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

INTERPOL

Funded by
the European Union

Cybersecurity and New Technologies

Designing National Counter-terrorism Policy Responses to Counter the Use of New Technologies for Terrorist Purposes

---

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 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. Mariana Gonzalez Campbell** – Preventing Violent Extremism Consultant, Organizations of American States (OAS)
- **Mr. Michael O'Keefe** – Counter-Terrorism Specialist, Terrorism Prevention Branch of United Nations Office on Drugs and Crime (UNODC)
- **Mr. Victor Kipkoech** – Programme Associate, Global Center on Cooperative Security (GCCS)
- **Mr. Winthrop Wells** – Programme Manager, The International Institute for Justice and the Rule of Law (IIIJ)

Terms and Definitions

Anomaly Detection	The data mining process of identifying data points that fall outside or deviate from the norm.
Area of Responsibility (AOR)	The area or region is under the responsibility or jurisdiction of a practitioner.
Artificial Intelligence	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.
Darknet/Dark Web	The encrypted part of the Internet accessed using specific software that in themselves are not criminal, such as the Tor browser. However, it is recognized that the dark web contains many criminal websites and services which are hosted on these networks.[1]
Deradicalization	The process in which someone who shows signs of having been radicalized is retrained to abandon a radicalized ideology.[2]

1 European Cybercrime Center (EC3), "Internet Organized Crime Threat Assessment 2019" (Europol, 2019), 4, https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf.

2 Lorenzo Vidino and Clifford Bennett, "A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism" (The 3rd Conference of the European Counter Terrorism Centre (ECTC) Advisory Network on Terrorism and Propaganda, The Hague, Netherlands: Europol, 2019), 8, https://www.europol.europa.eu/cms/sites/default/files/documents/a_review_of_transatlantic_best_practices_for_countering_radicalisation_in_prisons_and_terrorist_recidivism.pdf.

Disengagement	The process in which someone who shows signs of having been radicalized is coached into either "leav[ing] their group or reject[ing] violence, while not necessarily aiming to change their underlying extremist viewpoints or ideology."[3]
Evidence	A formal term for information that forms part of a trial in the sense that it is used to prove or disprove the alleged crime. All evidence is information, but not all information is evidence. Information is thus the original, raw form of evidence.[4]
Evidence-based practice (EBP)	The use of concrete, qualitative data as a means of informing policy and implementation.[5]
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.
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.
Natural Language Processing (NLP)	A subset of artificial intelligence (AI) that deals with the ability of a machine to analyse and deal with human languages both as a source of input and as the product of an output (rather than, for example, data or code).[6]
New Technologies	While the New Technologies terminology covers a wide range of different technologies,[7] 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.[8]

3 Vidino and Bennett, 8.

4 CTED Guidelines to facilitate the use and Admissibility as evidence in national criminal courts of information Collected, handled, preserved and shared by the military to prosecute terrorist offences (2021)

5 Rebecca Freese, "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works," *Perspectives on Terrorism* 8, no. 1 (2014): 37.

6 Ross Gruetzemacher, "The Power of Natural Language Processing," *Harvard Business Review*, April 19, 2022, https://hbr.org/2022/04/the-power-of-natural-language-processing; Ben Lutkevich and Ed Burns, "What Is Natural Language Processing? An Introduction to NLP," Enterprise AI, accessed April 30, 2023, https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP.

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

8 CT TECH Programme Document – Annex I Description of the Action

Open-source Intelligence (OSINT)	Intelligence gathered from publicly available sources.[9]
Rehabilitation	A comprehensive process, ideally resulting in the rehabilitated person leading a self-determined and self-sustained life, without adhering to extremist views or participating in extremism-inspired activities (including violence).
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.
Security by Design	The installation of security measures as something is being built/designed such that it will be equipped to defend against a threat within its existing structure/build/framework.[10]
Security by Default	A programme/policy that reaches the consumer having already possessed necessary measures to ensure security (rather than the consumer needing to implement the security measures separately).[11]
Social Media Intelligence (SOCMINT)	Intelligence information gathered through social media.
Standard Operating Procedures	A predetermined series of steps that guides the implementation of policy.
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.[12]
Virtual Assets	Virtual/crypto assets refers to digital forms of currency and other assets.[13]
Zettabyte	One zettabyte is equal to one billon terabytes.

9 Rob Flanders et al., *Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts*, 2nd ed. (United Kingdom, 2019), 22–24, https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf.

10 European Commission, *Security by Design: Protection of Public Spaces from Terrorist Attacks* (Luxembourg: European Union, 2022), 23, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf.

11 Cybersecurity and Infrastructure Security Agency et al., "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default," April 13, 2023, 5–6, https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf.

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

13 Financial Action Task Force (FATF), "Virtual Assets," Financial Action Task Force (FATF), accessed May 7, 2023, https://www.fatf-gafi.org/en/topics/virtual-assets.html.

Executive Summary

This document "Designing National Counter-Terrorism Policy Responses to Counter the Use of New Technologies for Terrorist Purposes" is a comprehensive framework designed to assist policymakers and stakeholders in the field of counter-terrorism to understand the impact of new technologies on terrorism and to formulate effective counter-terrorism policy responses. It covers a broad range of key considerations for the design of national counter-terrorism policy responses to the use of new technologies for terrorist purposes and provides good practices and practical insights to help policymakers and practitioners develop effective counter-terrorism policies and strategies. The guide examines existing counter-terrorism policies and strategies and identifies gaps in the way in which they address the use of new technologies by terrorists.

The methodology for developing the guide includes research, analysis, and consultation with relevant stakeholders and experts. The research focused on identifying the key challenges and opportunities presented by new technologies in the context of terrorism and existing counter-terrorism policy and strategy responses. This involves reviewing existing literature, case studies, and best practices, and from those sources, identifying key components and effective strategies for developing counter-terrorism policy responses. The guide provides a detailed analysis of the challenges posed by the exploitation of new technologies by terrorists and offers practical recommendations for how to respond. It includes good practices and examples of successful policy responses from different Member States. While the terminology regarding new technologies covers a wide range of different technologies, the guide more specifically addresses the use and abuse of new technologies such as the Internet, social media, cryptocurrencies, facial recognition, and the darknet.

The guide acknowledges that technology is evolving at a faster pace than national policies can change, and therefore provides a framework for assessing the efficacy of policies and developing amendments to preserve their relevance. It also highlights that many existing counter-terrorism policies do not account for technological enablers such as artificial intelligence, the dark web, end-to-end encrypted apps, and digital assets. The guide is specifically focused on the use of new technologies for terrorist purposes and highlights potential uses of new technology to counter-terrorism. The guide is structured around four core considerations: awareness, threat intervention, national capabilities, and cooperation, each of which implements cross-components involved in the process of developing policy to enable effective responses to the use of new technologies for terrorist purposes.

The guide stresses the importance of comprehensive policies that define institutional mandates, organizational responsibilities, and cooperation and coordination mechanisms between organizations, as well as allocating resources to promote a national capabilities framework. It further states that the importance of formulating new practices, tools, and methods is one of the most significant challenges facing law enforcement communities. As such, a coordinated effort is required between various government agencies, law enforcement, the military, and other stakeholders to ensure national security while protecting individual rights and freedoms.

One of the main approach assumptions applied here is that the dynamic landscape of new technologies requires that the design of counter-terrorism policy responses needs to also account for the evaluation of the efficacy of the counter-terrorism strategy. This evaluation is necessary for adjustments based on a mechanism of ongoing feedback and collaboration between government agencies, the private sector, and civil society. The guide suggests that key matters need to be addressed within counter-terrorism policy to assess and respond to technological threats, including understanding technological capabilities and terrorist motivations, and placing an emphasis on gathering threat intelligence.

Designing National Counter-Terrorism Policy Responses to Counter the Use of New Technologies for Terrorist Purposes is an essential resource for governments, policymakers, and practitioners in the development of effective and comprehensive counter-terrorism strategies and policies. The guide provides a comprehensive framework that addresses the challenges posed by the exploitation of new technologies by terrorists and offers practical recommendations for how to respond. With its focus on the use of new technologies for terrorist purposes, it helps countries to maintain a sense of an upper hand, and to respond effectively to new threats.

[1]

Background

1.1 Overview

United Nations Member States attach great importance to addressing impact of new technologies in countering terrorism. During the seventh review of the United Nations Global Counter-Terrorism Strategy (A/RES/75/291)[14] 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)[15] and 2396 (2017)[16] 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,[17] 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 28-29 October 2022 in New Delhi and resulted in the adoption of a non-binding document, known as the Delhi Declaration.[18]

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

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

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

17 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).

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

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*".

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 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

