



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



INTERPOL



Funded by
the European Union

Cybersecurity and New Technologies



Guide for Establishing Law
Enforcement Cooperation with
Technology Companies in
Countering Terrorism

Disclaimer

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

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

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.

Copyright

© United Nations Office of Counter-Terrorism (UNOCT), 2023

United Nations Office of Counter-Terrorism

United Nations Headquarters

New York, NY 10017

www.un.org/counterterrorism

© The International Criminal Police Organization (INTERPOL), 2023

200, Quai Charles de Gaulle

69006 Lyon, France

www.interpol.int/en

Contents

Joint Foreword.....	5
Acknowledgements.....	6
Terms and Definitions.....	6
Executive Summary.....	8
[I]	
BACKGROUND	9
1.1 Overview	9
1.2 CT TECH Initiative.....	10
1.3 Document Purpose and Use	11
[II]	
APPROACH.....	13
2.1 Overview	13
2.2 Guiding Framework.....	13
2.3 Methodology.....	15
[III]	
INTRODUCTION	17
3.1 Overview	17
3.2 New Technologies and Counter-Terrorism	18
[IV]	
COOPERATION MODELS	21
4.1 Overview	21
4.2 Common Challenges for Cooperation	22
4.3 Motivation for Cooperation.....	24
4.4 Key Guiding Principles for Cooperation.....	25
4.5 Other Considerations.....	26
[V]	
COOPERATION MODEL 1 – INFORMATION SHARING	28
5.1 Purpose.....	28
5.2 Objectives	28
5.3 Cooperation Approach.....	29
[VI]	
COOPERATION MODEL 2 – CAPABILITY AUGMENTATION.....	30
6.1 Purpose.....	30
6.2 Objectives	30
6.3 Cooperation Approach.....	30

[VII]	
COOPERATION MODEL 3 –	
BUSINESS ALLIANCE / COUNCIL	32
7.1 Purpose.....	32
7.2 Objectives	32
7.3 Cooperation Approach.....	32
[VIII]	
COOPERATION MODEL 4 – ACTIVE INVESTIGATIONS	34
8.1 Purpose.....	34
8.2 Objectives	34
8.3 Cooperation Approach.....	34
[APPENDIX A]	
PRACTICAL GUIDELINES ON REQUESTING DATA FROM ONLINE SERVICE	
PROVIDERS	37
A.1 Overview	37
A.2 Types of Information.....	37
A.3 Request Types.....	39
A.4 Common Platforms.....	47

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:

- **Mr. Adam Calabro** – Manager, Cybercrime Investigation Group: Imminent Threats, Google LLC;
- **Ms. Anne Craanen** – Head of Research and lead for Terrorist Content Analytics Platform Tech Against Terrorism;
- **Ms. Gretchen Bueermann** – Research and Analysis Specialist Centre for Cybersecurity World Economic Forum;
- **Mr. Michael Maffei** – Senior Security Counsel Google LLC;
- **Mr. Michael O’Keefe** – Counter-Terrorism Specialist, Terrorism Prevention Branch of United Nations Office on Drugs and Crime (UNODC); and
- **Mr. Nagham El Karhili** – Programming and Partnerships Lead, GIFCT.

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 criminal charges against an individual or an entity and the court proceedings, judgement 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
ICT Companies	Information and Communications Technology (ICT) companies, refers to businesses that provide products or services related to information technology, telecommunications, or both.

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).

Intelligence	The product resulting from collecting, developing, disseminating, analysing, and interpreting of information gathered from a wide range of sources, to inform decision makers for planning purposes to take decisions or actions – strategic, operational or tactical level. Intelligence should be collected, retained, used and shared in compliance with relevant Member State obligations under international human rights law.
Criminal Investigations	The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support the prosecution in legal proceedings.
Law Enforcement Actions	Typically describes law enforcement actions taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e., content removal, asset seizures), etc.
New Technologies	While the New Technologies terminology covers a wide range of different technologies, ² for the purpose of this document, new technologies refers to the use and abuse of such new technologies as the Internet, social media, cryptocurrencies, facial recognition, and the darknet. ³
Online Service Providers	Companies or organizations that offer services over the Internet. These services can encompass a wide range of areas such as email, social media platforms, cloud storage, web hosting, search engines, e-commerce platforms, and various other online communication or infrastructure services.
Rehabilitation	In a criminal justice context, the term ‘rehabilitation’ is used to refer to interventions managed by the corrections system with the aim to change the offender’s views or behaviour, to reduce the likelihood of re-offending and prepare and support the offender’s reintegration back into society.
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.
Technological Services	Refers to the utilization of technology and its associated services to offer solutions to the users of ICT companies.
Terrorism	Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism. ⁴
Zettabyte	One zettabyte is equal to one billion 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 See S/RES/1566 (2004), para. 3.

Executive Summary

The importance of fostering cooperation between Law Enforcement Agencies (LEAs) and Information and Communications Technology (ICT) companies is vital for ensuring public safety. The technology landscape and its usage are rapidly evolving, and so too, are the methods abused by terrorists. As a result, this cooperation is crucial in countering the use of new and emerging technologies for terrorist purposes and harnessing the ICT capabilities for public safety.

This document aims to facilitate and highlight cooperation best practices between LEAs and ICT companies in mitigating the use of technology for terrorist activities.

While there are inherent challenges in this endeavour, we also identify many opportunities that can be harnessed effectively.

Our guidance for good practices with ICT companies is based on four primary models of cooperation:

- **Information Sharing:** This encourages the sharing of pertinent threat information, deepens understanding of terrorist tactics, and highlights potential threats linked to the abuse of ICT company services. This method equips LEAs and ICT companies with the necessary tools to respond to terrorist activities in a proactive and effective manner.
- **Capability Augmentation:** Many commercial entities offer their services to the intelligence community, deploying their technological resources in areas such as the darknet and cryptocurrency. Engaging with these entities can significantly enhance LEA's ability to combat terrorism.
- **Business Alliance / Council:** Forming a business alliance enhances counter-terrorism capabilities by facilitating the sharing of technologies, techniques, and knowledge about potential threats. This alliance aims to anticipate and prepare for upcoming challenges, understanding the potential risks and opportunities presented by future technologies.
- **Active Investigations:** A key goal of cooperation between LEAs and ICT companies lies in gathering information pertinent to ongoing terrorist investigations and countering the use of ICTs for terrorist purposes. This collaboration significantly contributes to enhancing public safety through proactive prevention and diligent prosecution.

Fostering this cooperation can bring about substantial improvements in public safety and counter-terrorism efforts, despite the challenges. The best practices and guidelines proposed herein serve to inform and guide Member States in this crucial mission.



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)⁵ 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)⁶ and 2396 (2017)⁷ call on Member States to act cooperatively when taking national measures to prevent terrorists from exploiting ICTs for terrorist purposes. 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,⁸ the Analytical Support and Sanctions Monitoring Team noted that “Many Member States highlighted the evolving role of social media and other online technologies in the financing of terrorism and dissemination of propaganda”, with platforms cited by Member States which include Telegram, Rocket.Chat, Hoop, and TamTam, among others. **ISIL supporters using platforms on the dark web** for storing and accessing training materials that other sites decline to host as well as **for acquiring new technologies** were also cited in the report.

Countering terrorist use of new and emerging technologies for terrorists’ purposes was discussed at the dedicated special meeting of the United Nations Security Council’s Counter-Terrorism Committee’s (CTC), which took place on 28–29th October 2022 in New Delhi and resulted in the adoption of a non-binding document, known as the Delhi Declaration.⁹

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**”

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

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

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

8 Thirtieth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISO: (Daesh), Al-Qaida and associated individuals and entities [S/2022/547\(undocs.org\)](#).

9 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’ LEAs in leveraging new and emerging technologies in the fight against terrorism.

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





TABLE 1. CT TECH Outcomes and Outputs

Outcome 1: Effective counter-terrorism policy responses towards the challenges and opportunities of new technologies in countering terrorism in full respect of human rights and the rule of law.



Output 1.1

Knowledge products developed for the design of national counter-terrorism policy responses to address challenges and opportunities of new technologies in countering terrorism in full respect of human rights and the rule of law is developed.



Output 1.2

Increased awareness and knowledge of good practices on the identification of risks and benefits associated with new technologies and terrorism in full respect of human rights and the rule of law.



Output 1.3

Increased capacities of selected Partner States to develop effective national counter-terrorism policy responses towards countering terrorist use of new technologies and leveraging new technologies to counter-terrorism in full respect of human rights and the rule of law.

Outcome 2: Increased law enforcement and criminal justice operational capacity to counter the exploitation of new technologies for terrorist purposes and use of new technologies to prevent and counter-terrorism in full respect of human rights and the rule of law.



Output 2.1

Practical tools and guidance for law enforcement on countering the exploitation of new technologies for terrorist purposes and use of new technologies to prevent and counter-terrorism in full respect of human rights and the rule of law is developed.



Output 2.2

Partner States' law enforcement and criminal justice institutions have enhanced skills to counter the exploitation of new technologies for terrorist purposes and use of new technologies to counter-terrorism in full respect of human rights and the rule of law.



Output 2.3

Increased international police cooperation and information sharing on countering terrorist use of new technologies and using new technologies to counter-terrorism.

1.3 Document Purpose and Use

The aim of this document is to support LEAs and ICT companies in establishing cooperation and coordination mechanisms for countering the use of new and emerging technologies for terrorist purposes.

The document aims to raise awareness of and provide an overview on good practices for LEAs in establishing a working relationship with ICT companies in their efforts to prevent violence and combat terrorism.

1.3.1 Scope

This document aims to provide practical advice and tools for LEAs, especially in countries with a less developed private sector ecosystem, to collaborate effectively with ICT companies. It may also be helpful for ICT companies to understand the scope of collaboration, the various methods available for cooperation with LEAs, and the potential challenges they may encounter.

Further, this document does not address individual Member States' local contexts in terms of legal requirements, human rights record, the rule of law, industry maturity and access, among others, which all may impact the levels of cooperation between LEAs and ICT companies.

