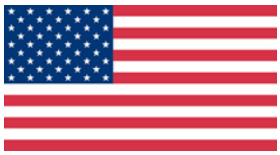
Comparative Practices on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Comparative Practices on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings

Council of Europe

The present publication was prepared through collaboration between the Council of Europe Committee on Counter-Terrorism (CDCT) and the International Institute for Justice and the Rule of Law (IIJ), with support from the United States Department of State. It reflects practices with use of information collected in conflict zones in the Council of Europe member and observer States, information on which was kindly provided by national authorities.



French edition:
Comparative Practices on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings

The opinions expressed in this work are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe.

All other correspondence concerning this publication should be addressed to the Directorate General of Democracy and Human Dignity. Violence against Women Division Council of Europe F-67075 Strasbourg Cedex France, Council of Europe

E-mail: conventionviolence@coe.int

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Cover Photos: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Printed at the Council of Europe

Contents

Executive Summary

Certain States members of the Council of Europe Committee on Counter-Terrorism (CDCT) (hereafter "States") have developed significant experience in identifying, obtaining, and sharing information and materials from conflict zones, and in using it as evidence in criminal proceedings related to terrorist offences. This set of Comparative Practices was developed by the CDCT Secretariat and the International Institute for Justice and the Rule of Law (IIJ), in partnership, to gather these States' methods and practices into a singular resource for practitioners, policymakers, and others.

The Comparative Practices build on Council of Europe Recommendation CM/Rec(2022)8 of the Committee of Ministers to member States on the use of information collected in conflict zones as evidence in criminal proceedings related to terrorist offences. They offer practical guidance on how to effectively use information and materials from conflict zones as evidence in criminal proceedings to advance justice and accountability, in accordance with national laws and relevant international human rights and rule of law standards.

This Executive Summary gives an overview of the key considerations detailed in the Comparative Practices. Moreover, the Practitioner's Frequently Asked Questions (FAQ) annex to this document addresses a number of overarching questions that practitioners may have about information from conflict zones.

1. Sources and Types of Information

As a matter of practice, numerous States have used information and materials from conflict zones as evidence in criminal proceedings related to terrorist offences. This information is diverse in nature and derived from a range of sources.

Potential sources of information include:

- **Domestic government agencies**, among them military and intelligence services as well as civilian criminal justice entities;
- **Foreign government agencies and intergovernmental mechanisms** for storing and sharing information (e.g., INTERPOL, European Union Justice and Home Affairs agencies (e.g., Europol), and Operation Gallant Phoenix databases and information systems);
- **Multilateral actors** (e.g., international courts and United Nations mechanisms); and
- **Non-governmental actors** (e.g., civil society organisations, academic researchers and experts, news media, and private companies and contractors).

Information and materials may come in a **variety of forms**, including:

- **Physical** (e.g., weapons, improvised explosive device components, mobile telephones, and hard drives and other storage media);
- **Digital** (e.g., content data, including text communications, audio files, photos and videos; traffic and subscriber data; and other electronic data such as cryptocurrency wallet information);
- **Documentary** (i.e. hardcopy written material);
- **Intercepted** telephonic or other communications and **satellite- or** unmanned autonomous system **(UAS)-generated** imagery and footage; and
- **Statements and testimony** (e.g. statements made voluntarily by defendants or by other subjects of interviews or interrogations, as well as testimony, statements, and other information provided by witnesses, victims, informants, and other human sources).

2. Mechanisms to Obtain and/or Share Information

States have used a range of mechanisms to obtain and/or share information from conflict zones for criminal justice use.

States promote **co-ordination and information sharing at the national level** in various ways.

- **Domestic legal frameworks:** Some military and intelligence services[1] rely upon their broad institutional mandates as the legal basis for sharing information with judicial authorities, while others find the authority — and sometimes the obligation — to do so in specific statutory provisions. "Double-hatted" services endowed with both law enforcement and intelligence functions can facilitate the sharing of information between domestic agencies or international partners.
- **Interagency co-ordination mechanisms:**[2] Procedurally speaking, States have designated focal points for interagency information sharing, established ongoing mechanisms for broader interagency co-ordination, and stood up *ad hoc* working groups when needed.
- **Declassification procedures:** States have also adopted formal processes to declassify information so it is more readily available for use in criminal justice cases.
  - Typically, the original classifying authority is legally considered to "own" the information and to hold the ultimate authority over the decision to declassify; some States have also established consultative bodies with the authority to access the information and render advisory opinions on whether it should be declassified.
  - One State has addressed the commonly identified challenge of overclassification by directing that materials and objects the military obtains in conflict zones should be presumed to be unclassified — as distinct from sensitive sources and methods of collection, which remain classified.

States take various **approaches to obtain information from foreign sources**.

- **Informal co-ordination:** Practitioners often begin the information-sharing process by co-ordinating with individual foreign counterparts informally.
- **Caveats on use or further sharing of information:** States generally recognise a "third party rule," or "originator control principle," whereby a State agency that receives information from a foreign State refrains from sharing it onward or divulging it publicly without the foreign information provider's authorisation.
- **Sharing through law enforcement or formal judicial channels:** States often initially, and sometimes exclusively, share information with foreign partners through intelligence or law-enforcement-to-law-enforcement channels. Where such channels do not suffice, or when national laws require, States make formal requests for information, including by relying upon mutual legal assistance and European Investigation Order processes. Many States draw upon all of the above approaches to obtain information, sometimes in sequence, depending on the nature and needs of a case.
- **Searches of intergovernmental databases and information systems:** INTERPOL databases, the European Union's Schengen Information System and Europol Information System, and Operation Gallant Phoenix have all proven valuable sources of information originally obtained from conflict zones.
- **Co-ordination with multilateral actors:** Multilateral actors operating in conflict zones, some of which have an affirmative obligation to safeguard and share information they collect, may themselves have collected relevant information — including the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD), the International, Impartial and Independent Mechanism on Syria (IIIM), and the International Criminal Court (ICC).

States have also **obtained conflict zone information from non-governmental actors**.

- A number of States have established channels to communicate with civil society or other non-governmental organisations, news media, and other private sector actors active in conflict-impacted areas and to encourage them to share information.

1. The term "service" refers throughout to all relevant government services, agencies, or departments with military and/or intelligence functions.
2. The phrase "interagency co-ordination" refers throughout to co-ordination between distinct governments services, agencies, or departments.

3. Steps to Analyse and Use Information

States have taken a range of steps to analyse the probative value of information from conflict zones and to make it easier for practitioners to use the information in criminal proceedings, whether as an investigative lead, as a way to otherwise support legal process, or as evidence in court.

In using information collected in conflict zones as evidence in civilian criminal proceedings related to terrorist offences, **States recognise the importance of acting in accordance with** the requirements of **the European Convention on Human Rights** — particularly the right to a fair trial protected by Article 6 — as well as other **applicable international human rights** standards.

When **practitioners** obtain relevant information from conflict zones, they **first assess its potential evidentiary value and determine the next investigative steps** to be taken.

- Practitioners typically exploit the information they have received to **generate additional investigative leads or evidence**. Using such information as evidence usually is subject to more formal requirements than using information as an investigative lead.
- When practitioners determine that information would be most valuable to an investigation in another jurisdiction, States sometimes proactively share it with foreign authorities, but the sheer **volume** of potentially relevant information collected **and the information's classification make proactive sharing rare**.

In most criminal procedure codes, there are no legal impediments to using information from conflict zones as evidence. States have used various mechanisms and procedures to **admit conflict zone information into evidence while protecting security interests**, including sources and methods of collection, **and complying with fair trial guarantees**.

- In many jurisdictions, **formal declassification, certification by its "owner" agency, and/or sharing** by law enforcement authorities can endow such information with the status of criminal evidence, and in some jurisdictions may be a prerequisite for using it as evidence.
- When information cannot be declassified in full, authorities have used **partial declassification with redactions and/or summaries**, and invoked security interests to justify **withholding related classified material**.
- Criminal procedure codes may also allow for the **selective closing of the courtroom** to the public when necessary to protect information or avoid other security risks.
- To provide an additional layer of protection, some courts have required prosecutors and defence counsel to obtain **security clearances** before getting access to sensitive information.

Practitioners have used **various techniques to** explain the significance of conflict zone information, describe the context of its collection, attest to its integrity and chain of custody, and otherwise **corroborate its authenticity and reliability and/or support its probative value**. Techniques include:

- **Reanalysing and re-exploiting original physical items**; **introducing copies** or descriptions when originals are unavailable; **and including contextual information**, such as official documentation of capture or acquisition circumstances and/or handling, transmission, storage, analysis, and sharing processes;
  - States have also developed policies and procedures and undertaken training to improve those processes in the first place;
- **Identifying and introducing additional material** generated from independent sources, both to verify the content of conflict zone information and to further substantiate the charges it tends to prove;
- **Introducing supporting testimony**, not just from who collected the information but also from State agencies' senior officials or technical specialists, academics or think tank experts, or victims, refugees, or FTF returnees or other "insider witnesses" who can elucidate the information's evidentiary significance;
  - States have also used **procedural devices** including physical screening, voice scrambling, anonymity, and/or out-of-court hearings **to protect vulnerable or otherwise sensitive witnesses** when necessary.

Information from conflict zones has also served as crucial evidence in criminal prosecutions for offences other than terrorism, including war crimes, crimes against humanity, and genocide. International crimes cases may require proof additional to that required in terrorism cases, and conflict zone information can be an important tool for meeting those requirements.

The use of information and materials from conflict zones will remain vitally important to criminal proceedings related to terrorist offences, as well as to the prosecution of acts prohibited under international humanitarian law and other offences, and **governments should therefore continue to strengthen international co-operation and domestic co-ordination on the effective sharing and use of such information** to advance justice and accountability.

Introduction

Outline of this resource's main aim, intended audience, sources, and definitions of key concepts ("information," "evidence," "conflict zone") following Recommendation CM/Rec (2022)8.

Effective investigation and prosecution of terrorism-related offences requires that criminal justice professionals have access to, and be able to introduce in court, sufficient reliable evidence to support the charges. **Given the number of terrorist groups operating in or otherwise linked to conflict zones, information from such areas is vitally important** to many terrorism-related investigations and prosecutions. Criminal justice practitioners must thus understand both how to obtain such information and how to analyse it, establish its reliability and authenticity, support its probative value, and introduce it as evidence before a national court in accordance with national laws and relevant international human rights and rule of law standards.

Certain States members of the Council of Europe Committee on Counter-Terrorism (CDCT) (hereafter "States")[3] that have prosecuted individuals accused of committing terrorist offences in conflict zones **have significant experience in identifying, obtaining, and sharing such information, and in using it as evidence in criminal proceedings related to terrorist offences**. These States have developed varied and context-specific, but nevertheless effective, methods for obtaining, authenticating, and introducing this type of information. **This set of Comparative Practices is designed as a singular resource to gather this experience and these methods and practices** and share them with practitioners and others in States.