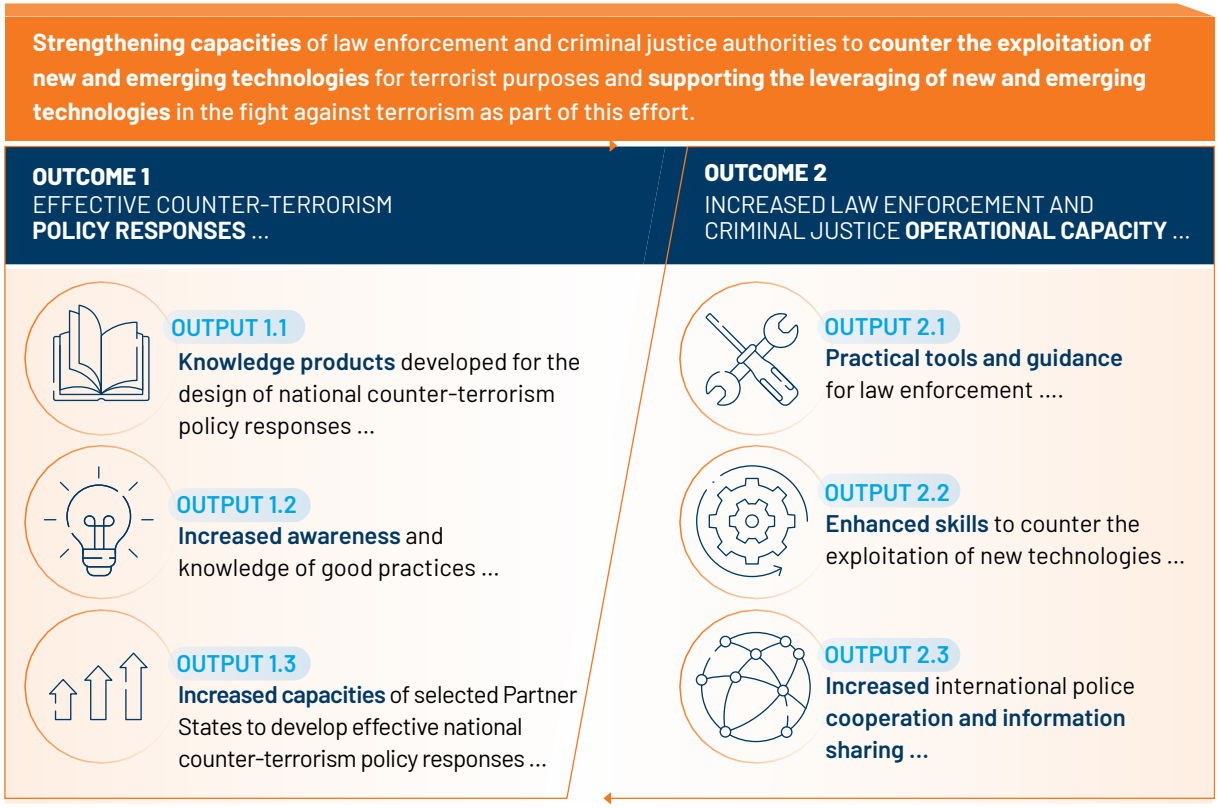


TABLE 1. **CT TECH Outcomes and Outputs**

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

The aim of this document is to provide Member States with the necessary understanding and tools to effectively assess, mitigate, and respond to threats in their areas of responsibility (AOR). It intends to provide guidance on the conduct of threat assessment at the national level, raise awareness and provide non-binding guidance of good practices for developing and implementing a threat and risk assessment process regarding the use of new technologies for terrorist purposes. Such an understanding will assist policymakers to increase their efficacy in planning policy responses to counter-terrorist threats, particularly as they pertain to the use and abuse of new technology for malicious activity.

1.3.1 Scope

The guide provides a detailed analysis of the challenges posed by the exploitation of new technologies by terrorists and offers practical recommendations for how to respond. The guide includes good practices and examples of successful policy responses from different Member States. While the terminology regarding new technologies covers a wide range

of different technologies, the guide will more specifically address the use and abuse of such new technologies as the Internet, social media, cryptocurrencies, facial recognition, and the darknet.

1.3.2 Target Audience

This document is intended primarily for policymakers, government officials, counter-terrorism practitioners, law enforcement agencies, intelligence agencies, and relevant stakeholders involved in counter-terrorism efforts. The guide aims to provide comprehensive information and guidance regarding formulating effective policies and strategies to address the emerging challenges posed by terrorists leveraging new technologies. The guide is designed to address the specific needs and responsibilities of these target audiences. It also provides practical guidance and best practices for other relevant stakeholders such as international organizations, diplomats, policymakers, researchers and academics specializing in fields such as counter-terrorism, technology, and policy development, experts engaged in international cooperation and collaboration on counter-terrorism, and members of the private sector and technology companies.

1.3.3 Benefits

The document reflects the needs and perspectives of a wide range of stakeholders including experts in the field of counter-terrorism, government officials, law enforcement and intelligence agencies, academic scholars, and civil society organizations. It is the goal of this document to increase the ability of policymakers to interact with new technologies as part of their strategic planning against terrorist actions, be it through response to the exploitation of these technologies or their use to respond to terrorist actions.

The guide provides a comprehensive framework and covers a broad range of key considerations for designing national counter-terrorism policy responses to counter the use of new technologies for terrorist purposes. It also includes good practices that illustrate how different Member States have either used new technologies to respond to terrorism or have responded to the use of new technologies for terrorist purposes. These practices provide practical insights to help policymakers and practitioners develop effective counter-terrorism policies and strategies. The guide is specifically focused on the use of new technologies for terrorist purposes, which are rapidly evolving and pose new challenges and threats. It also highlights some of the potential uses of new technology to counter-terrorism. By providing guidance on how to address these challenges, the guide will assist Member States to stay ahead of the curve and respond effectively to new threats.

1.3.4 Limitations

The Designing National Counter-Terrorism Policy Responses to Counter the Use of New Technologies for Terrorist Purposes has several limitations. While the guide is designed to be flexible and adaptable to different national contexts, it recognizes that different Member States maturity level of capabilities to design responses, different needs and priorities, and it encourages policymakers and practitioners to tailor their approach accordingly. The guide is based on the technology landscape and threat environment as of its publication. As new technologies emerge and existing technologies evolve, a need will arise for the development of strategic thinking that considers the needs and circumstances of the field according to future features of new technology that have not been addressed in the guide.

[II]

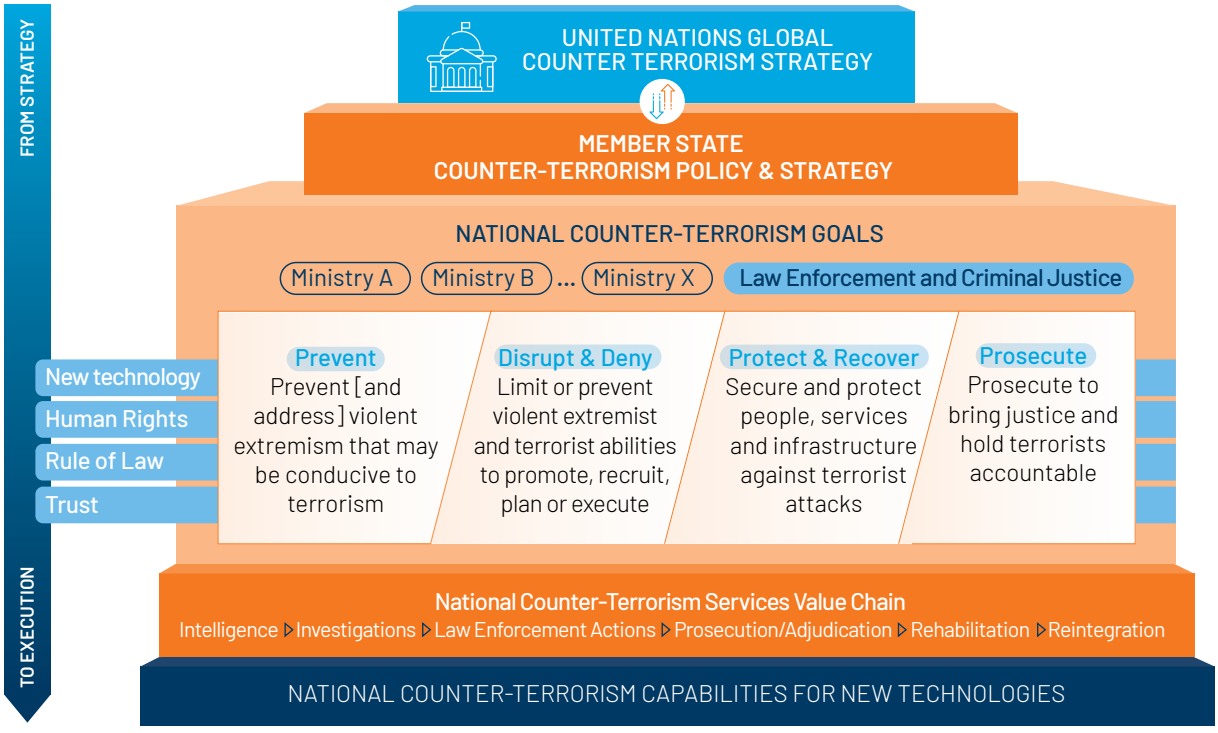
Approach

2.1 Overview

The report seeks to support and enable Member States to effectively develop counter-terrorism policy responses in countering terrorists' malicious use of new technologies, 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 threats, 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:

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 terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement and 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 reintegration to 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

The methodology for developing this document on "Designing National Counter-Terrorism Policy Responses to Counter the Use of New Technologies for Terrorist Purposes" includes research, analysis, and consultation with relevant stakeholders and experts, which include CT TECH project documents, stakeholder consultation, internal analysis, desktop research, expert group meetings, 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 research focused on identifying the key challenges and opportunities presented by new technologies in the context of terrorism as well as existing counter-terrorism policy and strategy responses.

The first step involved conducting extensive research on the challenges and opportunities presented by new technologies in the context of counter-terrorism. This desktop research involved reviewing existing literature, case studies, and best practices, to identify key components and effective strategies for developing counter-terrorism policy responses, including analysis of new technologies and their potential exploitation by terrorist actors as well as their potential for use by practitioners to respond to terrorism. The second step involved the identification of good practices within existing counter-terrorism policy and strategy responses that address new technology terrorism challenges. The third step included developing a draft

guide, which was shared with relevant stakeholders and experts for feedback. This feedback was incorporated into the final guide, where key consideration and cross components were identified, ensuring that it reflects the latest thinking and good practices in the field. Based on the research, analysis, and consultation, a comprehensive framework was developed for designing national counter-terrorism policy responses to counter the use of new technologies for terrorist purposes.

This framework includes several considerations which aim to address gaps in counter-terrorism strategies regarding new technology. It also aims to provide examples of good practices with the goal of designing counter-terrorism policy and protocols to address threats from new technology that can be exploited by terrorist actors.

Sources for the desktop research included national threat and risk assessments of Member States, intergovernmental organizations, documents from the public and private sectors regarding threat assessment, and academic sources. As this document focuses on the applications of threat and risk assessment as it relates to new technology, it is important to note that some of the models from which this document drew information were also influenced by threat assessment frameworks within the world of cybersecurity.

2.3.1 Expert Group Meetings and Consultation

This guide has been developed with input by experts through the Expert Group Meeting (EGM) sessions as well as individual consultations and review. The EGM brought together a group of experts and practitioners from counter-terrorism and law enforcement agencies, human rights, private sector, academia, and civil society to discuss how to counter the 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 law.

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 Amritt, Carl, Eliot Bradshaw, and Alyssa Schulenberg. "Threat Assessment and Management: Practices Across the World." Domestic Preparedness, February 1, 2023. https://www.domesticpreparedness.com/preparedness/threat-assessment-and-management-practices-across-the-world.

