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

INTERPOL

Funded by
the European Union

Cybersecurity and New Technologies

Conducting Terrorist Threat Assessment: The Use of New Technologies for Terrorist Purposes

Disclaimer

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

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

Contents of this publication may be quoted or reproduced, provided that the source of information is acknowledged. The authors would like to receive a copy of the document in which this publication is used or quoted.

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.

United Nations Office of Counter-Terrorism
United Nations Headquarters
New York, NY 10017
www.un.org/counterterrorism

200, Quai Charles de Gaulle
69006 Lyon, France
www.interpol.int/en

Contents

Joint Foreword

Advances in Information and Communication Technologies (ICT) 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

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 terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement and sentencing as well as corrections and rehabilitation.
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.[1]
Intelligence	The product resulting from collecting, developing, disseminating, analysing, and interpreting of information gathered from a wide range of source, 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.

[1] 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).

New Technologies	While the New Technologies terminology covers a wide range of different technologies,[2] for the purpose of this document, new technologies refer to the use and abuse of such new technologies as the Internet, social media, cryptocurrencies, facial recognition, and the darknet.[3]
Open-Source Intelligence (OSINT)	Intelligence gathered from publicly available sources.[4]
Prosecution / Adjudication	A legal process to bring about terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement of the case and sentencing of the conviction.
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 into society.
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.
Social Media Intelligence (SOCMINT)	Intelligence information gathered through social media.
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 as offences within the scope of and as defined in the international conventions and protocols relating to terrorism.[5]
Threat Actor	An individual or entity that uses new technologies for terrorist purposes, such as for radicalization, recruitment, and incitement to commit terrorist acts, for the financing and planning for their activities, as well as to commit an act of terrorism. In the case of counter-terrorism and new technology, this extends to using new technologies to either perform malicious actions or to use the technology to influence others to commit acts of terror.[6]
Threat Assessment	A product that through an agreed methodology provides analysis and guidance for action on tackling the issues identified that may cause harm to the State and society in the future.[7]
Threat Landscape	The threat landscape refers to the overall picture of potential terrorist threats that a country, region, or organization may face. It encompasses the range of terrorist groups, their capabilities, intentions, and tactics, as well as the vulnerabilities of potential targets and the potential impact of an attack.
Threat Target	A specific entity, location, or group that is identified as being at risk of a potential terrorist attack.
Threat Vector	The specific method or means through which a threat actor carries out an attack.[8]
Zettabyte	One zettabyte is equal to one billon terabytes.

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

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

[4] 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.

[5] See S/RES/1566 (2004), para. 3.

[6] Canadian Centre for Cyber Security, *An Introduction to the Cyber Threat Environment 2023-2024* (Communications Security Establishment of Canada, 2022), 2, https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.

[7] United Nations Office on Drugs and Crime, *Guidance on the Preparation and Use of Serious and Organized Crime Threat Assessments: The SOCTA Handbook* (New York, NY: United Nations, 2010), https://www.unodc.org/documents/organized-crime/SOCTA_Handbook.pdf.

[8] Mary E. Shacklett, "What Is Attack Vector?," Tech Target, April 2021, https://www.techtarget.com/searchsecurity/definition/attack-vector.

Executive Summary

This document aims to provide guidance to Member States in effectively assessing, mitigating, and responding to terrorist threats, specifically those related to the use of new technologies. By conducting a structured threat and risk assessment process, Member States can enhance their situational awareness, response capabilities, and public safety, thereby improving their counter-terrorism efforts. This document was compiled as the product of desktop research, stakeholder consultations, expert group meetings, and good practices from existing threat and risk assessment methodologies. Countering the use of new technologies for terrorist purposes requires understanding their use, developing legal frameworks and policies, and building operational capacity, while upholding human rights and international law.

Threat and risk assessments are a crucial component in countering counter-terrorism efforts, as it provides policymakers with a better understanding of existing and potential threats and the resources required to address them. This document provides a methodological structure for the threat and risk assessment process. It also aims to provide good practices for conducting threat and risk assessments on the use of new technologies for terrorist purposes. It offers a unique threat and risk management cycle, which is a structured process aimed at assessing and managing potential threats from the exploitation of new technologies to a country at a national level. The process includes the identification of threat actors, and an analysis based on their intent and technological capability to commit an act of terror. The next step is the development of threat scenarios, which involves analysing threat actors' capabilities and access to new technology and involves determining both the types of potential attacks and the level of sophistication of those attacks. The resulting threat scenario encompasses each of the iterations of the types of attacks against different vulnerabilities. The following stage is the evaluation and prioritization of threats, which is done within the context of threat responses to the use of new technologies for terrorist purposes. This stage can include actions such as the creation of standard operating procedures (SOPs) for responding to specific forms of technology that can be easily adapted to fit multiple scenarios. Developing a threat response is an ongoing process that involves regular reviews of existing threat scenarios, the identification of new potential threats, and updates to the threat assessment and response strategies.

This document is intended primarily for practitioners responsible for conducting national terrorist threat and risk assessments with the cooperation of involved stakeholders to better understand the terrorist threat and use of new technologies to inform national policy and decision-makers. This guide also provides them with good practices and actionable information to enhance their situational awareness and response capabilities. By developing a robust understanding of the use of new technologies for terrorist purposes through a structured threat and risk assessment process, Member States can improve the efficiency of counter-terrorism efforts, including actionable information regarding the threat landscape. Additionally, the practice of conductive effective threat and risk assessments can help enhance public safety and can assist in the development of proactive measures to prevent or minimize the impact of terrorist activity.

[I]

Background

1.1 Overview

United Nations Member States attach great importance to addressing the impact of new technologies in countering terrorism. During the seventh review of the United Nations Global Counter-Terrorism Strategy (A/RES/75/291)[9] in July 2021, Member States expressed their deep concern about *"the use of the Internet and other information and communications technologies, including social media platforms, for terrorist purposes, including the continued spread of terrorist content"*, and requested the Office of Counter-Terrorism and other Global Counter-Terrorism Compact entities *"to jointly support innovative measures and approaches to build the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism".* Security Council Resolutions 2178 (2014)[10] and 2396 (2017)[11] call for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology and communications for terrorist acts. Security Council Resolution 2396 (2017) also encourages Member States **to enhance cooperation with the private sector, especially with ICT companies,** in gathering digital data and evidence in cases related to terrorism.

In its 30th Report to the United Nations Security Council,[12] the Analytical Support and Sanctions Monitoring Team noted that "Many Member States highlighted the evolving role of social media and other online technologies in the financing of terrorism and dissemination of propaganda", with platforms cited by Member States that 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.[13]

The CTC noted ***"with concern the increased use, in a globalized society, by terrorists and their supporters of the Internet and other information and communication technologies***, including social media platforms, for terrorist purposes"

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

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

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

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

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

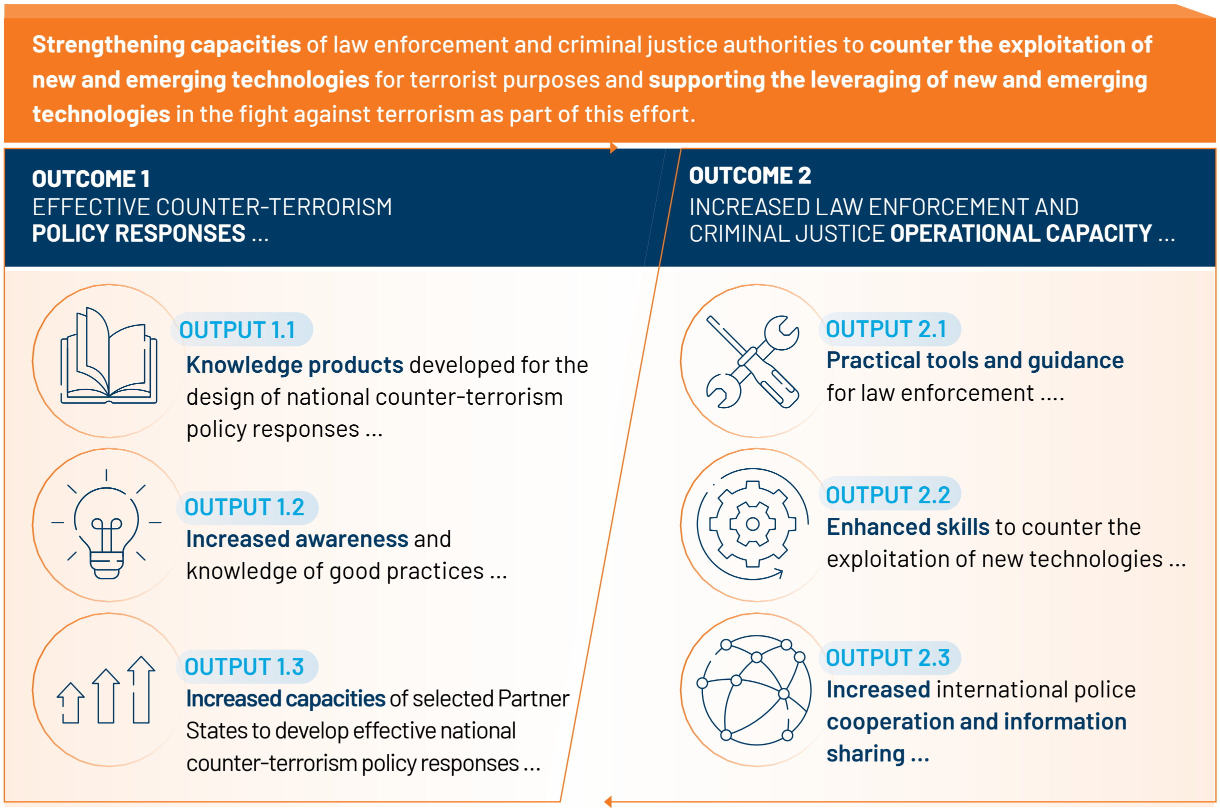
and acknowledged ***"the need to balance fostering innovation and preventing and countering the use of new and emerging technologies, as their application expands, for terrorist purposes"***, while emphasizing "the need to preserve ***global connectivity and the free and secure flow of information*** 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



Strengthening capacities of law enforcement and criminal justice authorities to **counter the exploitation of new and emerging technologies** for terrorist purposes and **supporting the leveraging of new and emerging technologies** in the fight against terrorism as part of this effort.

OUTCOME 1
EFFECTIVE COUNTER-TERRORISM
POLICY RESPONSES ...

OUTPUT 1.1
Knowledge products developed for the design of national counter-terrorism policy responses ...

OUTPUT 1.2
Increased awareness and knowledge of good practices ...

OUTPUT 1.3
Increased capacities of selected Partner States to develop effective national counter-terrorism policy responses ...

OUTCOME 2
INCREASED LAW ENFORCEMENT AND CRIMINAL JUSTICE **OPERATIONAL CAPACITY** ...

OUTPUT 2.1
Practical tools and guidance for law enforcement ....

OUTPUT 2.2
Enhanced skills to counter the exploitation of new technologies ...

OUTPUT 2.3
Increased international police **cooperation and information sharing ...**

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 terrorists' 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 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 document focuses specifically on the process of threat and risk assessment on the national level. It aims to raise awareness and provide guidance on good practices for developing and implementing a threat and risk assessment process. The goal of the document is to support and enable Member States to conduct national threat and risk assessments on the use of new technologies for terrorist purposes, including both current and future threat landscapes. The document is aligned with the United Nations Global Counter-Terrorism Strategy and emphasizes the importance of respecting human rights and the rule of law in counter-terrorism efforts. It is based on desktop research regarding existing threat assessment methodologies, consultations with stakeholders, and expert group meetings. The sources for the desktop research included national threat and risk assessments of Member States.