The Comparative Practices were **developed by the CDCT Secretariat,** in partnership with **the International Institute for Justice and the Rule of Law (IIJ)**. They **build on Council of Europe Recommendation CM/Rec(2022)8** of the Committee of Ministers to member States on the use of information collected in conflict zones as evidence in criminal proceedings related to terrorist offences (hereafter "CM/Rec(2022)8," or "the Recommendation"). They are rooted in international norms and best practices, previous recommendations of the CDCT, and the experiences of Council of Europe member States, observer States and leading international institutions with relevant expertise.

While there are several other relevant sources of guidance on this subject (see annexed "Practitioner's Frequently Asked Questions (FAQ)" Section), these Comparative Practices are distinct from those publications in scope, source material, and aim.

- **Scope**: They focus on criminal offences linked to conflict zones, but address the full range of potential sources of information and materials collected there (not just military-collected material).
- **Source Material**: They are primarily based on information that States' competent authorities provided in response to a detailed questionnaire the CDCT Secretariat distributed in 2020 and 2023 (the Questionnaire). They also draw on personal and institutional expertise shared by members of the CDCT Working Group on Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings Related to Terrorist Offences (CDCT-CZ).
- **Aim**: They present concrete cases and examples of how information and materials collected in conflict zones has been accessed, shared, and used as evidence in civilian criminal proceedings. They offer practical guidance on how information from conflict zones can be effectively used as evidence in criminal proceedings to advance justice and accountability, in accordance with national laws and relevant international human rights and rule of law standards.

3. For the avoidance of doubt, wherever it is not indicated differently, the capitalised word "States" refers to states that are members of the Council of Europe Committee on Counterterrorism (CDCT), which includes Council of Europe member States and observer States.

Definitions: In these Comparative Practices, as in the Recommendation,

- "evidence" means all information that complies with the legal rules of evidence of member States as set out in their domestic criminal law and that is used in judicial proceedings to prove or disprove the alleged crime;
- "information" means the raw, original form of evidence and refers to material or nonmaterial objects collected in a conflict zone; and
- "conflict zone" means an area affected by armed conflict, or an area in an immediate post-conflict or a high-risk situation, where terrorist-related offences have been perpetrated.

These definitions of "evidence", "information", and "conflict zone" apply only within the context of the Recommendation and these Comparative Practices. Council of Europe member States are not required to adopt these definitions into their national laws.

This document uses the terms "terrorism-related offences" and "terrorist offences" interchangeably to refer to the full range of criminal offences which may be linked to terrorism as defined in national legislation, including, but not limited to, the planning or perpetration of terrorist attacks, membership in or material support to designated terrorist groups, and financing of terrorism. As Chapter VII of the Recommendation and Chapter 3.5 of these Comparative Practices observe, information collected in conflict zones may also be used as evidence for the prosecution of other offences, including acts prohibited under international humanitarian law.

1. Sources and Types of Information Collected in Conflict Zones

Responses to the Questionnaire distributed in 2020 revealed that, at the time of their responses, a majority of States (18 out of 29 respondents)[4] had already used information obtained from conflict zones as evidence in criminal proceedings related to terrorist offences. At least two States that in 2020 reported no experience with conflict zone information have since used such information. And nearly all the others reporting a lack of experience in 2020 explained that they had simply not yet handled terrorism-related cases in which information from conflict zones would have been relevant, but that if the need arose they could indeed use such information as evidence. Moreover, in response to the additional Questionnaire distributed in 2023, several States that had not responded to the 2020 Questionnaire reported that they too had used information from conflict zones in terrorism-related proceedings. Overall, this indicates that to date at least 22 of the States surveyed have used conflict zone information in terrorism-related cases.

The information States have used is diverse in nature and derived from a range of sources. Section 1 will outline the potential sources and types of information from conflict zones.

1.1. Sources of Information

Range of sources of information from conflict zones, including from domestic government agencies, agencies in other jurisdictions and intergovernmental mechanisms for storing and sharing information, multilateral actors, and non-governmental actors.

1.1.1. Domestic Sources

Civilian criminal justice actors are usually responsible for gathering evidence in the aftermath of a crime, but often lack either access to potential crime scenes in conflict zones or the authorisation or capacity to collect information there (as has been the case in Syria and, to a great extent, in Iraq). On the other hand, other State actors — notably **militaries and intelligence services** — are often present in conflict zones, and while they do not typically act in a law enforcement capacity, regularly gather significant volumes of information relevant to their own core missions. Information such actors acquire, even if originally collected for military or intelligence purposes, may be crucial to effective criminal prosecutions related to terrorist offences committed in such hard-to-access locations.[5]

1.1.2. Foreign Governmental Sources and Intergovernmental Sharing Mechanisms

Information central to criminal justice investigations can also be obtained from foreign governments and multilateral databases. As recognised in the Recommendation's preamble, the investigation and prosecution of suspected terrorism offences often have a transnational character, making co-operation among States necessary. This has been particularly true in States' efforts to bring to justice members of the self-proclaimed Islamic State of Iraq and Al-Sham (ISIL(Daesh)). It has been estimated that since 2014, ISIL(Daesh) attracted more than 40,000 Foreign Terrorist Fighters (FTFs) from 120 countries to travel to territories it controlled in Syria and

4. This total of 29 respondents does not include Russia, which is no longer a member of the Council of Europe.
5. See CM/Rec (2022)8 Chapter III - Information collected by military personnel, para 6, and Chapter IV – Information collected by intelligence services, para 11. 10 States responding to the 2020 Questionnaire reported that they had used information from military sources as evidence, and at least 10 – not including one which declared itself "not at liberty to reply" to this question – reported that they had used information from intelligence sources. However, the Questionnaire did not ask States to differentiate in these responses between the use of information from their own military or intelligence agencies and foreign agencies.

Iraq.[6] After a Global Coalition of over 80 countries militarily reversed ISIL(Daesh)'s control of territory, many of these individuals returned to their home countries or relocated elsewhere, while others remain detained in camps and prisons in Syria and Iraq — in both cases presenting security challenges.

As the experience combatting ISIL(Daesh) has highlighted, in terms of ensuring accountability for FTFs and others who commit terrorism-related crimes, information collected by the **law enforcement, military, or intelligence** personnel of one State may often be of interest in investigations and/or criminal proceedings carried out **in another jurisdiction**.

One critical resource for sharing information across international boundaries are governmental databases that may encompass information collected by multiple types of agencies. For example, the United States Federal Bureau of Investigation's (FBI) **Terrorist Explosive Device Analytical Center (TEDAC)**, established in 2003, maintains a large database of Improvised Explosive Devices (IEDs), bomb components, and detonators seized by both U.S. military and civilian law enforcement personnel, in addition to some handed over by third countries. TEDAC conducts strategic exploitation of these devices to determine how they function and where the components were sourced, as well as to recover any DNA, fingerprints, or other trace evidence that can link them to individuals.

Intergovernmental mechanisms for storing and sharing information originally obtained by various States represent another important source. **INTERPOL**, for example, maintains numerous databases. Its **Project Watchmaker** database, established in 2014, records the identities and/or methodologies of thousands of known or suspected makers of IEDs. European Union member States also have access to information that other EU member States have obtained and entered into the **Schengen Information System (SIS)**, as well as other databases and information systems including the **Europol Information System (EIS)** and the **Eurodac** asylum fingerprint database.

Operation Gallant Phoenix (OGP), a United States interagency and multinational initiative launched in 2014 to counter violent extremist organisations, has been a particularly important mechanism for international sharing of information from conflict zones. OGP maintains a massive database of information collected in Syria, Iraq, and other conflict zones. Numerous States have cited information provided to them through OGP as crucial to their investigation and prosecution of crimes committed by ISIL(Daesh) and other terrorist organisations.

1.1.3. Multilateral Actors

Multilateral entities that operate in conflict zones have also collected information that may be valuable in terrorism-related proceedings.

In Resolution 2379 (2017), the United Nations Security Council requested the Secretary-General to establish an Investigative Team to support domestic efforts to hold ISIL(Daesh) accountable by "collecting, preserving, and storing evidence in Iraq of acts that may amount to war crimes, crimes against humanity and genocide committed by the terrorist group in Iraq".[7] Since its creation, this team — the **United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL** (**UNITAD**) — has gathered a massive amount of data with significant potential value in proceedings for such crimes committed by ISIL(Daesh). Among other forms of information, the Team has digitised more than 8 million pages of ISIL(Daesh) documents.[8] In addition, the **International, Impartial and Independent Mechanism on Syria (IIIM)** has gathered data that may be similarly valuable, and like UNITAD, is mandated to share it. Other multilateral actors, including the **Independent International Commission of Inquiry on the Syrian Arab Republic (UN CoI Syria),** also maintain relevant databases.

1.1.4. Non-Governmental Actors

Finally, information that a range of private sector actors collect in conflict zones for their own use may have potential evidentiary value in civilian court proceedings. Relevant stakeholders mentioned by the Recommendation and Questionnaire include **civil society** or other **non-governmental organisations (CSOs/**

6. See Explanatory Memorandum to Recommendation CM/Rec(2022)8 (hereafter "CM/Rec (2022)8 EM"), para 20.
7. Security Council Resolution 2379 (2017), para 2.
8. Letter dated 22 May 2023 from the Special Adviser and Head of the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/Islamic State in Iraq and the Levant addressed to the President of the Security Council. It should be noted that in Resolution 2697 (2023), the United Nations Security Council only extended UNITAD's mandate until 17 September 2024, so, while information from UNITAD has been valuable in investigations and prosecutions, as of April 2024 it is yet to be determined whether states will have access to this information for their cases in the future. See Section 2.2.5.

NGOs), **academic researchers and experts**, **news media**, and **private companies and contractors**. A majority of States responding to the Questionnaire reported having used evidence that such non-governmental sources have collected from conflict zones to prosecute suspected terrorists.

1.2. Types of Information

Range of types of information collected in conflict zones, including physical, digital, documentary, intercepted, satellite- or UAS-generated, and statements and testimony.

1.2.1. Physical

The range of material objects recovered from conflict zones is vast, but typically includes **weapons, IED components, mobile telephones,** and **hard drives and other storage media**. Various national and international databases — including some mentioned above such as TEDAC and Project Watchmaker — preserve, store, and analyse specific types of physical material.

1.2.2. Digital

Information may also come in the form of **digital content data**, including **text and other messaging platform communications**, **photos and videos**, **traffic and subscriber data**, and other electronic data such as **cryptocurrency wallet information**. As with physical evidence, various national and international databases are dedicated to preserving, storing, and analysing of such material.

1.2.3. Documentary

Huge volumes of **hardcopy written or printed material** may also be obtained from conflict zones. This includes both personal notes, letters, and journals, as well as official or quasi-official records. In its efforts to bureaucratically establish a self-proclaimed territorial State structure, ISIL(Daesh) was particularly given to documenting all manner of relationships and transactions. Recovered ISIL(Daesh)-related items have included individual enrolment forms, group registration lists, fighters' service records, payroll documents, and documents related to births, deaths, housing, hospitalisation, and taxation, among others.