2 Bloom, Mia, Hicham Tiflati, and John Horgan. "Navigating ISIS's Preferred Platform: Telegram." *Terrorism and Political Violence* 31, no. 6 (November 2, 2019): 1242–54. https://doi.org/10.1080/09546553.2017.1339695.

3 "Counter Terrorism Legal Framework: Lessons Learned from IDLO Policy Dialogues in Collaboration with UNODC." Development Law Update, no. 2 (2007). https://www.files.ethz.ch/isn/138640/14.pdf.

4 Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, Australian Cyber Security Centre, Canadian Centre for Cyber Security, New Zealand Computer Emergency Response Team, United Kingdom National Cyber Security Centre, Germany Federal Office for Information Security (BSI), and Netherlands' National Cyber Security Centre. "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default," April 13, 2023. https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf.

5 European Commission. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, Belgium: European Commission, 2020. https://home-affairs.ec.europa.eu/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf.

6 European Commission. "Cyber Resilience Act," September 15, 2022. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

7 European Commission. Security by Design: Protection of Public Spaces from Terrorist Attacks. Luxembourg: European Union, 2022. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf.

8 European Commission: Cordis. "Detecting and Analysing Terrorist-Related Online Contents and Financing Activities." Accessed April 23, 2023. https://cordis.europa.eu/project/id/700367.

9 European Commission: Cordis. "Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition." Accessed April 23, 2023. https://cordis.europa.eu/project/id/700024.

10 European Cybercrime Centre (EC3). "Internet Organized Crime Threat Assessment 2019." Europol, 2019. https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf.

11 European Union. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Pub. L. No. 2002/475/JHA, 088 OJ L 6 (2017). http://data.europa.eu/eli/dir/2017/541/oj/eng.

TABLE 3. References

12 Financial Action Task Force (FATF). "Virtual Assets." Financial Action Task Force (FATF). Accessed May 7, 2023. https://www.fatf-gafi.org/en/topics/virtual-assets.html.

13 Finland Ministry of the Interior. National Counter-Terrorism Strategy 2022–2025. Publications of the Ministry of the Interior, 2022:38. Helsinki, Finland: Finland Ministry of the Interior, 2022. https://julkaisut.valtioneuvosto.fi/handle/10024/164447.

14 *Flanders, Rob, Lucy Johnson, Matthew Trevelyan, Anna Whitmore, Lisa Lesowiec, and Rajinder Tumber. Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts. 2nd ed. United Kingdom, 2019. https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf.*

15 *Freese, Rebecca. "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works." Perspectives on Terrorism 8, no. 1 (2014): 37–56. http://www.jstor.org/stable/26297099.*

16 Government of Australia. Safeguarding Our Community Together: Australia's Counter-Terrorism Strategy 2022. Australia: The Commonwealth of Australia, 2022. https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/safeguarding-community-together-ct-strategy-22.pdf.

17 Gruetzemacher, Ross. "The Power of Natural Language Processing." Harvard Business Review, April 19, 2022. https://hbr.org/2022/04/the-power-of-natural-language-processing.

18 Interior Ministry of Spain. National Counter-Terrorism Strategy, 2019. https://www.dsn.gob.es/eu/file/4271/download?token=-K6uOf-C.

19 Joint Counter-terrorism Assessment Team (JCAT). "Counter Terrorism Guide for Public Safety Personnel." Government. Director of National Intelligence. Accessed April 10, 2023. https://www.dni.gov/nctc/jcat/index.html.

20 *Lutkevich, Ben, and Ed Burns. "What Is Natural Language Processing? An Introduction to NLP." Enterprise AI. Accessed April 30, 2023. https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP.*

21 National Cyber Security Centre. "Secure by Default." National Cyber Security Centre, March 7, 2018. https://www.ncsc.gov.uk/information/secure-default.

22 New Zealand Security Intelligence Service. "How You Can Help: Public Contribution Form." Accessed April 23, 2023. https://providinginformation.nzsis.govt.nz/.

23 New Zealand Transport Agency. "Risk Register." Government. Waka Kotahi NZ Transport Agency. Accessed April 1, 2023. https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register.

24 OSCE Transnational Threats Department. "Status of the Universal Anti-Terrorism Conventions and Protocols as Well as Other International and Regional Legal Instruments Related to Terrorism and Co-Operation in Criminal Matters in the OSCE Area." Organization for Security and Co-Operation in Europe (OSCE), July 2018. https://www.osce.org/files/f/documents/5/8/17138_0.pdf.

TABLE 3. References

25 *OSCE Transnational Threats Department*. Status of the Universal Anti-Terrorism Conventions and Protocols as Well as Other International and Regional Legal Instruments Related to Terrorism and Co-Operation in Criminal Matters in the OSCE Area." Organization for Security and Co-Operation in Europe (OSCE), July 2018. https://www.osce.org/files/f/documents/5/8/17138_0.pdf.

26 Romyn, David, and Mark Kebbell. "Terrorists' Planning of Attacks: A Simulated 'Red-Team' Investigation into Decision-Making." *Psychology, Crime & Law* 20, no. 5 (May 28, 2014): 480–96. https://doi.org/10.1080/1068316X.2013.793767.

27 Schneier, Bruce, and Tarah Wheeler. "Hacked Drones and Busted Logistics Are the Cyber Future of Warfare." Brookings. Tech Stream (blog), June 4, 2021. https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/.

28 Spulak, Robert G. "Science Technology and Innovation in Combating Terrorism.," February 2015. https://www.osti.gov/biblio/151395.

29 Talley, Ian. "Islamic State Turns to NFTs to Spread Terror Message." Wall Street Journal, September 4, 2022, sec. Politics. https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.

30 Terrell Hanna, Katie. "What Is the Dark Web (Darknet)?" WhatIs.com. Accessed May 7, 2023. https://www.techtarget.com/whatis/definition/dark-web.

31 *The Commonwealth of Australia. 2017 Foreign Policy White Paper. Edited by Morris Walker Pty Ltd. Australia, 2017. https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.*

32 UKC3. "Cyber Cluster Operating Framework." UK Cyber Cluster Collaboration (blog). Accessed March 30, 2023. https://ukc3.co.uk/cyber-cluster-operating-framework/.

33 *United Kingdom. CONTEST: The United Kingdom's Strategy for Countering Terrorism. United Kingdom: The Crown, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.*

34 United Kingdom Department for and Business, Energy and Industrial Strategy. National Security and Investment Bill, Pub. L. No. BEIS006(F)-20-CCP (2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf.

35 *United Nations Counter-Terrorism Centre (UNCCT). "Summary of Discussions: International Conference on National and Regional Counter-Terrorism Strategies- January 31-February 1, 2013." Conference Summary. Bogota, Colombia, 2013. https://www.un.org/counter-terrorism/sites/www.un.org.counter-terrorism/files/bogota_jan-feb2013.pdf.*

36 *United Nations Counter-Terrorism Centre and United Nations Interregional Crime and Justice Research Institute. "Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia." Joint Report. United Nations, 2021. https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence.*

TABLE 3. References

37 *United Nations Counter-Terrorism Centre and United Nations Interregional Crime and Justice Research Institute. "Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia." Joint Report. United Nations, 2021. https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence.*

38 United Nations Office of Counter-Terrorism. "International Legal Instruments." Accessed April 25, 2023. https://www.un.org/counter-terrorism/international-legal-instruments.

39 United Nations Office on Drugs and Crime. "Counter-Terrorism Module 12 Key Issues: Accountability, Oversight of Intelligence Gathering Methods." United Nations Office on Drugs and Crime (UNDOC), July 2018. https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/accountability-oversight-of-intelligence-gathering-methods.html.

40 United Nations: Office on Drugs and Crime. "International Legal Framework." Accessed April 25, 2023. https://www.unodc.org/unodc/en/terrorism/expertise/international-legal-framework.html.

41 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED). "CTED Analytical Brief: Countering Terrorist Narratives Online and Offline." United Nations, 2020. https://www.un.org/securitycouncil/ctc/content/cted-analytical-brief-%E2%80%93-countering-terrorist-narratives-online-and-offline.

42 United States. National Strategy for Counter-terrorism of the United States of America. Washington, DC: The White House, 2018. https://purl.fdlp.gov/GPO/gpo109871.

43 Vidino, Lorenzo, and Clifford Bennett. "A Review of Transatlantic Best Practices for Countering Radicalization in Prisons and Terrorist Recidivism." The Hague, Netherlands: Europol, 2019. https://www.europol.europa.eu/cms/sites/default/files/documents/a_review_of_transatlantic_best_practices_for_countering_radicalisation_in_prisons_and_terrorist_recidivism.pdf.

[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 integration of technology into the arsenal of terrorist groups poses unprecedented challenges, requiring governments to reassess their strategies and adapt their approaches.

In formulating counter-terrorism policies, Member States must recognize the critical need to understand, anticipate, and effectively respond to terrorists' exploitation of emerging technologies. Such policies focus on a range of aspects, including awareness, threat interventions, national counter-terrorism capabilities, cooperation, and capacity-building initiatives. By adopting comprehensive and agile national counter-terrorism policies, governments aim to stay ahead of the curve, proactively mitigating the risks associated with terrorists' utilization of new technologies while safeguarding the security, privacy, and fundamental rights and civil liberties of their citizens.

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,[19] of which over 93 per cent are social media users.[20] Globally, it is estimated that in 2022 over 97 zettabytes[21] of information was generated.[22] 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 of technologies that allow for anonymity and the ability to coordinate and operate remotely.

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

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

21 One zettabyte equals to one billion terabytes.

22 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 could allow law enforcement authorities to do more with less, fast track timely decision-making, generate new insights, and conduct disruptive operations remotely.

Countering the use of new technologies for terrorist purposes hinges on understanding how terrorist actors are using new technologies, developing effective legal framework and policy responses, and building operational capacity to counter 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 Information and Communication Technologies (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 law enforcement agencies 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 safety and security of communities.

3.2.3 Human Rights and New Technologies

Terrorism poses a serious challenge to the very tenets of the rule of law, the protection of human rights and their effective implementation. It can destabilize legitimately constituted governments, undermine pluralistic civil society, jeopardize peace and security, and threaten social and economic development. States have the obligation to take appropriate measures to protect persons within their jurisdiction against reasonably foreseeable threats of terrorist attacks. States' duty to safeguard human rights includes the obligation to take necessary and adequate measures to prevent, combat, and punish activities that endanger these rights, such as threats to national security or violent crime, including terrorism. All such measures, must themselves be in line with international human rights law and rule of law standards.