1.3.2 Target Audience

This document is intended primarily for practitioners responsible for conducting national terrorist threat and risk assessments with the cooperation of involved stakeholders to better understand the terrorist threat and use of new technologies to inform national policy and decision-makers. It also aims to provide them with relevant and actionable information and enhance their situational awareness and response capabilities.

1.3.3 Benefits

By developing a robust understanding of the use of new technologies for terrorist purposes through a structured threat and risk assessment process, Member States can improve the efficiency of counter-terrorism efforts, by including actionable information within the threat landscape. This can help improve situational awareness, allowing for a more effective and integrated response to potential threats, resource allocation, and strategic planning. Additionally, threat and risk assessments can help enhance public safety, and assist in the development of proactive measures to prevent or minimize the impact of terrorist activity.

1.3.4 Limitations

While there are many benefits for "Conducting Terrorist Threat Assessment: The Use of New Technologies for Terrorist Purposes", there are also some limitations and challenges that need to be taken into account. Some of these limitations include:

- Rapidly evolving threat landscape: The threat landscape is constantly evolving, which means that any threat assessment merely represents a snapshot of the time in which it was conducted. As such, these threat assessments may quickly become outdated without updates that are necessary to ensure that they remain current and accurate in the face of an evolving threat landscape and ongoing progress in technology.
- Limited access to information: Access to information about potential terrorist threats can be limited, particularly when it comes to classified intelligence or information held by foreign governments or entities in the private sector. This can make it challenging to conduct a comprehensive threat and risk assessment.
- Complexity of the technology landscape: The technology landscape is complex and rapidly changing, and it can thus be difficult to keep up with emerging technologies and their applications for potential terrorist activities.
- Limited resources: Resources (such as money, manpower, technological capability) for conducting threat assessments may be limited.
- The size and complexity of the country, and the maturity of its counter-terrorism capabilities may also influence how a country decides to assess and understand its threats and risks.

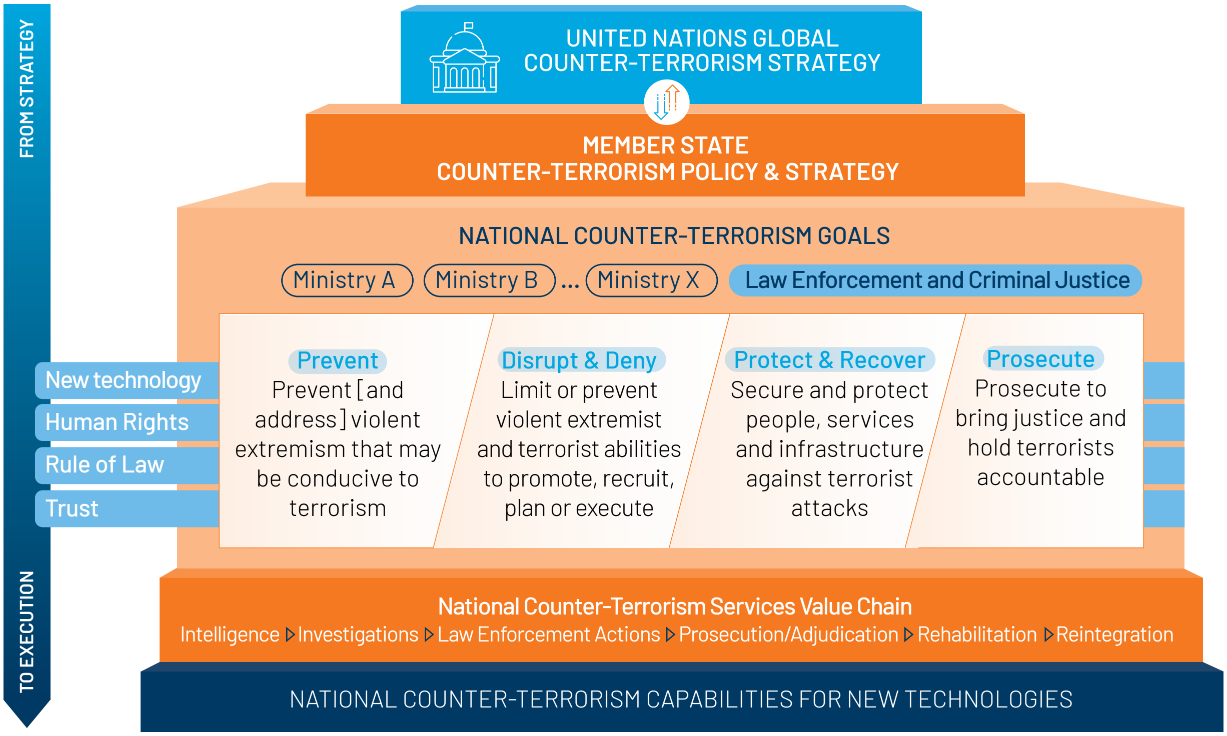
[II]
Approach

2.1 Overview

The report seeks to support and enable Member States to conduct effective threat assessments in countering the use of new technologies for terrorist purposes, which are aligned to the United Nations Global Counter-Terrorism Strategy and in full respect of human rights and the rule of law.

2.2 Guiding Framework

FIGURE 2


FROM STRATEGY
TO EXECUTION
UNITED NATIONS GLOBAL COUNTER-TERRORISM STRATEGY
MEMBER STATE COUNTER-TERRORISM POLICY & STRATEGY
NATIONAL COUNTER-TERRORISM GOALS
Ministry A
Ministry B
...
Ministry X
Law Enforcement and Criminal Justice
New technology
Human Rights
Rule of Law
Trust
Prevent
Prevent [and address] violent extremism that may be conducive to terrorism
Disrupt & Deny
Limit or prevent violent extremist and terrorist abilities to promote, recruit, plan or execute
Protect & Recover
Secure and protect people, services and infrastructure against terrorist attacks
Prosecute
Prosecute to bring justice and hold terrorists accountable
National Counter-Terrorism Services Value Chain
Intelligence ▷ Investigations ▷ Law Enforcement Actions ▷ Prosecution/Adjudication ▷ Rehabilitation ▷ Reintegration
NATIONAL COUNTER-TERRORISM CAPABILITIES FOR NEW TECHNOLOGIES

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 the following:

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

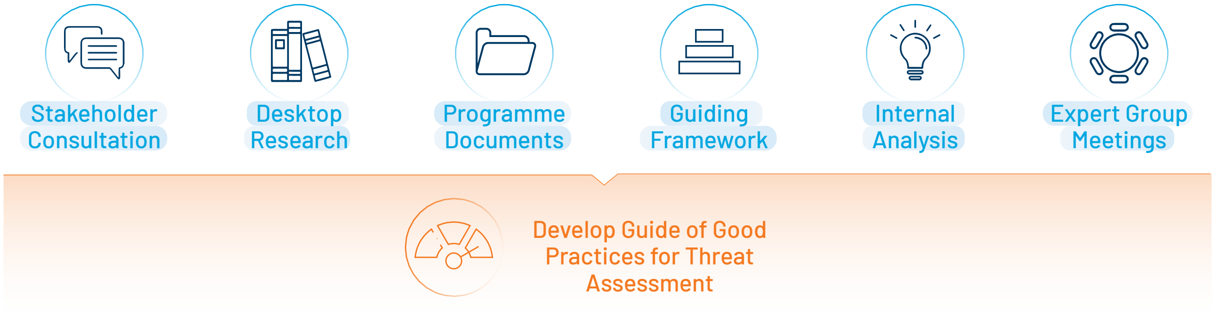
Services	Description
Criminal Justice Process	A legal process to bring about terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement and sentencing as well as corrections and rehabilitation.
Criminal Intelligence	The product resulting from collecting, developing,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

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

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

2.3 Methodology

FIGURE 3



This document was developed and informed by a wide range of inputs which include CT TECH project documents, stakeholder consultation, internal analysis, desktop research, expert group meetings, co-ordination with the United Nations Global Counter-Terrorism Coordination Compact entities, and the guiding framework as described above in Section 2.2. The research and consultation with stakeholders and experts focused both on determining an effective method for threat assessment and response, as well as the ways in which this methodology can address the types of threats posed by the exploitation of new technologies or can be aided by the use of new technologies by practitioners to respond to threats.

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 particular 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 use of new technologies for terrorist purposes and use new technologies as part of this effort, identify good practices in this regard, and also discuss risks, challenges, and not so good practices that require attention and caution. The guide was further refined through engagement with the United Nations Global Counter-Terrorism Coordination Compact and its Working Group on Emerging Threats and Critical Infrastructure Protection, which promotes coordination and coherence to support the efforts of Member States to prevent and respond to emerging terrorist threats, with respect for human rights and the rule of law as the fundamental basis, in line with international law, including human rights, humanitarian, and refugee laws.

2.3.2 Reference Document Review

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

TABLE 3. **References**

1	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	Canada, Public Safety. "Canada's National Terrorism Threat Levels." Consultations, August 25, 2016. https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html.
4	Canadian Centre for Cyber Security. An Introduction to the Cyber Threat Environment 2023-2024. Communications Security Establishment of Canada, 2022. https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.
5	Centre for Terror Analysis (CTA). "Assessment of the Terrorist Threat to Denmark." Denmark: Centre for Terror Analysis (CTA), March 2022. https://politi.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-terrortruslen-mod-danmark/vtd_2022_uk.pdf.
6	CIVI.POL Conseil and Royal United Services Institute. "Operational Guidelines on the Preparation and Implementation of EU Financed Actions Specific to Countering Terrorism and Violent Extremism in Third Countries." European Commission, 2018. https://issat.dcaf.ch/sqi/download/131230/2684696/EU-CT-CVE-guidelines.pdf.
7	Cole, Mara. "Towards Proactive Airport Security Management: Supporting Decision Making through Systematic Threat Scenario Assessment." Journal of Air Transport Management 35 (March 1, 2014): 12–18. https://doi.org/10.1016/j.jairtraman.2013.11.002.
8	Coordination Unit for Threat Analysis (CUTA). "The Common Database (CDB)." Accessed April 23, 2023. https://cuta.belgium.be/the-common-database-cdb/.
9	Coordination Unit for Threat Analysis (CUTA). "The Strategic Note Extremism and Terrorism (Strategy T.E.R.)." Accessed April 23, 2023. https://cuta.belgium.be/action-plan-against-radicalism-plan-r/.
10	Erez Magen, and R. "Enabling Advancements in Security-Danger and Opportunities." Maarachot (Systems) (blog), March 29, 2022. https://www.maarachot.idf.il/2022.
11	European Commission. Security by Design: Protection of Public Spaces from Terrorist Attacks. Luxembourg: European Union, 2022.
12	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.
13	European Commission: Cordis. "Detecting and Analyzing Terrorist-Related Online Contents and Financing Activities." Accessed April 23, 2023. https://cordis.europa.eu/project/id/700367.
14	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.

15 Financial Action Task Force (FATF). "National Money Laundering and Terrorist Financing Risk Assessment." Financial Action Task Force (FATF), February 2013. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/National_ML_TF_Risk_Assessment.pdf.coredownload.pdf.

16 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.

17 Hemmingsen, Ann-Sophie. "An Introduction to the Danish Approach to Countering and Preventing Extremism and Radicalization." Copenhagen, Denmark: Danish Institute for International Studies, 2015. https://www.ft.dk/samling/20151/almdel/reu/bilag/248/1617692.pdf.