1.2.4. Intercepted and Satellite- or UAS-Generated

Various State actors **intercept telephonic or other communications** from conflict zones, whether for judicial purposes or in furtherance of their own missions, that may contain information relevant to the investigation and prosecution of terrorism-related crimes. Moreover, given the difficulties of access to the terrain, **geospatial imagery generated by satellites** and **footage obtained by unmanned autonomous systems** (often referred to as "drones") may also have particular evidentiary value.

1.2.5. Statements and Testimony

Finally, statements made voluntarily by defendants or by other subjects of interviews or interrogations, as well as **testimony**, **statements**, and **other information** provided by **witnesses, victims, informants, and other human sources** may also be valuable.

2. Mechanisms to Obtain and/or Share Information

States have used a range of mechanisms to obtain and/or share information from conflict zones for criminal justice use.[9] In any given case, practitioners may not be aware of what relevant conflict zone information is actually available, so whether seeking information from domestic government agencies, from foreign government agencies and intergovernmental mechanisms, or from multilateral and non-governmental actors, the first step to obtain information is a request to search for such information.

2.1. Co-ordination and Information Sharing at the National Level

Legal and procedural mechanisms States have used to mandate or authorise information sharing, enhance domestic interagency co-ordination, and declassify information when feasible and appropriate.

2.1.1. Domestic Legal Frameworks

Some military and intelligence services draw upon their broader institutional mandates for the authority to share conflict zone information with other national or foreign agencies. In other cases, statutory law specifically grants agencies the authority — and sometimes the obligation — to share information. Relevant provisions may be found both in criminal procedure codes and in the statutes governing those agencies themselves. Legislation may thus provide clarity by expressly permitting — or in some circumstances, when it comes to domestic interagency sharing, even requiring — the transfer of information, either at the initiative of those agencies or at the request of judicial authorities.

In Germany, to take one example,[10] the Code of Criminal Procedure allows public prosecutors and police authorities to request information from all public authorities, including intelligence and military agencies, to assist in the investigation of facts surrounding a suspected criminal offence. In terrorism cases, the Federal Prosecutor General regularly requests such information not only from the German Federal Criminal Police, but also from the German intelligence services and other relevant German government agencies. The intelligence services, for their part, are as a general rule not merely authorised to provide prosecutors' offices with relevant information, but may be obligated to do so, if factual indications suggest that doing so is necessary to prevent or prosecute specific crimes.[11]

In a number of States, **services legally endowed with both law enforcement and intelligence functions** can be particularly effective at facilitating the exchange and use of information. The *Direction générale de la sécurité intérieure* (DGSI, or General Directorate for Internal Security) in France is a prominent example. The coexistence of judicial police and intelligence officers in the DGSI enables French judicial authorities to be notified of, and when appropriate obtain, after a declassification procedure, information derived from intelligence collection, including in conflict zones, that may be useful in a criminal investigation.

Other such "double-hatted" services include the FBI, as well as the Swedish Security Service, which possesses law enforcement capacities and can share information with the Swedish Police Authority and the Swedish Prosecution Authority.

9. This supports the Recommendation that States "further strengthen international co-operation and domestic co-ordination on the use of information from conflict zones as evidence for the purpose of criminal prosecution of terrorist and other offences, so as to enhance the exchange of information and best practices."
10. Similarly, in Moldova, the Criminal Code of Procedure allows intelligence services to transmit information to prosecutors for use in criminal proceedings (although the country reports lacking experience doing so for terrorism-related cases).
11. § 20 of the Federal Act on Protection of the Constitution so provides with respect to the Federal Office for the Protection of the Constitution; analogous regulations apply to other intelligence services.

2.1.2. Interagency Co-ordination Mechanisms

Procedurally speaking, States have found that **designating interagency focal points** can facilitate the transfer of information. In the Czech Republic, for instance, transfers of military-collected information to judicial authorities pass through a specialised law enforcement liaison which serves as a point of contact for all the Czech intelligence services.

Several States have also promoted broader co-ordination at the domestic level by establishing **ongoing mechanisms for interagency exchange** and collaboration. **Germany**, for example, has set up a **Joint Counterterrorism Centre (GTAZ)** of this type in Berlin. This information platform conducts daily and weekly briefings for its member agencies, which include the Federal Criminal Police, police offices and intelligence agencies of the German states ("Länder"), the Federal intelligence agencies, the Customs Criminal Office, the Federal Office for Migration and Refugees, and the General Prosecutor's Office General. **Poland** passed counterterrorism legislation in 2016 that created a similar mechanism for security services and other relevant government agencies to co-operate and co-ordinate to prevent and respond to terrorist activity.

In addition to such longer-term mechanisms, States including **Germany** also stand up **special working groups** on an ***ad hoc*** basis when needed to surge resources to address immediate threats. **Denmark** similarly sets up steering committees to enable the Danish Security and Intelligence Service, police, prosecution service, and other relevant stakeholders to collaborate in terrorism-related criminal cases.

These standing and *ad hoc* co-ordination mechanisms have multiple purposes. First and foremost, they can achieve better outcomes in particular investigations and prosecutions. They can also importantly enhance "the mutual trust and co-operation between all competent authorities and services involved".[12] And they can improve relevant domestic actors' familiarity with the availability and usefulness of information from conflict zones and understanding of how to obtain it.[13] Germany reported that by 2020, the possibility of requesting

military-collected information from other countries was common knowledge among prosecutors and investigators in terrorism cases. To this end, some States have also conducted joint trainings of multiple types of practitioners to "improve their knowledge and understanding of the unique nature of the evidence at stake and the exceptional environment in which relevant stakeholders operate in conflict zones".[14]

2.1.3. Declassification Procedures

States have also adopted formal processes to declassify information so it is more readily available for criminal justice uses. Indeed, in some jurisdictions, declassification is a precondition for evidentiary use (see Section 3.4 below).[15] Typically, the **original classifying authority**, which is legally considered to "own" the information, can downgrade its classification either *sua sponte* or at the request of judicial authorities; in some cases, only the most senior figure within that "owner" agency can do so.

Some States have also established **consultative bodies** with the authority to access the information and render advisory opinions on whether it should be declassified. In France, for instance, judicial authorities may ask the *Commission du secret de la défense nationale* (CSDN, or Commission for National Defence Secrecy) to undertake this analysis. The CSDN inspects the material, assesses its purported relevance to criminal proceedings, and issues a reasoned opinion on the advisability of declassification, taking into consideration the interests of justice, the imperative of respecting the presumption of innocence and the rights of the defence, and the need to ensure France complies with international commitments and preserves both its defence capabilities and the safety of its personnel. The Minister at the head of the agency that "owns" the information retains the ultimate authority over the decision to declassify and is not bound by the CSDN's opinion but must take it into account.

Overclassification of information remains a commonly identified challenge. In 2020, in a significant departure from prior policy, the **United States Secretary of Defense** directed that, from that point forward, all newly acquired and unexploited collected exploitable material captured, collected, or handled by U.S. Armed Forces during military operations may be presumed to be unclassified unless sensitive sources, methods, or activities were used to acquire such materials.[16] The Department of Defense made this policy change partly with the

12. CM/Rec (2022)8 Chapter III – Information collected by military personnel, para 10.
13. See CM/Rec (2022)8 Chapter VIII – Co-ordination within States, para 24.
14. CM/Rec (2022)8 Chapter VIII – Co-ordination within States, para 26.
15. See CM/Rec (2022)8 Chapter III – Information collected by military personnel, paras 9 and 10, and Chapter IV – Information collected by intelligence services, paras 11 and 14.
16. That presumption does not apply, however, to intelligence agencies' collections.

aim of sharing such information with partner nations more easily and in order to support investigations and prosecution of individuals that pose a threat to the safety and security to the United States and partner nations.

2.2. International Co-operation

Range of approaches that States take to obtain information, including informal co-ordination, law-enforcement-to-law-enforcement information transfers, and formal mutual legal assistance, sometimes in sequence, as well as investigative co-operation through Eurojust, co-ordination with international organisations and agencies, and searches of international databases.

2.2.1. Informal Outreach to Foreign Counterparts

Practitioners report that in cases where they have shared information from conflict zones with international counterparts, they have often begun the process with informal dialogue between individual law enforcement or other government practitioners. A practitioner in one government, for example, may reach out to a foreign counterpart to discuss an ongoing investigation and broach the possible availability of relevant information in the foreign government's possession. Professional connections based on previous collaborations, as well as larger institutional relationships, can facilitate such informal outreach. Moreover, as law enforcement actors have become more familiar with the evidentiary value of conflict zone information of various types, including digital content, and from various sources, including from military and intelligence agencies, professional connections of this type have played a critical role. International exchanges of information and expertise, including meetings organised by the Council of Europe CDCT, the European Union, the Global Counterterrorism Forum, the IIJ, NATO, and United Nations Global Compact Against Terrorism entities, have nourished and enlarged such connections.

2.2.2. Caveats on Use or Further Sharing of Information

States generally recognise a "**third party rule**", whereby a State agency that receives information from a foreign State refrains from sharing it onward or divulging it publicly without the authorisation of the State that provided it. The rule, also referred to as the "originator control principle", is sometimes but not always enshrined in formal agreements and serves multiple purposes. It not only promotes mutual trust but prevents a State that receives the same piece of information through multiple channels from incorrectly believing it has received multiple pieces of information from independent sources that corroborate each other.

2.2.3. Information Sharing between States through Law Enforcement or Formal Judicial Channels

States often initially, and sometimes exclusively, share information relevant to terrorism investigations and prosecutions in another State directly through **intelligence or law-enforcement-to-law-enforcement channels**. In many cases, the recipient State can then use the information not only for investigative purposes but as evidence in criminal proceedings, unless subject to specific caveats and classification determinations. "Double-hatted" services, such as the French DGSI and U.S. FBI mentioned above, can facilitate such international sharing, particularly since practitioners in some countries are unable to use information received directly from a foreign military or intelligence service for criminal justice purposes.

Dialogue through law enforcement or intelligence channels may lead the originator State to declassify the material, remove caveats attached to its initial sharing, or otherwise authorise its use for criminal justice purposes. In Switzerland, for example, when the *Service de renseignement de la Confédération Suisse* (Swiss Federal Intelligence Service, or SRC), receives information from a foreign service that has evidentiary value in a terrorism case, the SRC requests the partner service's authorisation to use the information in legal proceedings. In the United Kingdom, law enforcement agencies receiving material from a foreign government that has evidentiary value similarly endeavour to obtain the material in declassified form.

In other cases, States may choose, or may even be required, to make **formal requests for assistance through diplomatic channels**. States including Austria, Germany, and the Netherlands have found the **mutual legal assistance (MLA)** process a valuable tool. Relevant authorities may issue MLA requests for information originally obtained from conflict zones just as they would for information originally obtained elsewhere. In doing

so, however, they should be aware that as a practical matter, it is less likely than in other MLA cases that the original collectors will be made available for testimony (see Section 3.5.2 below).

Within the European Union, information-sharing is underpinned by Council Decision 2005/671/JHA on the exchange of information and co-operation concerning terrorism offences, as recently amended by Directive (EU) 2023/2123.