In the context of employing new and emerging technologies to counter-terrorist activities, States have to ensure that relevant laws, policies, and practices respect rights such as the right to privacy, the rights to freedom of expression, freedom of association, freedom of thought, conscience, and religion, the right to liberty and security of the person, the right to fair trial, including the presumption of innocence as well as the principle of non-discrimination. States must also uphold the absolute prohibition of torture and cruel, inhuman or degrading treatment or punishment.

The UN, Interpol and the EU have repeatedly underlined the interrelationship between new technologies, counter-terrorism, and human rights, including gender equality. The UN Global Counter-Terrorism Strategy and various General Assembly and Security Council resolutions underscore Member States' obligations under international human rights law, international humanitarian law, and international refugee law when countering terrorism. In particular, the UN's Counter-Terrotism strategy recognizes that "effective Counter-Terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing" and requires measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism. Specifically, the Strategy encouraged Member States to address 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 while respecting international law, including international human rights law, and the right to freedom of expression.

3.2.4 Gender, Technology, and Policy Responses

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.[23] 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.[24] Evidence also suggests that terrorist groups instrumentalize gender in their online messaging; for example, Daesh used contradictory gendered messaging strategically in their recruitment and communications, shifting their discourse according to their target group.[25] 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.[26]

Integrating gender dimensions within national counter-terrorism policy is therefore critical, 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.

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

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

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

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

[IV] National Counter-Terrorism Policy Review

4.1 Overview

The purpose of creating a document for designing national counter-terrorism policy responses to counter the use of new technologies for terrorist purposes is to enable policymakers to develop and/or update counter-terrorism strategies and policies in a way that accounts for the complexities of technological developments. New technologies pose opportunities such as the ability to both prioritize and invest in innovation and to modernize counter-terrorism capabilities with new technologies, as well as to increase cross-sector collaboration between the private and public sectors. New technologies can be used and abused by terrorist actors in harmful ways. Terrorist organizations use technology by combining online activities with activities in the real world. Challenges posed by new technologies include the use of the Internet, social media, and the darknet, as well as the use and abuse of virtual assets for terrorist purposes (such as money laundering). The use of new technologies for terrorist purposes also opens the possibility for cyber-attacks to be launched by terrorist actors.

In acknowledging that developments in new technologies occur at a pace far faster than the pace at which national policies can be changed, this document seeks to provide a framework for assessing the efficacy of policies in addressing the threats posed by the exploitation of new technologies for terrorist purposes. It is also through the framework of assessing the efficacy of the policies that new amendments to policy may be created to preserve its continued relevance. National Counter-Terrorism policies are important for creating a common, holistic governmental approach to terrorist threats, with a clear, high-level mandate. Comprehensive policy is important for intragovernmental coordination purposes, and integration with relevant national security, cybersecurity, and cybercrime policies. 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 national capabilities framework. National Counter-Terrorism policies are also necessary for collaboration with non-governmental stakeholders and organizations. The policies need to support coordination, communication, and cooperation with the private sector, the general public, and with international partners.

4.2 New Technologies: Use by Terrorists and Uses to Combat Terrorism

To develop a counter-terrorism policy that relates to new technologies, it is important to understand both sides with regards to the use of new technologies and counter-terrorism; practitioners must understand the ways in which technologies can be used for terrorist purposes and the ways in which it may be used by practitioners as a tool to combat terrorism. The table below highlights new technologies and their potential use for terrorist purposes, as well as their potential use by practitioners to respond to terrorism. Understanding the ways in which new technologies may be used to respond to terrorism can inform practitioners in integrating these uses as part of policy responses to terrorism.

It is important to note that, while the table is accurate as of the writing of this Report, the content in the table must be consistently evaluated to ensure that it remains accurate and relevant to the reality of those utilizing it. Due to the constant evolution of new technologies, there will continue to be new ways in which they may be used for terrorist purposes and there will also be new ways in which technologies may be used to counter-terrorism.

TABLE 4. **Examples of Malicious Use of Technology and Opportunities for Law Enforcement**

Technology Type	Use for Terrorist Purposes	Law Enforcement Use to Counter-Terrorism
Internet	• Recruitment to terrorist organization through propaganda spread on the Internet • Publication of information online for how to conduct terrorist attacks[27] • Terrorism financing • Radicalization to terrorism • Intelligence collection about potential targets for attacks • Spread of terrorist content and distorted narratives • Communication, coordination, and otherwise supporting terrorist acts or activities • Cyber enabled information operations	• Countering violent extremism and terrorist narratives[28] • OSINT gathering and analysis • Information sharing platform for stakeholders • Identify terrorist content online and stop its dissemination • Referral teams that report extremist content to tech companies that will address the extremist content on their platform • Identifying emerging terror groups and their intentions

27 European Union, "Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA," Pub. L. No. 2002/475/JHA, 088 OJ L 6 (2017), 88/7-8, http://data.europa.eu/eli/dir/2017/541/oj/eng.

28 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), "CTED Analytical Brief: Countering Terrorist Narratives Online and Offline" (United Nations, 2020), https://www.un.org/securitycouncil/ctc/content/cted-analytical-brief-%E2%80%93-countering-terrorist-narratives-online-and-offline.

TABLE 4. **Examples of Malicious Use of Technology and Opportunities for Law Enforcement**

Technology Type	Use for Terrorist Purposes	Law Enforcement Use to Counter-Terrorism
Social Media	• Recruitment to terrorist organizations through propaganda spread on social media • Disinformation campaigns • Spreading terrorist content and distortive narratives, propaganda and/or material to be posted as propaganda on social media through an encrypted channel[29] (see UNSCR 2396) • Radicalization to terrorism • Encrypted messaging services allow for communications that are harder to monitor for those not included in the chat	• SOCMINT gathering/monitoring • Countering violent extremism and terrorist narratives • Referral for report of extremist content to tech companies • Prevent the creation of new terrorists' accounts
Darknet	• Hacking forums through which malware, ransomware, and other malicious programmes can be acquired to launch cyberattacks • Weapons acquisition • Recruitment • Encrypted communications among members	• OSINT gathering and analysis
Virtual assets *(cryptocurrencies, NFTs, mobile payment systems, etc.)*	• Use of cryptocurrencies/NFT-s for terrorist financing • Use of cryptocurrencies/NFT-s in money laundering activities	• NFTs can be used for counter-narrative functions to terrorist propaganda (known example of ISIS using NFTs to spread propaganda)[30] • Fundraising/crowdfunding in virtual assets can support grassroots efforts to counter-terrorism (for example purchase of equipment needed locally)
Facial Recognition	• Currently unknown – N/A	• Anomaly detection (data mining process of identifying data points that fall outside or deviate from the norm) • Global terrorist database

29 Mia Bloom, Hicham Tiflati, and John Horgan, "Navigating ISIS's Preferred Platform: Telegram," *Terrorism and Political Violence* 31, no. 6 (November 2, 2019): 1242–54, https://doi.org/10.1080/09546553.2017.1339695.

30 Ian Talley, "Islamic State Turns to NFTs to Spread Terror Message," *Wall Street Journal*, September 4, 2022, sec. Politics, https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.

TABLE 4. **Examples of Malicious Use of Technology and Opportunities for Law Enforcement**

Technology Type	Use for Terrorist Purposes	Law Enforcement Use to Counter-Terrorism
3D Printing	• Building weapons/weapon parts	• 3D printing can be used to counter-terrorism by, for example, printing UAS parts, which, in turn, can be used for Intelligence, Surveillance, and Reconnaissance (ISR)
Artificial Intelligence/ Machine Learning	• Disinformation campaigns and cyber-attacks powered by AI[31] • Weapons powered by AI[32] • Social engineering campaigns[33] • May be used to upgrade malicious exploits or writing malwares for sophisticated cyberattacks	• Use of AI/Machine learning to automate monitoring and analysis in Counter-TerrorismI (e.g., automation sorting of posts on social media/online forum)[34] • Big Data analysis powered by AI[35] • Using Natural Language Processing (NLP) techniques to detect symbols and patterns used by terror groups online • Monitoring for misinformation and disinformation[36]

4.3 Reference Benchmark

This document aims to build from existing good practices within counter-terrorism policies to help further develop the use and response to new technologies in the hands of terrorists. In creating this document, multiple counter-terrorism strategy and policy documents were surveyed from both the public and private sectors. The purpose of this was to both assess whether there are good practices within current policies that ought to be emulated in future policies, and to better understand the status of counter-terrorism policies regarding how they address new technologies. From surveying publicly available counter-terrorism documents, there is an opportunity to further strengthen policy responses to address the use of new technologies for terrorist purposes.

31 United Nations Counter-Terrorism Centre and United Nations Interregional Crime and Justice Research Institute, "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes," Joint Report (United Nations, 2021), 39-40, https://www.un.org/counter-terrorism/sites/www.un.org.counter-terrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

32 See e.g., ibid, 33-35.

33 Ibid, 45.

34 United Nations Counter-Terrorism Centre and United Nations Interregional Crime and Justice Research Institute, "Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia," Joint Report (United Nations, 2021), 20-21 and 23-30, https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence.

35 Ibid, 17.

36 United Nations Counter-Terrorism Centre and United Nations Interregional Crime and Justice Research Institute, "Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia," 27-28.

4.4 General Findings

Many of the counter-terrorism strategies surveyed for the creation of this document, when discussing new technologies, frequently turned to matters such as the use of the Internet and social media for terrorist purposes. While this is the case, many strategies do not touch upon technological enablers that are used or potentially can be used by terrorists for new types of operations, such as the use of artificial intelligence, the darknet, end-to-end encrypted apps, and digital assets. This can be attributed to the fact that many of these strategies have not been updated at a fast enough pace to keep up with the developments and potentially increased use of these technologies.

In surveying published counter-terrorism strategies and policies of different countries, it is clear that these policies have acknowledged the digital age and the complexities that arrive with it. On the other hand, many of these strategic documents do not provide a clear and a more detailed framework with which to tackle the threats that new technologies pose in the hands of terrorist actors, nor do they touch upon the potential for the new technologies to aid law enforcement agencies and other stakeholders in addressing terrorism. Although these strategic documents discuss the importance of information-sharing, there is a gap within some of these documents regarding the best practices for information sharing; for example, that it is efficient, secure (from an informational/operational security perspective), and legal (within the context of data sharing).

