jurisdiction is understood as being composed of three different authorities: Prescriptive authority – that is, authority pertaining to the authority to impose laws; adjudicative authority – that is, authority pertaining to the authority to investigate and resolve disputes; and enforceable authority – that is, authority pertaining to the power to induce or punish pursuant to its prescriptive authority and subsequent to its adjudicative authority.

36 See for example article 32 of the Counsel of Europe Cybercrime convention: Article 32 – Trans-border access to stored computer data with consent or where publicly available: A Party may, without the authorization of another Party: a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

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 define 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 reflect 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 defined but also "owned" by the institution receiving support. Doing so creates an institution-wide "culture", one which is exemplified by leadership from above and which is implemented at all levels. Without commitment from the top to a clearly defined process of change, it will be difficult 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 difficulties 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 difficult 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 efficiency, and reduce possible operational conflicts.

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 partners. To ensure the effectiveness of national counter-terrorism policy implementation, governments need to establish clear goals, allocate adequate resources, and regularly evaluate and adjust their policies and strategies based on changing threat environments.

Ref.	Sub-Capabilities	Description
2.2.1	Capability development	The effective prioritization and development of required national capabilities to counter-terrorist use of new technologies.
2.2.2	Threat interventions	The effective prioritization of interventions (prevent, disrupt, deny, protect, and prosecute) in countering terrorist use of new technologies aligned to national Counter-Terrorism Policy, Strategy, and National Action Plan.
2.2.3	Institutional roles and responsibilities	Policy needs to clearly define institutional mandates and interagency cooperation mechanisms with clear roles and responsibilities with regards to Counter-Terrorism efforts in countering terrorist use of new technologies.
2.2.4	Resource management	Prioritization and allocation of required resources to enable the fulfilment of policy goals and objectives.
2.2.5	Collaboration management	Counter-Terrorism organizations (if more than one) and other organizations coordinate their activities within the counter-terrorism value chain. This is important to provide a comprehensive counter-terrorist response. It enables locating 'blind spots' that may cause gaps in the counter-terrorist value chain.

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 performance management requires the establishment of clear performance metrics and indicators, data collection and analysis, and reporting mechanisms to communicate policy performance to key stakeholders.

Ref.	Sub-Capabilities	Description
2.3.1	Policy performance measures	Defined policy performance indicators define as desired objectives and outcomes to be achieved.
2.3.2	Policy impact assessment	A process to regularly assess the effectiveness and impact of national policies implemented to counter-terrorist use of new technologies.
2.3.3	Policy review management	A process of regularly reviewing policy choices and its efficacy and updating policy choices to achieve desired outcomes.

4.3.4 Policy Communications Management

Policy communications management involves the development of clear and concise messaging, communication channels, and engagement strategies to promote understanding, transparency, and trust in government policies. By developing a strong national policy communications management capability, governments can enhance the impact of their policies, foster public support, and build more effective and trusted relationships with citizens and stakeholders.

Ref.	Sub-Capabilities	Description
2.4.1	Strategic communications	Communicating policy goals and measures is important to promote trust and cooperation with private sector organizations, citizens, and international partners. It enables public discussion and transparency, which help reduce concerns about the way counter-terrorist powers are used.

4.3.5 Public Private Cooperation

Dealing with new technologies requires cooperation with private sector companies. The unique features of new technologies, and their use, require cooperation and partnerships to achieve effective law enforcement activity.

Ref.	Sub-Capabilities	Description
2.5.1	Public private partnership	Public private partnerships include cooperation with ICT providers to better understand technical features, as well as with service providers that can help in locating or stopping malicious activity. In some cases, private sector resilience to the misuse of new technologies is the most effective prevention method against a specific threat. Cooperation is especially important with international companies, to which formal legal frameworks may apply differently. This should be an important part of the high-level policy governance.

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 classification and development of international cooperation. A comprehensive mitigation plan needs to be developed with relevant organizations. Incident classification 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 Classification 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 classification	In order to support national level policy, a national level body should be tasked with producing a national level incident classification 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 frameworks, operational cooperation mechanisms, and contact points.

40 In the cyber incident context see: OSCE, Cyber Incident Classification: A report on emerging practices within the OSCE region, 2022, https://www.osce.org/secretariat/530293. The insights from the OSCE report are relevant not only for cyber-related events.

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.

3.2.3	Compliance	Refers to the set of policies, procedures, and guidelines that an institution puts in place to ensure that it complies with applicable laws, regulations, and industry standards.
3.2.4	Human rights impact assessment	Identify, assessment, and mitigation of the potential human rights impacts of institutional operational, activities, policies, and actions with regards to new technologies and counter-terrorism.
3.2.5	Data protection	LEAs collect and process personally identifiable information and are subject to specific legal principles to prevent risk to privacy. These principles need to be operationalized through a dedicated independent, internal framework that includes subject matter experts, policies, and procedures. (Safeguard personal information from unauthorized access, use, disclosure, or destruction. It is critical for protecting individual privacy, maintaining trust, and complying with legal and regulatory requirements.)

4.4.3 Mission Management and Coordination

Mission management and coordination based on relevant information enables more effective LEA's operations and cooperation with other agencies.

Ref.	Sub-Capabilities	Description
3.3.1	Horizon scanning	A systematic process of gathering and analysing information from a wide range of sources to identify emerging trends, risks, and opportunities of emerging technologies and its impact on terrorism and States' capabilities. It is a forward-looking activity that helps anticipate and prepare for future challenges and opportunities.
3.3.2	Threat management	A systemic process of gathering and analysing information from a wide range of sources to identify emerging threats, classify their severity, and prioritize counter-terrorist measures.
3.3.3	Information sharing	To facilitate cooperation and coordination, LEAs should have in place organizational, legal, and technical tools for information sharing that can be used to mitigate terrorist use of new technologies. This would include information sharing agreements and protocols as well as an information classification framework.

4.4.4 Partnership and Cooperation

The unique features of new technologies, and their use, require cooperation and partnerships to achieve effective law enforcement activity. These include cooperation with ICT providers to better understand technical features, as well as with service providers that can help in locating or stopping malicious activity. In some cases, promoting private sector resilience to malicious use of new technologies is the most effective prevention method against a specific threat. Cooperation is especially important with international companies, to which formal legal frameworks may apply differently. Involving the private sector from the beginning of developing the framework can be beneficial.

Ref.	Sub-Capabilities	Description
3.4.1	Government relationship management	LEAs need to coordinate intragovernmental activities across the counter-terrorism lifecycle. In order to do so it is useful to create one central external facing function that supports intra governmental cooperation.

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, procedures, and expectations
3.4.3	Public / community engagement	Formalized policy and process for the clearance and authorization of sharing pertinent information to the public which, among others, may include information of threats, awareness, operations, etc., with the intent of increasing trust and reputation of LEAs.
3.4.4	International cooperation	Formalized policy and process, as well as dedicated personnel, to support cross-border collaboration. (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.)

4.4.5 Operational Management

Operational management deals with policies and procedures that enable delivery of the counter-terrorism value chain. Operational management should be capable of coordinating strategic counter-terrorism efforts, as well as quick decision-making cycles to respond, task, and coordinate LEAs' operations in changing circumstances.

Ref.	Sub-Capabilities	Description
3.5.1	Oversight management	Effective mechanism to manage and oversee their operations, ensuring LEAs operate in compliance with relevant laws and regulations, and that they are effective in fulfilling their missions. This should include policies, procedures, and dedicated support functions for reporting, tasking, and coordination. Policies, procedures, and capabilities should support management situational awareness and operations at the long, medium, and short term.
3.5.2	Intelligence management	Intelligence is an essential part of dealing with terrorist threats, and it includes collection of information, analysing and evaluating it, creating intelligence 'products' and delivering them to relevant operators, and planning and decision- makers. The introduction of new technologies requires new types of collection about new tools and techniques, but also enables new collection, processing, and delivery methods in the intelligence lifecycle. The intelligence cycle can be described as including 'tasking', 'collection', 'evaluation', 'collation', 'analysis', 'inference development', and 'dissemination'. Given the global nature of the ICT environment and that much of it is a private sector, market-based ecosystem, intelligence activity relies strongly on the ability to understand technological trends, and cooperate with other public sector actors, private sector, and international partners. When collecting intelligence and information about malicious cyber activity it is important to take into consideration new modes of operating, new computer systems and tools, or new payment services.

3.5.3	Investigations management	A formalized process of conducting thorough and effective investigations by gathering information and evidence to assess actions to be taken. Effective law enforcement investigation capability requires a combination of specialized skills, training, and technology. Investigators must have knowledge of relevant laws and procedures, as well as expertise in areas such as forensic analysis, surveillance, and interview techniques. They must also have access to tools such as crime scene analysis equipment, databases of criminal records and other information, and communication systems that allow them to work with other agencies and share information.
3.5.4	Law enforcement agency actions	Operational and intelligence considerations can lead to choosing prevention or disruption actions. Organization should have in place an oversight management capability, that includes policies, procedures, and dedicated support functions for reporting, tasking, and coordination of these activities with other law enforcement functions, and other civilian agencies. Policies, procedures, and capabilities should support management situational awareness and operations at the long, medium, and short term.
3.5.5	Criminal justice interface management	The 'criminal justice' workflow is well defined and cooperation with prosecutors, courts, and other relevant agencies is effective. Management reviews these interfaces regularly and assures the process is functioning according to expectations.
3.5.6	Incident response	Dealing with incidents requires key processes and actions, by LEAs and other relevant authorities. Planning, preparation for, defining clear responsibilities, and cooperation mechanisms are important in dealing with incidents. Testing and exercising incident handling improves awareness and preparedness. These elements are especially important for events which have a national impact or require inter-agency cooperation to mitigate incident's effects.

4.4.6 Operational Support

LEAs need robust organizational infrastructure and technical solutions to support the diverse operations that are part of the counter-terrorism life cycle. This infrastructure includes policies, personnel, and technologies that need to be integrated in operations management.

Ref.	Sub-Capabilities	Description
3.6.1	Data and information management	Capability to obtain, retain, and access data based on operational requirements and in compliance with data privacy and retention policies and requirements. This includes all data such as from LEA systems, other organizations, video feeds, sensors or devices, Internet and social media and the capability to join all the data sources together into a single window to provide access to LEAs.
3.6.2	Technical support	Means of providing technical solutions (include technologies) to operationalize and enable law enforcement activities across intelligence, investigation, operations, and prosecution support. LEAs require a robust ICT infrastructure to support operational and support capabilities. LEAs need to harness technology for operations, including adapting civilian technologies for law enforcement purposes. This includes technologies for processing information and communications. This is especially important in the 'new technologies' context. These may include supporting a forensic lab, analysing digital data, and collection of open-source information.