EU member States seek information from each other using the **European Investigation Order (EIO)**. An EIO is a judicial decision issued in or validated by the judicial authority in one EU country to have investigative measures to gather or use evidence in criminal matters carried out in another EU country.[17] Several EU member States, including Germany, Poland, and Spain, report having used the EIO to share and request information from conflict zones.[18]

Eurojust also facilitates mutual legal assistance processes, including the use of judicial co-operation instruments such as the EIO and joint investigation teams (JITs), allowing *inter alia* the transfer of evidence from one country to another. Eurojust can also contribute to enhancing the use of information from conflict zones through its co-ordination among national authorities and can provide guidance on the categories of information that will be useful for criminal proceedings.

Sometimes formal processes may simply improve the odds of obtaining the information in declassified and/or unrestricted form. In the United Kingdom's successful prosecutions that have relied upon military-collected information provided by foreign governments, for example, formal MLA requests led those international partners to declassify the information for use at trial.[19]

In other instances, obtaining the information through formal judicial channels may be a condition for admissibility. In Italy, for instance, prosecutors may use information gathered by military services in criminal proceedings, but only if they receive the information via the judicial police. Even in jurisdictions where admission into evidence is more discretionary, courts may have greater confidence admitting and relying upon information that has been shared via formal processes.

Many States draw upon all of the above approaches to obtain information, sometimes in sequence, depending on the nature and needs of a case. This **flexible approach** might commence with informal officer-to-officer exchanges, followed by exchanges through more institutional law enforcement or intelligence channels, and concluding — in the final pre-trial phase — with formal requests.[20] Türkiye reports, for example, that international judicial co-operation may proceed according to a relevant Council of Europe convention, if both Türkiye and the other country are parties; under a bilateral agreement, if one exists; or on the basis of the international law principle of reciprocity, where no convention or agreement is in force. Austria's *Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* (BVT, or Federal Office for the Protection of the Constitution and Counter Terrorism) shares evidence and intelligence both on a bilateral and multilateral basis. And German authorities seek to obtain conflict zone information from another government, where there are indications that such information is available, either through a police request, an EIO, or a judicial request for mutual legal assistance.

States may increase the likelihood of receiving the information they request by providing not just specific details about the particular crime under investigation or a particular individual suspected of committing it, but also details showing that the information will make a concrete difference to the investigation or prosecution in question. States therefore broadly consider it vital for practitioners who receive the information they request to **share feedback with information providers**, whether through informal or formal channels, to update providers on how the information was used and why it proved valuable. This feedback encourages collaboration and can improve future co-operation.

2.2.4. Intergovernmental Databases and Information-Sharing Initiatives

States also regularly conduct or submit requests for targeted searches of intergovernmental databases and information systems, and have found the results to be valuable sources of information originally obtained from conflict zones.

17. See Eurojust, "European Investigation Order," at https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order.
18. The EIO Directive, which establishes a single regime for obtaining evidence held and gathered in another EU member State, applies to all EU member States bound by it (Ireland and Denmark are not bound by it).
19. Such treaty-based sharing may also come with some conditions specifying the information's permissible uses, of course.
20. It might also include requests for searches of intergovernmental databases and information systems. See Section 2.2.4 below.

INTERPOL, for example, maintains a range of relevant databases in addition to Project Watchmaker's, including databases specifically focused on FTFs and travel documents. And through the **Military-to-Law-Enforcement Exchange Programme, or Mi-Lex,** pioneered in Afghanistan and Iraq, INTERPOL has enabled its member States to share information derived from military sources with law enforcement officers, through regional *Plateformes de Cooperation en Matière de Sécurité* (PCMS, or Security Cooperation Platforms), and INTERPOL's network of National Central Bureaus.[21]

The EIS and SIS databases mentioned in Section 1.1.2 above are more limited in scope: only EU member States can nominate information for inclusion, and only EU member States can make search requests. In a number of instances, States have submitted information to the EIS and SIS that has later proven valuable in terrorism investigations and prosecutions: France, Hungary, and the Netherlands, among others, report obtaining conflict zone information from these databases that was later used as evidence.

States also use a well-developed process to request searches for information stored at Operation Gallant Phoenix (OGP). The United States has created a standardised form that States can use to make targeted but detailed requests. Agencies are encouraged to prioritise suspects in terrorism-related investigations, and to provide as much relevant information on their highest-priority suspects as possible. This might include the criminal conduct the individual is suspected of committing, any record of previous criminal activity, travel history, role in terrorist group, associates, and family members. Providing information on the potential charges, and on how the information sought is important to securing a conviction on those charges, may also be helpful. FBI legal attachés at U.S. Embassies around the world (or "Legats") act as conduits for the submission of search requests to OGP, engage in preliminary discussions with government agencies to help them frame search or information requests they are considering; facilitate the passing of responsive results through appropriate channels, and provide any follow-on assistance required.

To further facilitate the flow of information, some States have also deployed representatives from various agencies, including intelligence as well as law enforcement personnel, to OGP on an ongoing basis. Some States also see value in designating a single national focal point for the sharing of information from military sources that has potential evidentiary value. Spain, for instance, has established the Counterterrorism and Organised Crime Intelligence Centre (CITCO) as a national contact point in charge of co-ordinating the exchange of information with OGP. Formally designating such focal points may clarify which agency, and within that agency which individual, has primacy in this process. It could also build more institutional memory of sharing conflict zone information internationally. Initiating this process through the informal, often personal arrangements discussed above may be effective in many cases, but carries the risk that, when the individuals involved leave government or simply take on new roles, relationships must be rebuilt or are lost.

2.2.5. Co-ordination with Multilateral Actors

Some States actively co-ordinate with multilateral actors operating in conflict zones that may themselves have collected relevant information. For example, the French *Parquet national antiterroriste* (PNAT, or National Counterterrorism Prosecutor's Office) at times makes mutual legal assistance requests to obtain evidence collected by a range of United Nations bodies, including the IIIM, UNITAD, and various commissions of inquiry.

Many of these bodies have an affirmative obligation to safeguard and share information they collect. UNITAD's Terms of Reference, for instance, mandate that "[t]he Investigative Team shall systematically organise, catalogue, record, preserve and store … evidence and materials in Iraq … in order to ensure their broadest possible usability and admissibility in fair and independent criminal proceedings, consistent with applicable international law, conducted by competent domestic courts in Iraq and other States".[22] According to the 16 November 2023 letter from the Special Adviser and Head of the Investigative Team to the President of the Security Council, UNITAD has fielded requests for assistance from 20 other States in addition to Iraq - and from 45 competent authorities within those States - and has supported ongoing proceedings in a growing number of those jurisdictions. The Special Adviser writes, "[t]he ability of the Team to collect testimonial evidence from witnesses in direct response to requests for assistance, combined with its capacity to identify corroborating internal Da'esh/ISIL documentation from digital battlefield evidence, has been and continues to be of significant assistance in supporting investigations by national jurisdictions".[23] In Resolution 2697 (2023), the United Nations Security Council only extended UNITAD's mandate until 17 September 2024, so, while information from UNITAD has

21. See INTERPOL, "G5 Sahel," located at https://www.interpol.int/en/Crimes/Terrorism/Counter-terrorism-projects/G5-Sahel#:~:text=Ensuring%20military%20to%20law%20enforcement,and%20INTERPOL%27s%20network%20of%20NCBs.
22. Emphasis added. See https://www.unitad.un.org/sites/www.unitad.un.org/files/general/tor_1.pdf
23. See Letter dated 16 November 2023 from the Special Adviser and Head of UNITAD to the President of the Security Council.

been valuable in investigations and prosecutions, as of April 2024 it is yet to be determined whether States will have access to this information for their cases in the future.

The UN General Assembly created the IIIM in 2016, intending it to operate both "as a clearinghouse of information produced over the years by other entities - including the [UN CoI Syria], civil society actors, and governments - but also as a proto-investigative team gathering its own information to fill gaps in the evidentiary record and prepare files for future prosecutions"[24] of atrocity crimes committed on Syria's territory since March 2011. According to its 14 February 2024 report to the General Assembly, the IIIM has fielded 344 requests for assistance from 16 competent jurisdictions, already "assisted 166 distinct national investigations… through the sharing of information, evidence and/or analytical products", and to an increasing extent also proactively shares relevant information with judges and prosecutors.[25]

The International Criminal Court (ICC) may also share information with domestic judicial authorities under some circumstances. The ICC's jurisdiction, which is "limited to the most serious crimes of concern to the international community as a whole", namely genocide, crimes against humanity, war crimes, and the crime of aggression,[26] is "complementary to national criminal jurisdictions".[27] Article 93(10) of the Rome Statute empowers the ICC to engage in what scholars have termed "positive complementarity", providing that "the Court may, upon request, co-operate with and provide assistance to a State Party conducting an investigation into or trial in respect of conduct which constitutes a crime within the jurisdiction of the Court or which constitutes a serious crime under the national law of the requesting State" — assistance which may include the "transmission of statements, documents or other types of evidence obtained in the course of an investigation or a trial conducted by the Court".[28]

2.3. Obtaining Information from Non-Governmental Actors

Channels to communicate with NGOs/CSOs, news media, and other private sector actors and encourage them to share information.

A number of States have also established channels to communicate with NGOs/CSOs, news media, and other private sector actors and to encourage them to share information. The French PNAT has received information from NGOs working in conflict zones that collect testimony and various documentation, take photos that may have evidentiary value, and produce videos that can constitute evidence; the reliability of this information is closely verified by the judicial authorities. The Netherlands has similarly established working relations with some NGOs that maintain databases of digital material documenting crimes in Syria and/or Iraq, and Dutch judicial authorities have obtained relevant videos or other information from these databases for use as evidence in a number of cases.

Austria, Denmark, Georgia, Germany, Hungary, Serbia, Spain, the United Kingdom, and the United States have also used documents, forensic evidence, or witness statements provided by NGOs, private companies, or news media. Spain, for example, has used information obtained from news media as the basis for issuing an INTERPOL Red Notice.

In the ***Mohammed Abdallah*** **case**, for example, the United Kingdom introduced into evidence at trial a registry of ISIL(Daesh) fighters that a defector from the group had originally provided to Sky News. The defendant Abdallah, whom the registry categorised as a volunteer sniper and described with personal details that the police later corroborated, was found guilty of terrorism-related charges and sentenced to 10 years' imprisonment.

The **Commission for International Justice and Accountability (CIJA)**, a non-profit NGO working to gather evidence of atrocities committed in difficult-to-access areas, has proven a particularly prominent non-governmental source of conflict zone information. As of April 2024, CIJA's website reports that since 2014 its field investigators in Syria and Iraq have secured "a wide range of Da'esh-related material including foreign fighter passports, computer hardware, recruitment forms, and other organisational documents, preserving over 58,000 pages of documents in its dedicated Da'esh archive", as well as interviewing more than 1,300

24. Beth Van Schaack, "Innovations in International Criminal Law Documentation Methodologies and Institutions," February 5, 2019, SSRN, at https://ssrn.com/abstract=3329102 or http://dx.doi.org/10.2139/ssrn.3329102.
25. Letter dated 14 February 2024 from the United Nations Secretary-General, transmitting to the General Assembly the tenth report of the International, Impartial and Independent Mechanism to Assist in the Investigation and Prosecution of Persons Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011.
26. Rome Statute of the International Criminal Court, Article 5(1).
27. Rome Statute, Article 1.
28. Rome Statute, Article 93(10).

related witnesses.[29] CIJA's team, made up of individuals experienced in the investigation and prosecution of international crimes, conducts structural investigations and assembles legal briefs that it provides to courts with jurisdiction, in a number of cases supporting convictions of ISIL(Daesh) fighters.