4.4.1 Key Issues to Address

When designing a comprehensive counter-terrorism strategy and a policy that addresses the use of new technologies for terrorist purposes, there are a few key matters that need be addressed to ensure that countries are sufficiently prepared to face current and future threats.

Within counter-terrorism policy, the ability to assess and respond to threats is of high importance. This includes understanding technological capabilities, technological exposure in economic and social activities that may be exploited, and terrorist motives. As part of this assessment process, an emphasis must also be placed on the process of gathering the threat intelligence (e.g., through means such as SIGINT, OSINT, and SOCMINT) to enable practitioners to proactively and effectively be able to respond to threats.

Here, one of the key issues to address is cross-sector collaboration (with an emphasis on information-sharing) among stakeholders, including engaging with national, sub-national, and local stakeholders. In the digital and new technologies age, cross-sector collaboration between public sector law enforcement agencies and private sector, academia, and non-profit organizations is critical, especially in a time where technologies are constantly evolving. Though many of the counter-terrorism strategies surveyed for this Report include an element of information-sharing, they do not address how the information will be shared.

Another key issue that will be addressed in this document is how to better train stakeholders to utilize new technologies to respond to terrorist threats. The ability of stakeholders to remain up to date on the challenges and opportunities posed by new technologies will enable them to better respond to the constantly evolving and ever-changing threat landscape in an effective manner.

4.4.2 Formulation of New Practices, Tools, and Methods

One of the most significant challenges facing the law enforcement communities is the formulation of new practices, tools, and methods for combating the use of new technology for terrorist purposes such as eliciting information, monitoring, and enforcing the use of social media; foiling incitement that leads to terrorism; and engaging in proactive efforts to thwart potential attacks. This requires enriching the Law Enforcement Agency (LEA) toolset to enable understanding, managing, and performing LEA activities in the technological context. Many countries lack clear directives on how they can act against online terrorist activity, and significant judicial and enforcement mechanisms still need to be implemented, including the formulation of legislation and enforcement codes against online radicalization and incitement.

All of this must be done in a manner that protects privacy rights, freedom of expression and association, the right to non-discrimination, and other fundamental rights, or if necessary, restricts these rights in strict accordance with the principles of legality and proportionality.

[V] National Counter-Terrorism Policy Response Considerations

5.1 Overview

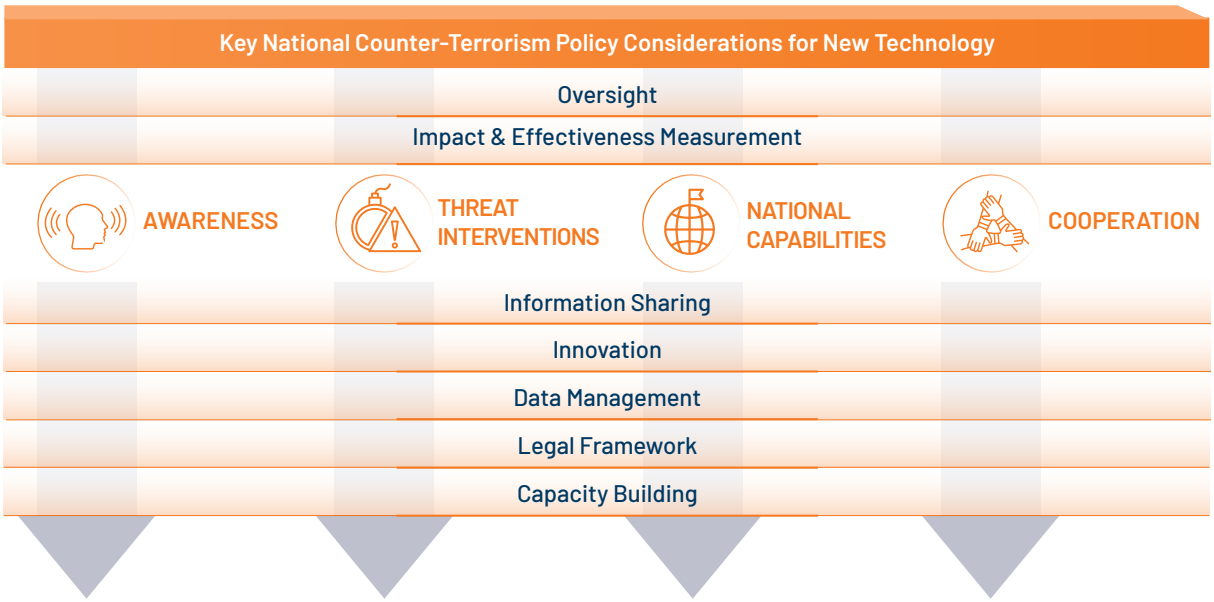
This chapter aims to address gaps in counter-terrorism strategies regarding new technologies and provide examples of good practices in counter-terrorism policy for the goal of designing policy and protocols to address threats from new technology. Other objectives highlight the use of new technologies to combat terrorism and optimize counter-terrorism security responses and countermeasures. The National Counter-Terrorism Policy Response Considerations are based on a multifaceted approach that encompasses main counter-terrorism policy dimensions, with the aim of ensuring national security effectiveness with the oversight required to protect individual rights and freedoms.

Overall, national counter-terrorism policy response considerations require a coordinated effort between various government agencies, law enforcement, the military, and other stakeholders to ensure the safety and security of citizens while protecting individual rights and freedoms.

The human rights at greatest risk with respect to counter-terrorism and new technologies are: privacy, freedom of expression, and risk of discrimination. There can be no restrictions on the prohibition against discrimination, and indeed, discrimination is often a critical root cause of terrorism. Any restrictions on privacy rights and freedom of expression must be established by law or according to law, in accordance with Articles 17 and 19 of the International Covenant on Civil and Political Rights. Additionally, any restrictions must be deemed necessary and proportionate to the legitimate aim pursued.

The diagram (Figure 4) presents the model upon which the key national counter-terrorism policy response considerations rest. The top rows of the diagram, oversight, and impact & effectiveness measurement, highlight overarching considerations that should be incorporated into the entirety of a counter-terrorism policy response and each of the components that make it up. These two 'umbrella considerations' are followed by four integral considerations: awareness, threat interventions, national capabilities, and cooperation. Each of these integral considerations serve as the guiding principle considerations in the five cross-components of national counter-terrorism policy response listed below, including: information sharing, innovation, data management, legal framework, and training & preparation. It is through a combination of all key components that the goals set out in the four integral considerations may be achieved.

FIGURE 4



5.1.1 Oversight

When designing counter-terrorism policy responses, it is important to consider policy oversight to ensure that matters of data, privacy, and human rights are upheld throughout the implementation of the counter-terrorism policy. Oversight measures should be built into multiple steps within the counter-terrorism policy response to ensure that such considerations are met throughout the process, particularly throughout the intelligence gathering and data management components.

There are two types of oversight that are recommended to be implemented within the counter-terrorism policy: judicial and non-judicial oversight.[37] Judicial oversight would involve the courts to oversee and hold stakeholders accountable for their actions as part of both intelligence collection and as a response to the intelligence gathered.[38] Non-judicial oversight can be implemented by parliamentary committees, oversight by data protection agencies, internal law enforcement, or intelligence oversight bodies.[39] In addition, international organizations and civil society organizations play a role in monitoring the compliance of government responses within international legal obligations. In both cases, the body conducting the oversight must be independent of policymakers.[40]

As part of oversight efforts, cooperation with the private sector, particularly with regard to data and intelligence gathering, should involve a level of transparency with the public regarding online monitoring efforts.[41]

37 United Nations Office on Drugs and Crime, "Counter-Terrorism Module 12 Key Issues: Accountability, Oversight of Intelligence Gathering Methods," United Nations Office on Drugs and Crime (UNDOC), July 2018, https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/accountability-oversight-of-intelligence-gathering-methods.html.

38 United Nations Office on Drugs and Crime.

39 United Nations Office on Drugs and Crime.

40 United Nations Office on Drugs and Crime.

41 Government of Australia, *Safeguarding Our Community Together: Australia's Counter-Terrorism Strategy 2022* (Australia: The Commonwealth of Australia, 2022), 29, https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/safeguarding-community-together-ct-strategy-22.pdf.

5.1.2 Impact and Effectiveness Measurement

Just as technologies continue to evolve, so too must counter-terrorism policy to best respond to the current threat landscape. As such, a framework should be built into the counter-terrorism policy to assess the efficacy and impact of the counter-terrorism policy and related measures in being able to mitigate and respond to terrorist threats. One method proposed in the United States' Counter-Terrorism strategy is to conduct yearly analyses with regard to both the effectiveness of the strategy in meeting counter-terrorism goals and progress in addressing these goals as they relate to new and existing threats.[42]

Prior to assessing the impact and efficacy of counter-terrorism responses, it is recommended for Member States to clearly define its desired goals and strategic outcomes.[43] One of the most important factors to assess the threat and response is how well the existing policy meets or does not meet the intended goals for the action or policy. Member States should consider both qualitative and quantitative measurements to assess the impact and efficacy of policy choices in countering the terrorist threat.

When considering the impact and efficacy, there are other considerations that policymakers must also evaluate. One of these considerations is the limitation of the given policy relative to technological or other advancements since the previous assessment of the policy. The cost to implement the policy (e.g., through manpower and other resources) in relation to the benefit and what the policy provides should also be addressed when evaluating the impact and efficacy of the policy.[44]

When assessing the impact and the efficacy of a counter-terrorism policy, it is recommended to utilize the process of evidence-based practice (EBP) to provide concrete measurements of the impact of the policy and its level of efficacy across different factors so that future decisions regarding the policy can be made.[45] There are two different factors that must be considered when designing EBP evaluation of a counter-terrorism policy: the goals of the policy (and the specific means of measuring how the policy attained or failed to attain a particular goal) and the potential consequences of the policy (and the frequency with which these consequences present themselves).[46] In order to assess these factors and the policy as a whole, evaluative research methods must be conducted in which the resources, processes, and outcomes of the policy, in light of the previous two factors, are assessed.[47] It is from these evaluations that policymakers will know where and how the counter-terrorism policy response must be adjusted for continued relevance and efficacy.

42 United States, *National Strategy for Counter-terrorism of the United States of America* (Washington, DC: The White House, 2018), 11, https://purl.fdlp.gov/GPO/gpo109871.

43 United Kingdom Department for and Business, Energy and Industrial Strategy, "National Security and Investment Bill," Pub. L. No. BEIS006(F)-20-CCP (2020), 7, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf.

44 United Kingdom Department for and Business, Energy and Industrial Strategy, 30.

45 Freese, "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works," 37–38.

46 Freese, 41.

47 Freese, 45–46.

5.2 Core Considerations of Counter-Terrorism Policy Response Regarding New Technologies

The following core considerations encompass important factors that are necessary for the development of a comprehensive counter-terrorism policy response. By focusing on these core considerations, counter-terrorism policymakers can develop policies that balance the need to address security imperatives and protect individual rights, while effectively countering the use of new technologies for terrorist purposes. This section explores the core considerations that need to be considered when formulating counter-terrorism policy responses to the challenges posed by new technologies. By understanding and addressing these core considerations, policymakers can develop robust and adaptive policies that stay ahead of terrorists' exploitation of new technologies, ensuring the safety and security of societies in the digital age.

5.2.1 Awareness

Awareness in counter-terrorism policy must be enforced on the level of the stakeholders and through members of the public. For example, practitioners should have a deep understanding of not only how to identify and respond to threats and threatening behaviour, but also how to educate the public and respond to concerns raised by the public regarding threats.[48] Awareness, as it relates specifically to counter-terrorism policy, involves training practitioners and members of the public to be able to both identify terrorist activity stemming from forms of new technologies and the ways in which practitioners may be able to utilize new technologies to effectively respond to terrorism.

Part of increasing awareness in counter-terrorism policies and responses involves making the reporting of information easier, particularly for members of the public that would like to report critical pieces of information regarding threats.[49] As such, the public needs to be informed about threatening behaviours or actions and the channels they can turn to for reporting an incident to be further addressed by practitioners or other relevant stakeholders who have been trained to do so. This can be accomplished through training for the identification of signs of threatening behaviour or behaviour reminiscent of incitement to terrorist action. Trainings on these matters must be careful to make clear that identification of threatening behaviours must not allow for the discrimination of individuals on the basis of sex, race, colour, language, religion, political or other opinion, national or social origin, or other status. Additionally, the platform through which members of the public are able to share threat information with relevant authorities must be both easy to access and easy to use to prevent lack of reporting due to its difficulty.

In addition to public awareness, law enforcement agencies and other stakeholders must also be trained in the identification of threatening behaviour or behaviour reminiscent of incitement to terrorist action. Beyond this, they must be trained in how to properly respond to reports that they receive (e.g., from the public) or intelligence gathered with regard to threatening behaviour or behaviour reminiscent of incitement to terrorist action. Within these trainings, it must be stressed that the gathering of intelligence and the plan of response to detected threats must be conducted without the discrimination of individuals on the basis of sex, race, colour, language, religion, political or other opinion, national or social origin, or other status.

48 Joint Counter-terrorism Assessment Team (JCAT), "Counter Terrorism Guide for Public Safety Personnel," Government, Director of National Intelligence, accessed April 10, 2023, https://www.dni.gov/nctc/jcat/index.html.

49 Carl Amritt, Eliot Bradshaw, and Alyssa Schulenberg, "Threat Assessment and Management: Practices Across the World," Domestic Preparedness, February 1, 2023, https://www.domesticpreparedness.com/preparedness/threat-assessment-and-management-practices-across-the-world.

5.2.2 Threat Interventions

Threat interventions refer to various measures and actions taken to prevent, detect, and respond to terrorist threats posed by the use of new technologies. These interventions involve the use of advanced technologies, tools, and strategies to identify, track, and neutralize potential threats. For example, threat interventions may include the use of artificial intelligence, machine learning, and big data analytics to analyse and interpret large volumes of data and identify patterns and trends that may indicate potential threats. Threat interventions play a critical role in the fight against terrorism and require the use of advanced technologies and tools. It is essential that these interventions are carried out in a manner that respects individual rights and freedoms and complies with legal and ethical standards regarding the absolute prohibition on discrimination, at a minimum, on the basis of sex, race, colour, language, religion, political or other opinion, national or social origin, or other status.

The ability for a country to conduct effective threat assessment and response is closely tied with its ability to implement counter-terrorism policy against those threats. Within threat response, practitioners and other relevant stakeholders must be able to proactively launch threat interventions to prevent these threats from coming to fruition.

There are multiple means through which stakeholders can engage in threat intervention across different sectors. In partnership between the private and public sectors, for example, threat intervention can be accomplished through public sector work in tandem with technology companies to prevent and disrupt terrorist usage of online platforms. Within the public sector, threat intervention can be accomplished through the coordination between Member States and law enforcement agencies to monitor and counter-terrorist usage of digital platforms.

One of the approaches to threat interventions that can be implemented into the counter-terrorism strategy of Member States is the implementation of a proactive response to addressing threats before they materialize. This may be attained through a multitude of prevention measures. Preventative measures may include specific security measures built into the policy itself (safety-by-default and safety-by design) or means through which to address terrorist actors before they can perpetrate an attack through actions such as deradicalization programmes, both of which will be discussed below.[50]

5.2.3 National Capabilities

National capabilities describe a way in which to measure the capability of a country in their counter-terrorism efforts by considering the resources that an entity has (financial, technological, manpower, etc.). When designing a counter-terrorism policy response, a State's national capabilities must be assessed to make the policy fitting to the specific State. Because each country possesses different resources and skill levels, a monolithic policy model will not be feasible and effective across all Member States. As such, the assessment of national capability is integral to the design of a counter-terrorism policy response that directly fits the needs of the Member State for which it is written.

An assessment of a country's national capabilities considers both the existing resources and the resources that are available for the State to acquire through means such as collaboration with other sectors and/or Member States. As technology becomes increasingly more advanced, it is important for Member States to maintain and grow their level of national capability so that they may continue to be sufficiently prepared to handle both new challenges and to utilize the new technologies towards new opportunities in countering terrorist actions. As will be discussed below, some of the means through which the national capability of a Member State may be increased are through training and preparation of relevant practitioners and stakeholders and through means such as information sharing and innovation.

50 Cybersecurity and Infrastructure Security Agency et al., "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default"; Vidino and Bennett, "A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism."

5.2.4 Cooperation

Cooperation is important for creating a common, holistic governmental approach to terrorist threats, with a clear, high-level mandate. Additionally, for intragovernmental coordination purposes, and integration with other relevant stakeholders. Policies need to define the cooperation mechanism between organizations. National counter-terrorism policies are also necessary for collaboration with non-governmental stakeholders and organizations. The policy needs to support coordination, communication, and cooperation with the private sector, the general public, and with international partners.

As technology enables terrorist threats to increasingly become matters that cross borders as well as different realms (digital action vs. physical harm), an emphasis in counter-terrorism policy must be placed on cooperation among stakeholders. This includes interagency coordination within a Member State and between Member States, partnerships between NGOs and civil society, and the development of information-sharing tactics. Here, cooperation must also include cross-sector collaboration among the public sector, elements of the private sector such as tech companies, and consultation with experts from the professional world and from academia.

The threat of the use of new technologies for terrorist purposes requires comprehensive and coordinated efforts among relevant stakeholders. Member States should also engage with the general public to promote education and awareness. Engaging with communities is also important to build trust. Good practices also point out the need for governmental entities working with a variety of stakeholders (including companies, community leaders, schools, religious organizations, etc.) to identify and address potential vulnerabilities. The use of the shared language can contribute to minimizing fear and bias and can educate the public on how to best utilize its services to foster relationships on transparency and stewardship.

5.3 Key Cross-Cutting Components of Counter-Terrorism Policy for Addressing New Technologies

To address the challenges posed by new technologies, it is essential to incorporate key cross-cutting components into counter-terrorism policy frameworks. These components cover information sharing, innovation, data management, the utilization of legal frameworks, and capacity building. The 'cross-cutting' nature of these components refers to the ways in which each of these components enhances the ability of the policy to accomplish the goals set out in the four core considerations. By recognizing and integrating these key components, counter-terrorism policies can effectively address the unique threats and risks associated with the use of new technologies for terrorist purposes.

5.3.1 Information Sharing

Within the field of collaboration, one of the key practices that needs to be focused on as part of a counter-terrorism policy is information sharing that refers to intelligence and open source gathering, analysis, and dissemination of information with relevant stakeholders, including law enforcement and other government agencies. As part of cross-sector collaboration, this may also include select information-sharing and advisement with members of academia, the private sector, and NGOs.

When designing a counter-terrorism policy response, there are a few key challenges that arise when discussing information-sharing. The first of these challenges is the ease and efficacy through which information is shared. To ensure that information is shared among stakeholders in an efficient manner, there needs to be a common terminology among stakeholders for both how to assess the terrorist threat and how to respond to it. The shared language of response should also include the types of responsibilities allocated to different stakeholders.

Another key component in developing information-sharing practices is determining the means through which the information is shared. Information shared between stakeholders in different locations must be done through a secure means to enable the stakeholders to maintain operational security in threat assessment and threat response. In addition to information sharing among stakeholders and practitioners, it is also important that there is an easily accessible way through which the public can share information with relevant law enforcement bodies. One example is a platform for the public to note their assessment of the severity of the threat information and also to share it with the relevant authorities.[51]

5.3.2 **Innovation**

Terrorists are constantly exploring new ways to exploit technology to further their goals. As a result, counter-terrorism policies, measures, and strategies must also evolve to keep up with these threats. This requires innovation in both technology and policy. There are multiple types of innovation that are relevant to counter-terrorism policies, including operational innovation and technological innovation, the goal of which is to enhance information gathering and law enforcement capabilities to ensure a rapid and effective response to terrorism.[52]

Technological innovations shape both potential threats and new ways to combat those threats. As part of assessing the efficacy of a counter-terrorism policy (as discussed in Section 5.1.2), the way in which the policy meets (or fails to meet) the growth in technological innovation must be evaluated. An effective counter-terrorism policy should acknowledge the technological innovations that exist as of the date of its publication and should also attempt to predict potential future innovations that may require policy responses.[53] Operational innovation describes the way in which stakeholders adjust their approach to threat assessment and response tactics in a way that utilizes technological innovation and, more generally, strategic/tactical/methodological innovation.[54] Innovation often requires collaboration between government agencies, private companies, and academic institutions. Member States' policy response should consider driving and enabling innovation, which requires investment, resources, and support for developing and implementing innovative technologies. Governments and private organizations must be willing to invest in research and development, as well as provide support to implement new measures. In addition, to the quick pace of change, policies need to build policy frameworks that are able to adapt to changing threats. This includes cross government "horizon scanning"[55] on the policy level and innovation management on the institutional level.

51 "How You Can Help: Public Contribution Form," New Zealand Security Intelligence Service, accessed April 23, 2023, https://providinginformation.nzsis.govt.nz/.

52 Robert G. Spulak, "Science Technology and Innovation in Combating Terrorism.," February 2015, https://www.osti.gov/biblio/1513954.

53 See e.g., United Kingdom, *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (United Kingdom: The Crown, 2018), 24, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.

54 Spulak, "Science Technology and Innovation in Combating Terrorism."

55 The Jon Day review defined horizon scanning as: A systematic examination of information to identify potential threats, risks, emerging issues and opportunities, beyond the Parliamentary term, allowing for better preparedness and the incorporation of mitigation and exploitation into the policy making process.

5.3.3 **Data Management**

Data management in the context of counter-terrorism and new technologies refers to the processes and systems used to collect, analyse, store, and share information related to terrorist threats. With the increasing use of new technologies such as artificial intelligence, machine learning, and big data analytics, data management has become a critical component of counter-terrorism efforts.

Effective data management is essential in the fight against terrorism and requires the use of new technologies and tools to collect, analyse, and share information in a timely and secure manner. It enables law enforcement and intelligence agencies to identify and track potential threats, monitor the activities of known terrorists and their associates, and prevent or disrupt terrorist attacks. This involves the collection and analysis of a wide range of data. Enabling collaboration across sectors and among stakeholders from multiple regions and/or Member States requires that data pertaining to relevant threats should be handled properly. This includes matters such as proper organization and documentation style of the data, so that it may be accessed and shared easily and securely among stakeholders from across sectors and across Member States. Additionally, counter-terrorism policies must address the ways in which the data is protected to ensure that privacy of an individual is not disturbed and/or data collection retains certain limits in order to protect human rights.

As part of data management, counter-terrorism policies should outline both the process and the policy through which data analytics and databases are used as a means of gathering information and analysing terrorist threats. Counter-terrorism policies should consider the ways in which new technologies such as artificial intelligence may be used to sort, process, and analyse the data that has been collected by stakeholders regarding threats.[56] Care must be taken to ensure that the data collected and retained does not infringe upon privacy rights and does not discriminate against individuals on the basis of: sex, race, colour, language, religion, political or other opinion, national or social origin, or other status. Within the practice of information sharing between stakeholders, especially stakeholders across multiple borders, policies must be set in order to ensure that the data shared is done in a secure way that does not compromise the operational security of practitioners addressing the threat. It must also be done in a way that protects the privacy of the individuals whose data has been gathered such that only practitioners involved in a particular case may have access to this data, implementing encryption and other security measures to protect data from unauthorized access or hacking, and complying with relevant data protection laws and regulations.

56 United Kingdom, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, 24.

5.3.4 **Legal Framework**

The legal framework in the context of counter-terrorism and new technologies refers to the set of laws, regulations, and policies that govern LEA operations and collection, use, retention, and sharing of information related to terrorist threats, as well as the use of new technologies to combat terrorism. The legal framework is essential to ensure that counter-terrorism efforts comply with legal and ethical standards, protect individual rights and privacy, and avoid abuse of power by law enforcement and intelligence agencies. This involves striking a strictly proportionate balance between the need for effective counter-terrorism measures and the protection of individual rights and freedoms. It plays a critical role in ensuring that counter-terrorism efforts are effective, lawful, and respectful of individual rights and freedoms, while leveraging new technologies to address the evolving threat of terrorism.

It is important to have a working level definition of terrorism that can be used as the basis for legal action, including considerations of the ways in which terrorists may exploit new technologies.[57] The global nature of the digital age poses a unique difficulty in the ability for countries to formulate and implement counter-terrorism policies, as terrorism in the age of new technologies is one that can easily cross multiple borders. Even if the terrorist actor acts within the borders of one state, this actor can cause others to engage in incitement to terrorism and further terrorist actions within the borders of a different country. When considering the legal framework surrounding a counter-terrorism policy, an emphasis must be placed on the protection of human rights. The legal frameworks under which a counter-terrorism policy operates should also include a presumption against the use of illegally obtained evidence in courts as part of the protection of human rights and privacy throughout the counter-terrorism response process.

5.3.5 **Capacity Building**

When designing a counter-terrorism policy, it is important to build a framework within the policy that deals with matters such as training and preparation. Here, training refers to training relevant stakeholders and practitioners as well as training members of the public. The goal in training decision-makers and other stakeholders is to assist them in devolving knowledge and capabilities to respond to terrorist threats. This can involve educational seminars, simulations, refresher courses, and other means to enable them to understand their role in combatting terrorist threats that stem from new technologies and to ensure that the nature of their response remains up to date with continuous technological developments. Additionally, training practitioners and members of the public as part of a counter-terrorism policy response both increases the awareness of these groups and enables an increase in the national capability to respond to terrorist threats and acts of terror.[58] For example, creation and implementation of programmes that specialize in training practitioners in deradicalization and/or disengagement efforts for known terrorist actors may provide the necessary threat intervention to prevent further terrorist action by these actors.[59]

57 Freese, "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works," 43.

58 The Commonwealth of Australia, *2017 Foreign Policy White Paper*, ed. Morris Walker Pty Ltd (Australia, 2017), 38, https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.

59 Vidino and Bennett, "A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism," 7–8.

[VI]

Good Practices in Counter-Terrorism Policy Response

6.1 Overview

When designing a model for a counter-terrorism policy response that can effectively address the potential opportunities and challenges presented in the use of new technologies, sources from international organizations, Member States, academia, and the private sector were consulted. The following are some of the findings regarding practices that may be included in counter-terrorism policy responses. The selection of findings aims to address both elements of building a successful counter-terrorism policy to respond to the use of new technologies for terrorist purposes and the ways in which policymakers and other practitioners may improve their ability to address these threats. These findings are presented in the following sections through the lens of the four integrals considerations of counter-terrorism policy (Section 5.2), as taken from the model presented in Section 5.1. Within these considerations, the resources presented here cover some good practices within the key components of counter-terrorism policy for addressing new technologies (Section 5.3).

6.2 Awareness

Awareness, as discussed in Section 5.2.1, is in the context of providing tools, knowledge and engagement of practitioners and members of the public, to identify and report or respond to threats. The OSCE proposes approaches to training and preparation programmes. The first of these programmes is a set of seminars specifically aimed at increasing counter-terrorism response awareness among members of the public.[60] For counter-terrorism practitioners, the OSCE recommends holding "tabletop exercises", which serve as both working groups for experts from the government, private sector, and academia (among others) and as a forum in which scenarios may be discussed, providing a means of further developing the capacity of the State to respond to terrorist actions.[61] In addition to training sessions and 'tabletop exercises,' the Brookings Institute recommends conducting "war game" simulations in which practitioners from different agencies and sectors participate.[62] The goal of such exercises is to practice responses to attacks (including

60 OSCE Transnational Threats Department, "OSCE Anti-Terrorism Reference" (Organization for Security and Co-Operation in Europe, July 2020), 25.

61 OSCE Transnational Threats Department, 25-26.

62 Bruce Schneier and Tarah Wheeler, "Hacked Drones and Busted Logistics Are the Cyber Future of Warfare," Brookings, *Tech Stream* (blog), June 4, 2021, https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare.

alternative plans of action).[63] Here, the goal is similar to that of red-team exercises, which, other than allowing for the practice of response procedures, also helps those designing policy responses to understand gaps in which response policies need to be improved.[64]

In the discussions at the OSCE tabletop exercises as well as in the United States' Counter-Terrorism strategy, there is an emphasis placed in ensuring that matters of protecting critical infrastructure from terrorist attacks are part of the larger counter-terrorism agenda, especially as these are vulnerable to cyberattacks.[65]

Desired policy outcomes should consider the following:

- Deep understanding of threat detection and threat response by stakeholders;
- General public awareness of threats and policy responses to such threats;
- Enhance awareness through training and preparation programmes, such as:
  - Education for practitioners and members of the public;
  - Simulations and 'red teaming';
  - Tabletop exercises;
  - 'War game' simulations.

6.3 Threat Interventions

As previously mentioned, one of the means through which a Member State can implement measures of threat intervention is through the use of a proactive approach to security. Such an approach involves threat intervention at an early enough stage and as close to the source as possible to prevent terrorist actions from coming to fruition.[66]

A method through which threat intervention can be attained is through the implementation of the principles of security by design and security by default. The concept of security by design refers to the idea that one of the goals when building or designing a product or a policy is to design it with security measures in place such that it can effectively deal with a threat.[67] The approach of security by design is advocated for by the European Commission in its discussion of the protection of public spaces.[68]

Additionally, in a recent publication by United States' Cybersecurity and Infrastructure Security Agency (CISA), Germany's Federal Office for Information Security (BSI), and eight other security and cybersecurity bodies of Member States, the importance is placed on security by design within the specific context of technology.[69] In addition to security by design,

63 Schneier and Wheeler.

64 David Romyn and Mark Kebbell, "Terrorists' Planning of Attacks: A Simulated 'Red-Team' Investigation into Decision-Making," *Psychology, Crime & Law* 20, no. 5 (May 28, 2014): 483, https://doi.org/10.1080/1068316X.2013.793767.

65 OSCE Transnational Threats Department, "OSCE Anti-Terrorism Reference," 26; United States, *National Strategy for Counter-terrorism of the United States of America*, 19-20.

66 National Cyber Security Centre, "Secure by Default," National Cyber Security Centre, March 7, 2018, https://www.ncsc.gov.uk/information/secure-default.

67 European Commission, *Security by Design: Protection of Public Spaces from Terrorist Attacks*, 23; Cybersecurity and Infrastructure Security Agency et al., "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default," 3-4.