1.3.2 Target Audience

This guide is designed for LEAs and counter-terrorism agencies of Member States, as well as ICT companies.

1.3.3 Benefits

By establishing good and effective cooperation with technology companies, LEAs can achieve the following:

- Gain better insight into key trends in the use of technology platforms and services for terrorist purposes;
- Increase coordination between LEAs and ICT companies to proactively and effectively counter the use of technology platforms and services for terrorist purposes;
- Leverage ICT companies' technical expertise in counter-terrorism operations;
- Provide ICT companies domestic-level insight into counter-terrorism operations to help them focus their operations and proactively address terrorist misuse of their platforms; Share more relevant information to obtain intelligence and evidence faster and with a greater rate of success; and
- Improve the sharing of threat information and mutually reinforce learning and understanding of developing threats, enhancing capabilities to adopt industry solutions to counter-terrorism.

1.3.4 Limitations

Recognizing that both terrorist tactics and the technology landscape are dynamic and constantly changing, this document cannot foresee, address, or provide good practices for all scenarios, platforms, or technologies services. It is intended to provide guidance and approaches based on the current understanding of terrorist misuse and abuse of technology services.

Cooperation between ICT companies and LEAs will depend on local regulations, which may vary based on the jurisdiction, as well as methods to keep human rights safe and address privacy concerns. It should be noted that this document cannot comprehensively cover all the legal nuances of each jurisdiction and its impact on the cooperation.

It aims to help countries identify the most relevant channels for collaboration and anticipate challenges that may arise over time.



Approach

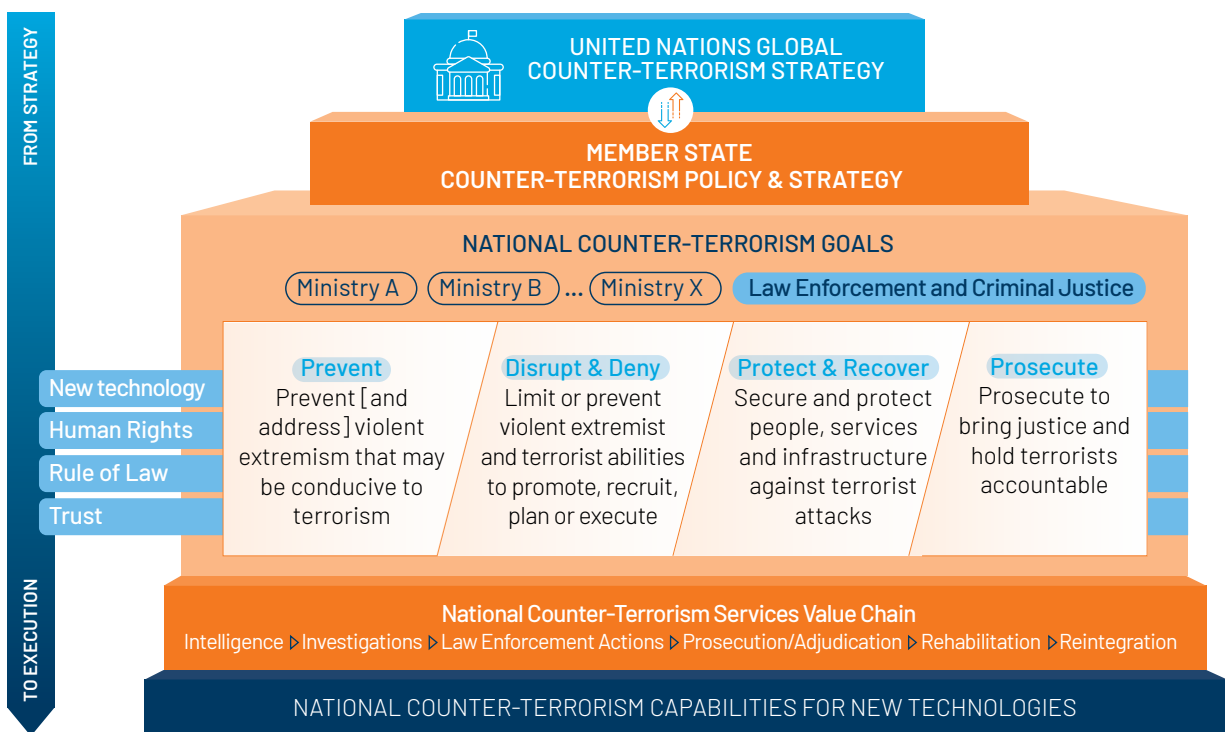
2.1 Overview

The report seeks to support and enable Member States to enhance cooperation between LEAs and ICT companies in countering the use of new and emerging technologies for terrorist purposes, which are aligned to the United Nations Global Counter-Terrorism Strategy (GCTS) and in full respect of human rights and the rule of law.

2.2 Guiding Framework



FIGURE 2



The guiding framework is a conceptual model that is intended to guide, align, and inform the development of the report. It seeks to ensure coherence from strategy to execution between the United Nations Global Counter-terrorism Strategy (GCTS) and a Member State's National Counter-terrorism Policy and Strategy goals and outcomes, services, and capabilities from a law enforcement and criminal justice perspective, regarding new technologies.

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

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

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

To achieve the counter-terrorism outcomes and goals, Member States' national law enforcement and criminal justice authorities have a set of tools at their disposal. These include, but are not limited to 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.
Intelligence	The product resulting from collecting, developing, disseminating, analysing, and interpreting of information gathered from a wide range of sources, to inform decision makers for planning purposes to take decisions or actions – strategic, operational or tactical level. Intelligence should be collected, retained, used and shared in compliance with relevant Member State obligations under international human rights law.
Criminal Investigations	The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support criminal justice proceedings.
Law Enforcement Actions	Typically describes law enforcement actions taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e., content removal, asset seizures), etc.
Rehabilitation	In a criminal justice context, the term 'rehabilitation' is used to refer to interventions managed by the corrections system with the aim to change the offender's views or behaviour to reduce the likelihood of re-offending and prepare and support the offender's reintegration back into society.
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.

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

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

2.3 Methodology



This document was developed and informed by a wide range of inputs which include stakeholder consultation, desktop research, CT TECH Initiative programme documents, Expert Group Meetings (EGM), internal analysis and guidance, and the guiding framework as described above in Section 2.2. From these activities the key outputs of this document include identifying different cooperation models, suggests an approach to consider when implementing a cooperation model, and provides practical guidelines for requesting information from online service providers.

2.3.1 Expert Group Meetings and Consultation

This guide has been developed with inputs from experts through Expert Group Meeting (EGM) sessions, as well as individual consultations and reviews. The EGM convened a diverse group of experts and practitioners from counter-terrorism, law enforcement agencies (LEAs), human rights, the private sector, academia, and civil society. The objective was to discuss effective strategies for countering terrorist use of new technologies, leveraging new technologies in counter-terrorism efforts, identifying good practices in this regard, and addressing risks, challenges, and practices that require caution.

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	United Nations Security Council (CTED), the state of international cooperation for lawful access to digital evidence, 2022.
2	United Nations Vienna, data disclosure framework, general practices developed by international service providers in responding to overseas government requests for data, 2021.
3	United Nations Vienna, practical guide for requesting electronic evidence across borders, 2021.
4	INTERPOL, E-evidence collection guidelines, 2018.
5	Directive (EU) 2017/541 on combating terrorism impact on fundamental rights and freedoms, 2021.
6	Council of Europe, Economic Crime Division Directorate General of Human Rights and Legal Affairs France, cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines (revised study and guidelines), 2020.
7	GNET King's College London, tackling online terrorist content together: cooperation between counter-terrorism law enforcement and technology companies, Professor Stuart MacDonald and Andrew Staniforth, 2023.
8	ICT & CTED, Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes, 2016.





Introduction

3.1 Overview

In an increasingly interconnected world where digital landscapes are perpetually evolving, the fight against terrorism necessitates a multi-faceted and collaborative approach. This guide is focused on identifying, developing, and promoting best practices for cooperation between ICT companies and LEAs in the global endeavour to combat terrorism.

ICT companies play a crucial role in this fight, given the vast expanse of data they possess and their potential to act as conduits for vital information sharing. Simultaneously, LEAs are at the forefront of counter-terrorism efforts, relying heavily on data analysis and intelligence to thwart potential threats.

However, effective collaboration between these two entities can often be complex due to distinct operational procedures, legal constraints, and data privacy concerns. It becomes essential, therefore, to establish an optimum framework that fosters mutual understanding and streamlined cooperation.

This guide seeks to navigate these complexities and build a robust partnership model that respects both the operational requirements of LEAs and the business protocols of ICT companies. Drawing on insights from entities like the Counter-Terrorism Committee Executive Directorate (CTED) and guidelines from international bodies such as the United Nations and INTERPOL, this guide aims to create a sustainable and efficient cooperative environment that enhances our collective capacity to fight terrorism.

Establishing partnerships with ICT companies can prove to be a challenging endeavour, given that every company operates under distinct procedures and collaboration protocols when interacting with LEAs. Numerous ICT firms even provide unique platforms specifically designed to handle requests from LEAs, each having its own designated point of contact. The United Nations has promulgated a useful handbook¹⁰ aimed at facilitating the process of requesting electronic evidence across international borders. It is recommended that Member States leverage this guide as a beneficial resource, given its comprehensive compilation of information pertinent to cooperation with all leading ICT enterprises.

Various strategies exist for establishing collaborative relationships with ICT companies. While our method diverges from some, we have incorporated elements of key cooperation principles gleaned from the Counter-Terrorism Committee Executive Directorate (CTED).¹¹ This organization has provided insights into the diverse operating methods ICT companies utilize when partnering with LEAs.

¹⁰ United Nations Vienna, practical guide for requesting electronic evidence across borders, 2021.

¹¹ United Nations Security Council (CTED), the state of international cooperation for lawful access to digital evidence, 2022.