Conflict Armament Research (CAR), a non-governmental investigative entity, documents illicit weapons, IEDs, ammunition, and related material in conflict-affected locations across the globe. CAR then traces supply sources and releases the data onto the European Union-funded iTrace system, a rapidly expanding global dataset which may contain information with evidentiary value.[30]

Generally speaking, States assess on a case-by-case basis whether a non-governmental actor is a reputable and reliable source of information related to a particular conflict zone. It is worth noting that in 2022 Eurojust and the Office of the Prosecutor at the ICC issued a set of guidelines that aim to assist civil society organisations in collecting and preserving information related to international crimes and human rights violations that may become admissible evidence in court.[31]

29. CIJA, "Da'esh / Islamic State," at https://cijaonline.org/daesh-islamicstate.
30. See Conflict Armament Research, "iTRACE," at https://www.conflictarm.com/itrace/.
31. See Eurojust, "Eurojust and ICC Prosecutor launch practical guidelines for documenting and preserving information on international crimes," at https://www.eurojust.europa.eu/news/eurojust-and-icc-prosecutor-launch-practical-guidelines-documenting-and-preserving-information.

3. Steps to Analyse and Use Information

States have taken a range of steps to analyse the probative value of information from conflict zones and to make it easier for practitioners to use the information in criminal proceedings, whether as an investigative lead, as a way to otherwise support legal process, or as evidence in court.

3.1. Human Rights Standards and Safeguards[32]

Fair trial rights (Art 6 ECHR) and applicable human rights standards (Art 3 ECHR).

In the prevention and suppression of terrorism, member States may never act contrary to their obligations under international law, including international human rights, humanitarian and refugee law. In using information collected in conflict zones as evidence in civilian criminal proceedings related to terrorist offences, member States recognise the importance of acting in accordance with the requirements of the **European Convention on Human Rights**, as well as other applicable international human rights standards. All action should be proportionate to legitimate aims and in accordance with the rule of law. No measure should be applied in a way that is discriminatory as regards sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

The **right to a fair trial enshrined in Article 6** of the European Convention on Human Rights applies to criminal proceedings regardless of the criminal offence.[33] National security considerations may, in certain circumstances, call for heightened procedural restrictions. Nevertheless, even where national security is legitimately at stake, member States must ensure that measures affecting fundamental human rights, such as the right to a fair trial, are proportionate, lawful, and necessary to achieve their protective function. And irrespective of the seriousness of the charges, using statements obtained in breach of **Article 3** of the European Convention on Human Rights will render the proceedings as a whole unfair, constituting a breach of Article 6.[34]

3.2. Analysis for Case-Building Purposes

Assessment of the information's potential evidentiary value and determination of the next investigative steps to be taken, including to generate further evidence for use either in support of or in lieu of the conflict zone information itself, to otherwise support domestic legal process, or to advance investigations and prosecutions in other jurisdictions.

3.2.1. Assessment and Use to Generate Investigative Leads

When criminal justice practitioners obtain information from conflict zones that appears relevant to a terrorism case, they first assess the information's potential evidentiary value: is it authentic and reliable? What facts does it tend to prove? What criminal conduct might it be linked to? Would a court likely admit and rely upon it? They then determine the next investigative steps to be taken, evaluating the investigative avenues the information suggests (including opportunities to gather further information through various forms of international co-operation discussed above).

In any investigation, law enforcement officers, examining magistrates, and prosecutors – depending on the jurisdiction – attempt to gather all relevant information to establish whether a crime has occurred, and if so, how it was committed and who is responsible. The first way information from conflict zones is used, therefore, is to aid in this endeavour by **generating investigative leads and filling gaps in the understanding of the facts**.

32. While human rights standards and safeguards are referenced in this Section, as the criminal process is the most likely stage for the adjudication of related issues, they may also apply to the means by which States gain access to and share information.
33. See ECtHR, *Ramanauskas v. Lithuania* [GC], 2008, § 53.
34. See ECtHR, *Gäfgen v. Germany* [GC], 2010, § 166. Many States have reinforced this ban by expressly incorporating it into their domestic codes of criminal procedure.

Key types of additional information to which conflict zone information may lead practitioners include social media posts or messages and other open-source digital material; intercepts of suspects' communications; interviews with family members, friends, co-workers, and other associates; statements of "insider witnesses" who have disengaged from terrorist organisations and can recount first-hand versions of events; and interviews of suspects themselves. Türkiye, among other States, observed that information from conflict zones can lead to the uncovering of by independent physical evidence, digital information from a variety of sources, and testimonies of multiple witnesses.

Conflict zone information can be a critical investigative building block even when it is incomplete, unverified, and/or inadmissible in court. Some courts have recognised this expressly. In 2022, for instance, the **Supreme Court of the Czech Republic** upheld a Czech citizen's conviction for **terrorist offences on the Ukrainian territory of Donetsk and Luhansk**, rejecting claims that the conviction was infirm because the investigation had relied in part on a report from Ukraine's counterintelligence service containing information it had gathered from the conflict zone in Ukraine. The court ruled that while Czech authorities had used the information in question to further their investigation, they had not introduced the report itself as evidence, so its admissibility was not at issue.

Practitioners may also use conflict zone information at various stages of legal process in other ways that do not depend on a judicial finding of admissibility. Depending on the governing domestic criminal procedure framework, information may be used, for instance, to justify subpoenas and other formal requests for information, obtain judicial authorisation for a search warrant, or elicit a suspect's co-operation or a defendant's guilty plea, without being introduced as criminal evidence in court.

3.2.2. Proactive Sharing with Foreign Authorities

The "assessment of what is most efficient in terms of ensuring justice"[35] will often require practitioners to review charging options and to identify and attempt to resolve jurisdictional issues. This may lead practitioners to conclude that the information would be most valuable to an investigation in another jurisdiction. In such cases, although the sheer volume of potentially relevant information collected and the information's classification make sharing more challenging, States sometimes proactively push out such information, whether formally or informally, through bilateral or multilateral channels (see Section 2.2.2 above). The Netherlands, for example, reports spontaneously sharing with other countries information obtained from refugees, victims, FTF returnees, or witnesses when it relates to international or terrorism-related crimes. In determining what information to share, States that possess significant volumes of information may prioritise information that is likely to advance the investigation and prosecution of particularly serious crimes. The United States' stores of documentary and digital information obtained from conflict zones are so massive that it must conduct this type of triage, and will conduct searches upon request. However, when TEDAC's exploitation and analysis of biometrics recovered from IEDs or components appears to uncover the identity of a bombmaker, the United States typically takes the initiative to share that information with that individual's country of origin and/or likely location.

3.3. Admitting Conflict Zone Information into Evidence

Procedures and techniques for introducing conflict zone information as evidence while protecting sources and methods and other national security interests.

3.3.1. General Admissibility Considerations

Generally speaking, the criminal procedure codes of States that are members of the Council of Europe do not prevent information that implicates national security matters from being introduced as evidence in national civilian criminal proceedings. Numerous States have taken the position that such information should be considered, admitted, and weighed according to the **same procedural and evidentiary rules as any other information**. Many civil law jurisdictions adhere to the foundational principle of free evaluation of evidence, or *liberté de la preuve*, according to which the court can evaluate evidence unfettered by formal rules excluding certain categories of evidence or assigning predetermined levels of probative value. Even in most common

35. CM/Rec (2022)8 Chapter VII – Use of information collected in conflict zones for the prosecution of offences other than terrorism, para 22.

law systems, however, there is no categorical bar to admitting information from conflict zones. In the United Kingdom, for instance, if such information is assessed to be authentic and reliable and meets ordinary standards of admissibility, then the court may admit it as evidence.

It is worth noting that the results of this survey of States' practices are consistent with the findings of Eurojust's September 2020 Memorandum on Battlefield Evidence, which focused specifically on military-collected information. That study concluded that, as a general matter, "use of battlefield evidence is not excluded under national law".[36]

Some national courts have explicitly stated as much. In Switzerland, for example, the Federal Court has held that unclassified reports that the Swiss Federal Intelligence Service draws up for the attention of the Federal Prosecutor's Office (MPC) may be considered as evidence and thus included in criminal case files. Such judicial validation of the evidentiary use of information provided by non–law enforcement agencies offers useful clarity and predictability to courts considering such evidence in the future.

3.3.2. Protection of National Security Interests

The larger issue for most States is not whether information from conflict zones is theoretically admissible as evidence, but **how to integrate such information into criminal proceedings** in a way that ensures the protection of sensitive sources and methods of collection, among other national security interests, while complying with fair trial guarantees. States have used various mechanisms and procedures to address this challenge.

In some systems, information may be introduced in criminal proceedings even *without* being formally declassified. Germany, Hungary, and Romania all report that this is the case. In most jurisdictions, however, material collected by military, intelligence, or other non–law enforcement actors must undergo **formal declassification, certification by its owner agency, and/or redrafting** by law enforcement authorities before it can be introduced as evidence.

Regardless of the prerequisites to admissibility, national security interests may warrant protective measures to avoid revealing information to a defendant alleged to have committed terrorism-related offences. As a practical matter, therefore, States have used the procedures described in Section 2.1.3 above to obtain information in declassified form for use in criminal proceedings. Often, however, the information and/or the sources and methods of its collection cannot be declassified in full. Authorities in many jurisdictions have used **partial declassification** and re-drafting to introduce the information in redacted or summarised form, blocking out or omitting passages that cannot be declassified or information about the sources and methods of its collection that cannot be exposed to the view of the defence or the public. They have likewise invoked **security interests** to **justify withholding related material** that might otherwise be subject to disclosure to the defence.

In **France**, for example, initially classified information can be incorporated into criminal proceedings following a spontaneous declassification process known as ***judiciarisation***. In practice, in proceedings concerning terrorist offences, declassified information is transmitted to the judicial authorities by the DGSI, the lead department in the fight against terrorism, after authorisation by the relevant ministry. The DGSI draws up a report summarising the information gathered by the intelligence services, initially covered by national defence secrecy, which it chooses to reveal to the judicial authorities, omitting the elements which remain covered by secrecy. This report is forwarded to the judicial authority.

The DGSI's "double competence" facilitates this process. In the case of information or items in the possession of the French military, the Minister of the Armed Forces can either respond directly to a request from the judicial authorities, or spontaneously send the documents or objects in question to the DGSI. The DGSI draws up a report including this information and sends it to the competent magistrate for inclusion in the proceedings. Exploited documents or objects are placed under seal.