68 European Commission, *Security by Design: Protection of Public Spaces from Terrorist Attacks*.

69 Cybersecurity and Infrastructure Security Agency et al., "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default."

these bodies also discuss the importance of security-by-default. This refers to the final 'product' (technological, or in this case, policy) being one that is secure and provides means for defence as part of the nature of the product/policy itself when it was released.[70] Drawing from the concepts presented in both of these examples of security by design and security by default, one may apply it to the design of counter-terrorism policy through means such as the creation of SOPs for responding to specific forms of technology that can be easily adapted to fit multiple scenarios. The implementation of these concepts may also be accomplished through an emphasis on the use of technologies by practitioners as a means of securing systems such as critical infrastructure systems of a Member State.

In a paper presented at a conference held by Europol, the authors propose multiple steps by which, through policy changes, a proactive approach may be taken in addressing terrorist radicalization, particularly in prisons.[71] Among its recommendations, the paper proposes information-sharing between prisons and other governmental bodies as a means of detecting signs of radicalization among prisoners as determined by practitioners who have undergone training in identifying and addressing such behaviour.[72] Should such behaviour be detected, the proposal advocates that such individuals undergo either deradicalization or disengagement.[73]

Another means through which threat intervention can be accomplished by Member States is through the implementation of a legal framework through which the policy operates. In the discussion on the use of security by design and security by default, the authoring organizations of the report, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default" note efforts by the European Union to provide a legal framework through which matters of cybersecurity are addressed in the Cyber Resilience Act.[74] This Act, proposed at the end of 2022, seeks to provide regulatory measures with the aim of ensuring that future technologies that are developed are done in a way that incorporates concepts of security by design, such that what reaches the market is less vulnerable by default to security breaches.[75] This would serve as a preventative measure to threat intervention by making the products available to consumers less vulnerable to potential threats.

An additional example of the use of a legal framework as a means of threat intervention is the system advocated for by the United Nations in which there is an international legal framework through which to address counter-terrorism efforts. The goal of such a framework is to enable legal enforcement for terrorist actions regardless of the location of the individual perpetrating the terrorist action.[76] As part of this international framework, the United Nations has outlined 19 international legal instruments to address counter-terrorism measures globally.[77] In order to enable the international legal framework to have the ability to work as intended among Member States, counter-terrorism policies must be established or authorized by law and must be subject to independent oversight.

70 Cybersecurity and Infrastructure Security Agency et al., 5-6.

71 Vidino and Bennett, "A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism."

72 Vidino and Bennett, 5-6.

73 Vidino and Bennett, 8.

74 Cybersecurity and Infrastructure Security Agency et al., "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default," 3.

75 "Cyber Resilience Act," European Commission, September 15, 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

76 "International Legal Framework," United Nations: Office on Drugs and Crime, accessed April 25, 2023, //www.unodc.org/unodc/en/terrorism/expertise/international-legal-framework.html; "Counter Terrorism Legal Framework: Lessons Learned from IDLO Policy Dialogues in Collaboration with UNODC," *Development Law Update*, no. 2 (2007), https://www.files.ethz.ch/isn/138640/14.pdf.

77 "International Legal Instruments," United Nations Office of Counter-Terrorism, accessed April 25, 2023, https://www.un.org/counter-terrorism/international-legal-instruments; OSCE Transnational Threats Department, "Status of the Universal Anti-Terrorism Conventions and Protocols as Well as Other International and Regional Legal Instruments Related to Terrorism and Co-Operation in Criminal Matters in the OSCE Area" (Organization for Security and Co-Operation in Europe (OSCE), July 2018), https://www.osce.org/files/f/documents/5/8/17138_0.pdf.

Desired policy outcomes should consider the following:

- Increased cooperation between sectors, agencies, Member States, etc., to counter the threat of terrorists' use of new technologies;
- Achieve national counter-terrorism goals of prevent, disrupt, deny, protect, recover, and prosecute;
- Develop proactive threat responses that may include:
  - Security by design / security by default;
  - Threat identification and prioritization;
  - Deradicalization and disengagement.

6.4 National Capability

With the aim of building the national capability of a Member State to respond to terrorism, there are good practices being implemented by Member States that are beneficial to draw from. Finland's counter-terrorism strategy, for example, makes note of the need for technological innovation by discussing the need for the country to continue building its cyber capabilities, particularly with regard to means for gathering intelligence.[78] Another intersection of innovation and national capacity can be found in the United Kingdom's counter-terrorism strategy. One of the forms of collaboration discussed is collaboration between government practitioners and the private sector, with a focus on building the relationship between the government and the tech sector as part of innovative efforts to continue growing the technological capability of the country to respond to terrorism.[79] Additionally, the counter-terrorism strategy stresses the importance of their own "capacity building" as well as the need to help other Member States increase their ability to respond to terrorist actions.

An increase in national capability can also be attained through the implementation of training and preparation programmes. In addition to the training and preparation practices discussed in Section 6.1(which, in addition to building awareness, also builds national capabilities to identify and respond to threats), the trainings detailed in the Europol document regarding deradicalization efforts (see also Section 6.2) in prisons can also build national capacity to reduce and respond to radicalization.

A key component to enhance innovation in Counter-Terrorism National Capabilities can be achieved by research and devolvement programmes innovation. EU security research[80] focuses on building initiatives intended to enhance the capacity of law enforcement authorities in fields like developing analytical solutions aimed to deal with big data. Additionally, under the future Research Programme of Horizon Europe, research is further integrated within the security policy cycle to ensure an impact-oriented output, responding to the identified law enforcement needs. [81]

78 Finland Ministry of the Interior, *National Counter-Terrorism Strategy 2022-2025*, Publications of the Ministry of the Interior, 2022:38 (Helsinki, Finland: Finland Ministry of the Interior, 2022), 24, https://julkaisut.valtioneuvosto.fi/handle/10024/164447.

79 United Kingdom, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, 28.

80 European Commission, *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions (Brussels, Belgium: European Commission, 2020), https://home-affairs.ec.europa.eu/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf.

81 See for example projects DANTE and TENSOR ("Detecting and Analysing Terrorist-Related Online Contents and Financing Activities," European Commission: Cordis, accessed April 23, 2023, https://cordis.europa.eu/project/id/700367.,"Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition," European Commission: Cordis, accessed April 23, 2023, https://cordis.europa.eu/project/id/700024.).

Desired policy outcomes should consider the following:

- Prioritize resources with clear roles and responsibilities.
- Increase national capabilities through:
  - Information sharing;
  - Innovation, research and development;
  - Cooperation and partnerships;
  - Capacity building.

6.5 Cooperation

Cooperation as a pillar for the design and implementation of counter-terrorism policy relating to new technologies is something that can take many forms and can take place across multiple levels (across States, between agencies, between sectors, etc.). As such, the literature that was surveyed for this Report yielded multiple forms of good practices that are helpful in the design and implementation of counter-terrorism policy responses.

In a summary of conference proceedings regarding national and regional counter-terrorism strategies, UNCCT recommends, for example, that Member States should collaborate and advise each other in formulating counter-terrorism strategies.[82] Here, the concept of information sharing, as introduced in Section 5.3.1 extends beyond information sharing as it relates to specific threats and highlights the importance of information sharing in the form of good practices. Such a recommendation is of particular importance when discussing the development of counter-terrorism policy as it relates to new technologies. Member States can share with one another developments in how to both combat the use of new technologies for terrorist purposes and how to use new technologies as a means to respond to terrorism. Another valuable good practice from this document is the practice of creating regional strategies for cases in which terrorist actions and incitement become cross-border matters, something that has become increasingly more common in the digital age.[83] Similarly, the European Union framed cross-border collaboration as the "international answer" to global threats.[84]

With regard to data management, Spain's counter-terrorism strategy addresses two primary aspects that must be considered in counter-terrorism policy: the ability for the data to be used and the ability for the data to be both accessible to those who need to access it and protected from those who should not be privy to that information.[85] The document stresses the need for encryption in order to share data across shareholders from differing sectors in a secure manner. It also stresses the need for the data to be organized in a way that makes it easy and efficient to sort through and be used by stakeholders.[86]

82 United Nations Counter-Terrorism Centre (UNCCT), "Summary of Discussions: International Conference on National and Regional Counter-Terrorism Strategies- January 31-February 1, 2013," Conference Summary (Bogota, Colombia, 2013), 5, https://www.un.org/counter-terrorism/sites/www.un.org.counter-terrorism/files/bogota_jan-feb2013.pdf.

83 United Nations Counter-Terrorism Centre (UNCCT), 7.

84 European Union, Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, 88/7.

85 Interior Ministry of Spain, *National Counter-Terrorism Strategy*, 2019, 53–54, https://www.dsn.gob.es/eu/file/4271/download?token=-K6uOf-C.

86 Ibid.

One method for information-sharing through the use of data management is the creation of a risk register that would serve as a database of existing threats and existing intelligence gathered about those threats among stakeholders. The model for a risk register from New Zealand's Transport Agency provides a good example for the types of information that should be included in a country's risk register such as a reference number for the threat, a section which lists the date and description of the last time that actions were taken against a threat, the plan of action should a threat come to fruition, and a breakdown of the roles that each stakeholder should play in the event that the threat materializes.[87]

One of the means through which such a register and the information that accompanies it may be shared in a secure way is through the adoption of a model similar to the 'cluster' model practiced in the United Kingdom. The cluster model is a means of cross-sector regional collaboration among government authorities, companies in the private sector, and academia. Within the model, each region has a cluster that operates semi-independently with regard to the threat prioritization that is most fitting to their specific area of responsibility (AOR). The stakeholders within each cluster share information and good practices. Here, the clusters engage in a form of centralization in which they ultimately report and share information with national stakeholders with regard to threats.[88] The localized nature of the model enables a more nuanced approach to threat assessment and prioritization as it relates to the AOR, while also enabling the national stakeholders to have an in-depth understanding of each of the regions within their responsibility.

Desired policy outcomes should consider the following:

- Enhance cooperation between National CSIRTs and Law Enforcement & Criminal Justice Authorities to investigate and prosecute terrorist;
- Enhance cooperation between law enforcement and Private ICT companies
- Enhance regional and international cooperation
- Enhance information sharing through:
  - Sharing good practice;
  - Establishing information sharing agreements;
  - Enhancing data management approach and practices.

87 New Zealand Transport Agency, "Risk Register," Government, Waka Kotahi NZ Transport Agency, accessed April 1, 2023, https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register.

88 UKC3, "Cyber Cluster Operating Framework," *UK Cyber Cluster Collaboration* (blog), accessed March 30, 2023, https://ukc3.co.uk/cyber-cluster-operating-framework.

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)