3.2 New Technologies and Counter-Terrorism

Today, the advancements of digital technologies, data, and the Internet have led to a hyperconnected world of which information is accessed, shared, and received nearly instantaneously. As of 2022, nearly 70 per cent of the global population uses the Internet,¹² of which over 93 per cent are social media users.¹³ Globally, it is estimated that over 97 zettabytes¹⁴ of information is generated annually in 2022.¹⁵ 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. Terrorist use of new technologies poses significant challenges to Member States in countering terrorism. Terrorists' use of new technologies allows 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 LEAs. For example, such technologies have the ability to allow for LEAs 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-terrorist use of such technologies, to include leveraging and adopting the use of new technologies.

3.2.1 Countering the Use of New Technologies for Terrorist Purposes

Advances in ICT and their availability have made it attractive for terrorist and violent extremist groups to exploit the Internet and social media to facilitate a wide range of activities, including incitement, radicalization, recruitment, training, planning, collection of information, communication, preparation, propaganda, and financing. For their purposes, terrorist groups also expertly exploit and manipulate gender inequalities, norms and roles, including violent masculinities. For example, Da'esh skilfully recruited women through social media, adapting their messages to appeal to women speaking different languages and living in different social, economic, and cultural contexts in Western Europe, Central Asia, and the Middle East and North Africa, often tapping into women's experience of gender inequalities. Terrorists also use encrypted communications and the darknet 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 and Law Enforcement

New technologies present endless opportunities for LEAs to effectively counter-terrorism while upholding responsible practices with respect to international human rights law. Narrative 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

¹² ITU Global Connectivity Report 2022, <https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/>.

¹³ Domo Data Never Sleeps, [Data Never Sleeps 10.0 | Domo](#).

¹⁴ One zettabyte equals to one billion terabytes.

¹⁵ Statista, [Total data volume worldwide 2010-2025 | Statista](#).

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.

These actionable insights by 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 technologies responsibly, law enforcement can significantly enhance their counter-terrorism efforts and safeguard the safety and security of communities.

3.2.3 Human Rights and New Technologies

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

3.2.4 Gender, Technology, and Law Enforcement

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.¹⁶ 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.¹⁷ 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.¹⁸ 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.¹⁹

Integrating gender dimensions within law enforcement activities 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.

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

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

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

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





[IV]

Cooperation Models

4.1 Overview

Four broad cooperation models were identified in which LEAs and ICT companies can effectively work together towards a common goal of counter-terrorist use of new technologies for terrorist purposes. This chapter will broadly describe the cooperation models, key challenges and opportunities, key guiding principles for cooperation.

The first model, Information Sharing, facilitates the real-time exchange of threat information. This exchange boosts situational awareness and provides insights into key trends, enabling a proactive approach to counter-terrorism, and the formation of an effective communication network, which empowers ICT companies to prevent the misuse of their services by potential threats.

The second model, Capability Augmentation, enables LEAs to outsource specific needs, thereby operating with enhanced effectiveness and resource flexibility. This model leverages the technical prowess of ICT companies, effectively broadening the capabilities of LEAs and enabling them to adapt swiftly to evolving threat landscapes.

In the third model, referred to as the Business Alliance, broader collaboration is facilitated. This model encourages LEAs and ICT companies to overcome insular perspectives, enhancing their collective awareness, and enabling them to prioritize areas of mutual interest. It emphasizes joint strategies, shared responsibilities, and common goals in combating terrorism.

Lastly, the fourth and most common model of cooperation is Active Investigation Cooperation. This model supports active investigations by providing data and technological aid for both disruption and prosecution of terrorists. It involves ICT companies working directly with LEAs, providing real-time data and technical assistance, and enhancing the speed and efficiency of investigations.

These four models, each with their unique advantages and applications, provide a comprehensive framework for strengthening the collaboration between LEAs and ICT companies in the effort to combat terrorism.



FIGURE 4

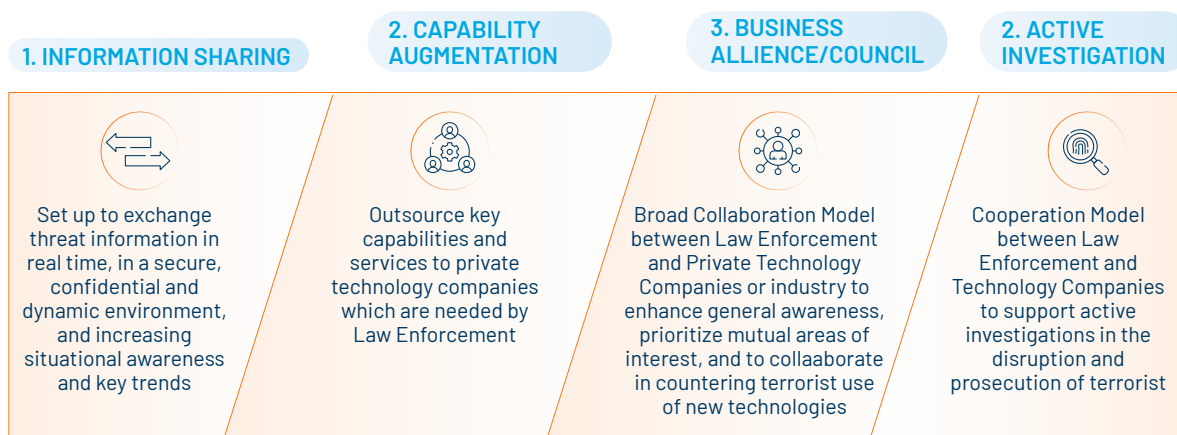


TABLE 4. Models of Cooperation

Information Sharing	Facilitate bi-lateral information sharing to include exchanging relevant threat information, understanding terrorist trends and tactics in using technology for malicious activities, alerting and taking action on suspicious or illegal behaviour. Additionally, it is important to prioritize identifying threats related to terrorist abuse of ICT company services, platforms, or products. By prioritizing these aspects, the cooperation can effectively address the challenges posed by terrorist activities.
Capability Augmentation	Commercial companies provide intelligence-gathering services to the intelligence community for a fee, investing resources and technology in various fields such as the darknet or cryptocurrency. Collaborating with such companies could be beneficial for both parties, as many have developed capabilities that LEAs can use to combat terrorism more effectively.
Business Alliance / Council	Establishing a business alliance aims to enhance the capabilities of fighting terrorism by sharing technologies and techniques, and gaining knowledge about potential threats. This collaboration can assist LEAs in better preparation for upcoming threats and provide insights into future developments to mitigate terror risks. The primary objectives of this council are to explore potential risks and opportunities that future technologies may unfold.
Active Investigations	The main goal of cooperation between LEAs and ICT companies is to collect data related to terrorist investigations and prevent terror groups from abusing their services. This cooperation is crucial for enhancing public safety through prevention and prosecution.

4.2 Common Challenges for Cooperation

Often there are good intentions and desires by LEAs and ICT companies to work together in countering terrorism. However, there are common challenges that limit the effectiveness and level of cooperation. Due to inherent differences in their motivations and interests, LEAs and the ICT companies may have conflicting perspectives, making collaboration a challenging process. Each operate with distinct mindsets and approaches that can create challenges to effective collaboration. Some common challenges which impact cooperation include the following:



TABLE 5. Common Challenges

Common Challenges	
Privacy & Human Rights Concerns	Cooperation between LEAs and ICT companies may raise substantial privacy concerns, particularly regarding sharing personal data. Private sector actors may be hesitant to share sensitive information with LEAs due to concerns about potential privacy rights violations. For example, encryption provides the privacy and security necessary for online freedom of expression, especially for vulnerable groups. ICT companies must protect user data and share only such information in accordance with relevant laws and regulations, especially when the request involves content removal, which may appear to be a violation of freedom of speech. Therefore, ICT companies must adopt transparent policies and practices that inform users about how their data is collected, stored, and shared with law enforcement.
Lack of Knowledge and Awareness or Miscommunication	One of the most significant challenges in interagency cooperation is the lack of coordination of expectations. LEAs often has unrealistic expectations or misunderstandings about what ICT companies can provide in terms of scope of data it retains, retention period, volume, delivery, and content-removal. This can lead to frustration, delays, or refusal to cooperate by ICT companies. On the other hand, ICT companies may not understand how terrorist groups abuse their services and what kind of data LEAs needs to prevent or investigate such activities.
Competing Interests	ICT companies may have different interests than LEAs, such as protecting their commercial interests or user privacy. The impact of cooperating with the government on their reputation may be viewed differently. This can lead to delays or difficulties in processing requests for information and resources, which will affect the time it takes the companies to respond and their motivation to cooperate with LEAs.
Legal Requirements	Incompatibility of laws and regulations across different countries or regions often limits the ability of LEAs and companies to share relevant information or cooperate on investigations, especially in cases involving incitement to violence or hate speech. Some companies may invoke national security laws or privacy regulations to protect their users' data, while others may claim freedom of speech as a defence against censorship or liability. These legal conflicts can hamper the efforts of LEAs to prevent or prosecute use of ICTs for terrorist purposes.
Technical Challenges	Technical challenges can also hinder cooperation between LEAs and ICT companies. In addition to the differential classification of computer systems and methodological procedures, different technologies and systems can make it difficult for both partners to exchange information and resources effectively. Moreover, LEAs may lack the necessary equipment, skills, or training to conduct digital forensics and open-source intelligence investigations (OSINT).
Priorities	Conflicting perspectives may lead to different perceptions of risks and responsibility. While LEAs may view a specific incident involving use of ICTs for terrorist purposes as an imminent threat to public safety that requires immediate action, ICT companies may perceive this as a potentially low risk that does not justify compromising their users' privacy. LEAs experienced with risk assessment have a legal responsibility to protect the public, while ICT companies need more understanding and trust of particular issues and LEAs interlocutors. This may lead to a lack of cooperation or even conflict between the two parties. Moreover, ICT companies may focus on providing services and information that meet their customers' needs and expectations, over actively monitoring on abuse of their services, while LEAs must always be actively on alert for potential threats. This different modus operandi may challenge the cooperation between the two sectors over their roles and responsibilities in ensuring public safety.
Resources	Smaller companies may not have sufficient resources to offer significant cooperation with LEAs, and they may be hesitant to collaborate in order to conserve their resources.

4.3 Motivation for Cooperation

Increasingly, terrorist actors are relying on technology platforms and services providers to carry out their malicious activities, as such LEAs often encounters technical challenges in combating, pursuing, and prosecuting terrorists. Such challenges include obtaining relevant data stored by ICT companies, working with limited resources, overcoming technology gaps, and the complexity of the threat itself. Law enforcement motivation for cooperation with ICT companies is driven by the following:



TABLE 6. Law Enforcement Motivation for Cooperation

Law enforcement Motivation	
Information and Evidence Collection	Cooperation between LEAs agencies and ICT companies is essential for obtaining valuable evidence or intelligence those companies hold. For example, ICT companies can provide access to user data, content, metadata, location data, etc., that can help LEAs identify and investigate terrorist suspects and networks.
Access to Advanced Technology	ICT companies often have access to cutting-edge technology and expertise that can assist LEAs in gathering evidence, tracking and monitoring potential threats, and responding to incidents. For example, ICT companies can provide tools for encryption, decryption, data analysis, mining, visualization, forensics, artificial intelligence, etc. This can enhance the capabilities of LEAs in combating terrorism.
Improved Coordination and Response	Joint efforts between LEAs and ICT companies can lead to improved coordination and more effective responses to incidents. For example, ICT companies can provide critical data, infrastructure, resources, and expertise that can support the efforts of LEAs in responding to terrorist incidents.
Cost-Effective Solutions	Cooperation between LEAs and ICT companies can provide cost-effective solutions to address the threat of terrorism. By combining the resources of both parties more effectively, LEAs can effectively allocate their resources, budgets, funds, manpower, equipment, materials, etc., where the unique value of the cooperation can reduce the cost of combating terrorism.
Increased Public Confidence	Effective partnerships between LEAs and ICT companies can increase public confidence in the ability of LEAs to address the threat of terrorism. This can help to build public trust and support the efforts of LEAs in combating terrorism.
Buffering and Countering use of the Internet and Social Media for Terrorist Purposes	Improved cooperation between LEAs and ICT companies discourages terrorists from using the Internet and social media for terrorist purposes.

The collaboration between LEAs and ICT companies can provide beneficial advantages to the ICT companies, either directly or indirectly. Such cooperation is likely to have positive impacts on the companies' long-term business. ICT companies' motivation for cooperation includes the following:



TABLE 7. ICT Companies Motivation for Cooperation

ICT Companies Motivation	
Reputation and Brand Image	Cooperation with LEAs can enhance the reputation and brand image of the company. The company can improve its credibility and reputation with customers, stakeholders, and the wider public by demonstrating its commitment to public safety and security. This cooperation can bring a better user experience for their clients and a safer environment that increases the platform’s attraction and produces greater revenues.
Public Safety	This cooperation can bring a better user experience for their clients and a safer environment that enhances the platform’s reputation and produces greater revenues.
Legal Obligations	ICT companies may have legal obligations to cooperate with LEAs, such as in response to a valid lawful request for information or in accordance with national or international laws and regulations.
Improved Security	Working with LEAs can help ICT companies to improve the security of their products and services. This can help to prevent their technology from being used for criminal or terrorist activities, and to mitigate the impact of incidents involving their technology.

4.4 Key Guiding Principles for Cooperation

In order to strengthen collaboration between LEAs and ICT companies, both entities need to adhere to key cooperation principles, such as shared goals to counter-terrorism, full respect of the rule of law, mutual trust and respect, and upholding privacy and human rights. The key principles listed in the table below serve as the foundation for building strong and lasting co-operation between LEAs and ICT companies in countering terrorism.



TABLE 8. Guiding Principles for Cooperation

Key Principles	
Shared Goal of Counter-Terrorism	Cooperation between LEAs and ICT companies should be a partnership. Both parties should work together to achieve common goals, each contributing their strengths and resources to support each other’s efforts while taking into consideration each others different interests and needs.
Full Respect of the Rule of Law	Cooperation should comply with relevant laws and regulations, including national and international privacy and data protection laws. Ensuring that will enable ICT companies to assist effectively and enhance trust.
Mutual Trust & Respect	Cooperation between LEAs and ICT companies should be based on mutual trust and respect.

Key Principles

Confidentiality	<p>Cooperation should respect the confidentiality of the data and resources shared between LEAs and ICT companies. Confidential information should only be shared on a need-to-know basis and should be protected against unauthorized disclosure. If the data might be presented in a court of law and might be publicly known, it should be clear to the company that this might be the case.</p> <p>ICT companies must get full justification for the requests, and some ICT companies may have a notification rule; once they provide data to any LEAs, they will automatically notify the client.</p>
Transparency	<p>Notification of relevant parties of existence and scope of such co-operation. Some companies may share the extent they share information with LEAs on their terms of use or publish a yearly report describing the extent of their cooperation, to increase transparency.</p>
Competence	<p>LEAs and ICT companies should be fully aware of the procedures for information sharing. LEAs representatives must understand what each company can offer, what resources it may take them to present this data, the time it might take to answer this request, and how it should be done. Meeting each other expectations is fundamental.</p>

4.5 Other Considerations

There are additional considerations that need to be taken into account when establishing co-operation between LEAs and ICT companies for countering terrorism. First, the nature of cooperation, which can either be long term or ad-hoc. Second, the number of parties building partnership, whether it is bilateral or multilateral partnership, spanning across multiple Member States. These aspects have a profound impact on the modalities of cooperation and must be taken into account while choosing a model. They affect the available resources, the time frame for yielding results, and the approach to be adopted.

4.5.1 Nature of Cooperation

Based on LEAs objectives and operational requirements, the nature of cooperation with individual ICT companies may vary. More specifically, LEAs may have a cooperation engagement with an ICT company that is limited and considered to be ad-hoc, based on a specific case or requirement.

This may involve requesting ICT companies to provide technical assistance or access to data in a particular investigation or operation, and it is obvious that this cooperation is a rare case and may not happen in the near future.

Usually, those cases that are considered as emergencies and may have no prior relationship between the LEAs and the specific ICT company, and there is no time to establish trust between parties, and it may be more challenging to coordinate the efforts. Since no long-term relationship is anticipated, communication will be limited for a specific case.

In those cases, LEAs should consider these actions:

1. **Locate the relevant point of contact at the company:** The legal departments are usually the best place to start, as they know the legal requirements and procedures for warrants and emergency cases. They can also direct LEAs to the appropriate person to assist with the request. Once the cooperation method has been established, the supported data can be discussed.
2. **Agree on the nature and means of the cooperation required:** Setting realistic goals is the best way to set a specific expectation on the right track, clear presentation of the urgency, and how long it will take the ICT company to produce the requested data, only after a discussion for the agreed means to deliver it.

That being said, it must be take into consideration that absence of past cooperation limits the trust, in this case, and there may be a need to share more data to present the scenario and the facts that support the request. One way to do so is by presenting all the relevant information at the first point of contact, and update any information accordingly. If there are delays or difficulties, consider getting the data in several packages instead of waiting for a complete set of data.

Another factor of cooperation is when conducting long-term cooperation between LEAs and ICT companies requires careful consideration of various factors and mechanisms. This is the most common type of cooperation between the parties, and built on the pillars presented beforehand.

It is essential to maintain consistent communication channels, and having a designated point of contact can help ensure effective collaboration. Establishing an infrastructure that includes mutual training, periodic meetings, data sharing, secure communication lines, and standard procedures for different scenarios can be a worthwhile investment for both parties.

4.5.2 Bi-Lateral vs Multi-Lateral Cooperation

Multilateral cooperation involves the collaboration between multiple parties in some cases even internationally. When cooperating multilaterally the focus is on addressing broader concerns that affect multiple parties, and collaboration can lead to the development of shared resources and best practices. While bilateral cooperation is more straightforward and faster to establish, multilateral cooperation can lead to more comprehensive and impactful solutions in the long run.

The most important thing to consider is that not all parties share the same values, resources, and legal aspects. While it may be a wise decision to diversify the group, make sure everyone focuses on the main goals.

Multilateral cooperation is better suited for general alliances that focus on promoting concepts and highlighting risks and opportunities rather than specific operational investigations. On the other hand, bilateral cooperation is typically utilized for operational tasks associated with ongoing cases.



[V]

Cooperation Model 1 – Information Sharing

5.1 Purpose

Information sharing is a crucial aspect of the cooperation between ICT companies and LEAs in combatting terrorism. ICT companies have access to valuable data and insights on their platforms that can help identify and prevent terrorist activities. For example, they can detect patterns of suspicious behaviour, flag content that violates their terms of service, or report accounts that are linked to known terrorists/terrorist organizations. On the other hand, LEAs can provide guidance and feedback to ICT companies on how to improve their security measures. By sharing information in a timely and effective manner, both parties can benefit from each other's strengths and resources while respecting the privacy and rights of their users.

5.2 Objectives

The aim is to establish a working relationship between ICT companies and LEAs in order to facilitate bi-lateral information sharing. More specifically, information sharing allows for the following:

- Exchanging of threat information that may be relevant for LEAs and ICT companies;
- Understanding key terrorist trends, identifiers, tactics and means of using technologies for malicious activities;
- Alerting and taking action of suspicious or illegal behaviour and activities and that may warrant an investigation; and
- Identifying threat priorities concerning terrorist abuse of ICT companies services, platforms, or products.

5.3 Cooperation Approach

Information sharing is a crucial aspect of the cooperation between ICT companies and LEAs in combatting terrorism. ICT companies have access to valuable data and insights on their platforms that can help identify and prevent terrorist activities. For example, they can detect patterns of suspicious behaviour, flag suspicious content, and LEAs can provide feedback on those matters.

1. Identifying the most suitable ICT companies for cooperation is a critical initial step in establishing collaboration with LEAs. This model of cooperation should be prioritized and set with as many ICT companies as possible.

The team responsible for this task should also identify companies that may be vulnerable and share pertinent information accordingly. It is recommended to share unclassified data with as many relevant companies as possible, while classified data should be shared selectively and with appropriate caution.

2. Motivating active cooperation between LEAs and ICT companies is crucial since it relies on active reports from the latter. One way to encourage information sharing is by providing feedback on the outcomes of the LEAs actions when appropriate. This feedback can help build trust between the two parties and incentivize ICT companies to continue sharing information that can aid in the fight against terrorism.

In addition to the fact that the information shared by LEAs may help the ICT company to keep their platform safer and may act as a motivating factor.

3. Continuous engagement with relevant companies can help to maintain their active cooperation and ensure the timely dispatch of relevant data, which in turn helps to enhance the safety of their platform.
4. One effective way to actively monitor social media platforms for suspicious terrorist activity is through the companies themselves. Some companies have already established mechanisms to track and prevent such activity.²⁰ It is recommended to assist these companies in any way possible, such as by sharing known indicators of terrorist activity. Examples of such indicators include factors of radicalization, proscribed groups, active group names and screen names, planned days of action, slogans, and symbolic content. While keywords were previously used to monitor activity, AI capabilities are now being utilized to scan platforms and identify new forms of threats. However, as this technology is still new and immature, it is advised to combine it with traditional methods.
5. There are many NGOs and international organizations that focus on monitoring different aspects of terror groups' online activity. Joining forces with these organizations may broaden the capabilities to proactively prevent threats and keep public safety at an optimum level.

Identify those organizations and start sharing information, expertise and resources, a collaborative network of actors can enhance the effectiveness and efficiency of counter-terrorism efforts.

²⁰ One example of this collaboration is The Christchurch Call which is a community of over 120 governments, online service providers, and civil society organizations acting together to eliminate terrorist and violent extremist content online.



[VI]

Cooperation Model 2 – Capability Augmentation

6.1 Purpose

Numerous commercial companies offer their intelligence-gathering services to the intelligence community for a fee. These companies invest significant resources and technology to acquire unique expertise in various fields, such as the darknet or cryptocurrency.

There are many companies that have invested a significant number of resources to develop a capability that LEAs might use to fight terrorism better. Collaboration with those companies could be beneficial for both.

6.2 Objectives

The aim is to enrich LEAs capabilities by using ICT companies' expertise and experience. More specifically, capability augmentation allows LEAs to:

- Save on R&D by cooperating with companies that have already acquired this capability;
- Facilitate cost-effective diversification of LEAs staff by incorporating individuals with varying skills and experience;
- Allow LEAs to quickly access cutting-edge technology and valuable intelligence databases; and
- Empower LEAs to adjust their workforce and expertise to meet their immediate needs.

6.3 Cooperation Approach

1. ICT companies function within civilian landscapes and often hail from diverse jurisdictions, each with its own set of regulations, potentially missing localized cultural nuances and facing language obstacles. Moreover, certain companies may not possess the requisite understanding or experience with local legal norms and ethical standards.

Therefore, it becomes of paramount importance to guarantee that any partnership with these organizations aligns with local legislation, ethical considerations, and procedural methods, all the while remaining compliant

with international law. These companies should adhere to legal constraints, uphold ethical conduct, preserve the integrity of evidence, and follow any other relevant directives.

To ensure due process in collaboration, it is recommended to carry out comprehensive due diligence on prospective partners prior to formalizing work agreements. This becomes particularly crucial when engaging with firms involved in commercial intelligence gathering.

2. In our current era, there is an observable surge of private commercial entities that concentrate on Internet-based intelligence gathering, focusing primarily on large-scale data collection and analysis. Some of these companies offer valuable intelligence services. They have harnessed technology and honed specialized expertise that LEAs can leverage for public safety.

These companies can often be more effective due to their capacity to invest substantial resources, enabling them to disseminate intelligence on a global scale, albeit for their own profit. A prime example is the darknet, a platform with global reach. A single agency with a specific geographical mandate may find itself having to sift through data unrelated to its jurisdiction. Conversely, a commercial company can analyse the entirety of the data and share pertinent information with the relevant countries.

The identification of suitable service providers that can best bolster specific initiatives is recommended. To effectively address deficiencies in data collection or technological capabilities, it is advised to initially conduct an exhaustive evaluation and prioritization of these shortcomings in conjunction with intelligence experts. Once the critical gaps have been pinpointed, the subsequent step involves surveying the market for potential companies that offer solutions designed to bridge these gaps.



[VII]

Cooperation Model 3 – Business Alliance / Council



7.1 Purpose

The goal of establishing a business alliance is to create a consortium of entities that can enhance the capabilities of fighting terrorism by sharing new technologies and techniques. Through collaboration, LEAs can gain knowledge about potential threats before they reach the market and fall into the hands of terror groups. Understanding these technologies can assist LEAs in better preparation for upcoming threats or setting guidelines to prevent such threats from materializing. Furthermore, this alliance can provide insights into future developments that may help mitigate terror risks. In other words, the primary objectives of this council are to explore the potential risks and opportunities that future technologies may unfold.

7.2 Objectives

The aim of this model is to set an alliance to work as a joint venture on concerning issues. More specifically, this alliance allows to:

- Prepare for future threats by anticipating new technologies before they are abused by terrorists;
- Prevent future threats by exploring pre-emptive measures needed to ensure public safety;
- Harness innovative technology to fight terror by acquiring the most advanced tools to counter-terrorism; and
- Alert companies of potential risks broadly and allowing them to mitigate the risks together.

7.3 Cooperation Approach

1. As the consortium's primary objective is to concentrate on emerging technologies, it is recommended to constantly seek out innovative companies that can contribute to the alliance.
2. Consider starting a new alliance only if there is no existing consortium or if the matter at hand pertains to local issues. It is recommended to search for and join an already established alliance instead of attempting to create a new one, as companies may be hesitant to join multiple alliances.

3. Considering that the most innovative companies might be small start-ups, it is important to ensure that this alliance is open to them and that they are aware of its existence.
4. Starting an alliance gradually is recommended by mapping the relevant ICT companies for the alliance and initially approaching only a few of them. Once the alliance has been established, it will become easier to add more members.
5. There are various alliance topics that LEAs can initiate or join, but those focusing on AI are distinctive. Such alliances consist of numerous countries that leverage diversity, which is essential for ensuring objective and efficient AI. Therefore, it is recommended to explore the existing groups that are already working on this matter. Although AI has immense potential to enhance prevention efforts, it also poses significant risks that must be addressed, and a diverse alliance can yield better outcomes.
6. Consider exploring existing international alliances that have already proven to be effective and potentially request to join or utilize their products.²¹

21 GIFCT – Global Internet Forum to Counter Terrorism, JCAT – Joint Counter-Terrorism Assessment Team, InfraGard – a partnership between the FBI and private sector.



[VIII]

Cooperation Model 4 – Active Investigations



8.1 Purpose

This is the most common and required form of cooperation between LEAs and ICT companies. The fundamental purpose of cooperation with ICT companies is collecting data related to terrorist investigations and to prevent terror groups from abusing their services. This cooperation is essential for enhancing public safety through prevention and prosecution.

8.2 Objectives

The aim of this model is to assist LEAs to pursue terrorists through active investigations with the help of ICT companies. More specifically, this cooperation allows to:

- Actively monitoring data to track potential terror attacks;
- Removing terror-related content from a public platform;
- Collecting data to prevent terror attacks or to identify new terror groups; and
- Collecting evidence needed for prosecution.

8.3 Cooperation Approach

1. A crucial factor that can greatly impact the success of the collaboration between LEAs and ICT companies is having a single point of contact. Both parties benefit from having a dedicated entity that has close relations with the company representative and is knowledgeable about their data, organization, procedures, and expected timeline for accessing it. Having all the necessary protocols for effective cooperation centralized in one entity can lead to a recipe for success.

NOTE: It is custom and best practice to use a single email address to ensure 24/7 availability (constantly monitored).

2. Infrastructure is an important component of successful collaboration between LEAs and ICT companies. It is essential to ensure that communication channels are secure and protect the privacy and integrity of shared data. It is also important to ensure that data is delivered in a timely and efficient manner while meeting international law

standards to ensure the admissibility of any information provided as evidence in court. Many global companies provide support to LEAs through a dedicated portal designed specifically for law enforcement requests.

Once registered, LEAs can log in and upload formal data requests. These companies also offer training to support LEAs in using their portals. It is important to note that the portal serves as an ongoing collaboration platform but may not be the only line of communication.

3. To ensure efficient collaboration, it is important to establish protocols for various scenarios. These protocols may include guidelines for handling emergency cases, such as defining what constitutes an emergency and setting time frames for taking necessary actions. By establishing clear protocols, the parties can work together more effectively and streamline their efforts to prevent and respond to terror threats.

Establishing procedures beforehand to ensure a well-structured and efficient collaboration. This includes defining the request process, specifying the required information for each type of request, outlining the terms of use, and determining the legal process and necessary approvals. To facilitate this, a set of forms can be developed. When working with local companies, it is common to sign a memorandum of understanding (MOU) which outlines response time frames and prioritization, data format, emergency protocol, points of contact, availability, and service-level agreement. Large international ICT companies already have dedicated portals for this purpose.

4. Training programmes that are mutually beneficial should be established to support both parties. The LEAs can provide training to the ICT company's representative on legal procedures, ethics, cybersecurity, and terminology. On the other hand, the ICT company can provide training to the LEAs on their technology, data retention policies, protocols, terms of use with their clients, notification alerts, and how to submit a data request. Regular meetings should be scheduled between the LEAs and the ICT company to address challenges, increase transparency, and improve the referral process. These meetings can also facilitate LEAs learning about new technologies in the company that may be useful in countering terrorism and identifying any potential misuse of technology by terrorists.
5. Considering that these companies are commercial entities, it is important to consider a compensation mechanism that covers their expenses for the operations conducted during the collaboration with LEAs, especially when dealing with small companies.
6. It is recommended to prioritize preservation requests with international companies. This will ensure that the data is retained for a specific period allowing a formal request is issued. It is also important to set a reminder to extend the preservation request if the formal request has not been received yet.

Ensure timely follow-up through a formal request or inform the company of the waiver of the preservation request, if the request has been fulfilled or no longer relevant.

7. Personnel from LEAs who are responsible for cooperating with ICT companies should have access to the appropriate technical resources, such as email addresses that clearly indicate their affiliation with the agency and other tools necessary to receive electronic information from the counter party securely.
8. It is essential to support any request made to ICT companies with an official written document. This is especially crucial when addressing urgent matters. Such documentation guarantees that the appropriate procedures are followed, and it increases trust and transparency in the partnership.
9. It is advisable for officers to minimize the use of emergency and urgent requests and avoid any misuse of these procedures. Such misuse can cause interference in the normal commercial course of ICT companies.
10. It is crucial to exercise extra caution when requesting removal of data, especially in cases such as terror propaganda, recruitment, and incitement.

A significant challenge in these scenarios is the potential divergence in views between LEAs and ICT companies. While LEAs may perceive a threat as imminent, companies may view it as freedom of speech – bridging this gap is critical. Local companies may be satisfied with a warrant, while international companies may require additional evidence of a threat.

Guidelines and legal frameworks are established by most countries for these situations. They assist both parties in evaluating each case while avoiding any infringement on human rights.

When it comes to content removal, commercial companies take the matter seriously and are more likely to cooperate when they understand the justification for it.

Therefore, it is crucial to present the whole situation to the company and take into consideration that, in many cases, the necessary supporting data is not publicly known and needs to be shared.

It is important to ensure that all the necessary data for prosecution is retained before content removal is carried out. In many cases, once the content is removed, the log files and documentation required for the prosecution process may also be removed.

Major corporations such as Meta, Google, and Microsoft have established their own protocols for content removal, and have developed proactive measures to identify cases in which it should be implemented. It is recommended to reach out to these companies and become familiar with their guidelines to effectively handle such situations.

There may be instances where LEAs decides to delay the removal of certain content for intelligence purposes. This could be when the content may provide crucial intelligence that cannot be obtained through any other means. However, in such cases, it is important to assess the potential impact of the ongoing threat on public safety and coordinate with the ICT company involved, considering the potential implications for them.

Consider recommending companies to label content removal as a legal request from the authorities. This labelling will allow them to maintain transparency with their users and remain neutral in the process.

8.3.1 Specific Considerations for Evidence Collection

1. To maintain the integrity of the data as part of the “chain of custody,”²² it is essential for LEAs to collaborate with the company and ensure that the data is securely stored and remains intact throughout the entire process, from storage to its final destination, in a court of law. It is recommended to establish a mechanism to verify that the data being sent is identical to the original data stored by the company. One effective method is to use digital signatures, where the company digitally signs the files before sending them, and the signature serves as proof that the copy is identical to the original. By keeping the signature with the file, its authenticity can be verified also in legal procedures.
2. Maintain a secure chain of custody throughout all processes. The files should be securely held, and for added security and integrity, the digital signature can be stored separately.
3. When evidence collection is necessary while collaborating with international companies, obtaining evidence may require going through a Mutual Legal Assistance Treaty (MLAT) process. Although this process is often bureaucratic and can take a considerable amount of time, it may be the only option for obtaining data from an international company that is admissible in a court of law. However, consider that some companies may permit multiple types of requests for the same data. This means that the requested data through the MLAT process for official use in prosecution, while also requesting the same data directly from the company for preventive measures. Once the data is obtained through the MLAT process, it can be used for prosecution purposes as well.
4. If the company does not permit parallel requests,²³ it is advisable to promptly split the requests and prioritize obtaining the necessary data for prevention purposes. At the same time, start the legal process to request the data needed for evidence through the MLAT process. This approach allows for accelerating the data collection for mitigating the threat, while waiting for the official data to use for prosecution later.

²² Pertains to the traceable and documented process of handling, preserving, and owning digital evidence from the point of collection to its use, ensuring its authenticity, reliability, and admissibility in legal proceedings.

²³ Some companies may argue that subscriber data can be sent without going through an MLAT process, while content requests must go through an MLAT process.

[APPENDIX A]

Practical Guidelines on Requesting Data from Online Service Providers

A.1 Overview

Terrorists and violent extremists increasingly use the Internet as a tool to support their activities. Consequently, it is important that LEAs are aware of the different options available to them to request and obtain Internet-related data from ICT companies and Online Service Providers (OSPs) to support their investigations and prosecutions. The aim of this section is to provide step-by-step guidelines on how to submit requests for data or evidence to OSPs, as well as best practices that will increase the chances of receiving information as requested and in a timely manner.

A.2 Types of Information

There are two main types of digital information: stored information and real-time information.

1. **Stored information.** This is the information that is already stored on the servers of the OSPs, before the request is made.
2. **Real-time information.** This is the information that is not yet stored on the servers, but that one hopes to obtain in real time; for instance, the time and location of an individual's login into their account.

Both stored and real-time information can be divided into:

- Basic Subscriber Information (BSI) and Login Information
- Traffic Data
- Content



TABLE 1. Basic Subscriber / Login Information vs Traffic Data

<p>Basic Subscriber Information and Login Information</p>	<p>Basic Subscriber Information includes all the information provided by the subscriber to the OSP during the creation of their account, as well as their IP address at that time. Subscriber Information generally includes the following:</p> <ul style="list-style-type: none"> • The subscriber’s name, postal or geographic address, IP addresses, telephone and other access number, email address, billing and payment information, available on the basis of the service agreement or arrangement. NOTE: These may be fake, as they are subscriber-generated inputs; • The subscriber’s account or login name; • The type of communication service used, the technical provisions taken thereto, and the period of service; and • Any other information on the site of the installation of communication equipment, available based on the service agreement. <p>Login Information consists of dates, times, and IP addresses of each log-in.</p>
<p>Traffic Data</p>	<p>Most commonly, traffic data includes a sender and recipient of communications, their IP addresses, as well as dates, times, and duration of communications, as well as websites the subscriber visited.</p> <p>Types of Traffic Data include the following:</p> <ul style="list-style-type: none"> • Connection information: destination or source of connection; connection time and date; disconnection time and date; method of connection to system (e.g., telnet, ftp, http); data transfer volume (e.g., bytes); and routing information; • Source or destination of any electronic mail messages sent or received by the account: the “header” of the e-mail or the “To” and “From” fields; date, time, and length of the message; • Information pertaining to any image(s) or other documents uploaded to the account: dates and times of uploading, and the sizes of the files but not including their contents; and • Name and other identifying details of individuals that accessed a specific image, file, or web page within a specified period of time or on a specified date. <p>One example of traffic data is a log of Facebook messages between two individuals. Note that this log will not contain any message content.</p>

The real-time collection of non-content information consists of a message from the provider to the police containing either:

- The time and IP address when a suspect logs in to their account, in order to help locate them; and/or
- The fact that the suspect sent a message to someone or received a message from someone. The telephone numbers / e-mail addresses of other suspects can also be obtained with the aim of identifying these other possible suspects in real time (but not containing any content).

3. Content. Everything that is not subscriber or traffic data. It can include written messages, embedded photographs, and attached files. Examples of content are:

- E-mail: the content of all e-mails stored in the account, including copies of e-mails sent from the account and drafts.
- Social Media Accounts: all posts, communications and messages sent or received by the user including private messages and attachments, and elements such as a friend list, pending friend requests, likes, and group membership.

A.3 Request Types

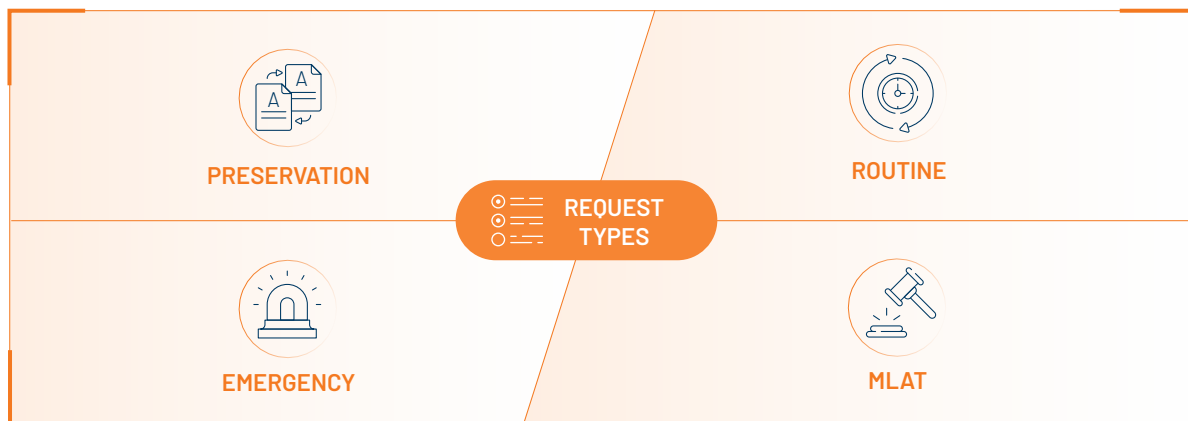
Digital evidence requests can be categorized into different types based on the nature of the evidence, the investigative requirements, and urgency. Each type serves a distinct function and is governed by different legal principles.

To request information from OSPs, there are generally four categories, which are the following:

- **Preservation:** to request digital artefacts that may serve as evidence to be preserved in its original state and not deleted or modified;
- **Routine:** standard requests that follow established legal processes and protocols;
- **Emergency:** made in urgent situations only, where immediate access to digital evidence is necessary to prevent imminent harm or protect public safety; and
- **MLAT:** typically made when an investigating authority or legal entity seeks to obtain digital evidence located in another country.



FIGURE 1



A.3.1 Preservation Requests

Preservation requests are aimed at ensuring the safeguarding and preservation of digital evidence, while the main data request is being executed.

NOTE: Preservation requests are recommended to be made systematically, prior every data request. If this is not done, the data being requested can be altered or deleted before the request is executed.

Preservation requests can be made by LEAs directly or through diplomatic channels of the OSP's jurisdiction country.

In general, a preservation request must include the following:

- Identification of the requesting authority: name, badge or ID number, e-mail address (most providers only accept requests from officials with a clear governmental e-mail address), telephone number, address;
- Basic facts of the investigation (very short);

- A description of the data to be preserved: type of data (BSI, traffic, or content) the specific account's unique identifier or IP address/website, and the time period for the requested data;
- A statement that the request for the data disclosure will be sent after the data has been preserved; and,
- If the subscriber should not be notified of the investigation, a demand to keep all requests confidential must be submitted.

NOTE: Preservation requests preserve data for a limited time only and are not renewed by OSPs automatically. Remember to submit renewal requests – otherwise preserved data will be lost.

A.3.2 Routine

A routine digital evidence request refers to a standard or regular procedure when seeking specific digital evidence as part of an investigation or legal process. It is a common and an expected step in gathering evidence in various types of cases.

Routine requests are typically non-urgent and allow for the completion of standard legal procedures. Routine requests typically follow established legal protocols, such as obtaining search warrants, court orders, or subpoenas, to ensure compliance with applicable laws and protect individuals' rights.

While routine digital evidence requests are standard procedures, emergency requests and MLAT requests address more urgent or cross-border situations that require expedited actions or international cooperation.

A.3.3 Emergency Disclosure

Emergency Disclosure Requests are made in urgent situations to prevent imminent harm. This is an extraordinary procedure and can only be used in true emergencies. Emergency requests may bypass certain standard legal procedures to expedite the process, but they still require proper authorization and adherence to criteria defined by law.

In the case of an Imminent Physical Threat (IPT), the digital evidence can be requested immediately and directly from the OSP without the need for an MLAT. Large OSPs such as Facebook or WhatsApp normally have someone available 24/7 and have emergency forms on their websites that must be filled in ("Emergency Disclosure Request Form").

Where direct contact with the OSP is not an option, police-to-police channels may be used (ex. i24/7 INTERPOL Network, G7 24/7 Network, Council of Europe (CoE) Budapest 24/7 Network, or bilateral Memorandum of Understanding between countries).

Once the OSP receives the request, it normally maintains the data for 90 or 180 days. This period is renewable every 90 or 180 days until the request is executed. NOTE: The request does not renew automatically – a renewal request must be sent. If the request is not renewed before its deadline, the digital evidence will be deleted. In addition, since preservation is not mandatory, some OSPs will refuse to do more than one or two renewals.

Most providers will answer within a few days with their reference number. To link the official request to the preserved data, mention that reference number.

The information that the OSP may voluntarily provide to foreign government entities through this procedure is basic subscriber information, recent login data and other stored information, except content. The content, on the other hand, can only be disclosed to an OSP's jurisdiction country's LEAs. If content is needed, a discussion with liaison officers might be useful before, and if a request is submitted, through diplomatic channels.

To use an Emergency Disclosure procedure, three criteria must typically be met:



TABLE 2. Criteria Requirements

Urgency that requires the disclosure of the information without delay:	The request must justify why the traditional procedure cannot be adopted; for example, because a terrorist attack must be stopped and the ordinary procedure is too time-consuming. Most providers strictly interpret the word “imminent” strictly, so when there is no longer an imminent physical threat, the OSP might refuse to disclose information under this category.
Real danger:	The request must clearly explain why the threat must be taken seriously. Hypothetical possibilities of danger are not sufficient. For example, if dangerous behaviour of the suspect is established, or a trustworthy source indicating the imminence of an attack.
Physical integrity:	According to most OSPs’ policies, the emergency must involve an immediate danger of death or serious physical injury to any person or persons.

The OSP itself decides whether these criteria are met, but their compliance is not mandatory. Therefore, it is important to give OSPs sufficient convincing elements, especially where OSPs possess less information on the urgency of the situation than the requesting LEAs. The more context that is given to meet the mentioned criteria, the higher the possibility of the provider’s willingness to action the procedure that satisfies both parties’ interests.

Additionally, the law enforcement officer must be able to identify themselves sufficiently, for example, with a copy of the service card or an official email address. If the provider refuses to voluntarily hand over the data to LEAs under this procedure, it is advised to make contact through diplomatic channels, or start a normal procedure for the request of subscriber and login information.

If the provider refuses to voluntarily hand over the data to LEAs under the Emergency Disclosure procedure, it is advised to start a normal procedure for the request of subscriber and login information, use a subpoena, or make contacts through diplomatic channels.

- **National subpoena.** Issued by requesting country’s judicial authority or through an official law enforcement request. If the OSP accepts a subpoena from the requesting country’s government, this is the easiest and fastest way to collect the subscriber and login information.
- **Foreign government’s subpoena.** Some foreign governments’ LEAs have the power to produce administrative subpoenas for their own national cases in legally well-defined cases.

If a national subpoena is not an option, it might be worth contacting a liaison officer of the OSPs jurisdiction country or go through diplomatic channels, to see whether a foreign country’s authorities can open their own case and use their administrative subpoena power. This might give a faster result and help avoid a time-consuming and expensive MLAT procedure.

A.3.4 Mutual Legal Assistance Treaty (MLAT)

Mutual Legal Assistance Treaty (MLAT) is a bilateral agreement providing cooperation between two countries. Facilitating cooperation and mutual legal assistance between two countries in cross-border legal matters, including the exchange of digital evidence.

Requests for digital evidence under MLAT are usually made where routine or emergency requests cannot be made.

- Facts of the case, evidence sought, and relevance of the records sought to the investigation;
- Time frame (i.e., dates) of the records being requested and the deadline by which the evidence sought should be produced;
- Major offences applicable or charged – must be criminal offences; and
- Procedures to be followed in executing the request.

There are two important considerations regarding these types of requests:

- The judge granting the search warrant must be convinced that the account will likely still contain evidence of the criminal activity under investigation. If there was a previous preservation request and the requesting country is now seeking production of those preserved records, there is a high probability of those records still existing, avoiding the problem of 'stale' data.
- There must be a reasonable basis to believe that an offence has been or is being committed and that the evidence of the crime is likely to be in the place to be searched.

In this sense, the following must be demonstrated:

- The information must be reasonably trustworthy: the information is considered trustworthy when the source providing it is a law enforcement agent or another government official, or a citizen with reasonable general knowledge. If the source is anonymous or is a criminal, additional support to prove the reliability of their information must be provided; for example, by showing that information received from this person in the past was trustworthy.
- Additionally, a detailed description of the source of the evidence and an explanation why the authority arrived at their conclusions must be provided.
- The request must explain that the evidence will be located among the records of the OSP and it is connected to a criminal investigation.

TIP: Whenever an OSP's jurisdiction country's prosecutor or police agency is already familiar with and interested in assisting the execution of the request, providing this information is recommended to ensure speedier coordination and execution.

NOTE: In the case of MLAT requests, the OSP's jurisdiction country may be unable to assist if the criminal activity being investigated in the requesting country is protected by its constitution. For example, hate speech is protected by the constitutions of certain countries.

A.3.5 Choosing the Right Request Type

Depending on the situation and the type of information sought, a relevant request type should be used. The more information that is sought, the more likely it is that an MLAT will be required.

NOTE: Requesting data through MLAT is extremely slow. Therefore, it is recommended to use other request types first, if possible. Note that MLAT will not revoke other requests, so, for example, one can ask for emergency data to prevent an attack and at the same time submit a request through MLAT for data intended to be used in prosecution.

a. Request for Subscriber Information of Login Details:

Can be requested through:



Preservation



Routine



Emergency



MLAT

Many jurisdictions do not expressly prohibit OSPs from providing this information to foreign judicial authorities or LEAs without a court order. Nor are the OSPs legally obligated to provide such data without a court order. In other words, OSPs' policies vary and while some OSPs may accept direct requests for subscriber and login information, others will not produce any material without being ordered to do so by a court.

b. Traffic Data:

Can be requested through:



Preservation



Routine



Emergency



MLAT

Similar to subscriber and login information, most traffic data is non-content information that could be provided by the OSP without a court order. However, most of the OSPs are not willing to disclose this information without a court order, so in most cases an MLAT request must be made.

c. Content:

Can be requested through:



Preservation



Routine



Emergency



MLAT

Generally, OSPs will not produce content information without first being served with a search warrant, which can only be obtained pursuant to an MLAT request.

NOTE: In emergencies, the content can only be disclosed to an OSP's jurisdiction country's LEAs

The following information needs to be included:

- Reliable facts indicating that a crime has been committed, including:
 - What sources are authorities relying on in their information about the crime?
 - When did the crime occur?

Reliable facts indicating that the target account would contain evidence related to the crime, including:

- How was the account identified?
- How was it connected to the suspect?
- Was the account used to further the crime?
- When and how was the account used to further the crime?

TIP: The facts must be recent enough that the judge can conclude it is probable that the evidence is still in the account. Therefore, make sure to include dates.

PRACTICAL EXAMPLE: *Why is it likely that the Facebook account would contain evidence of terrorist activities?*

According to the information available, terrorists tend to use Facebook for communication – is not a good enough reason for OSPs to divulge such information to LEAs.

Traffic data in possession of investigators shows the suspect exchanged messages on Facebook Messenger with accounts known to belong to an existing terrorist organization between 12 March 2022 and 09 February 2023 – likely enough to get the desired action from an OSP.

d. Real-Time Information

Can be requested through:



Preservation



Routine



Emergency



MLAT

Real-time information requests should generally be made through the MLAT channel.

Non-Content Information: The standard for obtaining non-content information is to specify the relevance of the records to the investigation. As this is an expensive and time-consuming process, the following must be justified:

- Why it is believed that the account belongs to the suspect; and
- That the suspect will most likely use this account again; for example, because of frequent recent use. This could be proven by first requesting recent login information and subsequently proceeding with the tap and trace / pen register procedure.

Once the court issues the order, law enforcement may collect the information in real-time for up to 60 days and renew the request for another 60 days, if needed and approved by the court. To obtain this extension, the judge must be convinced of the continuous relevance to the investigation. NOTE: after approximately 40 days the procedure for the additional MLAT must be initiated, so that there is sufficient time to complete the whole procedure.

Content Information: The judge can only order the disclosure of “real-time content interception” for an ongoing domestic investigation, never on petition from outside the country of the OSP’s jurisdiction.

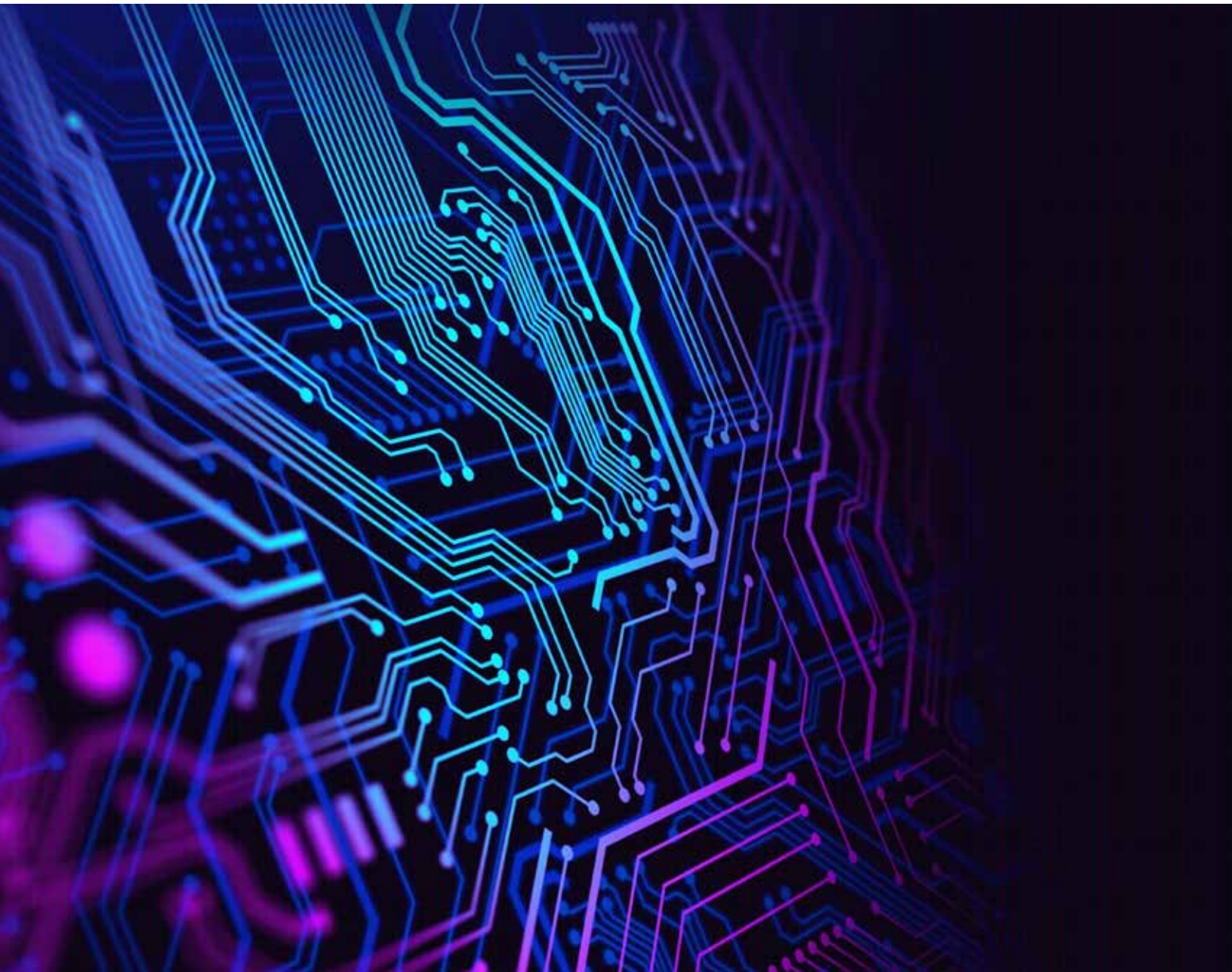
A.3.6 Steps Prior to Submitting Requests



TABLE 3. Steps to Take Prior to Submitting the Request

1. Is the OSP trustworthy?	When the OSP is not known, it is important to check its reliability and ensure that it is not a terrorist organization or individuals affiliated to it who run the OSP. In addition, today, there are many “bullet-proof hosting” providers that may be involved in criminal activity.
2. Is the data still available?	Every provider has its own data retention policy so this should be verified before submitting a request. Note: in some cases – there may be a regulatory requirement for data retention – for example, the EU “Terrorist Content Online”(TCO) Regulation came into force on 7th June 2022 and applies to all hosting service providers offering their services in the EU. Article 6 of the Regulation requires companies to preserve for six months the content that is removed or access to which is disabled.
3. What is the policy of the provider?	Most OSPs have law enforcement guidelines available online, which include specific requirements that law enforcement have to follow for the provider to deliver the data. For example, OSPs may require the URL or an ID number of the account – and not the name of the account itself – to disclose the information.

4. Does the provider notify the user?	<p>As a matter of policy, some OSPs will notify the account holder of any actions taken on behalf of law enforcement. It is advisable to ask the OSP (without mentioning specific accounts) whether the company notifies its customers of law enforcement requests.</p> <p>If the request needs to be confidential, include an explicit request not to inform the user in the request for information or in the MLAT together with a specific reason or, if possible, a legal provision, explaining why the user cannot be informed.</p>
5. Which country is the data located in?	<p>Some OSPs have servers in different countries. The law of the country where the data is stored may be applied. It is important to verify this by contacting the provider in question.</p>
6. Preserve	<p>Since the retention of data is a voluntary practice and its duration varies between providers, this request should be submitted immediately after ensuring the availability of the data. Once the information has been deleted, it generally cannot be recovered. However, preservation requests must be limited and reasonable.</p>



A.3.7 Good Practices for Submitting Requests



TABLE 4. Guidelines of Good Practices for Submitting Requests












Single Point of Contact (SPOC)	The requests, especially emergency requests, are likely to be addressed by OSPs and executed quickly when the same experts on the national level (SPOC) make the requests consistently.
Relevance	The requested data must be relevant to the investigation. It is important to explain in detail why the individual is a suspect, what crimes he/she is alleged to have committed, and what his/her role was, why it is believed they are the user of the account, and how the information sought is related to the investigation.
Confidentiality	<p>Some providers notify their clients of data requests. If the requests need to be confidential, include a paragraph with the request explicitly asking the service provider not to notify the user of the account. For requests made through MLAT, a non-disclosure order can be sought from a court.</p> <p>The request should contain information explaining why such non-disclosure is necessary, for example:</p> <ul style="list-style-type: none"> • endangering the life or physical safety of an individual; • flight from prosecution; • destruction of or tampering with evidence; • intimidation of potential witnesses; and/or • otherwise seriously jeopardizing an investigation or unduly delaying a trial. <p>It can also be requested that the application be sealed, which, if granted, would hide the filings and supporting documentation submitted to the court from public view for a set period of time.</p>
Scope	To increase the chance of getting the data, and to increase the speed of request fulfilment, it is recommended to keep the scope of the request as narrow as possible.
Time Frame	Specify the exact time frame for the data. For example, traffic data for the period between the 10th and 12th August 2023.
Official Email Address	Make sure to use an official government/law enforcement email address - otherwise an OSP may reject the request.
Compliance	<p>Ensure the request complies with the:</p> <ul style="list-style-type: none"> • Law of OSP's country • Law of the requesting country • International norms • OSP's policy

A.4 Common Platforms

Each provider has its own policies. Since these are frequently updated, it is recommended checking them before making any type of request. A list of some of the most prominent OSPs and links to their law enforcement portals and guidelines can be found below.



TABLE 5. Common Platforms Guidelines

	Facebook Requests: https://www.facebook.com/records/login/ . Guidelines: https://about.meta.com/actions/safety .
	Instagram Requests: https://www.facebook.com/records/login/ . Guidelines: https://www.facebook.com/help/instagram/494561080557017 .
	WhatsApp Requests: https://www.whatsapp.com/records/login/ . Guidelines: https://faq.whatsapp.com/444002211197967 .
	Google (Alphabet) Requests: https://lers.google.com/signup_v2/landing . Guidelines: https://policies.google.com/terms/information-requests .
	YouTube Requests: https://lers.google.com/signup_v2/landing . Guidelines: https://policies.google.com/terms/information-requests .
	TikTok Requests: https://www.tiktok.com/legal/report/lawenforcementrequest . Guidelines: https://www.tiktok.com/legal/page/global/law-enforcement/en .
	Snapchat Requests: https://less.snapchat.com/ . Guidelines: https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf .
	Twitter Requests: https://legalrequests.twitter.com/forms/landing_disclaimer . Guidelines: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support .
	Telegram Guidelines: https://telegram.org/faq . https://telegram.org/privacy?setln=it .
	LinkedIn Requests: https://app.kodex.us/linkedin/signin . Guidelines: https://www.linkedin.com/help/linkedin/answer/a1340284/linkedin-law-enforcement-data-request-guidelines?lang=en .
	Pinterest Requests: https://help.pinterest.com/en/law-enforcement . Guidelines: https://help.pinterest.com/en/article/law-enforcement-guidelines .

© United Nations Office of Counter-Terrorism (UNOCT), 2023

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)