In **Germany**, intelligence services in practice similarly transmit information to judicial authorities through a ***Behördenerklärung*** **(official governmental certification)** procedure, through which they provide relevant information accompanied by an assessment of its reliability without revealing where, how or from whom it was collected. Information shared through this procedure may be used to initiate an investigation or even be introduced as evidence in court, but in general is not sufficient to convict the accused without corroboration, at least by other circumstantial evidence. Likewise, in **Hungary**, intelligence-derived information may be transformed into evidence by the issuance of **legality documents** (or official permits), though only in cases involving crimes of a certain gravity. And in **Switzerland**, as already mentioned, the Swiss Federal Intelligence

36. Eurojust, *September 2020 Memorandum on Battlefield Evidence*, p 21.

Service also renders intelligence-derived information usable as evidence by sending the Federal Prosecutor's Office an **official report** containing the **information in unclassified form**.

In the **Netherlands**, documents produced by ISIL(Daesh) and obtained from military or intelligence sources have been transformed into evidence to sustain multiple guilty verdicts in terrorism-related proceedings. The first such case, tried to the **Rotterdam District Court** in 2017, involved an **ISIL(Daesh) membership registry**. Rather than declassify the entire document, which would not have been feasible, the Dutch Military Intelligence and Security Service prepared a **report containing declassified extracts** concerning the individual accused in the case at hand. The court admitted and relied upon this intelligence report in delivering a guilty verdict. In a separate but similar case, **Belgium**'s intelligence service provided judicial authorities with three **ISIL(Daesh) payroll roster entries**, which the **Court of Antwerp** relied on in convicting a suspect of membership in the group. The Belgian court explicitly stated that it considered this information proof that that the accused was an ISIL(Daesh) fighter.

In the **United States**, when evidence cannot be declassified in full, prosecutors may seek to declassify the relevant portions and, in conjunction, use the **Classified Information Procedures Act (CIPA)** to protect any remaining classified information, as well as sensitive sources and methods. CIPA is a procedural statute that protects against the unauthorised disclosure of classified information. Under CIPA, the prosecutors may seek court authorisation to delete certain classified information from discovery and/or to provide required information to the defence in the form of unclassified summaries.

Conflict zone information is routinely used in public hearings. In the Netherlands, for example, information the Dutch Military Intelligence and Security Service receives from foreign partners is not just included in the case file, which is shared with the defence as well as the judges, but also discussed in open court and mentioned in public judgments. In some jurisdictions, however, criminal procedure allows for the **selective closing of the courtroom** to the public when necessary to protect information or avoid other security risks. In Germany, for example, among other special procedures for introducing classified information as evidence, the court may exclude the public from a hearing or from a part thereof as needed.

In the United Kingdom, where secret/sensitive material is identified as meeting the disclosure test, the prosecutor can make a Public Interest Immunity (PII) application to the court for a court order to withhold the material from the defendant. The court will consider the PII application in a closed hearing, in the absence of both the defendant and his counsel. If the application is successful, the material will be withheld from the defendant. In some situations, the court may appoint an independent "special counsel" to assist the court and to safeguard the interest of the defendant. The special counsel may not disclose to the defendant the secret/sensitive material disclosed to him. If the PII application is unsuccessful, the options are to disclose the material in a way that does not compromise the sensitivities in issue; to abandon the case; or to disclose the material because the overall public interest in pursuing the prosecution is greater than in abandoning it.

To provide an additional layer of protection, some courts have required prosecutors and defence counsel to obtain **security clearances** before handling certain information. In Romania, for instance, criminal procedure permits classified information to be introduced as evidence at trial, but only if the agency providing the information clears both counsel to access it. Security clearances for counsel are also integral to CIPA's operation in the United States, and to the use of special advocates in PII hearings in the United Kingdom.

3.4. Corroborating Authenticity and Reliability and Supporting Probative Value

Techniques to explain the information's significance, describe the context of its collection, attest to its integrity and chain of custody, or otherwise corroborate its authenticity and reliability and/or support its probative value.

In many legal systems, nothing prevents conflict zone information from forming the decisive or even the sole basis for a criminal conviction. As a practical matter, however, **corroboration that bolsters the information's authenticity and reliability and supports its probative value is crucially important**. This is in part because the exceptional circumstances under which the information was collected often lead to gaps in its chain of custody.[37] Demonstrating an item's chain of custody can be particularly important when it comes to material evidence, such as weapons and phones, which can be indistinguishable on their face; it may be less so for documents that are significant for their contents, which can be independently verified.

In either case, a complete and unbroken chain of custody is not a requirement for admissibility. In common law as well as in continental jurisdictions, gaps in the chain typically go to the weight of the evidence, not to

37. See CM/Rec (2022)8 EM, Chapter VI – Chain of custody and risk of alteration.

its admissibility. Nevertheless, courts in many jurisdictions may attribute very little evidential value to evidence if they are unable to determine where, when, and/or by whom it was obtained. Moreover, beyond concerns about the information's provenance and any potential contamination, corroboration and support may be crucial to verifying its content and to explaining its significance to the prosecution's case.

3.4.1. Introducing Technical Analysis Results, Documentation, or Contextual Information

Practitioners have used a variety of techniques to corroborate and support conflict zone information. In some circumstances, they are able to obtain the **original physical item** itself. This allows law enforcement personnel to conduct their own **analysis and exploitation**, independent of any earlier analysis and exploitation by personnel of the foreign government that collected it. Italian authorities took this step in the so-called "**Mamma ISIS" case**, involving an Italian citizen who had travelled to Syria, together with his wife and their children, to join that organisation; the wife was later arrested and transferred to Italy. Operation Gallant Phoenix had in the meantime obtained information related to the couple's activities in Syria, including their mobile phones, which were analysed and found to contain information demonstrating the woman's willing participation in ISIL(Daesh). After the FBI provided the phones and analysis results to the public prosecutor at the court of Milan, Italian authorities conducted their own mobile forensic analysis and used the results at trial to help corroborate the incriminating information. The court found the woman guilty of membership and participation in a terrorist organisation and sentenced her to four years imprisonment.

French authorities have also taken possession of IEDs and original hardcopy documents that the United States originally recovered from conflict zones, then re-exploited and placed them under seal as evidence. In the Netherlands, the national forensic institute may analyse the authenticity of written documents, photos, or videos obtained from a conflict zone in order to facilitate their use as evidence.

In many instances, however, the original version of a document or the physical item itself maybe unavailable. In such cases, many systems permit a **copy or description of the item** to be introduced as evidence. In Germany and Denmark, for example, when an item itself is not available, a court may admit as evidence a photograph or (in the case of an electronic device) a forensic copy. Similarly, in Sweden a photograph of an item suffices in most cases, and in Belgium a prosecutor typically introduces a digital copy of a mobile phone's contents but not the phone itself.

To overcome any challenges to an item's authenticity or integrity, it may be valuable to include **official documentation of handling, transmission, storage, analysis, and sharing** processes. Even in a continental jurisdiction, where there is no chain of custody requirement, information about where, when, by whom, and under what circumstances evidence was collected or obtained can bolster its value in court.

Credibly documenting the processes by which evidence has been collected, handled and shared, however, depends on each State having implemented these types of standard processes in the first place. It is for this reason that the Recommendation — while stressing that "activities related to the collection of information in conflict zones by military personnel should by no means impair the effective performance of their primary tasks" — nevertheless suggests that States "should provide adequate training to officials involved in the process of collecting such information in order to improve its evidentiary value" and encourages States "to develop and provide relevant stakeholders with clear policies and procedures on how to preserve the chain of custody, ensure traceability and preclude any risk of alteration of the information collected in conflict zones".[38]

In practice, a number of States and multilateral actors have developed these types of policies and procedures and offered training on how to comply with them. In the United Kingdom, for example, national police investigators have delivered trainings for Global Coalition forces on collection, documentation, and storage processes for material they may seize on the battlefield. Various countries have also offered training for military as well as law enforcement personnel from partner countries on collecting and preserving data from sensitive sites to support terrorism investigations.

Operation Gallant Phoenix has notably established highly systematic processes for handling, storing, exploiting, and analysing material, with a view to preserving its integrity and ultimate usefulness for investigations and prosecutions. The FBI Legats which share information with partner countries are typically able to provide OGP documentation of these processes, along with specific contextual information on an item's place and

38. CM/Rec (2022)8 Chapter III – Information collected by military personnel, para 6; Chapter VIII – Co-ordination within States, para 25; and Chapter VI – Chain of custody and risk of alteration, para 19.

date of origin and the conditions of its storage. This documentation has reinforced courts' confidence that information supplied by OGP is authentic and reliable.

Providing contextual information about the circumstances of collection and subsequent processing has been crucial to corroborate and support the value of various types of conflict zone information. In a particularly striking example, the 2018 ***Khalid Ali* case** in the United Kingdom turned in part on the admission of the defendant's fingerprint, which TEDAC detected on IED components recovered in Afghanistan years earlier. The FBI provided UK authorities with a report documenting in detail how the IED components had been collected, preserved, and forensically examined. The report was instrumental in the admission of the fingerprint evidence, which led to Ali's conviction for possession of explosive substances, among other charges, and sentence of life imprisonment.

3.4.2. Introducing Additional Physical or Digital Evidence

More generally, beyond forensic or contextual confirmation of authenticity, States have found that **identifying and introducing corroborating evidence** is essential if information from conflict zones is to be accorded its full probative value in court.

In some cases, **multiple independent items of conflict zone evidence** concerning the same individuals and same conflict zone may be available and can corroborate each other's relevance. In France, the so-called **"Ulysses" trial** at the Special Assize Court of Paris in 2021 was one such case. One of the ISIL(Daesh) operatives on trial disputed not just allegations that he had joined the group and had recruited and raised funds on its behalf, but the very fact that he had travelled to Syria. Through co-operation with Operation Gallant Phoenix, a document drawn up by an ISIL(Daesh) administrative office clearly indicating that the accused had been present in Syria and registered by the terrorist organisation as a "combatant" was communicated to the DGSI and introduced in the proceedings. In the same way, further documents obtained in that conflict zone, including records of food and petrol distribution to the defendant, and the receipt for a pension given to his mother due to his status as a supposed "prisoner-martyr" were transmitted to the judicial authorities and included in the case file. The court took into account all these concordant elements demonstrating the accused's membership of the ISIL(Daesh) terrorist organisation, and sentenced the accused to 30 years imprisonment.

A recent example in the United States is the **2023 trial of Ibrahim "Izzy" Musaibli**. During that trial, prosecutors introduced various different ISIS records and documents relating to Musaibli, some obtained by the U.S. military and partner forces and others collected by UNITAD. The prosecutors were able to corroborate much of the content of each of the individual documents, as well as show that the content across these multiple documents was consistent, thereby helping to reinforce the authenticity of all of the documents. Musaibli was convicted of providing material support to ISIL(Daesh) after trial and sentenced to 14 years in prison.