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, scientific research, market trends, and technology providers to identify technologies that could disrupt or create new opportunities. As part of innovation, technology scanning helps organizations to stay ahead of the terrorist threat by identifying new technologies that can improve capabilities, increase efficiency, or reduce costs. It can also help them identify potential risks or challenges that may arise from emerging technologies and prepare for them in advance.
3.7.2	Innovation development and delivery	A formalized process that fosters a culture of innovation and services which allows for identifying priority opportunities and challenges, exploring potential solutions, determining feasibility through piloting, prototyping, and launching a minimum viable product, and scaling successful solutions in operations.
3.7.3	Partnership model	Identifying the right external partnership that can help enhance innovation capabilities and tools to deliver innovation projects by allowing institutions to access specialized skills, expertise, and technology at speed and scale.
3.7.4	Innovation support	Providing the necessary resources to support and enable innovation which includes strategic partnership, procurement mechanism, marketing and communications, funding mechanism, corporate culture, and innovation infrastructure.

4.4.8 Training and Workforce Development

Human capital is an essential part of LEA's capabilities and requires policy and management attention in order to adequately deal with new technologies. New technologies create additional challenges because of recruitment competition with private sector employers for qualified experts.

In addition, the use of technology for counter-terrorism and countering the use of new technologies for terrorist purposes requires adapting 'civilian' technological knowledge to the law enforcement context, such as working within legal authorities and digital forensics. The changing technological landscape also requires a training routine to adapt existing capabilities to new scenarios.

Ref.	Sub-Capabilities	Description
3.8.1	Knowledge development	Developing an LEA knowledge base and updating it as necessary enables clarity regarding the fields of knowledge that affect and inform LEA's activity and specifically human capital development and management. The knowledge base is composed of academic and industry knowledge regarding new technologies, as well as unique law enforcement areas such as legal procedure or digital forensics. The knowledge base should include areas relevant to all of the workforce, as well as more specific areas. Preparing the knowledge base focuses attention to areas that knowledge and training is available, and to areas where dedicated development is necessary. It also enables assessing what roles should be carried out by public servants, by contractors, or by outside service providers.

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	LEAs should have adequate legal support for its operational and support operations. Legal staff are part of the LEA's training programmes to improve a mission-focused approach and efficiency.

41 As these are general capabilities they are mentioned in brief. Where these capabilities require special attention in the counter terrorism context, they are mentioned above.

[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.

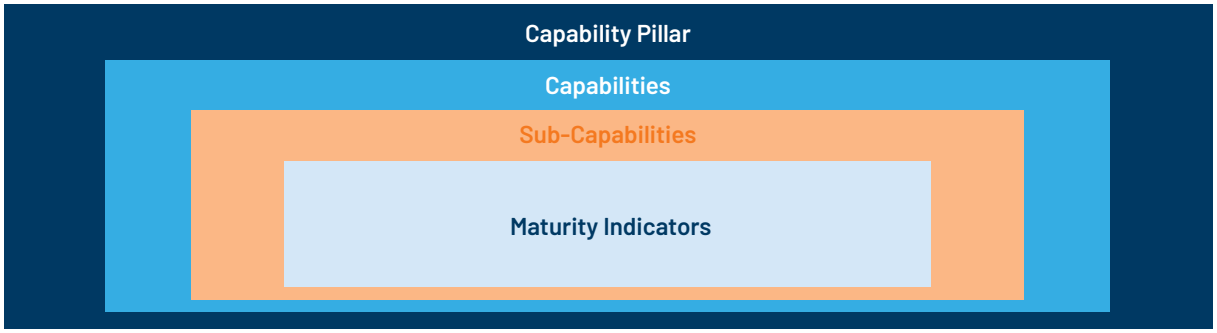
The maturity model developed here is based on the comprehensive research conducted by ENISA in its "National Capabilities Assessment Framework", with adaptations to the context of countering the use of new technologies for terrorist purposes.

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 continuous improvement that allows for regular assessment to establish priorities areas aligned to the States' national counter-terrorism policy and strategy. In addition, it can be used to benchmark against other States, and to identify leading practices and areas for collaboration.

Overall, the law enforcement capability maturity model is a valuable tool for law enforcement seeking to enhance their ability to counter the use of new technologies for terrorist purposes, and to stay ahead of evolving threats in an increasingly complex and digital world.

5.2 Maturity Model Structure

FIGURE 5



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

The model is intended to simplify assessment by aiming for indicative questions that require less qualitative assessment. These questions thus elaborate how the capabilities and sub-capabilities can be transposed. They are intended to be both open-ended and leave room for application by Member States, yet provide guidance to important elements needed. The indicators that have been developed will be checked against real-world cases which can inform an update of the model.

Each maturity level has a list of indicators that are framed as assessment questions at the sub-capability level. Indicators are used to describe and evaluate the capability. Indicators are structured into the following two tiers:

- **General:** General indicators are standard indicators to assess people, structure, processes, and infrastructure requirements;
- **Specific:** Where applicable, specific indicators are technical related to technology, human rights, and gender.

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
1.1	L2	Rule of Law		
1.1.1	L3	Rule of Law According to International Standards	Rule of Law According to International Standards does not exist	GENERAL: Are there formal outward-facing binding statements by government regarding applicability of the rule of law? Are there procedures for enhancing the rule of law principles in the legal system during preparation of legislation and legal guidance? Has the Member State been reviewed by the UN for rule of law violations? SPECIFIC: N/A
1.2	L2	Human Rights		
1.2.1	L3	Adherence / Compatibility with UN Guidance	Adherence / Compatibility with UN Guidance does not exist	GENERAL: Are there procedures for application of UN Guidance within preparation of legislation and legal guidance? Has the Member State been reviewed by the UN for human rights violations? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Does the constitutional legal framework establish rule of law principles? Is there a comprehensive internal facing legal policy to ensure application of rule of law principles? SPECIFIC: Is there a formal binding statement by the government regarding applicability of rule of law framework to counter-terrorist use of new technologies? Is there a formal binding policy requiring review of the legality of development or deployment of new technologies?	GENERAL: Is there a binding legal policy to independently review rule of law application according to UN Guidance? Is there active participation in UN discussions on development and application of guidance? SPECIFIC: Is there binding legal policy requiring legal institutions to mitigate risks from LEA's use of new technologies to rule of law principles? Is there active participation in UN discussions on development and application of guidance to new technologies? Is there a dedicated practice guide to implement rule of law principles to counter-terrorist use of new technologies? Is there formal binding policy requiring an independent review regarding legality of development or deployment of new technologies?	GENERAL: Do LEA's lead work groups on developing standards in the UN or other international venues? Is there a binding transparency policy about assessing the rule of law in LEA's counter-terrorism activity? SPECIFIC: Is there a legal framework for conducting civil society engagement in the intersection of the rule of law and LEAs? Is there a binding policy about publication of rule of law assessment and LEA's counter-terrorism activity that involves new technologies?
GENERAL: Are there formal outward-facing binding statements by government regarding applicability of the framework? Is there a comprehensive internal facing legal policy to implement UN guidance in legal policymaking? SPECIFIC: Is there a formal binding statement by government regarding applicability of the framework to counter-terrorist use of new technologies? Is there a dedicated practice guide to implement human rights principles to counter-terrorist use of new technologies? Is there adherence to international export controls requirements?	GENERAL: Is there a binding legal policy requiring human rights impact assessment for new LEA's activity according to UN Guidance? Is there active participation in UN discussions on development and application of guidance? SPECIFIC: Is there binding legal policy requiring human rights impact assessment for new uses of new technologies? Is there formal binding policy requiring a human rights impact assessment when developing or procuring new technologies? Is there active participation in UN discussions on development and application of guidance to new technologies?	GENERAL: Do LEA's lead work groups on developing standards in the UN or other international venues? Is there a binding transparency policy about human rights impact and mitigation in LEA's counter-terrorism activity? SPECIFIC: Is there a formal binding policy requiring an independent human rights impact assessment when developing or procuring new technologies? Is there a legal framework for conducting civil society engagement to support horizon scanning of potential human rights issues as a result of new technologies? Is there a binding transparency policy about human rights impact and mitigation in LEA's counter-terrorism activity that involves new technologies?

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 specific policy for use of new collection technologies? Do LEAs have a specific 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?
GENERAL: Are LEAs at maturity level 4 for data protection? Do LEAs have a privacy impact taxonomy that defines high, medium, and low impacts? SPECIFIC: Does introduction of new collection techniques or advanced analytics require a data protection impact assessment that addresses excessive collection, fairness, and bias risks?	GENERAL: Is there a binding policy for an independent audit to deal with fairness, bias, and risks from automated decisions that have high impact on privacy? SPECIFIC: N/A	GENERAL: Has LEAs published guidance on advanced analytics risk assessments? Do LEAs participate in global discussions about new collection methods and about advanced analytics? SPECIFIC: N/A

1	L1	Legal Pillar	Non-Existent	Basic
1.3	L2	Institutional Mandates		
1.3.1	L3	Defining Counter-Terrorism Leading Institutions	Defining Counter-Terrorism Leading Institutions does not exist	GENERAL: Is there a general written legally binding mandate according to law tasking LEAs and other institutions with a counter-terrorist mandate? SPECIFIC: Does the binding legal policy deal with countering terrorist use of new technologies?
1.3.2	L3	Defining Counter-Terrorism Support Institutions	Defining Counter-Terrorism Support Institutions does not exist	GENERAL: Is there a general written legally binding mandate according to law tasking institutions with counter-terrorist support? SPECIFIC: Does general legally binding support policy apply to new technologies?
1.3.3	L3	Defining Coordination Mechanisms	Defining Coordination Mechanisms does not exist	GENERAL: Are there general policies defining intragovernmental information sharing and cooperation? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a specific and detailed legal mandate for each counter-terrorism institution based in law? SPECIFIC: Does specific policy deal comprehensively with counter-terrorism new technologies activities?	GENERAL: Is there a binding legal policy to define authority and command lines for operations? SPECIFIC: Does specific legislation define LEA's legal mandate for countering terrorist use of new technologies?	GENERAL: Is the scope of the mandate reviewed periodically to take into account developments in terrorist activities? Does legislation enable updating or changing scope of mandate subject to parliamentary oversight? SPECIFIC: Is the scope of the mandate reviewed periodically to take into account developments in terrorist use of new technologies?
GENERAL: Is there a comprehensive legally binding directive for counter-terrorism support institutions? SPECIFIC: Does policy apply to new technologies?	GENERAL: Are coordination and communication mechanisms legally binding on CTcounter-terrorism support institutions? Are there mandatory reporting requirements from support institutions to law enforcement regarding suspect terrorist activity? SPECIFIC: Do coordination and reporting binding policies deal specifically with new technologies?	GENERAL: Is there an all of government binding legal policy to coordinate roles? SPECIFIC: Is the scope of the mandate reviewed periodically to take into account developments in terrorist use of new technologies?
GENERAL: Is there a comprehensive binding policy on Counter-Terrorism information sharing? Is there a comprehensive policy on coordination of Counter-Terrorism value chain activities across Counter-Terrorism organizations? Is there a comprehensive mapping of non-Counter-Terrorism organizations relevant to support the Counter-Terrorism value chain? SPECIFIC: Is there a LEA – national CSIRT coordination mechanism?	GENERAL: Is there a dedicated high level coordination function with adequate resources? Are lines of command during an national incident clearly articulated? Do coordination mechanisms have real-time capabilities for situational awareness? SPECIFIC: Is there a dedicated new technologies coordination policy? Is there a dedicated high level coordination function with adequate resources for new technologies? Do coordination mechanisms have real-time capabilities for situational awareness for ICT?	GENERAL: Is the coordination policy annually reviewed? SPECIFIC: N/A