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

19 International Organization for Standardization. ISO 31000 Risk Management-Guidelines. Second. Switzerland: International Organization for Standardization, 2018. https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf.

20 Lotz, Volkmar. "Threat Scenarios as a Means to Formally Develop Secure Systems." In Computer Security — ESORICS 96, edited by Elisa Bertino, Helmut Kurth, Giancarlo Martella, and Emilio Montolivo, 242–65. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996.

21 Ministry of Justice of Sweden. Prevent Pre-empt Protect: The Swedish Counter-Terrorism Strategy. Sweden: Government Offices of Sweden, 2014. https://www.government.se/contentassets/b56cad17b4434118b16cf449dbdc973d/en_strategi-slutlig-eng.pdf.

22 National Coordinator for Security and Counter-terrorism. "NCTV's Terrorist Threat Assessment: Threat in and to the Netherlands Has Become More Multifaceted and Diffuse – News Item – National Coordinator for Security and Counter-terrorism." Ministry of Justice and Security: National Coordinator for Security and Counter-terrorism. Ministry of Justice and Security, November 7, 2022. https://english.nctv.nl/latest/news/2022/11/07/nctvs-terrorist-threat.

23 National Coordinator for Security and Counter-terrorism. "Terrorist Threat Assessment Netherlands." Ministry of Justice and Security: National Coordinator for Security and Counter-terrorism. Ministry of Justice and Security, May 14, 2020. https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands.

24 Neil J. Smelser. "Motivation, Social Origins, Recruitment, Groups, Audiences, and the Media in the Terrorism Process." In The Faces of Terrorism: Social and Psychological Dimensions, 92–119. Science Essentials. Princeton, N.J.: Princeton University Press, 2007. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,sso&db=e000xww&AN=286616&authtype=sso&custid=s5903540&lang=he&site=eds-live&scope=site&authtype=ip,sso&custid=s5903540.

25 New Zealand Security Intelligence Service. "Combined Threat Assessment Group." New Zealand Security Intelligence Service. Accessed April 23, 2023. https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/combined-threat-assessment-group/.

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

27 New Zealand Security Intelligence Service. "National Terrorism Threat Level." Accessed April 23, 2023. https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level/.

28 New Zealand Transport Agency. "Risk Register." Government. Waka Kotahi NZ Transport Agency. Accessed March 31, 2023. https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register/.

29 ProtectUK. "Threat Levels," March 12, 2022. https://www.protectuk.police.uk/threat-levels.

30 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.

31 Security Service MI5. "Joint Terrorism Analysis Centre." Accessed April 23, 2023. https://www.mi5.gov.uk/joint-terrorism-analysis-centre.

32 Shacklett, Mary E. "What Is Attack Vector?" Tech Target, April 2021. https://www.techtarget.com/searchsecurity/definition/attack-vector.

33 Strachan-Morris, David. "Threat and Risk: What Is the Difference and Why Does It Matter?" Intelligence and National Security 27, no. 2 (April 1, 2012): 172–86. https://doi.org/10.1080/02684527.2012.661641.

34 Thorne, David. "National Level Threat Assessment-Canadian Model." 2nd Workshop on Proactive Approach to Counter Terrorism-Report. Islamabad, Pakistan: United Nations Office of Drugs and Crime, April 12, 2018. https://www.unodc.org/documents/pakistan//Report-2nd-Workshop-Proactive-Approach-to-CT-web.pdf.

35 UKC3. "Cyber Cluster Operating Framework." UK Cyber Cluster Collaboration (blog). Accessed March 29, 2023. https://ukc3.co.uk/cyber-cluster-operating-framework/.

36 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. https://www.un.org/counter-terrorism/sites/www.un.org.counter-terrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

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 on Drugs and Crime. Guidance on the Preparation and Use of Serious and Organized Crime Threat Assessments: The SOCTA Handbook. New York, NY: United Nations, 2010. https://www.unodc.org/documents/organized-crime/SOCTA_Handbook.pdf.

39 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.

40 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.

41 United States Department of State. "About Us: Global Engagement Center." Accessed April 23, 2023. https://www.state.gov/about-us-global-engagement-center-2/.

42 Waitzman, Eren. "National Risk Register: Preparing for National Emergencies." UK Parliament: House of Lords Library, December 14, 2022. https://lordslibrary.parliament.uk/national-risk-register-preparing-for-national-emergencies/.

[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. To effectively address this threat, it is crucial to conduct comprehensive threat assessments that encompass a multidimensional analysis of the potential risks, vulnerabilities, and impacts associated with terrorists' adoption of new technology. By understanding the intricacies of this complex relationship, law enforcement can develop proactive strategies and deploy appropriate measures to mitigate the threats posed by terrorists' exploitation of emerging technologies.

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,[14] of which over 93 per cent are social media users.[15] Globally, it is estimated that in 2022 over 97 zettabytes[16] of information was generated.[17] Whilst such technology advancements provide the opportunity to transform society for the greater good, terrorist actors are taking advantage of the same technology for their own nefarious purposes. The use of new technologies for terrorist purposes poses significant challenges to Member States in countering terrorism – in particular – the use technologies that allow for anonymity and the ability to coordinate and operate remotely.

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

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

[15] Domo Data Never Sleeps, Data Never Sleeps 10.0 | Domo.

[16] One zettabyte equals to one billion terabytes.

[17] Statista, Total data volume worldwide 2010-2025 | Statista.

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 security and safety 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 the 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-terrorism 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, as well as the right to freedom of expression.

3.2.4 Gender, Technology, and Threat Assessment

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.[18] 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.[19] Evidence also suggests that terrorist groups instrumentalize gender in their online messaging; for example, Da'esh used contradictory gendered messaging strategically in their recruitment and communications, shifting their discourse according to their target group.[20] 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.[21]

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

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

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

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

[21] DCAF, ´Gender Equality, Cybersecurity, and Security Sector Governance – Understanding the role of gender in cybersecurity governance´. January 2023.

[IV]
Threat and Risk Assessment

4.1 Overview

When conducting counter-terrorism efforts, it is important to differentiate between threat assessment and risk assessment. The combination of these two practices lays the foundation for stakeholders and practitioners to effectively respond to potential dangers within their AOR. Largely, the threat describes the "who" and "what" of threat actors and their intended actions. The risk describes how likely it is for the threat to come to fruition and what the potential damage from this action will be.[22] As such, the implementation of a risk assessment can be built and accomplished by a foundation being created through the threat assessment.[23]

The threat assessment is the first element of this cycle. Threat is the product of capability and intent.[24] Capability includes the known abilities of the group, logistical resources, command and control capability, success rate of previous attacks, sophistication of previous attacks, level of training, and whatever is known of the capabilities that the group is trying to acquire.[25] In the context of counter-terrorism efforts regarding the exploitation of new technologies by terrorist actors, capability would include the types of new technologies at the disposal of the threat actor and how well the threat actor can operate or utilize the technologies. Intent here is a measurement of both the will and opportunity of a threat actor to commit an attack.[26]

When determining the risk of different threats, the author states that one must assess the probability (both likelihood and frequency) with which an attack may occur and the harm that it may cause.[27] Within the context of new technologies, harm can be understood to include both physical damage (either as a direct result of an attack or as a residual effect of damage to a system) or damage to a system (e.g., varying cyberattacks which can cause loss or leakage of data, system crashes, failure of critical infrastructure to function, etc.).[28]

It is also critical to consider the inclusion of gender perspectives into the planning, collection, analysis, and dissemination of threat assessment and intelligence products, so as to support the identification of overlooked signs of instability, as

[22] David Strachan-Morris, "Threat and Risk: What Is the Difference and Why Does It Matter?," *Intelligence and National Security* 27, no. 2 (April 1, 2012): 172–86, https://doi.org/10.1080/02684527.2012.661641.

[23] Strachan-Morris, 180.

[24] Strachan-Morris, 174.

[25] Strachan-Morris, 174.

[26] Strachan-Morris, 173.

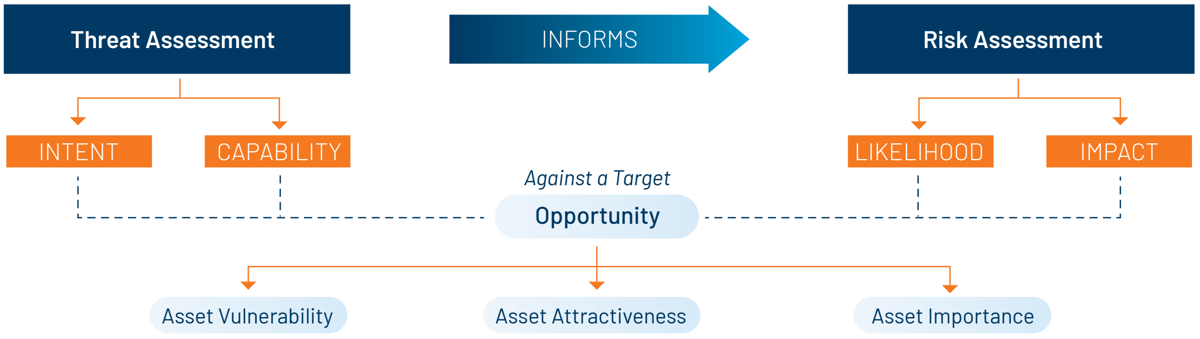
[27] Strachan-Morris, 173 and 180.

[28] Strachan-Morris, 180.

well as overcoming potential gender biases, and the development of a comprehensive grasp of social contexts and dynamics.[29] Integrating gender dimensions across all stages of the intelligence cycle, also enables anticipating and mitigating any potential adverse consequences of intelligence collection and dissemination for human rights of those affected. Hence, gender perspectives are not only essential to acquiring accurate and actionable intelligence, but also to ensure intelligence operations comply with international human rights and gender equality standards.

The diagram below illustrates threat assessment, risk assessment, their differences, and how they interact:

FIGURE 4



Threat and risk assessment is the process of evaluating potential threats by identifying potential threats and assessing the likelihood and potential impact of those threats with the goal of developing strategies and policies to mitigate or manage the risks associated with them. The threat and risk assessment process includes the identification of threats, and analysis based on the intent and capability of threat actors to commit an act of terror. The results of a threat assessment will be the foundation upon which the remaining steps in the cycle are based, as it provides the initial understanding of a potential terrorist threat.

Threat assessment is used to understand potential threats to individuals, organizations and/or Member States by considering factors such as the threat actor (their ideology, capability, and intent) and potential targets. It contributes to the development of policy choices and responses, and is an integral component in conducting counter-terrorism efforts, as it provides policymakers and other relevant stakeholders with a greater understanding of both the existing threats, as well as the types of resources that may be required to address these threats. One example of this is the way in which the use of threat assessments can identify uses of new technology by terrorist actors, or how new technology may be used as a resource to respond to new threats. Within the context of understanding the use of new technologies for terrorist purposes, threat assessments enable Member States to understand the potential threats that may arise as well as to deal with existing threats that demand attention at varying degrees through the process of threat prioritization.