More typically, practitioners have relied upon **material generated from other sources** to support findings that conflict zone evidence is authentic and reliable. In the **2017 case** in the Netherlands mentioned earlier, in which an ISIL(Daesh) registry recorded the suspect's membership, the **Rotterdam District Court** verified the document's authenticity and reliability by comparing the information it contained with that of the Dutch Civil Registry, as well as with the defendant's own statements and with his Yemeni passport, which was found elsewhere.

Courts have also found independently gathered supporting material to be valuable, not just to verify conflict zone information, but to further substantiate the elements of the charges that information is used to prove. In the ***Anis Sardar* case**, one of the U.K. Crown Prosecution Service's major tasks was demonstrating that the defendant's intent, in deploying IEDs in Iraq, was to kill U.S. soldiers, not solely Shi'ite militia members. It succeeded in doing so, in part, by introducing as evidence the collection of CDs that Sardar brought with him when he returned from Iraq to the United Kingdom, "within which there was not only an explosives manual, which included a formula to make TNT, but also material of a violently anti-American nature". The defendant himself, when subsequently "pressed in cross-examination[,] described [his] 'fury' at the Americans' intervention into Iraq". The sentencing judge called this "illuminating" and declared himself "satisfied that at the material time, [Sardar] had the mind-set that made the Americans every bit as much the enemy as the Shi'ite militia. Both were in your contemplation at all times".[39]

Open-source material, such as media reports or studies conducted by non-governmental organisations, may also help to contextualise and explain the significance of information obtained from conflict zones. **Digital**

39. *R* v *Anis Sardar* Sentencing Remarks.

open-source information may be particularly valuable; while the credibility of such information may itself be subject to challenge, a specific set of verification techniques has proven effective. The *Berkeley Protocol on Digital Open Source Investigations* sets forth a series of useful steps to establish the accuracy or validity of information that has been collected online.[40] In practice, when authorities in a country such as the Netherlands obtain digital material documenting crimes in Syria and/or Iraq, the police take advantage of geolocation and other digital forensic techniques to analyse and verify the information before using it in a criminal case.

3.4.3. Introducing Supporting Testimony

In many cases, States have found **supporting testimony** a powerful tool to corroborate the reliability and enhance the probative value of conflict zone information. In some instances, the individuals who actually collected the information may be available for testimony. More often than not, however, it may prove impossible to locate them or to secure their testimony. Yet a range of other witnesses may be able to describe the circumstances under which the information was collected, attest to its integrity and chain of custody, and/or explain its significance.

Potential witnesses include **senior officials or technical specialists representing** the **State agencies** involved. In the United Kingdom's ***Sardar* case**, the court heard testimony from the leaders of the U.S. Explosive Ordinance Disposal Team that was active in that conflict zone when the information was collected. These witnesses, while not involved in the actual collection of the particular IED components introduced as evidence, were able to describe how forces received, handled, and processed material generally, and to contextualise the evidence in this respect. They also brought their first-hand expertise to bear to demonstrate the evidence's significance to the charges in the case at hand: the sentencing judge found persuasive their explanation that "the deployment of the double pressure plates [used in the IEDs in question] was such that they were designed to be activated by heavy wide tracked vehicles such as those used by the American army rather than lighter narrower vehicles" used by Shi'ite militias.[41]

Germany also confirms that, in some circumstances, intelligence service personnel can be interviewed as witnesses in court. And in the aforementioned 2021 **"Ulysses" case** in France, to take another example, an investigator of the DGSI's judicial affairs division was called as a witness at the hearing in order to present in an adversarial setting various items of conflict zone information obtained by the service, enabling the court to assess their probative value.

Multilateral or non-governmental actors may also provide valuable testimony. In Germany, in the 2019 **case of *Zoher J.***, CIJA's Executive Director and one of its field investigators testified before the Higher Regional Court of Munich regarding "CIJA's objectives, structures and working methods" and, "[m]ore importantly ... regarding the individual criminal responsibility of the defendant", respectively. The court relied on this testimony in convicting Zoher for providing material support to a terrorist organisation and sentenced him to seven years imprisonment.[42] UNITAD representatives have also provided expert testimony and reports for use in various national proceedings.

In several jurisdictions, **academics, researchers, or other experts** have testified to subjects such as terrorist groups' structure and ideology to elucidate the evidentiary significance of conflict zone information.[43] Norway reports that expert witness statements have been central and at times even decisive to the outcome of terrorism cases, and Denmark agreed that credible expert testimony in court was strong evidence. France, Germany, Hungary, Switzerland, and the United States also report using information obtained from academic experts.

Victims, refugees, or **FTF returnees** or other **"insider witnesses**" have also provided valuable supporting testimony. Denmark, Finland, France, Germany, Hungary, Switzerland, the Netherlands, Norway, Serbia, Türkiye, and the United States all report using information obtained from such sources.

In most of the examples just described, neither security nor procedural considerations kept witnesses from providing relatively unrestricted testimony in open court. In other cases, however, the security or even the identity of some witnesses may demand special protection. Victims or eyewitnesses may live in conflict-impacted areas, have family members and associates at risk, or be otherwise vulnerable to reprisals from terrorist groups.

40. See UC Berkeley Human Rights Center and United Nations Office of the High Commissioner for Human Rights, *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, 2022, pp 62-65.
41. *R* v *Anis Sardar* Sentencing Remarks.
42. CIJA, "Da'esh / Islamic State", at https://cijaonline.org/daesh-islamicstate.
43. The United Kingdom identified courts' unfamiliarity with the facts of particular armed conflicts and with the nature and structure of terrorist groups involved, including the role of women in such groups, as a challenge in some terrorism cases.

Likewise, agents of the State may lose their future operational usefulness — not to mention jeopardise their personal safety — by testifying before a public audience.

States have used various **procedural devices to introduce the testimony of vulnerable or otherwise sensitive witnesses** while protecting their safety and — in some cases — their identity. These measures include closing the courtroom to the public for part or all of the proceedings, as already discussed.[44] Live witnesses may also be protected through **physical screening**, **voice scrambling**, or similar devices. In recent years, and particularly since the onset of the COVID-19 pandemic, courts in many jurisdictions have also grown more receptive to permitting **testimony by video** when the circumstances of the case justify it.

When strictly necessary, courts in some jurisdictions may even grant certain witnesses **anonymity**. In the United Kingdom, the prosecution may protect witnesses in terrorism cases by filing anonymity applications, among other special measure. The Netherlands resorted to this approach in **the prosecution of four individuals allegedly implicated in the 17 July 2014 downing of Malaysia Airlines flight MH17**. In that case, a chamber of the District Court of the Hague granted the examining magistrate's request to allow a dozen individuals who ran a genuine risk of serious reprisals to testify anonymously. Pursuant to specific provisions of the Dutch Code of Criminal Procedure, the examining magistrate questioned these witnesses in separate hearings. Both prosecution and defence were permitted to submit questions in advance, but were excluded from the hearings. Redacted transcripts were added to the case file with the witnesses identified only by code names. The trial court relied on this testimony, in conjunction with a host of other evidence, in finding three of the accused guilty of causing the flight to crash and of murdering the 298 persons on board, sentencing them to life imprisonment.[45]

Securing witness testimony is complicated when courts are hearing cases involving crimes linked to conflict zones in distant jurisdictions and arranging transport for witnesses may not be feasible. Finland found an innovative solution in **proceedings against Iraqi twin brothers who allegedly participated in the Camp Speicher massacre** near Tikrit, Iraq, in June 2014. After the trial court acquitted the brothers of charges of war crimes, murder, and assault with terrorist intent, citing a lack of evidence, the prosecution sought to introduce testimony from additional witnesses at the appeals stage. UNITAD, with the support and assistance of Iraqi authorities, arranged for eight individuals to give evidence at UNITAD headquarters in Baghdad, with the appeals court and the defendants viewing the hearing through a secure video link. Both the prosecutor and a defence lawyer were physically present at the hearing, and both prosecution and defence witnesses testified, counterbalancing any potential limitation on the accused's fair trial rights.[46]

Similarly, in the United States, during the **2017 trial of Mohamad Jamal Khweis**, a Kurdish Peshmerga official was allowed to testify by video from Iraq regarding the circumstances of his involvement in the collection of an ISIS document related to Khweis. This testimony contributed to Khweis' subsequent conviction for providing material support to ISIL(Daesh) and his sentence of 20 years in prison.

In many continental jurisdictions where procedural rules do not prohibit hearsay evidence, the **transcripts of depositions taken pre-trial** or the records of other out-of-court interviews may be introduced as substitutes for live testimony. In Germany, for instance, an out-of-court statement may be admitted as evidence when necessary to protect the identity of military or intelligence personnel, or when the person who made the statement would not be available for in-court testimony for other legitimate reasons. Even in common law jurisdictions, the prosecution can apply to admit hearsay evidence in certain circumstances.

Even when a witness is available to testify and all measures are taken to protect the witness' safety, additional challenges arise. For instance, establishing the reliability of witness testimony may be particularly challenging (a challenge that the protections put in place at times arguably magnify). Finland reports that the reliability of witnesses who live in or are otherwise linked to conflict zones is often questioned. Germany acknowledges that the statements of refugees, victims, and FTF returnees should be carefully scrutinised, both for intentional untruths and for inadvertent inaccuracies.

Several States consider previous experiences obtaining and assessing testimony in war crimes cases useful in addressing this challenge. The United Kingdom observes that ideally, witness statements should be taken in accordance with international criminal law standards and witnesses should provide informed consent to share the information with judicial authorities. And the Netherlands explains that, while judges typically assess

44. See Recommendation Rec(2005)9 of the Committee of Ministers to member States on the protection of witnesses and collaborators of justice, as referred to by CM/Rec (2022)8 Chapter V – Information provided by other sources, para 18.
45. See District Court of the Hague, MH17 verdict, 17 November 2022.
46. See TRIAL international, *Universal Jurisdiction Annual Review 2021*, p. 27, and Special Adviser and Head of UNITAD Karim Khan QC Speech at United Nations Security Council, 26 November 2019.

the reliability of statements made by defendants or taken from refugees, victims, witnesses, and FTF returnees about their experiences in Syria and/or Iraq just as they would the statements of any other witnesses, in international crimes cases judges use a particularly extensive reliability assessment framework, which includes taking cultural differences into account.

3.5. Use for the Prosecution of Offences other than Terrorism

Particular considerations involved with using information in cases involving war crimes, crimes against humanity, and genocide.

A 2020 Eurojust report concluded, "Existing national jurisprudence of EU member States and developing national practice demonstrate that it is possible to **cumulatively prosecute** and hold FTFs accountable for war crimes, crimes against humanity and the crime of genocide, in addition to terrorism-related offences", and that doing so "ensures the full criminal responsibility of perpetrators, results in higher sentences and delivers more justice for victims".[47] Indeed, in several cases, information collected in conflict zones has also served as crucial evidence in criminal prosecutions for offences other than terrorism, including **war crimes, crimes against humanity, and genocide**.[48]

The Netherlands has used information gathered from conflict zones to successfully prosecute terrorists for the war crime of inhuman treatment by degrading the human dignity of corpses. In France, in practice, prosecutions for crimes against humanity and war crimes are handled by the PNAT, which has a unit specialised in this field. As already mentioned, the PNAT has been able to obtain and make use of information transmitted by non-governmental organisations active in conflict zones and by UN bodies, the probative value of which is then debated in adversarial proceedings. Austrian judicial authorities have likewise used conflict zone information to prosecute war crimes and crimes against humanity, and Hungary has used it to initiate at least one prosecution of a suspected terrorist for alleged international crimes.