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: Does criminal code include some of the terrorist offences? Is legislation clearly defined and narrowly tailored? SPECIFIC: Does criminal code include some of the 'new technologies' terrorist offences'?
1.4.2	L3	Cybercrime – Computers	Cybercrime – Computer Criminal Law does not exist	GENERAL: Does criminal code include some of the cybercrime offences? Is legislation clearly defined and narrowly tailored? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Has draft legislation for offences not covered been introduced in a legislative branch? Is legislation clearly defined and narrowly tailored? SPECIFIC: Has draft legislation for 'new technologies' terrorist offenses' not covered been introduced in a legislative branch? Are speech offences applicable to incitement and recruitment and not to legitimate political speech?	GENERAL: Does primary legislation, secondary legislation, and other necessary rules cover all terrorist offences? Are legal rules defined and narrowly tailored? Has lead prosecution authority published prosecution guidelines? SPECIFIC: Does primary legislation, secondary legislation, and other necessary rules cover 'new technologies' terrorist offenses'?	GENERAL: Are prosecution guidelines public? Are terrorist criminal offences in line with leading global standards? SPECIFIC: Do LEAs participate in international counter-terrorism legal discussions?
GENERAL: Has draft legislation for cybercrime offences not covered been introduced in a legislative branch? Is legislation clearly defined and narrowly tailored? SPECIFIC: Are speech offences applicable to incitement and recruitment and not to legitimate political speech?	GENERAL: Does primary legislation, secondary legislation, and other necessary rules cover all cybercrime offences? Are legal rules defined and narrowly tailored? Has lead prosecution authority published prosecution guidelines? SPECIFIC: N/A	GENERAL: Are prosecution guidelines public? Are cybercrime criminal offences in line with leading global standards? SPECIFIC: Do LEAs participate in international discussions for developing a model regarding cybercrime offences?

1	L1	Legal Pillar	Non-Existent	Basic
1.4.3	L3	Ancillary Liability/ Material Support Offences	Rules as to Ancillary Liability/Material Support criminal law does not exist	GENERAL: Does the criminal code include ancillary liability offences? Is legislation clearly defined and narrowly tailored? SPECIFIC: Does legislation include some ancillary liability offences that apply to cybercrime offences? Does legislation include ancillary liability offences that apply to 'new technologies' terrorist offences'?
1.5	L2	Administrative and Procedural Law		
1.5.1	L3	General Law Enforcement Authorities	Administrative and Procedural law for General Law Enforcement does not exist	GENERAL: Does criminal procedural law enable carrying out some of the general law enforcement authorities? Are procedural safeguards in place for these authorities? Are there drafting activities to promote comprehensive legislative frameworks? SPECIFIC: N/A
1.5.2	L3	Authorities to Deal with Digital Information and Evidence	Administrative and Procedural law for Authorities to Deal with Digital Information and Evidence does not exist	GENERAL: Does the legal framework include new technologies' LEA's authorities? Are procedural safeguards in place for these authorities? [Are there drafting activities to promote comprehensive legislative frameworks?] SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Has draft legislation for offences not covered been introduced in a legislative branch? Is legislation clearly defined and narrowly tailored? SPECIFIC: Has draft legislation for ancillary liability offences that apply to ancillary liability cybercrime offences not covered been introduced in a legislative branch?	GENERAL: Does primary legislation, secondary legislation, and other necessary rules cover all relevant ancillary liability offences for terrorist offences? Are legal rules defined and narrowly tailored? Has lead prosecution authority published prosecution guidelines? SPECIFIC: Does primary legislation, secondary legislation, and other necessary rules cover all relevant ancillary liability offences for cybercrime terrorist offences? Does primary legislation, secondary legislation, and other necessary rules cover all relevant ancillary liability offences for 'new technologies' terrorist offences'?	GENERAL: Are prosecution guidelines public? Are terrorist criminal offences in line with leading global standards? SPECIFIC: Do LEAs participate in international counter-terrorism legal discussions?
GENERAL: Has draft legislation been introduced to complete legislative authorities? Does draft legislation include applicable procedural safeguards? SPECIFIC: N/A	GENERAL: Does legislation and secondary legislation cover comprehensively general law enforcement authorities? Does legislation include applicable procedural safeguards? Has the prosecution drafted implementation guidelines? Insert SPECIFIC: N/A	GENERAL: Are law enforcement authorities regularly reviewed based on deployment experience and developing jurisprudence? SPECIFIC: N/A
GENERAL: Has draft legislation been introduced to complete legislative authorities? Does draft legislation include applicable procedural safeguards? SPECIFIC: N/A	GENERAL: Does legislation and secondary legislation enable new technologies legal authorities? Does legislation include applicable procedural safeguards? Has the prosecution drafted implementation guidelines? SPECIFIC: N/A	GENERAL: Are law enforcement authorities regarding digital evidence legislation regularly reviewed based on global best practices, deployment experience, and developing jurisprudence? SPECIFIC: N/A

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-Terrorism Authorities	Administrative and Procedural law for Unique Counter-Terrorism Authorities does not exist	GENERAL: Does the legal framework enable some of the unique Counter-Terrorism authorities? Are procedural safeguards in place for these authorities? SPECIFIC: N/A
1.5.5	L3	Unique Administrative Support	Administrative and Procedural law for Unique Administrative Support does not exist	GENERAL: Does legal framework applicable to LEAs enable some of the elements of unique administrative support? SPECIFIC: N/A
1.6	L2	Jurisdiction and Cooperation		
1.6.1	L3	Clear Jurisdictional Legal Policy	Clear Jurisdictional Legal Policy does not exist	GENERAL: Has senior prosecutorial authority issued guidance about conducting LEA operations and jurisdictional policy? Is policy available to relevant organizational stakeholders? SPECIFIC: Has senior prosecutorial authority issued guidance about conducting LEA operations, unique Counter-Terrorism powers, and jurisdictional policy regarding new technologies? Is policy available to relevant organizational

Established	Advance	Leading
GENERAL: Has draft legislation been introduced to complete legislative authorities? Does draft legislation include applicable procedural safeguards? SPECIFIC: N/A	GENERAL: Does legal framework comprehensively include advanced new technologies for LEA's authorities? Does legislation include applicable procedural safeguards? Has the prosecution drafted implementation guidelines? SPECIFIC: N/A	GENERAL: Is the legislative framework regarding new technologies regularly reviewed based on global best practices deployment experience and developing jurisprudence? SPECIFIC: N/A
GENERAL: Has draft legislation been introduced to complete legislative powers? Does draft legislation include applicable procedural safeguards? SPECIFIC: N/A	GENERAL: Does the legal framework enable all unique counter-terrorism authorities? Does legislation include applicable procedural safeguards? Has the prosecution drafted implementation guidelines? SPECIFIC: N/A	GENERAL: Are unique counter-terrorism authorities regularly reviewed based on global best practices deployment experience and developing jurisprudence? SPECIFIC: N/A
GENERAL: Are there easily available practice guidance on unique administrative support tools? Are there drafting or rule-making activities to all of the elements of unique administrative support? SPECIFIC: N/A	GENERAL: Is there a comprehensive framework to support unique administrative support? Are there easily available practice guidance on unique administrative support tools? SPECIFIC: N/A	GENERAL: Are unique administrative support tools regularly reviewed based on operational needs? SPECIFIC: N/A
GENERAL: Has senior prosecutorial authority issued comprehensive guidance about conducting LEA operations ['counter-terrorism value chain'] jurisdictional policy? SPECIFIC: Has senior prosecutorial authority issued comprehensive guidance about jurisdictional policy? Is there a process in place to develop solutions for jurisdictional challenges for use of new technologies?	GENERAL: Are some elements of the jurisdictional policy included in legislation? Have elements of jurisdictional policy been affirmed by courts? SPECIFIC: Is the jurisdictional policy regarding LEA's use of new technologies included in legislation. Have elements of jurisdictional policy been affirmed by courts?	GENERAL: Do LEAs participate in international norm development activities in this area? SPECIFIC: N/A

1	L1	Legal Pillar	Non-Existent	Basic
1.6.2	L3	Formal Legal Arrangements for Cross-Border Cooperation	Formal Legal Arrangements for Cross-Border Cooperation does not exist	GENERAL: Does Member State have a legal framework that enables cross-border LEA's cooperation. Did LEAs sign cooperation agreements that enable cross-border assistance in the counter-terrorism value chain? SPECIFIC: Do LEA's cooperation agreements support collection and sharing of digital evidence?
1.6.3	L3	Legal Ecosystem that Enables Informal Cooperation	Legal Ecosystem that Enables Informal Cooperation does not exist	GENERAL: Are elements of data protection principles part of the legal ecosystem? Are there legal safeguards to limit the ability of the government to expropriate private sector intellectual property? Are foreign companies treated generally the same under domestic law? SPECIFIC: N/A

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?
GENERAL: Does the Member State have a data protection framework according to accepted principles? Is access to judicial redress generally available for foreign companies? SPECIFIC: N/A	GENERAL: Are government access activities reported in a mandatory, transparency report? Is there a multistakeholder forum hat includes private sector companies to promote public private counter-terrorism cooperation? SPECIFIC: N/A	GENERAL: Is a Member State active in international multistakeholder governance discussions? Is there a domestic multi-stakeholder forum? SPECIFIC: Is there a domestic multistakeholder forum for new technologies?

5.7 Capability Maturity Model – Policy Pillar

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.1	L2	Policy Development and Management		
2.1.1	L3	Governance	Governance does not exist	GENERAL: Is there an adequate high-level function that reports to the highest government level about development and deployment of national Counter-Terrorism policy? Does national Counter-Terrorism policy deal with environmental conditions that are conducive to the terrorist threat? Are governance procedures considered to be ad hoc or informal? SPECIFIC: Is Counter-Terrorism new technologies included in national Counter-Terrorism policy development and deployment?

Established	Advance	Leading
GENERAL: Are government institutions required to participate in the development of national Counter-Terrorism policy, including submitting information? Does adequate high-level function affect development and oversight of national Counter-Terrorism efforts? Does the highest government level have comprehensive mapping of national Counter-Terrorism efforts? Has the government defined Counter-Terrorism policy and performance goals? SPECIFIC: Does adequate high-level function have resources and authority to collect information about new technologies? Does highest government level have comprehensive mapping of national Counter-Terrorism efforts that involve new technologies? Has government defined Counter-Terrorism new technologies policy and performance goals? Does policy address utilizing new technologies to promote a culture of tolerance, respect, and responsible use of new technologies?	GENERAL: Has the highest government level approved a binding written policy on policies to guide policy development and oversight? Does the national Counter-Terrorism policy coordinate efforts to deal with conditions that are conducive to the terrorist threats? Has highest government level appointed policy governance and management teams to develop and oversee national Counter-Terrorism policy? Does policy enable oversight of national Counter-Terrorism efforts? Are policy goals and performance goals regarding Counter-Terrorism regularly assessed? Are costs and risks of policy transitions measured against their potential values? SPECIFIC: Does policy development mandate include Counter-Terrorism new technologies? Does policy development team include technological experts? Are policy goals and performance goals regarding Counter-Terrorism new technologies use regularly assessed? Does policy integrate digital literacy efforts that can promote a culture of tolerance online?	GENERAL: Is the national policy on policies fully in effect and transposed in the organizational planning and budgeting processes? Is the national policy on policies reviewed to adapt to changes based on effectiveness in achieving policy goals and preventing terrorist risk and impact? Is Counter-Terrorism policy coordinated with social and economic policy to promote social inclusion? SPECIFIC: Does the national policy on policies deal with new technologies according to state-of-the-art global policies? Is Counter-Terrorism policy coordinated with social and economic policy to promote social inclusion online?

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
GENERAL: Is there a comprehensive approach for preparation of reports on 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 the terrorist intelligence reporting strategy and plan aligned to the overall policy priorities? Is there a dedicated unit in place to compile reports? Does policy obligate other public organizations to participate and submit information to terrorist reporting activity? Is there a full-time research capability? Is academia consulted in the compilation of information and knowledge? Is there an independent review of reporting to improve focus and quality of reports? SPECIFIC: Is the technological reporting aligned to the overall policy priorities? 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 report preparation process. Is there a full-time research capability for new technologies? Is academia and industry in the technological field consulted in the compilation of information and knowledge?	GENERAL: Does the terrorist threat reporting unit have information sharing and cooperation relationships with units in other Member States? SPECIFIC: Does the terrorist threat reporting unit have information sharing and cooperation relationships with counter-terrorism new technologies units and technology companies in other Member States?

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 industry in the technological field consulted in the compilation of information, knowledge, and development of options?	GENERAL: Does the dedicated unit have information sharing and cooperation relationships with units in other Member States? Is the dedicated unit operating according to accepted best practices? SPECIFIC: Does the dedicated unit have information sharing and cooperation relationships with counter-terrorism new technologies units and technology companies in other Member States? SPECIFIC: N/A

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?

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for coordinating policy for development and deployment of national counter-terrorism policies and efforts? Is information about such national policies and efforts collected in a central unit? Does the approach use similar taxonomies of goals and measures to allow comparison? Is the approach structured, documented, and repeatable? Does strategic alignment take into account applicable regional policies? SPECIFIC: Does the comprehensive approach cover malicious use of new technologies? Are dedicated new technologies experts' part of policy coordination? Does strategic alignment take into account applicable regional policies regarding new technologies (if such exist)?	GENERAL: Is there a dedicated unit in place to compile information about applicable policies and possible responses? Does policy obligate other public organizations to participate and submit information to such activity? Are activities along the counter-terrorism life cycle coordinated at the policy level? Is policy binding on all relevant public bodies? Does policy deal with managing a national crisis? 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 industry in the technological field consulted in the compilation of information, knowledge, and development of options? SPECIFIC: N/A	GENERAL: Are policy goals and measures reviewed regularly to assess the need for a different division of responsibility between public organizations in the Counter-Terrorism activity? Is there an independent review of policy to improve focus and quality of recommendations? Is strategic alignment in line with global best practices? SPECIFIC: Is there a dedicated review of goals and measures based on new technologies?

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?

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.2.2	L3	Threat Interventions	Threat Interventions does not exist	GENERAL: Is there an adequate high-level function that develops guidelines on threat interventions? SPECIFIC: Are Counter-Terrorism new technologies included in Counter-Terrorism threat interventions guidelines?

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-Terrorismvalue chain? Is the threat intervention policy coordinated with the national incident classification? Is threat intervention coordinated with prosecution considerations? SPECIFIC: Does the comprehensive approach cover interventions to deal with malicious use of new technologies? Does the comprehensive approach cover interventions that utilize new technologies used by LEAs and necessary support for Counter-Terrorism LEA's value chain? Are dedicated new technologies part of policy development?	GENERAL: Is there a joint operational situational awareness capability for all Counter-Terrorism organizations? Is there a cross-border collaboration capacity for threat intervention? Is threat intervention policy informed by a national level event or exercise? Is there a shared national taxonomy to guide threat interventions across Counter-Terrorism organizations and operations? SPECIFIC: Is there a cross-border collaboration capacity to deal with new technologies?	GENERAL: Is the threat intervention policy reviewed annually? SPECIFIC: Does the threat intervention policy include operational collaboration with ICT companies?

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?
2.2.4	L3	Resource Management	Resource Management does not exist	GENERAL: Is there an adequate high-level function that reports to highest government level about resource management of national Counter-Terrorism policy? Are resource management procedures considered to be ad hoc or informal? Are there policy goals and objectives to guide resource management? SPECIFIC: Are Counter-Terrorism value chain new technologies activities included in national Counter-Terrorism resource allocation?

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 define 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 defined 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
GENERAL: Are government Counter-Terrorisminstitutions required to participate in the development of national Counter-Terrorism resource management, including submitting information? Does adequate high-level function affect development and oversight of national Counter-Terrorism resources management? Does the highest government level have comprehensive mapping of national Counter-Terrorism resource management? Has government defined comprehensive Counter-Terrorism policy and performance goals? SPECIFIC: Does adequate high-level function have resources and authority to collect information about resources for new technologies? Does highest government level have comprehensive mapping of national Counter-Terrorism requirements that involve new technologies? Has government defined Counter-Terrorism new technologies policy and performance goals?	GENERAL: Has highest government level approved a binding written policy on resource management? Are there resource officers in Counter-Terrorism organizations that report to the high-level resource management function? Does policy enable independent review resources use for national Counter-Terrorism efforts? Are policy goals and performance goals regarding use of Counter-Terrorism resources regularly assessed? Does resource management enable adapting to operational requirements? SPECIFIC: Does the resource management policy include Counter-Terrorism new technologies? Does the resource management team include technological experts? Are resources used regarding Counter-Terrorism new technologies use regularly assessed?	GENERAL: Is resource management in force for the short-tern, medium-term, and long-term periods? Is national resource management independently reviewed? SPECIFIC: Does resource management deal with new technologies according to state-of-the-art global policies?

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: Is there a comprehensive approach for collaboration management? Are there specialized personnel for collaboration management? Are collaboration management practices structured, documented, and repeatable? Do LEAs engage regularly with other Counter-Terrorism organizations to discuss cooperation and coordination? Does the policy mandate deal with coordination mechanisms between LEAs and other Counter-Terrorism organizations? Does the policy mandate define interaction with non-Counter-Terrorism organizations as part of the Counter-Terrorism value chain? 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?	GENERAL: Are there clearly defined communication lines and information sharing duties between Counter-Terrorism organizations? Does the policy cover dealing with 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 collaboration management? Is collaboration management independently assessed for effectiveness? SPECIFIC: N/A

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.3	L2	Policy Performance Management		
2.3.1	L3	Policy Performance Measures	Policy Performance Measures does not exist	GENERAL: Is there a procedure or practice to review performance? Are performance management practices considered to be ad hoc or informal? SPECIFIC: N/A
2.3.2	L3	Policy Impact Assessment	Policy Impact Assessment does not exist	GENERAL: Is impact assessment considered to be ad hoc, or informal? Are Counter-Terrorism policy goals clearly defined? SPECIFIC: N/A

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 defined, measurable, and monitored? Are performance management activities regularly reviewed and audited? Are there standards and requirements for performance management? SPECIFIC: Are there specific performance targets of operational controls 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 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 reflect international standards, guidance, and practices? SPECIFIC: Do performance management include targets and monitoring of performance indicators related to data and information sharing, technology, human rights, and gender?
GENERAL: Is there a comprehensive approach to measure impact? Are impact measurement practices structured, documented, and repeatable? Are Counter-Terrorism policy goals clearly articulated to enable impact assessment? Are policy impacts measured and monitored for effectiveness against clear performance metrics? Are policy impact assessment activities adequately resourced? Is there an impact matrix to support impact assessment? SPECIFIC: Do impact assessment practices cover LEA's Counter-Terrorism activities to counter-terrorist use of new technologies? Do impact assessment practices cover LEA's use of new technologies?	GENERAL: Is impact measurement informed by research, intelligence, and analysis? Is impact measurement informed by comprehensive consultations with government Counter-Terrorism organizations? Is there a dedicated unit to perform policy impact assessment with adequate resources and authorities? SPECIFIC: Are new technologies aspects of policy impact assessment supported by a technological expert?	GENERAL: Is impact assessment measurement reviewed and updated on a regular basis for continuous improvement? Is there an impact assessment governance advisory body that includes outside experts such as from industry, other government bodies, etc.? SPECIFIC: Are new technologies aspects of policy impact assessment supported by an independent technological expert?

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 hoc, or informal? Are Counter-Terrorism policy goals clearly defined? SPECIFIC: N/A
2.4	L2	Policy Communications Management		
2.4.1	L3	Strategic Communications	Strategic Communications does not exist	GENERAL: Are communication practices considered to be ad hoc or informal? SPECIFIC: N/A

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 and gender impact assessments? SPECIFIC: Has a survey about public use of new technologies been conducted? Is the LEA's public engagement policy aligned with the cybersecurity engagement policy? Is the communication policy aligned with transparency obligations and best practices regarding use of new technologies?	GENERAL: Is the communication policy reviewed and updated on a regular basis for continuous improvement? Does the policy support public disclosure of LEAs when it is in the interest of the public? Does the policy include communication of internal reviews and audits of Counter-Terrorism law enforcement activities and operations when in the interest of the public? Has public trust in LEAs been conducted? Has a public trust survey been shared with LEA's management? SPECIFIC: Does the policy support publishing internal reviews and audits concerning the use of technology and human rights and gender, the rule of law publicly disclosed when in the interest of the public?

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.5	L2	Public Private Cooperation		
2.5.1	L3	Public Private Cooperation	Public Private Cooperation Capability does not exist	GENERAL: Does the policy deal with public private partnership? SPECIFIC: N/A
2.5.2	L3	Stakeholder Consultations	Stakeholder Consultations does not exis	GENERAL: Are stakeholder consultations considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Does the policy deal in a comprehensive manner with public private cooperation? Does the LEAs need to report its public private cooperation initiatives? Are public private cooperation practices structured, documented, and repeatable? Is there an internal policy regarding roles rights and limitations regarding public – private relations? SPECIFIC: Is there cooperation and a partnership relationship with private ICT companies? Are there standard procedures and forms for cooperation regarding new technologies?	GENERAL: Are stakeholders' meetings conducted regularly as part of the overall organization strategy and priorities? Is stakeholder engagement measured and monitored for effectiveness against clear performance metrics? Does the LEAs communicate stakeholder engagement guiding principles to the private sector? SPECIFIC: Does the policy cover stakeholder consultation with global ICT companies? Is there a strategy to develop partnership with private ICT companies? Can ICT companies proactively seek to address emerging threats and use of technology?	GENERAL: Is there a public private cooperation plan? Are significant policy measures deliberated in public private cooperation meetings? SPECIFIC: Are technological companies regularly consulted during policy development? Does the policy promote strategic cooperation and partnership with private ICT companies?
GENERAL: Is there a comprehensive approach for stakeholder consultations? Are there specialized personnel for leading stakeholder consultations? Are stakeholder consultations structured, documented, and repeatable? SPECIFIC: Are ICT companies' part of the stakeholder consultation policy? Does the LEAs have a mapping of main ICT stakeholders that are relevant to LEA's Counter-Terrorism operations regarding new technologies? Do ICT companies have a clear point of contact for policy information sharing?	GENERAL: Are stakeholders' meetings conducted regularly as part of the overall organization strategy and priorities? Is stakeholder engagement measured and monitored for effectiveness against clear performance metrics? Does the LEAs communicate stakeholder engagement guiding principles to the private sector? SPECIFIC: Does the policy cover stakeholder consultation with global ICT companies? Is there a strategy to develop partnership with private ICT companies? Can ICT companies proactively seek to address emerging threats and use of technology?	GENERAL: Are relevant stakeholder consultation practices reviewed and updated on a regular basis for continuous improvement? SPECIFIC: Are global technical stakeholders' part of regular discussions?

2	L1	National Counter-Terrorism Policy Pillar	Non-Existent	Basic
2.6	L2	National Enabling Counter-Terrorism Components		
2.6.1	L3	National Incident Classification	National Incident Classification does not exist	GENERAL: Is there a public institution with authority to classify an incident as 'national'? Are national incident classification practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for incident classification? Are there comprehensive reporting mechanisms to enable incident classification? Is there a national level organization tasked with developing the national incident classification system? Is there a shared national taxonomy of incident classification across Counter-Terrorism organizations and operations? Is the national classification scheme communicated to all public organizations? Does the policy clearly define who can declare a national incident? Does the national incident classification enable defining authority in charge of the event? SPECIFIC: Does the national incident classification scheme include incidents caused as a result of malicious use of new technologies? Insert:	GENERAL: Is the national incident classification scheme based on ongoing national reviews to locate critical functions? Is the classification scheme informed by regulatory agencies in charge of important services? Is the national incident classification scheme aligned to the overall strategy and priorities? Are the thresholds of the national incident classification scheme reviewed regularly? Is the national classification scheme binding on all public organizations? SPECIFIC: Is the national classification scheme informed by intelligence about possible misuse of new technologies?	GENERAL: Is the national classification system reviewed and updated on a regular basis for continuous improvement? Has the national classification 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 define 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	Strategic Planning and Performance Management		
3.1.1	L3	National Action Plan	National Action Plan does not exist	GENERAL: Are there some elements of a National Action Plan (NAP) in place in a binding policy? Is the development of the NAP considered to be ad hoc or informal? SPECIFIC: N/A
3.1.2	L3	Operational Plan and Budget	Operational Plan and Budgeting does not exist	GENERAL: Are there some elements of an operational plan in place in a binding plan? Is the development of the operational plan and budget considered to be ad hoc or informal? Are elements of the operational plan included in the annual budget? Have elements of the operational plan been coordinated with relevant public institutions? SPECIFIC: Do operational plans reflect priorities for capability building related to new technologies?

Established	Advance	Leading
GENERAL: Is a National Action Plan (NAP) in place? Are the practices to develop an NAP structured, documented, and repeatable? Are there specialized personnel for developing a NAP? Does the NAP clearly establish and assign roles and responsibilities for key priorities and actions? Is the NAP formally reviewed, accepted, and approved by a ministerial body? SPECIFIC: Does the NAP address some elements of new technology, human rights, and gender? Does the NAP address Member State's unique technological and security characteristics?	GENERAL: Is the NAP fully aligned to the United Nations Global Counter-Terrorism Strategy? Is the development of the NAP coordinated centrally with a focal point in place? Is the NAP measured and monitored for effectiveness against clear performance metrics? Is the NAP in effect on all Counter-Terrorism organizations? Is the NAP in effect on supporting organizations? Is a redacted public facing version of the NAP published? SPECIFIC: Does the NAP include dedicated management for new technologies training? Does the NAP comprehensively address new technology, human rights, and gender?	GENERAL: Are relevant practices for developing the NAP reviewed and updated on a regular basis for continuous improvement? SPECIFIC: Does the NAP reflect non-binding best practices and international standards, guidance, and practices related to human rights, gender, data protection, governance, performance management, and the rule of law?
GENERAL: Is there an annual operational plan in place? Are there specialized personnel for operational planning? Are the practices to develop an operation plan structured, documented, and repeatable? Is there a planned annual budget allocated to deliver the operational plan? Has the operational plan been partly coordinated with other public institutions? SPECIFIC: Are operational plans regarding capability building related to new technologies informed by LEA's Counter-Terrorism experience? Is a technological expert involved in developing an operational plan and its budget?	GENERAL: Is the operational plan and budget aligned to the overall organization strategy and priorities? Is there a dedicated operational planning unit or focal point in place? Is the operational plan measured and monitored for effectiveness against clear performance metrics? Is the annual budget reviewed during the fiscal year and adjusted according to operational needs? Has the operational plan been coordinated with other public organizations? SPECIFIC: Are operational plans regarding capability building related to new technologies informed by research, intelligence, and analysis?	GENERAL: Are relevant operational planning practices reviewed and updated on a regular basis for continuous improvement? Are elements of operational plans or reports publicly disclosed when in the interest of the public? Are operational plans and budgets regularly reviewed and audited by an independent body? SPECIFIC: Do operational plans reflect priorities related to human rights, gender, and the rule of law? Is there a full-time technological expert supporting planning and budgeting regarding new technologies?

3	L1	Institutional Pillar	Non-Existent	Basic
3.1.3	L3	Performance Management	Performance Management does not exist	GENERAL: Are there some elements of defining performance management? Is there a procedure or practice to review performance? Are performance management practices considered to be ad hoc or informal? SPECIFIC: N/A
3.2	L2	Governance		
3.2.1	L3	Governance Model	Governance Model and Structure does not exist	GENERAL: Are there some elements of governance and structure in place? Are governance practices considered to be ad hoc, or informal? SPECIFIC: N/A

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 defined, measurable, and monitored? Are performance management activities regularly reviewed and audited? Are there standards and requirements for performance management? SPECIFIC: Are there specific 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 reflect international standards, guidance, and practices? SPECIFIC: Does performance management include targets and monitoring of performance indicators related to data and information sharing, technology, human rights, and gender?
GENERAL: Is there a comprehensive approach for governance? Are governance practices structured, documented, and repeatable? Does governance clearly define internal interfaces, communication lines, and command lines between organizational units? SPECIFIC: Do governance practices provide some elements of oversight over the use of new technologies, human rights, gender, the rule of law, and compliance	GENERAL: Is there a governance model that is aligned to the overall organization strategy and priorities? Is there a formal governance model and structure in place that is inclusive of risk management, and compliance? Are governance practices measured and monitored for effectiveness against clear performance metrics? Is there a clear delegation of authority and role and responsibilities defined for decision-making? SPECIFIC: Do governance practices comprehensively provide oversight over operational deployment of new technologies? Do governance practices comprehensively provide oversight over new technologies, human rights, gender, the rule of law, and compliance? Is there an independent body that reviews the practices of the use of new technology and its implications on human rights, the rule of law, and regulatory compliance?	GENERAL: Are relevant governance practices reviewed and updated on a regular basis for continuous improvement? Are elements of governance decisions and reports publicly disclosed when in the interest of the public? Is there a governance advisory body that includes outside experts such as from industry, other government bodies, etc.? Do governance practices reflect international standards, guidance, and practices? SPECIFIC: Are governance safeguards and decision-making inclusive of information sharing, use of data and new technologies, human rights, and gender equality considerations, and the rule of law that are reflective of international guidance and practices?

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 to be ad hoc or informal or apply to only part of the organization? SPECIFIC: N/A
3.2.3	L3	Compliance	Compliance Capability does not exist	GENERAL: Are there some elements of the compliance mechanism and process in place? Are the compliance assurance practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for risk management? Are there specialized personnel for risk management? Are risk management practices structured, documented, and repeatable? Is there a comprehensive risk policy that applies to all the organization? Does the policy include review of the 'risk library'? SPECIFIC: Does risk management address some elements of the risk related to, human rights and gender, the use of new technologies?	GENERAL: Is there a risk management strategy or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated risk unit in place? Is risk management performance measured and monitored for effectiveness against clear performance metrics? Are risk management activities regularly reviewed and audited? Are there standards and requirements for risk management? Are national risks cascaded down to operational risks and assigned to a lead authority responsible for the risk? SPECIFIC: Do risk management practices inform specific risk treatment measures for information sharing, use of data and new technologies, human rights and gender, and legal requirements?	GENERAL: Are relevant risk management practices reviewed and updated on a regular basis for continuous improvement? Are elements of risk assessment reports publicly disclosed? Are risk management practices regularly reviewed and audited by an independent body? Do risk management practices reflect international standards, guidance, and practices (i.e., ISO31000)? SPECIFIC: Does risk management include relevant aspects of information sharing, use of data and new technologies, human rights and gender, and legal requirements?
GENERAL: Is there a comprehensive approach for compliance? Are there specialized personnel for compliance? Are compliance practices structured, documented, and repeatable? SPECIFIC: Do compliance practices address some elements of use of new technologies, human rights, and gender according to national requirements?	GENERAL: Is there a compliance plan that is aligned to the overall organization strategy and priorities? Is there a dedicated compliance unit in place? Is compliance performance measured and monitored for effectiveness against clear performance metrics? Are compliance activities regularly reviewed and audited? Are there standards and requirements for compliance? SPECIFIC: Are there compliance safeguards in place for Counter-Terrorism law enforcement activities regarding sharing of information and the use of technology related to human rights and gender, and the rule of law?	GENERAL: Are relevant compliance practices reviewed and updated on a regular basis for continuous improvement? Are elements of compliance reports publicly disclosed? Are compliance practices regularly reviewed and audited by an independent body? Do compliance practices reflect international guidance and practices? SPECIFIC: Are compliance safeguards inclusive of information sharing, use of data and new technologies, human rights and gender, and the rule of law that are reflective of international guidance and practices?

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
GENERAL: Is there a comprehensive approach for human rights and gender impact assessment? Are there specialized personnel for human rights and gender impact assessment? Are the human rights and gender assessment practices structured, documented, and repeatable? Is there a human rights and gender impact assessment policy that includes clear thresholds, assessment methods, and mitigation measures? SPECIFIC: Are the human rights and gender impact assessments inclusive of the use of technology?	GENERAL: Is there a human rights and gender plan that is aligned to the overall organization strategy and priorities? Is there a dedicated human rights and gender unit in place that reports to top management? Is human rights and gender impact performance measured and monitored for effectiveness against clear performance metrics? Do human rights and gender impact assessments influence operational activities and decision-making? Are human rights and gender impact activities regularly reviewed and audited? Are there standards and requirements for human rights and gender? Is human rights and gender aligned with the Data Protection Office? SPECIFIC: Is the operational work informed by human rights and gender analyses? Are there human rights and gender safeguards in place for Counter-Terrorism law enforcement activities regarding sharing of information and the use of technology, and the rule of law? Are impact assessments embedded in new technologies procurement processes and inform procurement and design of new technologies' use?	GENERAL: Do human rights and gender measures reflect international standards, guidance, and practices? Are relevant human rights and gender practices used to inform activities and impact decision-making? Are relevant human rights and gender practices reviewed and updated on a regular basis for continuous improvement? Are elements of human rights and gender reports publicly disclosed? Are human rights and gender practices regularly reviewed and audited by an independent body? Is there a human rights advisory committee to support the human rights office composed of relevant governmental and non-governmental stakeholders? Are there sufficient human and financial resources allocated to human rights and gender impact assessments? SPECIFIC: Do the human rights and gender office provide input to policy processes concerning use of technology and its impact on human rights and gender?

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
GENERAL: Is there a comprehensive approach to data protection? Are there specialized personnel for data protection? Are data protection practices structured, documented, and repeatable? Is there an appointed data protection officer with a clear organizational mandate? SPECIFIC: Does the data protection policy inform operations and the use of new technologies and data, human rights and gender according to national requirements? Are there special data and privacy protection practices for Counter-Terrorism intelligence and investigations?	GENERAL: Is there a data protection strategy or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated data protection unit in place that reports to top management? Is data protection performance measured and monitored for effectiveness against clear performance metrics? Are data protection activities regularly reviewed and audited? Are there internal organizational standards and requirements for data protection? Has management received data protection training? SPECIFIC: Are there data protection safeguards in place for Counter-Terrorism law enforcement activities regarding sharing of information and the use of technology, human rights and gender, and the rule of law? Is there a general policy requiring privacy impact assessments for introduction of new technologies? Are privacy impact assessments embedded in new technologies procurement processes and inform procurement and design of new technologies use?	GENERAL: Are relevant data protection practices reviewed and updated on a regular basis for continuous improvement? Are elements of data protection reports publicly disclosed? Are data protection practices regularly reviewed and audited by an independent body? Do data protection measures reflect international guidance and practices? Does the Data Protection Office consult in government policy processes regarding LEA's capabilities that implicate privacy? Have organizations deployed data protection training? SPECIFIC: Are data protection practices regularly reviewed and audited by an independent body specifically concerning use of technology, data and human rights and gender? Does the Data Protection Office publish redacted information about privacy impact assessments conducted?

3	L1	Institutional Pillar	Non-Existent	Basic
3.3	L2	Mission Management and Coordination		
3.3.1	L3	Horizon Scanning	Horizon Scanning Capability does not exist	GENERAL: Are there elements of horizon scanning capability in place and considered operational? Is the horizon scanning practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for horizon scanning? Are horizon scanning practices structured, documented, and repeatable? Are there specialized personnel for horizon scanning? Are horizon scanning activities planned and delivered at regular intervals (i.e., annually, every 4 years, etc.) SPECIFIC: Is the horizon scanning team capable of generating foresight regarding new technology use by terrorists?	GENERAL: Is there a horizon scanning plan that is aligned to the overall organization strategy and priorities? Is this topic included in the national action plan? Is there a dedicated horizon scanning unit in place? Is horizon scanning performance measured and monitored for effectiveness against clear performance metrics? Are horizon scanning activities regularly reviewed and audited? Are there standards and requirements for threat management? Are the findings and outputs of horizon scanning used to inform strategic and long-term national policy and capability development? Does horizon scanning practices consult and engage a wide range of stakeholders from industry, government, civil society, academia, etc.? SPECIFIC: Are there human rights and gender, and the rule of law safeguards in place for horizon scanning regarding sharing of information and the use of technology ?	GENERAL: Are relevant horizon scanning practices reviewed and updated on a regular basis for continuous improvement? Are elements of horizon scanning publicly disclosed when in the interest of the public? Are horizon scanning practices regularly reviewed and audited by an independent body? Are horizon scanning activities coordinated with allies? SPECIFIC: Are horizon scanning practices regularly reviewed and audited by an independent body specifically concerning use of technology and human rights and gender?

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 specifically 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 considered to be ad hoc or informal? SPECIFIC: N/A
3.4	L2	Partnership and Cooperation		
3.4.1	L3	Government Relationship Management	Government Relationship Management Capability does not exist	GENERAL: Are there informal policies or elements of government relationship management? Are government relationship management practices considered to be ad hoc or informal? SPECIFIC: N/A

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 classification 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 a dedicated information sharing unit? Is information sharing performance measured and monitored for effectiveness against clear performance metrics? Are information sharing activities regularly reviewed and audited? Are there standards and requirements for information sharing? Are information sharing arrangements aligned with other information sharing activities (such as national CSIRT information sharing)? SPECIFIC: Are there human rights, gender, and the rule of law with safeguards in place for information sharing regarding sharing of information and the use of technology concerning human rights and gender, and the rule of law?	GENERAL: Are relevant information sharing practices reviewed and updated on a regular basis for continuous improvement? Are elements of information sharing publicly disclosed when in the interest of the public? Are information sharing practices regularly reviewed and audited by an independent body? SPECIFIC: Are information sharing practices regularly reviewed and audited by an independent body specifically concerning use of technology and human rights and gender?
GENERAL: Is there a comprehensive approach for government relationship management? Are there specialized personnel for government relationship management? Are government relationship management practices structured, documented, and repeatable? Is there a central focal point for government relationship management? Do LEAs engage regularly with relevant government stakeholders to discuss cooperation and coordination? SPECIFIC: Is there a dedicated procedure for government relations management for dealing with new technologies risk scenarios? Does the dedicated procedure include relevant contacts for quick response?	GENERAL: Is there a government relationship management plan and practices that is aligned to the overall organization strategy and priorities? Is there a dedicated government relationship management unit or focal point in place? Is government relationship management performance measured and monitored for effectiveness against clear performance metrics? Are international cooperation activities regularly reviewed and audited? Are there standards and requirements for government relationship management? SPECIFIC: Are there human rights and gender and the rule of law safeguards controls in place for government relationship management regarding sharing of information and the use of technology?	GENERAL: Are relevant government relationship management practices reviewed and updated on a regular basis for continuous improvement? Are elements of government relationship management publicly disclosed when in the interest of the public? Are government relationship management practices regularly reviewed and audited by an independent body? SPECIFIC: Are government relationship management practices regularly reviewed and audited by an independent body specifically concerning use of technology and human rights and gender? Are LEAs integrated in non-law enforcement policy processes relating to new technologies?

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 Counter-Terrorism partnership management practices considered to be ad hoc or informal? SPECIFIC: N/A
3.4.3	L3	Public / Community Engagement	Public / Community Engagement Capability does not exist	GENERAL: Are there elements of public / community engagement in place? Are public / community engagement practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for Counter-Terrorism partnership management? Are there specialized personnel for Counter-Terrorism partnership management? Are Counter-Terrorism partnership management practices structured, documented, and repeatable? SPECIFIC: Is there a dedicated procedure for Counter-Terrorism partnership management for dealing with new technologies risk scenarios? Does the dedicated procedure include relevant contacts for quick response? Are non-LEA's Counter-Terrorism agencies part of technical risk assessment?	GENERAL: Is there a Counter-Terrorism partnership management plan that is aligned to the overall organization strategy and priorities? Is there a dedicated Counter-Terrorism partnership management unit or focal point in place? Is Counter-Terrorism partnership management performance measured and monitored for effectiveness against clear performance metrics? Are Counter-Terrorism partnership management activities regularly reviewed and audited? Are there standards and requirements for Counter-Terrorism partnership management? SPECIFIC: Are there human rights, gender, and the rule of law safeguards in place for Counter-Terrorism partnership management regarding sharing of information and the use of technology? Is there a clear procedure for coordination with national CSIRT/cybersecurity agencies?	GENERAL: Are relevant Counter-Terrorism partnership management practices reviewed and updated on a regular basis for continuous improvement? Are elements of Counter-Terrorism partnership management publicly disclosed when in the interest of the public? Are Counter-Terrorism partnership management practices regularly reviewed and audited by an independent body? SPECIFIC: Are Counter-Terrorism partnership management practices regularly reviewed and audited by an independent body specifically concerning use of technology and human rights and gender? Are LEAs integrated in non-LEA's Counter-Terrorism new technologies policy processes?
GENERAL: Is there a comprehensive approach for public / community engagement? Are there specialized personnel for public / community engagement? Are public / community engagement practices structured, documented, and repeatable? SPECIFIC: Do public / community engagement practices 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 LEAs use social media for communication and public engagement? Is there clear guidelines and activity to support victims of new technologies misuse (i.e., ransomware)? Have you published information about LEA's role and potential support for victims of new technologies misuse (i.e., ransomware)?	GENERAL: Is there a public / community engagement strategy or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated public affairs unit in place? Is public / community engagement performance measured and monitored for effectiveness against clear performance metrics? Is public / community engagement regularly reviewed and audited? Are there standards and requirements for public / community engagement? SPECIFIC: Has a survey about public use of new technologies been conducted? Have community leaders been consulted on locating critical digital social functions? Is the LEA's public engagement policy aligned with the cybersecurity engagement policy?	GENERAL: Are relevant public / community engagement practices reviewed and updated on a regular basis for continuous improvement? Are elements Counter-Terrorism law enforcement activities and operations publicly disclosed when in the interest of the public? Are elements of internal reviews and audits of Counter-Terrorism law enforcement activities and operations publicly disclosed when in the interest of the public? Has a public trust and engagement survey been conducted? SPECIFIC: Are internal reviews and audits concerning the use of technology and human rights and gender, the rule of law publicly disclosed when in the interest of the public?

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: Is there a comprehensive approach for international cooperation? Are there specialized personnel for international cooperation? Are international cooperation practices structured, documented, and repeatable? SPECIFIC: Do units along the Counter-Terrorism new technologies value chain have clear guidelines about jurisdiction and cross-border international cooperation? Do LEAs have trusted communications with other LEAs? Is the LEAs side to agreements that apply to cross-border cooperation along the Counter-Terrorism new technologies value chain? Do LEAs participate in a trusted LEA's 24/7 cybercrime network (such as Interpol)? Do LEA's exchange 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: Are there human rights, gender, and the rule of law safeguards in place for international cooperation regarding sharing of information and the use of technology? Do LEAs regularly participate in relevant Counter-Terrorism new technologies international discussions? Has the LEAs participated in an international operation or exercise that includes new technologies?	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? Do LEAs engage regularly with non-governmental stakeholders in other countries which are important to Counter-Terrorism operations? SPECIFIC: Are international cooperation practices regularly reviewed and audited by an independent body specifically concerning use of technology and human rights and gender? Is the LEAs active 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.) Do LEAs engage regularly with new technologies non-governmental stakeholders in other countries which are important to Counter-Terrorism operations?

3	L1	Institutional Pillar	Non-Existent	Basic
3.5	L2	Operational Management		
3.5.1	L3	Oversight Management	Oversight Management Capability does not exist	GENERAL: Are there elements of oversight management in place? Are oversight management practices considered to be ad hoc or informal? SPECIFIC: N/A
3.5.2	L3	Intelligence Management	Intelligence Management Capability does not exist	GENERAL: Are there elements of intelligence management practices in place? Are intelligence management practices considered to be ad hoc or informal? Are intelligence products available to relevant operational Counter-terrorismT activities? SPECIFIC: N/A

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? Is there an independent oversight mechanism that audits and reviews operations? SPECIFIC: Does the oversight management mandate include operational oversight concerning use of technology and human rights and gender?
GENERAL: Is there a comprehensive approach for intelligence management? Are there specialized personnel for intelligence management? Are intelligence management practices structured, documented, and repeatable? SPECIFIC: Is the organization part of private sector information sharing arrangements or does it receive products from such arrangements? Is there a basic capability of producing intelligence on terrorist use of basic technology such as the Internet, social media, etc.? Does the organization employ technologists to support intelligence management capabilities?	GENERAL: Is there an intelligence management plan and practices that is aligned to the overall organization strategy and priorities? Is there a dedicated intelligence unit in place? Is intelligence management performance measured and monitored for effectiveness against clear performance metrics? Are intelligence activities regularly reviewed and audited? Are there standards and requirements for intelligence? Are intelligence products developed for strategic, operational, and tactical use according to practitioners requirements? SPECIFIC: Is there advanced intelligence capability of producing intelligence of terrorist use of new technologies such as the Dark Web, cryptocurrencies, etc.? Are there human rights and geneder and the rule of law safeguards in place for the use of technology for intelligence practices? Are intelligence practices human-rights complaint and gender-sensitive?	GENERAL: Are relevant intelligence and intelligence management practices reviewed and updated on a regular basis for continuous improvement? Are elements of intelligence and cases publicly disclosed when in the interest of the public? Are intelligence practices regularly reviewed and audited by an independent body? Are intelligence products shared as part of information sharing based on information security classification? Are intelligence products fused with other intelligence products and sources? SPECIFIC: Are intelligence practices regularly reviewed and audited by an independent body specifically concerning use of technology and human rights and gender? Are intelligence practices fully human-rights complaint and gender-sensitive?

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
3.5.4	L3	Law Enforcement Agency Actions	CT Law Enforcement Agency actions Capability does not exist	GENERAL: Are there elements of Counter-Terrorism LEA's actions in place? Are Counter-Terrorism LEA's actions structured, documented, and repeatable? 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 specifically 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 effectiveness against clear performance metrics? Are Counter-Terrorism LEA's actions regularly reviewed and audited? Are there standards and requirements for Counter-Terrorism LEA's actions? SPECIFIC: Do Counter-Terrorism LEA's administrative actions have the capability to disrupt or prevent terrorist use of new technologies (i.e., the Dark Web, cryptocurrencies, etc.)? Are there controls for human rights, gender, and the rule of law safeguards in place for the use of technology?	GENERAL: Are relevant Counter-Terrorism LEA's actions reviewed and updated on a regular basis for continuous improvement? Are elements of Counter-Terrorism LEA's actions publicly disclosed when in the interest of the public? Are Counter-Terrorism LEA's actions regularly reviewed and audited by an independent body? SPECIFIC: Are Counter-Terrorism LEA's actions regularly reviewed and audited by an independent body specifically concerning use of technology and human rights and gender?

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 practices considered to be ad hoc or informal? SPECIFIC: N/A
3.5.6	L3	Incident Response Management	Incident Response Management Capability does not exist	GENERAL: Are there elements of incident response plans or practices in place? Are incident response practices considered to be ad hoc or informal? SPECIFIC: N/A
3.6	L2	Operational Support		

Established	Advance	Leading
GENERAL: Is there a comprehensive approach for criminal justice interface management? Are there specialized personnel for a criminal justice interface? Are criminal justice interface practices structured, documented, and repeatable? Are criminal justice processes streamlined between law enforcement, prosecution, courts and detention authorities? SPECIFIC: Are there standards or minimal requirements for digital evidence and chain of custody? Have criminal justice practitioners received special training in Counter-Terrorism use of new technologies?	GENERAL: Is the criminal justice interface management plan aligned to the overall organization strategy and priorities? Is the criminal justice interface management performance measured and monitored for effectiveness against clear performance metrics? Has the criminal justice process been independently reviewed for effectiveness and efficiency? Are there standards and requirements for the criminal justice interface management? SPECIFIC: Are criminal justice practitioners integrated by training in Counter-Terrorism use of new technologies?	GENERAL: Are relevant criminal justice interface management practices and incidents reviewed and updated on a regular basis for continuous improvement? Is policy informed by a survey that assessed effectiveness and satisfaction amongst the criminal justice stakeholders? Does the criminal justice system perform well according to international benchmarks? SPECIFIC: N/A
GENERAL: Is there a comprehensive incident response management approach in place? Are incident response practices structured, documented, and repeatable? Are there incident response plans? Are the roles and responsibilities during an incident response clearly identified and understood and individuals trained? SPECIFIC: Are there specific incident response plans to deal with digital and new technologies?	GENERAL: Is incident response management plan aligned to the overall organization strategy and priorities? Is incident response management performance measured and monitored for effectiveness against clear performance metrics? Are incident response plans developed according to risk assessment and likely scenarios? Is there an escalation mechanism and command structure to escalate incident response? SPECIFIC: N/A	GENERAL: Are relevant incident response management practices and incidents reviewed and updated on a regular basis for continuous improvement? Are elements of incident review reports publicly disclosed when in the interest of the public? Are incident response plans dynamic to manage complex scenarios? SPECIFIC: Are incident response plans dynamic to manage complex scenarios involving both physical and digital incident responses?

3	L1	Institutional Pillar	Non-Existent	Basic
3.6.1	L3	Data and Information Management	Data and Information Management Capability does not exist	GENERAL: Are there elements of data and information management practices in place? Are data and information management practices considered to be ad hoc or informal? SPECIFIC: N/A
3.6.2	L3	Technical Support	Technical Support Capability does not exist	GENERAL: Are there elements of technical support in place? Are technical support practices considered to be ad hoc or informal? SPECIFIC: N/A

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 intelligence collected and managed?	GENERAL: Is there a data and information strategy or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated data and information management office? Is data and information management performance measured and monitored for effectiveness against clear performance metrics? Is data available to all LEA's clients based on a need-to-know basis? Do LEA's deploy advanced analytic capabilities? SPECIFIC: Is technical data collected and managed according to accepted cybersecurity standards? Is the organization part of public private information sharing arrangements? Do LEA's share technical information with national CSIRT?	GENERAL: Are relevant data and information management practices reviewed and updated on a regular basis for continuous improvement? Do LEA's conduct data science capabilities on its data? SPECIFIC: N/A
GENERAL: Is there a comprehensive approach and controls in place for technical support? Are there specialized personnel to deliver technical support? Are technical support practices structured, documented, and repeatable? SPECIFIC: Can technical support provide basic technical solutions for intelligence and investigations activities? Do LEA's have access to ICT forensic services?	GENERAL: Is there a technology strategy or plan that is aligned to the overall organization strategy and priorities? Is technical support performance measured and monitored for effectiveness against clear performance metrics? Is technical support fully capable of supporting and delivering technical solutions for Counter-Terrorism law enforcement requirements? Is there a specialized dedicated unit to develop or procure technical solutions for intelligence and investigations? SPECIFIC: Can technical support provide advanced technical solutions for intelligence and investigations activities? Do LEA's have an ICT forensic facility with adequate technical staff? Are human rights requirements and gender impacts incorporated in providing technical solutions?	GENERAL: Are relevant technical support practices reviewed and updated on a regular basis for continuous improvement? SPECIFIC: Is there research and development (R&D) capability to support future technical solutions? Is there an R&D partnership model with industry, academia, and others, to drive innovation?

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
3.7.3	L3	Innovation Partnership Model	Partnership Model Capability does not exist	GENERAL: Are there some elements of innovation partnership in place? Are innovation partnership model 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 defined 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? SPECIFIC: Are there dedicated experts in ICT innovation?	GENERAL: Are relevant innovation practices reviewed and updated on a regular basis for continuous improvement? Is there a dedicated change management unit to realize innovation? Is innovation prioritized, endorsed, and promoted from top down? SPECIFIC: N/A
GENERAL: Is there a comprehensive innovation partnership approach in place? Are partnership model practices structured, documented, and repeatable? SPECIFIC: Does this approach apply to LEA's activity against terrorist use of new technologies?	GENERAL: Is there an innovation partnership model plan that is aligned to innovation strategy or plan, and the overall organization strategy and priorities? Is the innovation partnership model performance measured and monitored for effectiveness against clear performance metrics? SPECIFIC: N/A	GENERAL: Are relevant innovation partnership practices reviewed and updated on a regular basis for continuous improvement? tIs there a means to incubate and invest in start-ups related to promising technologies related to the Counter-Terrorism law enforcement value chain?

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 defining workforce skills requirements? Are workforce skills requirements practices considered to be ad hoc or informal? SPECIFIC: Does workforce skill requirements include some LEA's use of new technologies?
3.8.2	L3	Training Needs Assessment	Training Needs Assessment Capability does not exist	GENERAL: Are there elements of conducting training needs assessment? Are training needs assessment practices considered to be ad hoc or informal? SPECIFIC: N/A

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
GENERAL: Is there a comprehensive approach to define workforce skills requirements? Are there specialized personnel for defining workforce skills requirements? Are workforce skills requirements practices structured, documented, and repeatable? SPECIFIC: Do workforce skills requirements identify technical skills required for new technologies? Do workforce skills new technologies skill assessment and requirements apply to all roles in the counter-terrorism value chain and criminal justice process. Do the workforce skill requirements include periodical training for new technologies?	GENERAL: Are workforce skills requirements aligned to the overall HR strategy and organization strategy and priorities? Are workforce skills requirements defined by current capability and tasking requirements? Are there standards and requirements in defining workforce skills requirements? Is the skills level of existing workforce measured regularly? SPECIFIC: Do the workforce skills requirements incorporate gender considerations as it relates to new technologies?	GENERAL: Are relevant workforce skills requirements practices reviewed and updated on a regular basis for continuous improvement? SPECIFIC: Do workforce skills requirements identify emerging technical skills required for future technology capability?
GENERAL: Is training needs assessment aligned to the overall HR strategy and organization strategy and priorities? Is there a comprehensive approach to conduct training needs assessment? Are there personnel trained in conducting training needs assessment? Are training needs assessment practices structured, documented, and repeatable? SPECIFIC: Do training needs assessments identify required technical training for new technology capability?	GENERAL: Are training needs assessments conducted on an individual basis? Are there standards and requirements in conducting training needs assessments? SPECIFIC: Are training needs assessments inclusive of capacities on gender requirements?	GENERAL: Are relevant training needs assessment practices reviewed and updated on a regular basis for continuous improvement? SPECIFIC: Do training needs assessment identify future training requirements for emerging capabilities? Does training needs assessment examine gender aspects (both knowledge and skills)?

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 training aligned to the overall HR strategy and organizations strategy? Is there a comprehensive training approach in place? Is there specialized training for management personnel? Is the training model suited for different professions and roles? Are training delivery model practices structured, documented, and repeatable? SPECIFIC: Does the training delivery model apply to all roles that need new technologies skills in the counter-terrorism value chain and criminal justice process? Does training include engagement with industry and academia?	GENERAL: Is training delivered aligned to individual requirements and position? Is there a dedicated training management unit? Is training measured and monitored for effectiveness against clear performance metrics? Is training aligned to workforce skills requirement, training needs assessment, and career development progression? SPECIFIC: Does training include industry and academic level courses? Does training include the use of new technology, legal, human rights, and gender consideration?	GENERAL: Are relevant training delivery practices reviewed and updated on a regular basis for continuous improvement? Does training delivery consider opportunity for an exchange programme with Counter-Terrorism partners? SPECIFIC: Is the training delivery model integrated with academic training in new technologies?
GENERAL: Are there specialized human resources personnel for career development? Are career development practices structured, documented, and repeatable? SPECIFIC: Are there career development paths for specialized skills related to technologies?	GENERAL: Is career development aligned with overall HR strategy and organization strategy? Is there a dedicated human resources unit to manage career development? SPECIFIC: Do career development and progression strategies and practices consider gender equality and promote women's leadership? Are there mechanisms that enable private sector experts joining LEAs for dedicated periods of time?	GENERAL: Is career development and progression reviewed and updated on a regular basis for continuous improvement and following principles of equality and non-discrimination? SPECIFIC: Are there mechanisms for LEA's experts to have professional leave for dedicated terms at private sector technological companies?
GENERAL: Is there a comprehensive procurement approach and control in place? Are there specialized personnel for procurement? Are procurement practices structured, documented, and repeatable? SPECIFIC: Are there practices for the procurement of operational technology solutions for Counter-Terrorism law enforcement?	GENERAL: Is there a procurement strategy or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated procurement unit in place? Is procurement performance measured and monitored for effectiveness against clear performance metrics? SPECIFIC: Are there special practices or rules for the procurement of operational technology solutions that are considered sensitive for Counter-Terrorism law enforcement?	GENERAL: Are relevant procurement practices reviewed and updated on a regular basis for continuous improvement? Are procurement activities independently reviewed and audited on a regular basis? Are elements of procurement practices and contracts publicly disclosed when in the interest of the public? SPECIFIC: N/A

3	L1	Institutional Pillar	Non-Existent	Basic
3.9.2	L3	Finance	Finance Capability does not exist	GENERAL: Are there elements of financial management practices in place? Are finance practices considered to be ad hoc or informal? SPECIFIC: N/A
3.9.3	L3	ICT	ICT Capability does not exist	GENERAL: Are there elements of ICT practices and support in place? Are ICT 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/A
GENERAL: Is there a comprehensive ICT management approach and controls in place? Are there specialized personnel for ICT? Are ICT practices structured, documented, and repeatable? SPECIFIC: N/A	GENERAL: Is there an ICT strategy or plan that is aligned to the overall organization strategy and priorities? Is there a dedicated ICT unit in place? Are ICT requirements informed by and aligned to the organization business processes and requirements? Is ICT performance measured and monitored for effectiveness against clear performance metrics? Is ICT policy aligned with innovation management? SPECIFIC: N/A	GENERAL: Are relevant ICT measures and ICT incidents reviewed and updated on a regular basis for continuous improvement? SPECIFIC: N/A

3	L1	Institutional Pillar	Non-Existent	Basic
3.9.4	L3	Security	Security Capability does not exis	GENERAL: Are there elements of security practices in place? Are security practices considered to be ad hoc or informal? SPECIFIC: N/A
3.9.5	L3	Cybersecurity	Cybersecurity Capability does not exist	GENERAL: Are there elements of cybersecurity practices in place? Are cybersecurity practices considered to be ad hoc or informal? SPECIFIC: N/A

Established	Advance	Leading
GENERAL: Is there a comprehensive security approach and controls for physical and personnel security based on a threat assessment? Are there specialized personnel for security? Are security practices structured, documented, and repeatable? SPECIFIC: Are there personnel and physical security measures in place to protect technology, technology capabilities, and sensitive information?	GENERAL: Is there a security strategy or plan that is aligned to the overall organization strategy and priorities and overall threat assessment? Is the security strategy aligned with other security organizations? Is there a dedicated security unit in place? Is security policy and practices informed by a security threat / risk assessment process? Is security performance measured and monitored for effectiveness against clear performance metrics? SPECIFIC: Are there personnel and physical security measures in place to protect technology, technology capabilities and sensitive information based on security risk assessment and individual security clearance, job role, and technology? Is security risk assessment performed on technology?	GENERAL: Are relevant security measures and security incidents reviewed and updated on a regular basis for continuous improvement? Are elements of security incidents publicly disclosed when in the interest of the public? Is there an escalation mechanism to escalate security incidents? SPECIFIC: N/A
GENERAL: Is there a comprehensive security approach and controls in place for cybersecurity based on risk and threat assessment? Are there specialized personnel for cybersecurity? Are cybersecurity practices structured, documented, and repeatable? Are ICT management aware of cybersecurity considerations and take them into account? Do LEAs have binding employee guidance on cybersecurity? SPECIFIC: Are there specific cybersecurity measures in place for operational technologies used by Counter-Terrorism law enforcement?	GENERAL: Is there an organizational cybersecurity strategy that is aligned to the overall national cybersecurity and organizational strategy and priorities? Is there a dedicated internal unit for cybersecurity? Is the cybersecurity unit integrated in organizational processes? Is cybersecurity policy and practices informed by cyber threat / risk assessment processes? Is security performance measured and monitored for effectiveness against clear performance metrics? Does the cybersecurity policy align with international best practices and standards for organizational cybersecurity? Has annual employee awareness and training been carried out? Has cybersecurity been independently audited? Do LEAs have real-time situational awareness capabilities regarding its ICT? Is there coordination and cooperation with national CSIRTs? SPECIFIC: Has the cybersecurity unit integrated procurement and development of new ICT capabilities?	GENERAL: Are relevant cybersecurity measures and cybersecurity incidents reviewed and updated on a regular basis for continuous improvement? Does cybersecurity report to top management? Are elements of cybersecurity incidents publicly disclosed when in the interest of the public? Is there an escalation mechanism to escalate cybersecurity incidents? SPECIFIC: N/A

3	L1	Institutional Pillar	Non-Existent	Basic
3.9.6	L3	Legal	Legal Capability does not exist	GENERAL: Do LEAs have dedicated legal support personnel? SPECIFIC: N/A

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 specific 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 fields of LEA's operations and support activities? Does the legal department carry out training and continuing legal education activities? SPECIFIC: Does the legal department have a data protection legal expert? Does the legal department have an expert on Internet intermediaries? Does the legal department have a legal expert on content takedown rules?	GENERAL: Are relevant legal practices reviewed and updated on a regular basis for continuous improvement? Is the legal department involved in international legal discussions on Counter-Terrorism issues? Are elements of legal reports publicly disclosed when in the interest of the public? SPECIFIC: Is the legal department involved in international legal discussions on Counter-Terrorism issues and new technologies issues?

United Nations Office of Counter-Terrorism
United Nations Headquarters
New York, NY 10017

www.un.org/counterterrorism

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)