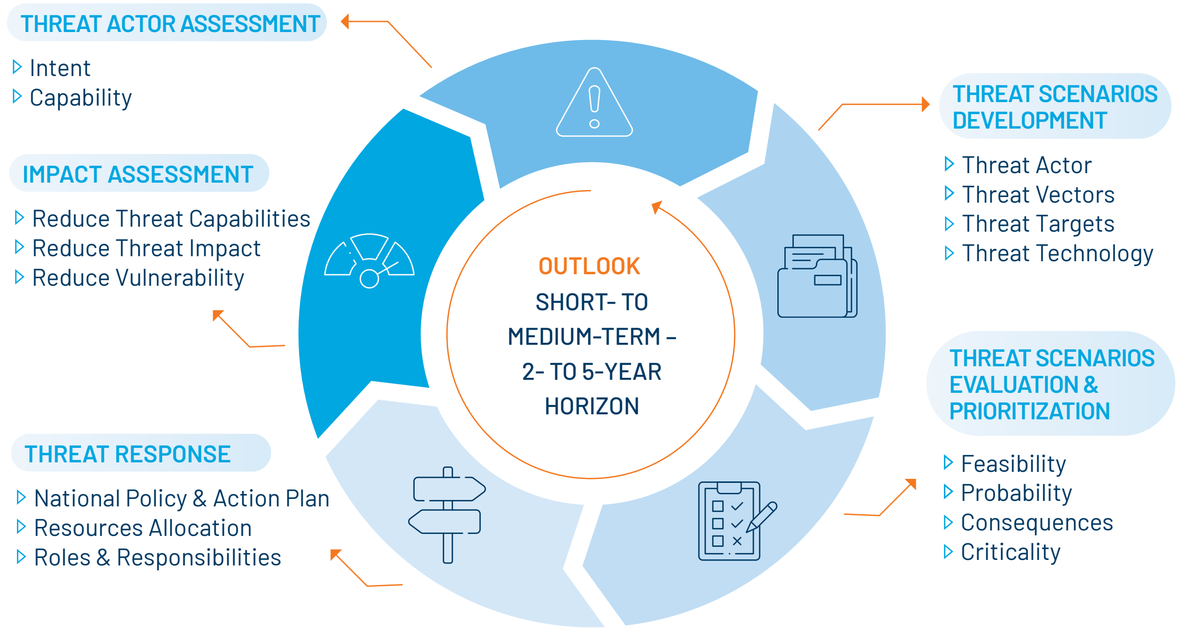
Threat and risk assessments provide a process for the development of a holistic understanding of threats, security measures, and the potential plans for decision-makers to combat those threats. Each of the following sections will provide an explanation of the key components needed in order to form the threat and risk assessment. It will cover threat assessment, as well as threat scenarios, threat actor and scenario evaluation, and risk prioritization, threat response, and the impact assessment of the previous components' response plan.

The following sections describe a methodology for threat and risk assessment and response, as well as resources for good practices within the field of threat and risk assessment as implemented across Member States and international organizations.

[29] Lauren Hutton et al., Intelligence and Gender, (OSCE, 2019).

4.2 Threat and Risk Management Cycle

FIGURE 5



THREAT ACTOR ASSESSMENT

- Intent
- Capability

IMPACT ASSESSMENT

- Reduce Threat Capabilities
- Reduce Threat Impact
- Reduce Vulnerability

THREAT RESPONSE

- National Policy & Action Plan
- Resources Allocation
- Roles & Responsibilities

OUTLOOK

SHORT- TO MEDIUM-TERM – 2- TO 5-YEAR HORIZON

THREAT SCENARIOS DEVELOPMENT

- Threat Actor
- Threat Vectors
- Threat Targets
- Threat Technology

THREAT SCENARIOS EVALUATION & PRIORITIZATION

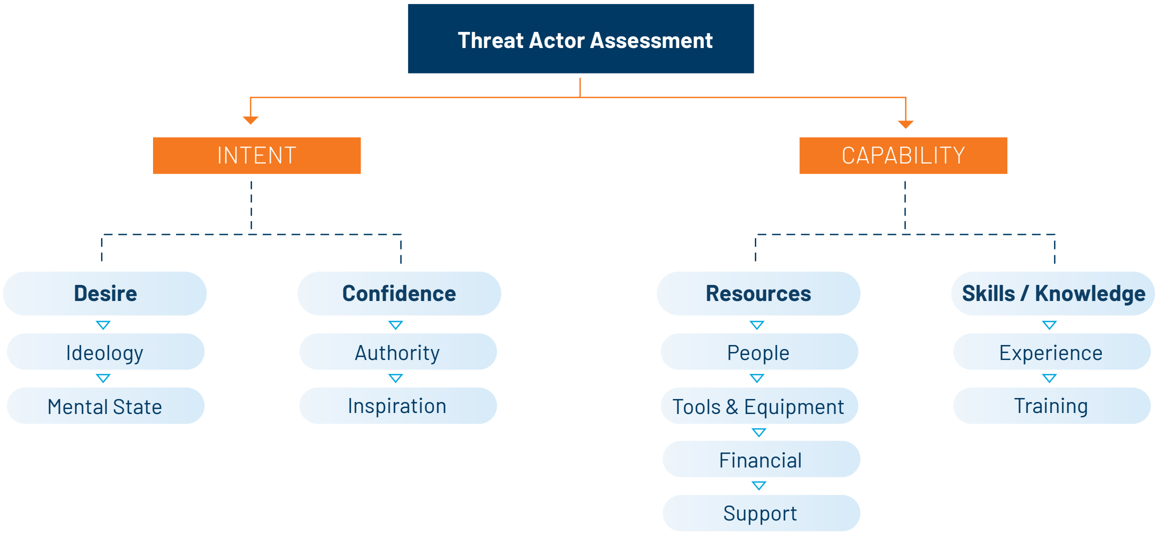
- Feasibility
- Probability
- Consequences
- Criticality

The threat and risk management cycle presented above is a structured process aimed at assessing potential threats to a country on a national level. It involves a series of stages that are taken to assess and mitigate potential threats and the risk that those threats pose. The "horizon" of a threat and risk management cycle refers to the time frame within which potential threats are evaluated and their risks managed. In the case when evolution of new technologies is considered as part of the threat and risk assessments, it may have a longer horizon that extends over a period of two to five years.

The framework for the threat and risk assessment model for the use of new technologies for terrorist purposes consists of the combination of multiple stages, which together form the threat and risk management cycle. It includes threat assessment, the development of threat scenarios, threat actor and scenario evaluation, and risk prioritization, threat response, and impact assessment.

4.2.1 Threat Actor Assessment

FIGURE 6



To conduct a threat actor analysis, there are multiple situational factors that need to be examined. Two of these factors are measures of intent and of capability. Here, intent refers to a combination of the threat actor's desire and their confidence. The capability of a threat actor describes both the resources at their disposal (e.g., financial, technological, manpower, etc.), and the skills or knowledge they possess to utilize their resources.

To understand the concept of intent with regard to threat actor analysis, it is also important to understand that intent (or motivation) is not a monolithic element, but is composed of multiple factors that serve to drive the threat actor to perpetrate an attack.[30] The motivation of a threat actor to commit an attack is "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."[31] These actions can be tied to underlying grievances tied

[30] Neil J. Smelser, "Motivation, Social Origins, Recruitment, Groups, Audiences, and the Media in the Terrorism Process," in *The Faces of Terrorism: Social and Psychological Dimensions*, Science Essentials (Princeton, N.J.: Princeton University Press, 2007), 92–119, https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,sso&db=e000xww&AN=286616&authtype=sso&custid=s5903540&lang=he&site=eds-live&scope=site&authtype=ip,sso&custid=s5903540.

[31] See UN Security Council Resolution 1566.

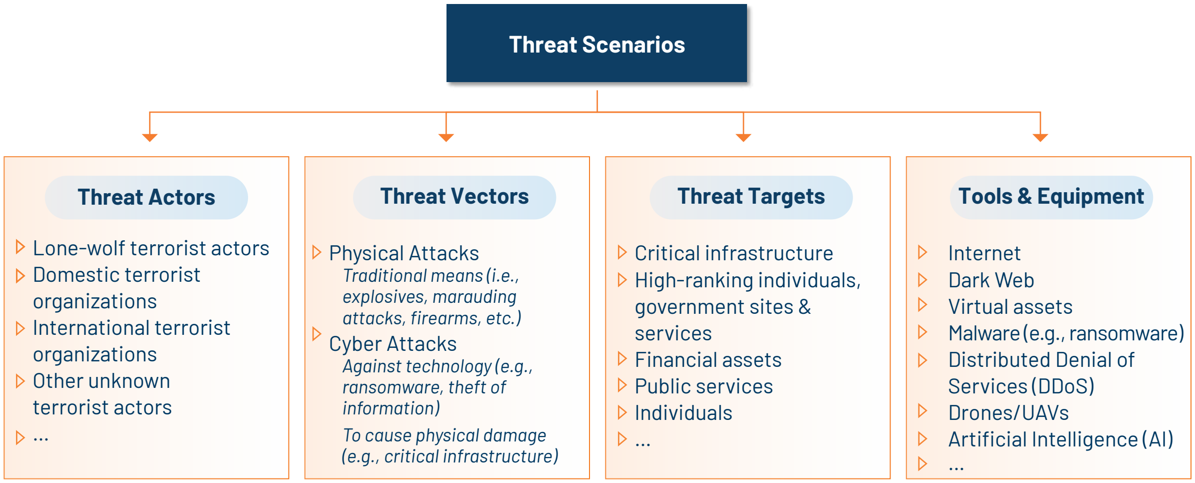
to religious, political, social, economic matters, or a combination thereof. Such a goal will also differ from threat actor to threat actor.[32] This includes understanding the reasons why the threat actor may want to engage in terrorism, or the threat actor's motivation or goal in carrying out a terrorist attack. Such factors can be ideological, tied to political beliefs, desire, or mental health, which can all impact the threat actor's intent to commit a terror attack. For example, misogyny is often present in narratives used to justify attacks by groups that operate on the basis of xenophobia, racism, and other forms of intolerance, or in the name of religion or belief, and they also tend to demonstrate intolerance regarding sexual orientation and gender identity.[33] By assessing the threat actor's intent, analysts can determine the potential targets and types of attacks that the actor may be planning. One of the other key components to understanding the intent behind a threat is understanding the intended target of the threat actor, as the awareness of one's audience and the impact of an attack on that audience can have a significant impact on the threat actor and the ways in which they execute an attack.[34]

Capability refers to the resources and skills/knowledge (or expertise) that the actor has at their disposal to carry out a terrorist attack. This includes access to people or an organization, tools and equipment (such as access to weapons or/and technology), training, and the level of financial or other means of support. By assessing the threat actor's capability, practitioners can determine how likely it is that the threat actor will be able to carry out a successful terror attack.

Both intent and capability are important factors in the analysis of threat actors, as a threat actor with a strong intent but limited capability may not be able to carry out a terrorist attack, while a threat actor with strong capability but a weaker intent may not be motivated to act. By considering both factors, the threat assessment can achieve a more comprehensive understanding of the threat posed by a particular threat actor or a terrorist organization and take appropriate measures to prevent or mitigate the threat of a terrorist attack.

4.2.2 Threat Scenario Development

FIGURE 7



Threat Scenarios
Threat Actors
Lone-wolf terrorist actors
Domestic terrorist organizations
International terrorist organizations
Other unknown terrorist actors
...
Threat Vectors
Physical Attacks
Traditional means (i.e., explosives, marauding attacks, firearms, etc.)
Cyber Attacks
Against technology (e.g., ransomware, theft of information)
To cause physical damage (e.g., critical infrastructure)
Threat Targets
Critical infrastructure
High-ranking individuals, government sites & services
Financial assets
Public services
Individuals
...
Tools & Equipment
Internet
Dark Web
Virtual assets
Malware (e.g., ransomware)
Distributed Denial of Services (DDoS)
Drones/UAVs
Artificial Intelligence (AI)
...

[32] Canadian Centre for Cyber Security, *An Introduction to the Cyber Threat Environment 2023-2024*, 2.

[33] A/77/266.

[34] Neil J. Smelser, "Motivation, Social Origins, Recruitment, Groups, Audiences, and the Media in the Terrorism Process," 106.

The second step in the threat and risk management cycle is the development of threat scenarios, in which the threat information gleaned from the threat actor analysis is further analysed to include an understanding of the threat actor(s), threat vectors, threat targets, and threat technology. Threat actor analysis and threat scenario are two interconnected concepts that are used in both threat and risk management and security planning. While threat assessment is the process of identifying and evaluating potential threats, the threat scenarios are specific examples of those threats that are used to plan and prepare for them. The result of the developed threat scenarios will be a deeper understanding of the mechanics behind a potential attack, technology being used to conduct the attack, and the attacker behind it.

Developing threat scenarios involves identifying potential threat actors that may use new technology for terrorist purposes. This could include known terrorist groups, individuals with extremist beliefs, or others who may seek to use technology for malicious purposes. Next, the capabilities of the threat actors must be analysed in addition to considerations regarding their access to new technologies and their technical expertise. This analysis can help determine the types of attacks that may be possible and the level of sophistication of those attacks. This should then be followed by analysing potential vulnerabilities or types of attacks that could impact that part, including the threat actors behind them.[35]

Part of developing test scenarios for threat and risk assessment and response is enabling stakeholders to take a proactive approach to threat management. Within a proactive approach, another action that stakeholders can take is the implementation of 'security by design'. The concept of security by design refers to the installation of security measures as something is being built such that it will be equipped to defend itself against a threat within its existing structure/build/framework.[36] Within the context of threat response to the use of new technologies for terrorist purposes, this can take forms such as the creation of SOPs for responding to specific forms of technology that can be easily adapted to fit multiple scenarios.

The resulting threat scenario encompasses each of the iterations of the types of attacks against different vulnerabilities.[37] Within this analysis, one of the key components in developing threat scenarios is the understanding of context, and the "combination of certain core elements."[38] In other words, the severity of the threat will differ depending on how many of the core elements exist within a given scenario. When preparing to protect against threats, developing and analysing threat scenarios becomes a key piece in preventing future threats from causing damage. A threat scenario describes a hypothetical example of different events that could occur and is generally designed after threats have been identified and assessed (Section 4.2.1). The purpose of creating threat scenarios is to be able to proactively prepare for and defend against future attacks before they become serious threats. Figure 8 below describes elements of each of the threat scenario components.[39]

[35] Volkmar Lotz, "Threat Scenarios as a Means to Formally Develop Secure Systems," in *Computer Security — ESORICS 96*, ed. Elisa Bertino et al. (Berlin, Heidelberg: Springer Berlin Heidelberg, 1996), 250; Mara Cole, "Towards Proactive Airport Security Management: Supporting Decision Making through Systematic Threat Scenario Assessment," *Journal of Air Transport Management 35* (March 1, 2014): 15, https://doi.org/10.1016/j.jairtraman.2013.11.002.

[36] 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.

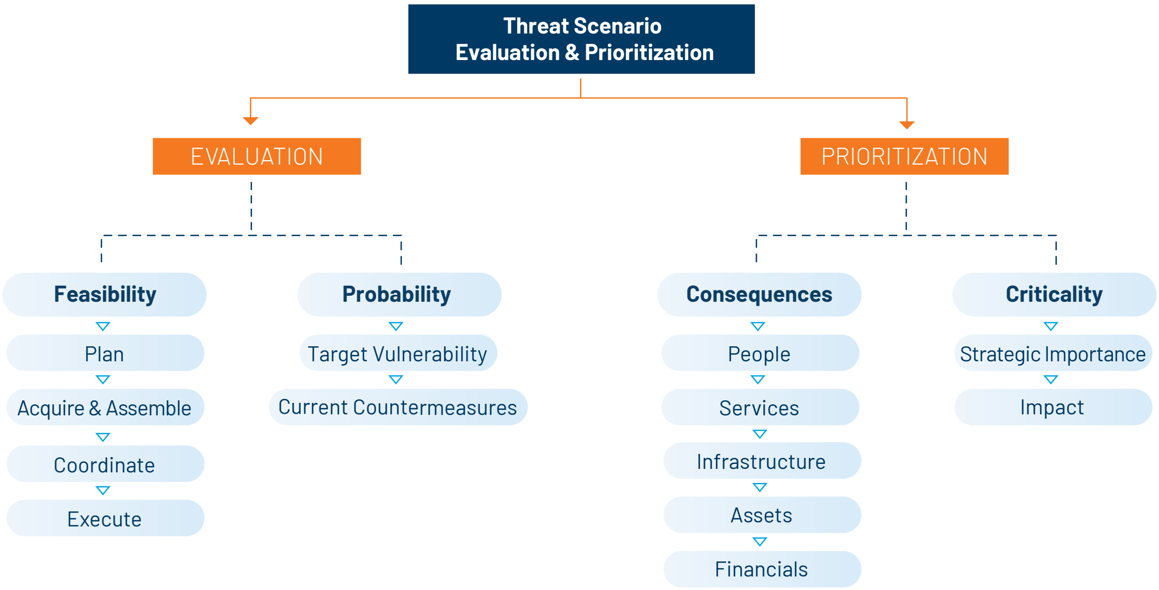
[37] Ibid.

[38] Cole, "Towards Proactive Airport Security Management: Supporting Decision Making through Systematic Threat Scenario Assessment," 12.

[39] For threat actors, see also Canadian Centre for Cyber Security, *An Introduction to the Cyber Threat Environment 2023–2024*, 2.

4.2.3 Threat Scenario Evaluation & Prioritization

FIGURE 8



The third step in the threat and risk management cycle is the threat actor and scenario evaluation and risk prioritization, in which threats and the risks that they pose are examined through the factors of feasibility, probability, consequences, and criticality. The goal of this part of the cycle is to enable practitioners to understand the severity of the threat and associated risks so that they make informed decisions about which threats require more resources allocated to a response to them. Th result of evaluation and prioritization will be the determination of a severity level through the traffic light model (which will be expanded upon below) which will aid in setting the policy options for threat response (see Section 4.2.4). Threat evaluation and risk prioritization serve as a means to validate how realistic a potential threat is and serves as a process to prioritize the most dangerous threats to a Member State. It enables the proper allocation of state resources to respond to or mitigate a threat, while also acknowledging that Member States do not possess the resources to address every threat that is detected. Threats need to be prioritized in order to maximize the impact of threat response efforts.

Before a risk can be prioritized, it needs to undergo an evaluation in which practitioners that are subject matter experts determine factors such as the feasibility of the presented threat as well as the probability that such a threat or attack could potentially happen. Measuring the feasibility of a potential attack involves understanding the threat actor's intent and capability, as well as the details regarding the attack that may be carried out. Should the intent, capability, and preliminary acts leading up to the attack not match up, the threat can be deemed low in feasibility. When discussing the probability or likelihood of an attack, the focus should be placed on analysing the potential risk of a terror attack that may occur. Target vulnerabilities within a State and the availability of a State's countermeasures must also be assessed. If the threat is feasible but the target is either not incredibly vulnerable and/or the countermeasures already in place to respond to potential threats are strong, the threat being assessed will be a lower priority than a threat that is feasible but the target either does not have proper defence mechanisms in place or has a vulnerability that have not yet been addressed.

After threats have been evaluated, the risks that they pose must be prioritized to ensure that a response plan is developed, and resources are effectively allocated. When prioritizing threats and their associated risks, factors to take into consideration include an understanding of both the consequences of a threat should it come to fruition and the criticality of the risk posed by the threat. Within the understanding of the risk posed by a threat, practitioners need to assess the potential impact of the new technology as part of a threat on points of infrastructure, services, and people.

Part of properly evaluating a threat is understanding how to best categorize it in order to efficiently be able to respond to it. In order to categorize the threat, its likelihood, impact, and threat control measures must be evaluated. Here, 'likelihood' refers to the likelihood of a threat occurring, and 'impact' refers to the severity and the scope of the impact. 'Threat control measure' refers to the policy or the technology in place to be able to defend against the threat. The table below provides a format which may be used for assessing and categorizing threats.

FIGURE 9

Threat	Likelihood	Impact	Initial Risk Rating	Current Countermeasures	Residual Risk
Description of the threat actor and likely scenario which includes the means and target	An assessment of the threat actor's likelihood to carryout the attack	If successful, what is the impact of the attack	A function of likelihood and impact of the threat scenario without any countermeasures	Description and assessment current countermeasures to reduce the threat	An overall assessment of risk by the threat actor **after** the current countermeasures are considered

An additional component in the threat evaluation and risk prioritization process involves rating the severity of a threat and its associated risks. In determining the severity of a threat and the associated risks, it is recommended to utilize a traffic light model in order to ease the ability to prioritize threats in a clear fashion.

Below is an illustrative model of how different levels of threat severity are highlighted and how they should be assessed when determining the severity level of a threat as part of the threat and risk assessment.

FIGURE 10

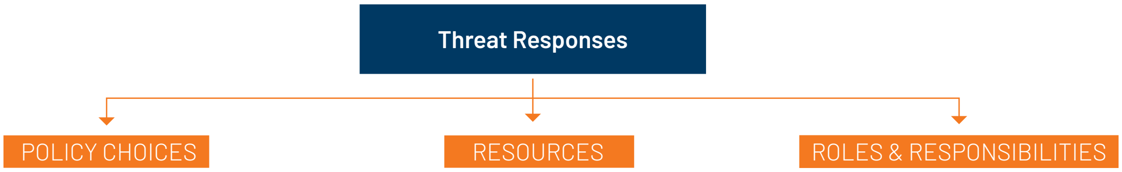
LIKELIHOOD					
Very Likely	MEDIUM	HIGH	VERY HIGH	VERY HIGH	VERY HIGH
Likely	MEDIUM	HIGH	HIGH	VERY HIGH	VERY HIGH
Somewhat Likely	LOW	MEDIUM	MEDIUM	HIGH	VERY HIGH
Unlikely	LOW	LOW	MEDIUM	HIGH	HIGH
Very Unlikely	LOW	LOW	LOW	MEDIUM	MEDIUM
	Minor	Limited	Moderate	Significant	Catastrophic
	IMPACT				

The mapping of what is considered low, medium, high, or very high may vary and is informed by decision-makers in setting the threshold, in other words known as the 'risk appetite'.

Another component in enabling policymakers' sufficient preparation for potential threats is the process of 'red teaming'. This process involves simulating potential threats so that the team involved in responding to threats can practice the proper response and learn where other weaknesses may lie in the threat response. This is accomplished by setting up a 'red team' whose job it is to simulate an attack.[40] An exercise of this nature will both help response teams practice proper protocol with regard to active threats, and will, at the same time, highlight elements of the protocol that need to be improved in order to move a threat response from the theoretical sphere to a practical sphere where it would be put into use, if a threat was detected and required an immediate response.

4.2.4 Threat Responses

FIGURE 11



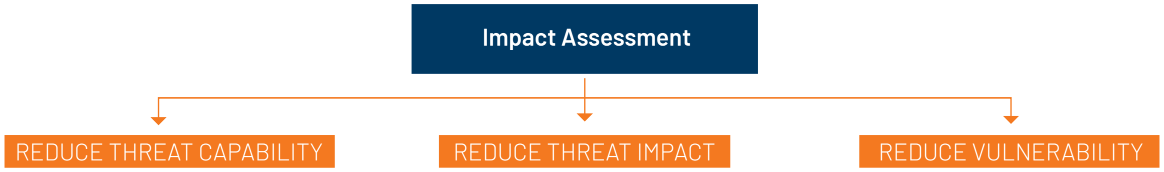
[40] David Romyn and Mark Kebbell, "Terrorists' Planning of Attacks: A Simulated 'Red-Team' Investigation into Decision-Making," *Psychology, Crime & Law 20, no. 5* (May 28, 2014): 483, https://doi.org/10.1080/1068316X.2013.793767.

The fourth step in the threat and risk management cycle is threat response, in which practitioners create a plan of action, discuss the required resources needed to respond to a threat, and assign roles and responsibilities to specific practitioners. The goal of this part of the cycle is to lay the foundation for future actions to be taken to prevent or lessen the damage of an attack. The result of the threat response step will be a detailed plan of action, a list of resources required to fulfil the plan of action, and a list delineating the roles and responsibilities of each of the practitioners involved in the plan of action.

The creation of a plan of action includes details regarding which resources will be allocated to the threat response. Any threat response must be consistent with fundamental human rights principles, including those of legality, proportionality, and non-discrimination. The response also needs to consider the gender dimensions of the threat, so as to ensure that the response is aligned to the specific needs and vulnerabilities of different genders. In order to ensure an effective threat response, it is also critical to define the roles and responsibilities of each of the stakeholders to ensure that all moving parts work towards a cohesive goal, and that the steps of one stakeholder do not negate the efforts of another.

4.2.5 Impact Assessment

FIGURE 12



Impact assessment involves a comprehensive analysis of various factors, such as the nature and severity of the terrorist threat, the effectiveness of the proposed counter-terrorism measures to reduce threat capabilities, the threat impact and reduced target vulnerabilities. Impact assessment is a process of evaluating and analysing the potential effects or consequences of a proposed policy and operational plan to mitigate the threat. It is a tool to identify and manage potential threats and responses associated with a decision or action.

In this stage, the impacts are identified and evaluated for the consideration of the potential impacts of a proposed action in decision-making processes and can help to ensure that any negative impacts are minimized, and any positive impacts are maximized. Overall, the goal of impact assessment is to provide policymakers and decision-makers with an understanding of the potential effects of a threat assessment, enabling them to make informed decisions about the best course of action to take.

[IV]
Good Practices for Threat Assessment

5.1 Overview

By implementing good practices, threat and risk assessment practitioners at the national level can improve the quality and accuracy of their assessments, better identify potential threats, and make informed decisions about appropriate interventions. In preparing the model for the threat and risk management cycle, multiple sources regarding threat and risk assessment and management practices from different Member States were consulted. The following sections provide some of the findings from this research in the form of good practices. In principle, a threat and risk assessment can be composed of different types of assessments on different levels (local, regional), and the different levels may be combined together to form a national-level understanding of the terrorism threats with each limited-scope assessment contributing to the overall picture. Additionally, these practitioners need to be prepared for threats from new and emerging technologies, that are used or can potentially be used as an integral part of a terrorist attack. While each approach adopted by each Member State may be dependent on the country's counter-terrorism framework, counter-terrorism strategy, coordination, and operation mechanism, the following are some recommendations for good threat and risk assessment practices, the adoption of which will benefit counter-terrorism threat and risk assessment practitioners with enhanced capabilities to implement new technology use for terrorist purposes as part of the threat and risk management cycle (as presented in Section 4).

5.2 Multi-Agency Approach & Fusion Centres

An effective threat actor and scenario assessment process involves the collaboration between various government agencies (including law enforcement, intelligence, border security, etc.). Implementing the process as a multi-agency effort allows for a more comprehensive and holistic understanding of potential threats. One of the good practices proposed in a publication by the European Commission, CIVI.POL Conseil, and Royal United Services Institute (RUSI) is the notion of mapping stakeholders.[41] Here, relevant stakeholders are defined as "partners, target groups and beneficiaries."[42]

[41] CIVI.POL Conseil and Royal United Services Institute, "Operational Guidelines on the Preparation and Implementation of EU Financed Actions Specific to Countering Terrorism and Violent Extremism in Third Countries" (European Commission, 2018), 32, https://issat.dcaf.ch/sqi/download/131230/2684696/EU-CT-CVE-guidelines.pdf.

[42] Ibid.

The United Kingdom Government CONTEST programme is a framework that enables the reduction of the risk to the UK through the involvement of multiple government agencies.[43] In this programme, threat levels are set independently by the Joint Terrorism Analysis Centre (JTAC).[44] JTAC brings together counter-terrorist expertise from the police and from government departments and agencies, such that information may be analysed and processed through shared efforts. JTAC is a self-standing organization comprised of representatives from 16 governmental departments and agencies. It issues threat levels and warnings of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies, and also produces more in-depth reports on trends, terrorist networks, and capabilities.[45]

Denmark's approach to preventing and countering violent extremism and radicalization is based on extensive multi-agency collaboration between various social-service providers, the educational system, the health-care system, the police, and the intelligence and security services.[46] The Centre for Terror Analysis (CTA) publishes an annual Assessment of the Terrorist Threat to Denmark, determining the general terrorist threat level in Denmark and assessing the threat to Danish interests abroad. CTA was set up as a Danish fusion centre for analysis and assessment of the potential or likelihood of a terrorist threat to Denmark and the country's interests abroad. It comprises of staff from four Danish authorities (the Danish Security and Intelligence Service, the Danish Defence Intelligence Service, the Ministry of Foreign Affairs, and the Emergency Management Agency). The terrorist threat level in the Assessment of the Terrorist Threat to Denmark reflects cases and trends in Denmark and abroad which have a combined effect on the assessment.[47]

In New Zealand, the Combined Threat Assessment Group (CTAG) is an inter-agency group hosted and led within New Zealand Security Intelligence Service (NZSIS).[48] The group gives independent assessments to government agencies about threats to New Zealand, New Zealanders, and New Zealand's interests abroad. CTAG is made up of analysts from NZSIS and other government agencies, including the New Zealand Police Force, New Zealand Defence Force, the Government Communications Security Bureau (GCSB), the Civil Aviation Authority and Aviation Security Service, and the Department of Corrections. CTAG is also supported by other agencies, including the Ministry of Foreign Affairs and Trade, the Ministry of Transport, and the New Zealand Customs Service.

In Canada, the Integrated Terrorism Assessment Centre (ITAC) determines the national threat level of the country. It works as a partnership between government agencies within Canada and full-time staff within the centre. ITAC also works in partnership with threat assessment bodies in Australia (NTAC), New Zealand (CTAG), the United Kingdom (JTAC), and the United States (NCTC).[49] Here, the model not only works with an internal multi-agency team but extends the country's efforts for cooperation with international teams, which can help broaden elements such as the scope of the threat intelligence gathered on specific threat actors. Sweden's National Centre for Terrorist Threat Assessment relies on multi-agency cooperation between the military, the National Defence Radio Establishment, and the Swedish Security Service. In this model, the agencies work together to gather and analyse intelligence and assess the country's threat level.[50]

[43] 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.

[44] "Joint Terrorism Analysis Centre," Security Service MI5, accessed April 23, 2023, https://www.mi5.gov.uk/joint-terrorism-analysis-centre.

[45] Ibid.

[46] Ann-Sophie Hemmingsen, "An Introduction to the Danish Approach to Countering and Preventing Extremism and Radicalisation" (Copenhagen, Denmark: Danish Institute for International Studies, 2015), https://www.ft.dk/samling/20151/almdel/reu/bilag/248/1617692.pdf.

[47] Centre for Terror Analysis (CTA), "Assessment of the Terrorist Threat to Denmark" (Denmark: Centre for Terror Analysis (CTA), March 2022), https://politi.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-terrortruslen-mod-danmark/vtd_2022_uk.pdf.

[48] New Zealand Security Intelligence Service, "Combined Threat Assessment Group," New Zealand Security Intelligence Service, accessed April 23, 2023, https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/combined-threat-assessment-group/.

[49] David Thorne, "National Level Threat Assessment-Canadian Model," 2nd Workshop on Proactive Approach to Counter Terrorism-Report (Islamabad, Pakistan: United Nations Office of Drugs and Crime, April 12, 2018), 87, https://www.unodc.org/documents/pakistan//Report-2nd-Workshop-Proactive-Approach-to-CT-web.pdf.

[50] Ministry of Justice of Sweden, *Prevent Preempt Protect: The Swedish Counter-Terrorism Strategy* (Sweden: Government Offices of Sweden, 2014), https://www.government.se/contentassets/b56cad17b4434118b16cf449dbdc973d/en_strategi-slutlig-eng.pdf.

5.3 Risk-Based Approach

Several countries and international organizations use a risk-based approach in their counter-terrorism threat actor and scenario assessments. By adopting a risk-based approach, organizations can make informed decisions, allocate resources effectively, and manage risks proactively, reducing the likelihood of adverse terror events and their impact. In a risk-based approach, the likelihood and potential impact of a terrorist attack are assessed in order to prioritize the allocation of resources and the development of response plans.

The United Kingdom (UK) National Risk Register (NRR) is the public-facing version of the national security risk assessment (NSRA), the government's classified assessment of the national security risks facing the UK or its overseas interests. It provides information to the public on the "most significant risks" that the government has assessed could occur and which could have a wide range of impacts on the country, such as terrorist attacks or natural events like flooding. It also details how the government is identifying, assessing, preparing for, and dealing with such potential emergencies. In another example, 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 and a breakdown of the roles that each stakeholder should play in the event that a threat of attack materializes.

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction. FATF recommends that a risk-based approach for countering money laundering and/or terrorist financing (ML/FT) should be an essential part of the basis upon which resources are efficiency allocated. Furthermore, it indicates that risk assessments carried out by countries should be used for determining higher and lower risks that may then be addressed by applying enhanced measures or allowing simplified measures respectively. FATF recommends that determining the sources of data, type of information, tools, and which analytical techniques will be used is therefore essential in conducting risk assessments. For a national risk assessment to arrive at the most accurate findings, it is advisable that as much of analysis and conclusions presented within the assessment as possible be based on objective information. The information used in a risk assessment may be derived from various sources (both qualitative and quantitative).

5.4 Measuring Threat Levels

Measuring the threat level is an important aspect of the threat actor and scenario assessment as well as of threat management. Threat level measurements allow individuals and organizations to assess the level of threat associated with a terror situation or event and take appropriate actions to mitigate or manage that threat.

UK's JTAC[51] measures the threat level in any given circumstance with several factors, including:

- **Available intelligence.** This will often be based on a wide range of information, some of which is often fragmentary, including the level and nature of current terrorist activity, comparison with events in other countries, and previous attacks.

[51] "Threat Levels," ProtectUK, March 12, 2022, https://www.protectuk.police.uk/threat-levels.

- **Terrorist capability.** An examination of what is known about the capabilities of the terrorists and the method they may use based on previous attacks or from intelligence. This would also include the analysis of the potential scale of the attack.
- **Terrorist intentions.** Using intelligence and publicly available information to examine the overall aims of the terrorists and the ways they may achieve them including what sort of targets they would consider attacking.
- **Timescale.** The threat level expressed and the likelihood of an attack in the near future.

New Zealand's CTAG Assessments involve looking at a threat actor's intent to conduct an attack, and their capability to carry it out. Assessments are a qualitative and analytical judgement. CTAG uses structured analytical techniques and tools to help with assessments. It considers the domestic terrorism context and relevant international threat factors.[52] CTAG assess threat levels by considering the current intent and capability of individuals or groups to undertake an act of terrorism. Canada's ITAC produces threat assessment products that address and evaluate the national threat level as well as products that evaluate how the threat level may shift with regard to a "special event" (e.g., a summit).[53] The addition of "special event" assessments highlights that the threat level (national or on a smaller, more local scale) may increase should there be a high-profile event, but that such a shift is event-dependent and temporary relative to the consistency and scope of the rest of the national threat assessment. Within the scale of threat levels, the Canadian model also notes how, in a general way, a threat may impact the public and its ability to adhere to routine conditions.[54]

In measuring the threat level, one of the good practices observed is the creation of a scale through which to organize the threat levels of the country. New Zealand's Security Intelligence service presents a five-level model for threat level assessment ranging from very low to extreme.[55] Canada and the Netherlands also provide models for threat levels that may be helpful to draw upon in which the actions taken at each level are further elaborated upon. In the Canadian model, threat levels are split into five categories: very low, low, medium, high, and critical, signifying threats as ranging from highly unlikely to highly likely (and perhaps, immanent).[56] From the earliest stages, the Canadian model notes that measures are already in place to secure and protect the population from a potential attack. When a threat level is deemed to be "medium", additional safety measures are put in place. In both the "high" and "critical" levels, the security measures continue to increase and there is an added element of communication with the public regarding potential actions that they may need to take to ensure their safety.[57] Like in the previous models, the model from the Netherlands runs on a scale of five levels ranging from level 1 (minimal) to level 5 (critical).[58] In addition to publishing this model, the National Coordinator for Counter-Terrorism and Security publishes a few infographics a throughout the year in which the threat level is noted alongside explanations behind the designation of the threat level.[59]

[52] "National Terrorism Threat Level," New Zealand Security Intelligence Service, accessed April 23, 2023, https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level/.

[53] Thorne, "National Level Threat Assessment-Canadian Model," 87–89.

[54] See chart in ibid, 88.

[55] "National Terrorism Threat Level."

[56] Public Safety Canada, "Canada's National Terrorism Threat Levels," consultations, August 25, 2016, https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html.

[57] Canada.

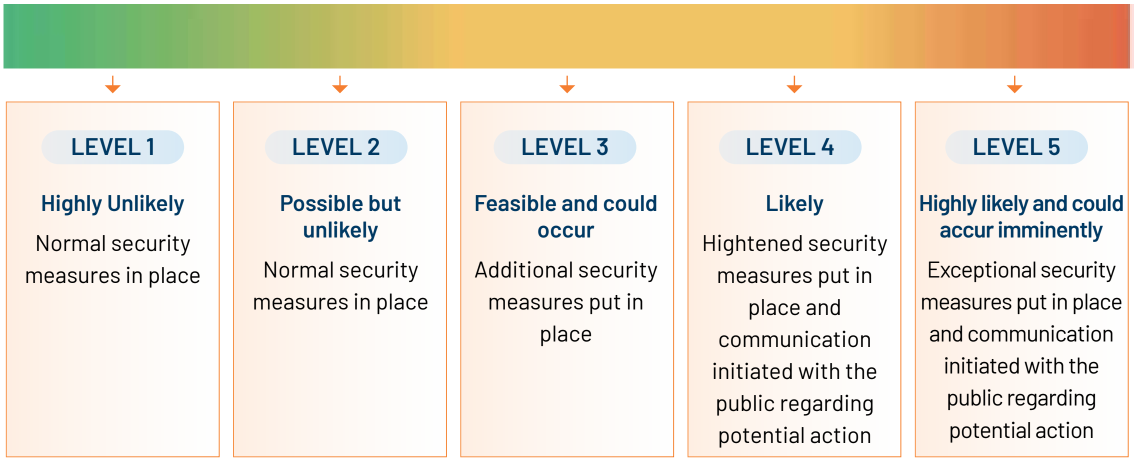
[58] National Coordinator for Security and, "Terrorist Threat Assessment Netherlands," Ministry of Justice and Security: National Coordinator for Security and (Ministry of Justice and Security, May 14, 2020), https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands.

[59] See e.g., National Coordinator for Security and , "NCTV's Terrorist Threat Assessment: Threat in and to the Netherlands Has Become More Multifaceted and Diffuse – News Item – National Coordinator for Security, and Ministry of Justice and Security: National Coordinator for Security and (Ministry of Justice and Security, November 7, 2022), https://english.nctv.nl/latest/news/2022/11/07/nctvs-terrorist-threat-assessment-threat-in-and-to-the-netherlands-has-become-more-multifaceted-and-diffuse.

BOX 1. Example from Canada's Public Safety – National Terrorism Threat Levels

TREAT LEVEL*

This diagram represents the concept of threat level as understood in the policiesof Canada, New Zealand, and the Netherlands. Each of these models has five levels, but each described these levels differently. The resulting diagram is a combination of the three models.



LEVEL 1

Highly Unlikely

Normal security measures in place

LEVEL 2

Possible but unlikely

Normal security measures in place

LEVEL 3

Feasible and could occur

Additional security measures put in place

LEVEL 4

Likely

Hightened security measures put in place and communication initiated with the public regarding potential action

LEVEL 5

Highly likely and could accur imminently

Exceptional security measures put in place and communication initiated with the public regarding potential action

***Model and phrasing for each ot the stages taken from the following sources:**
Canada, Public Safety. "Canada's National Terrorism Threat Levels." Consultations, August 25, 2016. https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html.
National Coordinator for Security and Counterterrorism. "Terrorist Threat Assessment Netherlands." Ministry of Justice and Security: National Coordinator for Security and Counterterrorism. Ministry of Justice and Security, May 14, 2020. https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands.
New Zealand Security Intelligence Service. "National Terrorism Threat Level." Accessed April 23, 2023. https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level/.

5.5 Gathering and Analysing Threat Information

An integral component of executing effective threat actor and scenario assessments and threat management is a strong basis in the gathering and analysis of threat information. The following is a collection of good practices gleaned from documents of Member States regarding the collection and analysis of threat information.

A good practice for practitioners regarding threat evaluation as it relates to the use of new technologies for terrorist purposes is to perform an analysis of cyber threat intelligence (CTI). The United Kingdom's model for CTI defines it as an intelligence situational assessment that takes into consideration both the potential threats and the threat actors behind them as it relates to the use and abuse of technology.[60] One of the methods for collecting this intelligence is OSINT, a form of intelligence, by its very nature would be more easily accessible to stakeholders and have fewer resources like other types of intelligence. Additional practices that can be used for CTI include collaboration with members of the private sector in tech companies and in academia to both gather and analyse available data on potential threats. As part of conducting CTI, it is critical to develop regularly produced knowledge products in which the intelligence gathered is assessed and centralized into a report so that stakeholders may have an easily accessible situational assessment of different threats.[61]

[60] Flanders et al., *Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts, 15.*

[61] Ibid, 36.

The report published by the European Commission, CIVI.POL Conseil, and Royal United Services Institute (RUSI) also notes a good practice for the gathering and analysis of threat information. This report highlights the importance of a "context analysis" to be paired with the threat analysis. An approach of this nature involves "taking into account any political, economic, security and environmental issues at the local, national and regional levels." [62] ISO 31000 also advocates for a context-informed approach in risk management.[63] According to their guidelines, an understanding of "internal" and "external" contexts helps stakeholders "customize" their response to a particular group and understand the ways in which the context of certain threats may impact the ensuing risk associated with the threat.[64] Using such an approach in forming a threat actor analysis and in developing threat scenarios will help stakeholders have a more thorough understanding of the threat landscape prior to the risk analysis process.

5.6 Continuous Assessment

Threat and risk assessments must be regularly updated. Just as threat actors can develop and evolve over time and with new technology, so too can countries grow and develop in the ways in which they may prepare for such threats. This is done in part to understand shifts in a given threat due to counter-terrorism efforts or other changes.[65] This process is ongoing, with regular reviews and updates based on new intelligence and changing circumstances such as technology advancements. Additionally, the methodology through which a threat is assessed and managed must undergo an impact assessment to ensure that it continues to be both relevant to the reality that it is trying to understand and in its efficacy.

The United States assesses effectiveness and adjusts operations with an annual independent strategic assessment informed by research, intelligence, and analysis to ensure measurable progress toward the strategic objectives. These assessments identify strategic weaknesses and recommend adjustments to the strategy to outpace dynamic adversaries. They also aim to ensure progress is sustainable and addresses the full range of contemporary national security challenges.[66] According to the United States' counter-terrorism strategy, this is a product of research, intelligence, and analysis in which each assessment builds off a previous assessment completed. The production of an annually threat assessment report highlights the ways that threats have changed and are expressed through the level of severity of the threat, the nature of the threat actor and resources available to the threat actor, and the resources that the country has to combat the potential threats faced. In New Zealand, the national terrorism threat level is formally reviewed annually but can also change at any time based on the current intelligence picture.

[62] CIVI.POL Conseil and Royal United Services Institute, "Operational Guidelines on the Preparation and Implementation of EU Financed Actions Specific to Countering Terrorism and Violent Extremism in Third Countries," 30.

[63] International Organization for Standardization, *ISO 31000 Risk Management-Guidelines*, Second (Switzerland: International Organization for Standardization, 2018), 3 and 6, https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf.

[64] Ibid.

[65] 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.

[66] Ibid.

5.7 Enhancing Intelligence-Sharing

Information sharing and a culture of cooperation that is multi-disciplinary and multi-level remain key for a solid threat assessment that can form the basis of a counter-terrorism policy.[67] This includes sharing intelligence between government agencies and with international partners. It is important to educate widely on threat assessment in order to enable cooperation and understanding from multiple sources/entities to make scope for a wider impact.[68] Spain's counter-terrorism strategy, for example, focuses on the ability for data to be used and to be both accessible to those who need to access it and protected from those who should not be privy to that type of information.[69] It includes the need for encryption in order to share data across shareholders from differing sectors.[70]

One example of a good practice within information sharing is the model of The Common Database (CDB) as practiced by the Belgian Coordination Unit for Threat Analysis (CUTA). The database serves as a means for different government agencies to access and add to data regarding the following categories: foreign terrorist fighters, home-grown terrorist fighters, hate propagandists, potentially violent extremists, and persons convicted of terrorism. [71]

Information shared between stakeholders in different locations must be done through a secure means to enable the stakeholders to maintain operational security in matters such as threat actor assessment and threat response. Like in Spain's model, the CDB model bases its secure information sharing model on the "need-to-know principle," meaning that users have access to different amounts of data (and have the ability to contribute) based on the type of information relevant for their specific role.[72] In regulating the type and amount of information available from the database to different users, a higher level of operational security is maintained, thereby reducing the possibility that the information can reach users who should not be privy to it.

Another way in which such a register/database 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 centralization in ultimately reporting and sharing information with national stakeholders with regard to threats.[73] The Belgian Strategic Note Extremism and Terrorism (Strategy T.E.R.) presents a similar model of having more localized practitioners operating towards counter-terrorism efforts. This model has a localized task force and also makes use of a localized team that addresses the prevention of radicalization.[74] These local

[67] 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.

[68] 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/.

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

[70] Ibid.

[71] "The Common Database (CDB)," Coordination Unit for Threat Analysis (CUTA), accessed April 23, 2023, https://cuta.belgium.be/the-common-database-cdb/.

[72] Ibid.

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

[74] "The Strategic Note Extremism and Terrorism (Strategy T.E.R.)," Coordination Unit for Threat Analysis (CUTA), accessed April 23, 2023, https://cuta.belgium.be/action-plan-against-radicalism-plan-r/.

levels report to the National Task Force (NTF), which partners on a larger scale with the different government and military agencies. 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 sphere of responsibility.

With regard to information-sharing, it is also important to make the reporting of information easier, particularly for members of the public that would like to report critical pieces of information regarding threats. In order to accomplish this, the public needs to both be informed about threatening behaviours or actions and the channels that they can turn to in order to report an incident for further addressing of the matter by stakeholders who have been trained to do so.

This can be accomplished through school and workplace training for the identification of signs of threatening behaviour. Additionally, the platform through which members of the public are able to share threat information with the relevant authorities must be both easy to access and use to prevent lack of reporting due to its difficulty. One example of a site that serves as both a central and easily accessible model for threat reporting is a New Zealand site, in which the public can both note their assessment of the severity of the threat information and share it with the relevant authorities.[75] This site also provides the opportunity for individuals to submit the information anonymously.

5.8 Research and Innovation

The current reality is that modern technology requires an effective response that anticipates how technologies impact the terrorist threat to equip law enforcement authorities with the right tools. As part of conducting threat assessments and knowing how to properly respond to the threats using new technologies or threats stemming from the exploitation of new technologies, research and innovation are integral in ensuring that practitioners have an updated understanding of potential threats and can continue to develop new means for responding to the threats. As such, the European Commission, CIVI.POL Conseil, and Royal United Services Institute (RUSI) recommend that efforts towards continuously understanding technological advancements and the potential impact that it can have when exploited by terrorist actors, as an important component of understanding threat scenarios (See Section 4.2.2).[76] Such research and innovation should involve cross-agency and cross-sector efforts and should include contributions from academia as well as the tech industry.

EU security research 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.[77] EU-funded security research also aims to strengthen the early detection capacity of potential terrorist threats, notably by exploring the use of Artificial Intelligence to allow for more efficient and accurate processing of large amounts of 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.[78]

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

[76] CIVI.POL Conseil and Royal United Services Institute, "Operational Guidelines on the Preparation and Implementation of EU Financed Actions Specific to Countering Terrorism and Violent Extremism in Third Countries," 30.

[77] European Commission, *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond.*

[78] 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).

[APPENDIX A]

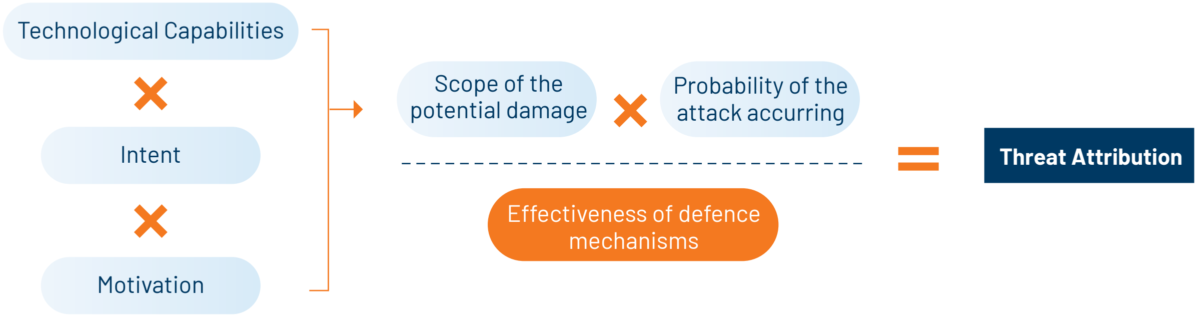
Illustrative Model Equation for Threat Attribution

A.1 Overview

The figure below provides a model through which practitioners can assess the threat attribution of a specific threat. Here, threat attribution refers to an assessment of the risk as informed by an assessment of the threat itself.[79] The model presented here focuses on how capabilities are assessed. Due to the focus of this guide on new technologies, the initial factor of "information, knowledge, and opportunity", which at large describes "capability", was amended to "technological capabilities."[80]

According to the model presented in the figure, one must first account for the technological capabilities, intent, and motivation of the threat actor. The result of this informs the analysis of the probability of the attack occurring and the scope of the potential damage it may cause. Following this step, practitioners assess the types of defences that they have in place and how effective those defences may be against the potential threat.[81] The understanding of the available capabilities in defending against a threat impacts the threat attribution. The more a country has effective measures in place to defend against threats, the lower the threat attribution will be.

FIGURE 1[82]


Technological Capabilities
×
Intent
×
Motivation
Scope of the potential damage
×
Probability of the attack accurring
Effectiveness of defence mechanisms
=
Threat Attribution

[79] Erez Magen and R., "Enabling Advancements in Security-Danger and Opportunities," Maarachot (Systems) (blog), March 29, 2022, https://www.maarachot.idf.il/2022/.

[80] Ibid.

[81] Ibid.

[82] Graphic translated and adapted from Erez Magen and R., "Enabling Advancements in Security-Danger and Opportunities."

[APPENDIX B]

Example of Abusive Use of Technology by Terrorists

B.1 Overview

The table below highlights new technologies and their potential exploitation by terrorist actors as well as their potential for use by practitioners to respond to terrorism. Understanding the ways in which new technology 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 terrorists may exploit the technology for malicious actions and there will also be new ways in which technology may be used to respond to terrorism.

TABLE 1. Illustrative examples

Technology Type	Malicious Use by Terrorist	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[83] • Terrorism financings • 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[84] • 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
Social Media	• Recruitment to terrorist organizations through propaganda spread on social media • Disinformation campaigns • Spread terrorist content and distortive narratives, propaganda and/or material to be posted as propaganda on social media through an encrypted channel[85] (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

[83] 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.

[84] 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.

[85] 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.

Dark Web	• 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 cryptocurrency/NFT for terrorist financing • Use of cryptocurrency/NFT in money laundering activities	• NFTs can also be used for counter-narrative functions to terrorist propaganda (known example of ISIS using NFTs to spread propaganda)[86] • Fundraising/crowdfunding in Virtual Assets can also 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
3D Printing	• Building weapons/parts of weapons	• 3D Printing can also be used to print parts that can be used to counter-terrorism, such as UAS parts, which, in turn, can be used for ISR

[86] 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.

Artificial Intelligence/ Machine Learning	• Disinformation campaigns and cyber-attacks powered by AI[87] • Weapons powered by AI[88] • Social engineering campaigns[89] • May be used to upgrade malicious exploits or writing malwares for sophisticated cyberattacks	• Use of AI/Machine Learning to automate monitoring and analysis in CTI (e.g., automation sorting of posts on social media/online forums)[90] • Big Data analysis powered by AI[91] • Using Natural language processing (NLP) techniques to detect symbols and patterns used by terror groups online • Monitoring for misinformation and disinformation[92]

[87] 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.orgsites/www.un.orgfiles/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

[88] See e.g., ibid, 33–35.

[89] Ibid, 45.

[90] 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.

[91] Ibid, 17.

[92] 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.

[APPENDIX C]

Threat Assessment Guiding Questions

C.1 Overview

The following section provides questions for use by stakeholders and law enforcement to help guide the different stages of the threat and risk assessment process, as described earlier in the document. The goal is to highlight factors that are critical to the threat and risk assessment process that should not be overlooked.

C.2 Guiding Questions

TABLE 1. **General Questions for Beginning the Threat Assessment Process**

Threat Landscape	• What new technologies are relevant to counter-terrorism efforts? • How are these technologies being exploited by terrorists or potential threat actors? • What are the potential risks and vulnerabilities associated with these technologies? • Are there any new technologies that could enhance vulnerabilities or pose new security challenges?
Threat Detection	• Are there any indicators or warning signs suggesting the potential for violence or harm? • What are the potential targets or locations at risk?
Information Gathering and Analysis	• What information sources are available (e.g., open-source intelligence, interviews, records)? • How reliable and credible are the information sources? • Are there any gaps in the information that need to be addressed? • What information should be shared while ensuring privacy and legal considerations?

TABLE 2. Threat Actor Assessment

Intent	• Who (group / individuals) are targeting the State and what is their motives? • What may be the motivations that the terrorist has to act? • Does the terrorist belong/adhere to a specific ideological/political group? • What may the threat actor be looking to gain through this attack (i.e., objectives)? • Who are the potential threat actors involved in technology-based terrorism? • Are there any indicators of radicalization or extremist ideologies related to the use of technology?
Capability	• What forms of new technology does the threat actor have access to? • How well does the threat actor know how to use the technology? • What are the resources available to the threat actor? • Has the threat actor previously launched an attack? • What kind of experience/training does the threat actor have? • Can the threat actor's feasibility procure the materials or services to deliver the attack? • What are the technical capabilities and expertise required to carry out technology-based attacks? • Are there any known or emerging threat actors or groups with the necessary technological capabilities? • What is the level of sophistication and access to resources of potential threat actors?

TABLE 3. Threat Scenario

Threat Actor	• Is the threat actor acting alone or as part of a group? • What is the affiliation of the threat actor?
Threat Vector	• Is the anticipated attack a physical attack or a cyberattack? • If it is a cyberattack, is there a potential threat to critical infrastructure? • If cyber, what are the likely means (tactics, techniques, procedures) to conduct the attack? • If cyber, what is the objective (i.e., disrupt critical infrastructure services, ransomware for funding, etc.)?
Threat Targets	• Which elements of critical infrastructure might be vulnerable to an attack? • Which people/places may be likely targets of an attack? • Does the attack target civilians?
Threat Technology	• Does the planned attack utilize new technology? If so, what is the technology intended for use in the attack? • Can new technology be used as a means to respond to the planned attack?

TABLE 4. Threat Scenarios Evaluation and Prioritization

Feasibility	• How likely is the occurrence of such attacks based on intelligence, historical data, or other relevant factors?
Probability	• Are there any specific factors or events that may increase the likelihood or severity of technology-based attacks?
Consequences	• What are the potential consequences of technology-based attacks in terms of casualties, infrastructure damage, or societal impact?
Criticality	• What are the vulnerabilities and weaknesses in critical infrastructure, systems, or networks that could be exploited by technology-based attacks?

TABLE 5. Threat Response

National Policy & Action Plan	• What response plans and mitigation strategies should be implemented in the event of a technology-based attack? • How can technology be leveraged to enhance response capabilities, such as real-time monitoring, incident response systems, or communication networks? • Are there any legal or ethical considerations that need to be addressed when responding to technology-based threats? • What documentation procedures should be followed throughout the threat assessment process? • How should the findings and recommendations be reported and shared with relevant parties?
Resources Allocation	• How effective are existing security measures in mitigating or preventing these vulnerabilities? • Are there any emerging technologies that could enhance vulnerabilities or pose new security challenges? • Do counter-terrorism personnel possess the necessary knowledge and skills to understand and address technology-based threats? • What training programmes or capacity-building initiatives are required to enhance technical expertise and awareness? • How can partnerships with technology experts, academia, or private industry support ongoing training and knowledge exchange?
Roles and Responsibilities	• Are there other agencies or stakeholders involved that need to be consulted or informed?

TABLE 6. Impact Assessment

Impact Assessment	• How effective are existing security measures in mitigating or preventing these vulnerabilities? • Can the impact be assessed as reducing the threat, reducing vulnerability, reducing threat impact?

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)