Germany has played a leadership role in prosecuting terrorist organisation members for international crimes. Particularly notable was the **case of *Taha Al J.***, an ISIL(Daesh) member who enslaved a Yazidi woman and her five-year-old daughter in northern Iraq and "punished the Yazidi girl by cuffing her to a window in the scorching heat, unprotected from the sun and letting her die in front of her mother".[49] The Higher Regional Court in Frankfurt am Main, Germany, found him guilty of war crimes, crimes against humanity, and genocide. The decision - the first by a criminal court anywhere to qualify crimes against the Yazidi people as genocide - sentenced Taha to lifetime imprisonment.

The European Network for investigation and prosecution of genocide, crimes against humanity and war crimes (or Genocide Network) facilitates close co-operation between national authorities investigating and prosecuting core international crimes. The Genocide Network convenes EU States' national Contact Points - specialised prosecutors, investigators, and officers for mutual legal assistance - along with representatives of observer States and entities from the European Union, United Nations, and beyond for biannual meetings that provide a platform for these practitioners to exchange operational information, experiences, and best practices.[50]

Introducing conflict zone evidence to prove international crimes requires the same analysis as is applicable to terrorism offences. That said, international crimes cases may involve additional evidentiary requirements. For example, certain international crimes may require proof of an armed conflict. To prove both this type of structural element, as well as specific facts relevant to cases for war crimes committed in Syria and Iraq, Sweden has used information gathered by NGOs and different United Nations bodies. This has included information from UN CoI Syria, the United Nations Assistance Mission for Iraq (UNAMI), the International Committee of the Red Cross (ICRC), Amnesty International, Human Rights Watch, and the Institute for the Study of War. While such additional hurdles increase the difficulty of securing convictions for international crimes, they also magnify the potential value of evidence obtained from the very conflict-impacted areas where those crimes were committed.

Going forward, it will be useful for States to track how they use conflict zone information to support prosecutions of terrorism-related and other criminal offences, in order to continue assessing this information's impact

47. Eurojust Report, *Cumulative Prosecution of Foreign Terrorist Fighters for Core International Crimes and Terrorism-Related Offences*, May 2020, p3.
48. See CM/Rec (2022)8 Chapter VII – Use of information collected in conflict zones for the prosecution of offences other than terrorism, paras 21 and 22, and Chapter IX – Co-operation between States and with international organisations, para 30.
49. Amnesty International, "Germany/Iraq: World's first judgment on crime of genocide against the Yazidis", November 30, 2021.
50. See Eurojust, "Genocide Network", at https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/genocide-network.

in advancing justice and accountability. Tracking the use of conflict zone information will also help identify any ongoing challenges for discussion and appropriate action in venues including the Council of Europe Committee on Counter-Terrorism.

Conclusion

As this set of Comparative Practices has demonstrated, States have the ability to use information from conflict zones as evidence in national civilian criminal proceedings related to terrorist and other offences. In any given case, relevant information of various types may be available from a variety of sources. States have at their disposal a range of mechanisms to gain access to and share such information, and may take a range of steps to analyse the information's probative value and to facilitate its use, whether as an investigative lead, as a way to otherwise support legal process, or as evidence in court.

The methods and practices described above are not an exhaustive set. Indeed, States will doubtless continue finding innovative techniques to identify, gain access to, share, and use relevant information. It will remain the case that in so doing, they should act in accordance with national laws and relevant international human rights and rule of law standards. Given the number of terrorist groups operating in or otherwise linked to conflict zones, information from such areas will remain vitally important to criminal proceedings related to terrorist offences, as well as to the prosecution of other offences, including acts prohibited under international humanitarian law. Governments should therefore continue to "strengthen international co-operation and domestic co-ordination on the use of information from conflict zones as evidence for the purpose of criminal prosecution of terrorist and other offences".[51] Investigators, prosecutors, policymakers, and others seeking to effectively use such information to advance justice and accountability may find these Comparative Practices instructive.

51. CM/Rec (2022)8.

Practitioner's Frequently Asked Questions (FAQ)

This annex to the Comparative Practices on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings addresses a number of overarching questions that practitioners may have about information from conflict zones. The goal is to guide practitioners in effectively sharing this type of information and using it as evidence when investigating and prosecuting terrorist offences, as well as of acts prohibited under international humanitarian law and other offences.

How can conflict zone information strengthen my case?

Conflict zone information can:

- **Establish or corroborate a suspect's identity**, which can be particularly challenging in cases involving complex crimes and/or fluid conflict situations;
- **Establish a suspect's physical location within a given time period** or on a particular date, which may itself constitute a criminal offence, given some States' legal prohibitions on travelling to particular conflict zones without proper authorisation, and may also help connect the suspect to the scene and time of a crime, draw the credibility of a suspect or other witness into question, or rebut an alibi;
- **Document a suspect's membership in a terrorist organisation** (which can itself constitute a crime in certain jurisdictions), including the suspect's willingness to commit specific criminal acts (such as suicide bombing);
- **Document the particular criminal act** that a suspect is charged with committing, either directly (e.g. through photos or videos) or through descriptions provided by witnesses, victims, or co-defendants;
- **Document a suspect discussing plans to commit a crime** beforehand, or **describing the crime** after the fact, or otherwise **help prove a suspect's criminal intent**; and/or
- **Otherwise help establish criminal liability** for preparatory acts, terrorist financing, or aiding and abetting crimes.

What types of information from conflict zones may exist?

- **Physical** (e.g., weapons, improvised explosive device components, mobile telephones, and hard drives and other storage media).
- **Digital** (e.g., content data, including text communications, photos and videos; traffic data; and other electronic data such as cryptocurrency wallet information).
- **Documentary** (i.e., hardcopy written material).
- **Intercepted** telephonic or other communications and **satellite- or** unmanned autonomous system **(UAS)-generated** imagery and footage.
- **Statements and testimony** (i.e., statements made voluntarily by defendants or by other subjects of interviews or interrogations, as well as testimony, statements, and other information provided by witnesses, victims, informants, and other human sources).

How can I identify information that is relevant to my case and obtain it in usable form?

- **Co-ordinate with colleagues** in military and intelligence services through existing interagency mechanisms to determine what information exists in domestic agencies' holdings.
- **Consider the full range of options for obtaining information from foreign government agencies and intergovernmental mechanisms** that store and share information, and use the fastest and most effective methods suitable to the case and legal system. Options can include:
  - **Engaging foreign counterparts directly** through intelligence and law enforcement channels;
  - **Making a formal request for information, including through** the mutual legal assistance (**MLA**) and European Investigation Order (**EIO**) processes; and
  - **Searching intergovernmental databases and information systems**:
    - INTERPOL: contact National Central Bureau;
    - European Union Schengen Information System: ask competent national authorities to consult common database;
    - Europol Information System: ask designated national authorities to run search in database;
    - Operation Gallant Phoenix: contact United States Embassy FBI legal attaché to initiate a request.
- **Check with relevant multilateral actors**:
  - United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD)[52];
  - International, Impartial and Independent Mechanism on Syria: initiate contact with the IIIM through their website before moving to more secure processes for information sharing;
  - International Criminal Court (ICC): submit communications to the Office of the Prosecutor electronically through the OTPLink.
- **Consider contacting** reputable and reliable **non-governmental actors** (e.g., civil society organisations, academic researchers and experts, news media, and private companies and contractors) to encourage them to share information on a case-by-case basis.

How can I corroborate conflict zone information for use as evidence?

- **Re-analyse and re-exploit physical items**; **introduce copies** when originals are unavailable; and **include contextual information**, such as documentation of how and when information was collected, transmitted, stored, analysed, and shared.
- **Introduce additional material** generated from independent sources (e.g., social media and other open-source digital material, communications intercepts, witness statements, and interviews of suspects themselves).
- **Introduce supporting testimony**, not just from those who collected the information, but also from government officials, technical specialists, experts, or witnesses with relevant knowledge. Consider **procedural measures to protect vulnerable or otherwise sensitive witnesses**, including physical screening, voice scrambling, anonymity, and/or out-of-court hearings, when necessary and appropriate.

What critical considerations should I keep in mind?

- **One search or request may not be enough.** The volume of available conflict zone information is not fixed, but rather growing all the time, as more information is collected and as previously collected information is processed, translated, and/or analysed and exploited. Even if a search for information is fruitless or yields insufficient results, **consider running it again, or expanding it, as the investigation advances**.
- **Information collected or obtained by military or intelligence services, or by multilateral or non-governmental actors,** may be **admissible as evidence.** Most jurisdictions impose no categorical bar to the introduction of such information at trial, so consider all options before concluding that a piece of information is not admissible.

52. In Resolution 2697 (2023), the United Nations Security Council only extended UNITAD's mandate until 17 September 2024, so, while information from UNITAD has been valuable in investigations and prosecutions, as of April 2024 it is yet to be determined whether states will have access to this information for their cases in the future.

- **Information from a conflict zone may be relevant even if** it **is incomplete, unverified, or inadmissible** in court. Consider its value for initiating or advancing an investigation and for generating further information that can be used as evidence.
- **Information from conflict zones may be relevant to crimes that took place elsewhere** (e.g. by documenting that a suspect who committed crimes elsewhere was a member of a terrorist organisation) or to **suspects themselves located elsewhere** (e.g., by establishing linkages between crimes that took place in a conflict zone and those who financed them).
- **Cases rarely turn on a single piece of information**, whether from a conflict zone or elsewhere. Criminal convictions are more often based on multiple types of evidence from multiple sources, with each piece of evidence contributing to a stronger case.

What other resources can I consult?

- **Relevant sources of guidance** on conflict zone information include:
  - Council of Europe Recommendation CM/Rec(2022)8 of the Committee of Ministers to member States on the use of information collected in conflict zones as evidence in criminal proceedings related to terrorist offences;
  - United Nations *Military Evidence Guidelines*;
  - Eurojust 2020 *Memorandum on Battlefield Evidence*;
  - Global Counterterrorism Forum *Abuja* Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects;
  - United States *Non-Binding Guiding Principles on Use of Battlefield Evidence in Civilian Criminal Proceedings*.

The CDCT Secretariat and the IIJ maintain a list of experts who contributed to the development of these comparative practices and who have experience using conflict zone information in terrorism cases; please contact either to ask a question or to provide feedback on these Comparative Practices.

For over forty years, the Council of Europe has helped to develop and reinforce key legal standards to prevent and suppress acts of terrorism. Taking a comprehensive approach, the Council of Europe works to help member States fight terrorism more effectively by strengthening and improving their national legislation, as well as facilitate international co-operation. In full respect for human rights and the rule of law, the Council of Europe is continuously working to improve international co-operation in bringing terrorists to justice.

PREMS 107924

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE