BATTLEFIELD EVIDENCE

Key insights for judicial practitioners

EUROJUST

BATTLEFIELD EVIDENCE

Accountability for terrorist offences and core international crimes (CIC), i.e. genocide, crimes against humanity and war crimes, is a priority for the European Union (EU). Such heinous crimes committed within the EU and outside EU borders pose a threat to our security and well-being. Investigating and prosecuting these acts is complex and challenging, not least because evidence may be located in or obtained from an armed conflict situation, or in other words, the battlefield.

Battlefield evidence is used increasingly in counter-terrorism, CIC and cumulative prosecutions for both types of crimes, and many cases in which battlefield evidence played a decisive role have already successfully been tried. Several EU Member States and partner countries have pending investigations and prosecutions that depend on battlefield evidence.

The use of battlefield evidence, however, comes with some challenges and for several years now, Eurojust has collected experiences and best practice of national authorities in obtaining and using battlefield evidence. Other organisations, including the Council of Europe, the United Nations and NATO have provided guidance to and mapped the experiences of national authorities in collecting and using such evidence in investigations and court proceedings.

In view of the anticipated rise in the number of cases relying on battlefield evidence brought before the courts across the EU and partner countries in the near future, judicial practitioners have expressed a **need for further experience sharing and capacity building on this topic**. This includes examining ways to improve how battlefield evidence is used in criminal cases, while carefully safeguarding fair trial standards and other human rights, and ensuring robust protection of victims' rights.

It is in this context that Eurojust has prepared this document, which is based primarily on reports drawn up in cooperation with the Genocide Prosecution Network and a meeting held in April 2024, as well as on the expertise gained by the Agency on the topic. Eurojust has extracted **practical and illustrative information that will bring judicial authorities up to speed on battlefield evidence** as a concept, how to access such information and how to use it in court. Additionally this document addresses new technologies and provides additional resources.

CONTENTS

WHAT DOES **‘BATTLEFIELD EVIDENCE’** MEAN AND WHY USE IT?

There are **no generally applicable definitions of ‘battlefield evidence’** and of the more general term ‘battlefield information’.

Both terms are used for **materials that originate from a conflict area** (and/or information derived through technical exploitation), including materials collected by state entities, UN entities and civil society and other organisations.

Battlefield evidence refers to **both personal and non-personal data**, without distinguishing between them.

TERMINOLOGY

Other terms are sometimes used to refer to the same type of materials.
These include in particular:

- ‘collected exploitable material’ (CEM); or
- ’military evidence’/’military collected information’

BATTLEFIELD EVIDENCE MAY TAKE MANY FORMS

It encompasses various materials collected from the battlefield, including the following:

PHYSICAL ITEMS (incl. biometric data extracted from them)

- **weapons** (including weaponised drones) and explosive devices, in particular unexploded improvised explosive device (IEDs) and components of exploded IEDs
- **electronic devices** (e.g. mobile telephones, hard drives, computers, SD cards and other storage media)
- **credit cards**

DIGITAL AND AUDIOVISUAL INFORMATION

- **content data**, including text communications, audio files, photos and videos (e.g. videos seized in conflict areas, YouTube videos or photos documenting plundering, killings/executions or abuses of civilians/prisoners, propaganda videos, social media content), and traffic and subscriber data
- **data and footage obtained using drones**
- **other electronic data**, such as cryptocurrency wallet information

CASE EXAMPLE – **FINLAND**

In March 2025, the Helsinki District Court sentenced a Russian national to life imprisonment for four different **war crimes** committed in eastern Ukraine in 2014.

The accused was the deputy commander of a volunteer group called Rusich, which fought against Ukraine on the side of Russia and the Ukrainian separatists supported by Russia. The Rusich group participated in an ambush against a convoy carrying soldiers of a Ukrainian battalion in the Luhansk region of eastern Ukraine. They allegedly misused the Ukrainian flag by displaying it at a checkpoint, thereby deceiving the Ukrainians in the convoy into believing that the checkpoint was still under the control of Ukrainian forces and stopping the vehicles. The Rusich soldiers opened fire on the vehicles and the Ukrainian soldiers who were exiting the vehicles, thereby killing and wounding them.

The accused was charged with the misuse of the Ukrainian flag, the unlawful killing of wounded soldiers, the assault of a wounded soldier, the degrading treatment of a deceased soldier and the issuance of threats of no mercy. He was acquitted of the first and convicted of all other charges.

The evidence presented in support of the indictment was based, among other things, on **image and video publications** from social media channels and video sites on the internet, concerning the Rusich group and its purpose and activities in the Luhansk region. In addition, **maps and satellite images**, videos and other visual material related to the locations of the events, along with **witness testimonies**, were used. The prosecution also relied on an **expert opinion in the field of military science** regarding the conflict situation in eastern Ukraine from the spring of 2014 onwards, along with a foreign court's decision in a criminal case concerning the downing of a passenger plane in eastern Ukraine in July 2014.

The judgement is under appeal.

TESTIMONIES

- **oral testimonies**, statements and other information provided by witnesses and victims (survivors accounts, video statements)
- **statements by community leaders**, informants and insiders
- **statements by suspects**

CASE EXAMPLE – SWEDEN

In a Swedish case, by using battlefield evidence (such as **hospital records, martyr lists and food stamps**), the prosecution could establish that a boy was a child soldier for several years in Syria and that his mother did not actively prevent this.

The court found the mother guilty of a grave **war crime** as she did not take adequate steps to stop the recruitment and use of her minor child.

HARD-COPY DOCUMENTS

- **relating to identity** (e.g. identity documents)
- **relating to membership** in or links to a terrorist organisation:
  - enlistment records
  - payroll documents
  - medical records
  - financial records (bank statements and transactions)
  - notebooks and diaries
  - maps
  - any other document, such as a will or a letter describing potential terrorist plots
- **relating to specific events**, i.e. reports or documents drawn up by the military about the situation in conflict zones (documents regarding specific attacks, analytical reports, military storyboards) and situational reports from international commissions of inquiry and civil society organisations (CSOs)
- **relating to crime scenes**, i.e. material documenting crime scenes such as mass graves, detention centres and headquarters of terrorist organisations

EXAMPLE

Battlefield evidence used so far to **establish membership in the ISIL (Da'esh)** terrorist organisation has taken many forms, including:

- registration forms
- enlistment records
- membership cards
- payroll rosters with information on ISIL (Da'esh) fighters and affiliates who received a salary from the organisation in Syria or Iraq
- records of service of combatants
- martyr lists
- lists of women registered in *madhafas*, i.e. guest houses
- marriage contracts drawn up by an ISIL (Da'esh) judge
- food stamps

WHY USE BATTLEFIELD EVIDENCE?

Investigating and prosecuting crimes committed on or originating from the battlefield poses substantial challenges, in particular in relation to the identification of victims, witnesses and evidence located outside the national borders and lack of direct access thereto due to the instability of conflict-affected areas.

Using evidence collected on the battlefield by stakeholders on the ground is therefore a **crucial asset to ensure accountability** of terrorists and perpetrators of CIC and bring justice to victims.

Battlefield evidence is increasingly used:

1.

in **criminal investigations and prosecutions** relating to counter-terrorism and CIC, and in cumulative prosecutions for both types of crimes:

- to provide **leads** for law enforcement to start an investigation
- to build a **contextual understanding** (e.g. of crime patterns, power structures and the broader context of a conflict) in structural investigations
- to provide **evidence**, including:
  - to determine the *modus operandi* of a terrorist organisation or an armed group
  - to establish a suspect's identity, membership in a specific terrorist group, presence, function and activities in a conflict area
  - to build a case (to connect the suspect to a particular crime, to prove the contextual elements for CIC, etc.)
  - to prove some factual elements disputed by the defence, to obtain convictions and appropriate sentences

EXAMPLES OF CASES WHERE BATTLEFIELD EVIDENCE HAS BEEN USED

In the past years, material collected in conflict zones in Syria, Iraq and Libya but also in Rwanda, Mali and Sri Lanka, among others, has been used in criminal proceedings in various jurisdictions in Europe and elsewhere.

These cases, which concerned both perpetrators still in the conflict area and tried *in absentia* and perpetrators who left the conflict zone to reach EU Member States or partner countries, covered a wide range of profiles, including:

- foreign terrorist fighters (FTFs), including returnees
- members of a terrorist organisation having committed war crimes
- child soldiers
- individuals involved in human trafficking cases (in particular, ISIL (Da'esh) FTFs married to young, trafficked women).

2.

for other purposes relevant for EU security:

- in border screening/visa adjudications
  - to detect FTFs before they enter the Schengen area
- in asylum/immigration proceedings
  - to identify abuses of asylum procedures by individuals not deserving of international protection or perpetrators seeking to evade being held accountable for serious crimes – both terrorist offences and CIC constitute grounds for exclusion from international protection.

HOW IS BATTLEFIELD EVIDENCE ACCESSED?

THROUGH COOPERATION!

When building a terrorism case with links to an armed conflict or a case concerning CIC, the identification and availability of battlefield evidence poses a challenge to practitioners.

The questions of **whether battlefield evidence** for the respective case **exists** and, if so, **where to find** it, often present greater challenges than those related to the authenticity and admissibility of the materials collected. The challenge of identifying relevant evidence increases with the quantity of documented information.

In recent conflicts, a **variety of stakeholders** have been **present in affected areas**.

While the purpose of their presence in the areas varies, these stakeholders may have **gathered information** that can be shared for use in criminal proceedings. In addition to the transmission of valuable material, these stakeholders may also be able to **share their expertise** or **identify further relevant information**.

Other stakeholders, in particular state authorities, may have received information originating from a conflict area through partners. **Cooperation at both national and international levels is key** to identifying and accessing battlefield evidence.

STAKEHOLDERS AT THE NATIONAL LEVEL

Improving information exchange in this field may not always be a legal requirement at the national level, however, establishing channels of communication between relevant stakeholders can be beneficial.

These stakeholders play a role in the access and use of battlefield evidence

The national stakeholders should develop:

1.

workflows and protocols that ensure awareness among the national stakeholders about the availability of battlefield information and allow for cooperation, including on burden sharing and to avoid duplicating efforts when it comes to the review and analysis of battlefield evidence

2.

legal frameworks to ensure that information collected by military or intelligence services in the context of their activities can be used as admissible evidence for law enforcement and judicial purposes

3.

procedures for the:

- preservation of information by stakeholders whose primary task is not the collection of evidence (e.g. military forces), in a way that ensures its admissibility in court
- protection of classified information
- declassification of information, whenever possible, including raw data

Cooperation with immigration and asylum authorities may also be of value in this context.

STAKEHOLDERS AT THE INTERNATIONAL LEVEL

National authorities of EU Member States and non-EU partner countries

National authorities in Member States and partner countries may hold information and evidence gathered during their presence in a conflict area or following requests to receive such materials from other States. They may provide various types of support through informal and/or formal cooperation.

Type of support

Upon request, national authorities may conduct searches for and share, when possible, all relevant types of battlefield evidence, including:

- **raw data**
- **contextual information**, subject to the need to protect sensitive sources and methods regarding the acquisition of the raw data provided, which may increase the evidentiary value of the information and its potential admissibility in judicial proceedings
- **resources in relation to a specific area**, *modus operandi*, etc on which that State has developed expertise

Cooperation modalities

Cooperation can be accomplished through:

- **informal cooperation**
  (e.g. through relevant practitioners' networks)
- **law enforcement cooperation** (e.g. through liaison officers deployed in Member States or non-EU countries and through Europol, Interpol and other stakeholders facilitating law enforcement cooperation)
- **judicial cooperation** among prosecuting authorities, and between prosecutors and courts through:
  - a spontaneous exchange of information;
  - the issuance of a formal European Investigation Order (EIO) or mutual legal assistance request (MLA); or
  - Eurojust, facilitating judicial cooperation and coordination.

USA

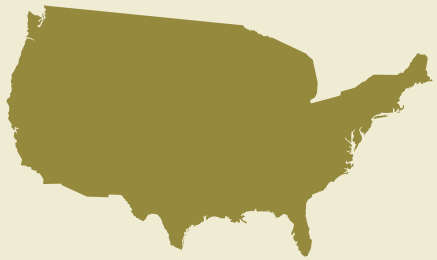
Type of support

The United States (USA) maintains a **large repository of battlefield evidence**, referred to generally as 'Collected Exploitable Material' (CEM), the vast majority of which is owned by the US military.

The material includes not just mobile phones, but other collected material, such as SD cards, documents, computers, external hard drives and improvised explosive device components.

Upon request, searches and identification of relevant collected battlefield evidence **can be conducted** by various institutional structures, including:

- the Terrorist Explosive Device Analytical Center (TEDAC)
- U.S. Department of Defense-led interagency and multinational organisations, through which the U.S. and partners examine and share terrorism-related information.



Cooperation modalities

Cooperation can be accomplished through:

- the relevant FBI Legal Attaché office; Battlefield Evidence Search Request Form
- the Liaison Prosecutor for the USA at Eurojust

USA - CHECKLIST

- **Start discussions and search requests early** to allow enough time for declassification of possibly classified information and approvals for judicial use.
- **Note** that the information requested can also benefit structural investigations.
- **Allow** for the informal exchange of information between experts first, before issuing formal requests.
- **Contact** the country's FBI Legal Attaché to discuss any relevant legal requirements that may affect search requests or the admissibility of evidence in judicial proceedings.
- **Provide** as much information as possible when submitting a request to the US authorities to facilitate the search and increase the chances of identifying relevant evidence.
- **Find out** whether a legal agreement in relation to sharing biometric data is necessary. This may take time but is worth doing as such data can help in achieving successful prosecutions.
- **Meet** frequently to discuss updates and clarify the exact scope and content of requests, along with any judicially imposed deadlines.
- **Consider sending supplemental search requests** after a period of six months or more has passed since a prior search was conducted (as battlefield evidence is frequently being acquired and forensically exploited).

Stakeholders facilitating cooperation among national authorities

Eurojust – international judicial cooperation

Eurojust assists national authorities by **coordinating** investigations and prosecutions and **facilitating judicial cooperation** in a large number of cross-border terrorism and CIC cases.

Eurojust notably provides comprehensive and tailor-made **operational and legal expertise**, and provides **analytical support** to referred cases.

Information analysed

- Cross-matching of data
- Identifying connections with other investigations
- Close cooperation with Europol

COORDINATION MEETINGS

Meetings with National Authorities (judiciary & law enforcement) to prepare the way forward

COORDINATION CENTRES

Coordinated action day in complex cross-border cases supported by Eurojust

Judicial cooperation instruments discussed

- European Arrest Warrant (EAW)
- European Investigation Order (EIO)
- Mutual legal assistance (MLA) request
- Freezing/confiscation order

Issues for cooperation addressed

- Conflicts of jurisdiction
- Parallel proceedings
- Transfer of proceedings
- Admissibility of evidence
- Cooperation with third States

JOINT INVESTIGATION TEAM (JIT)

Eurojust provides legal, practical & financial support

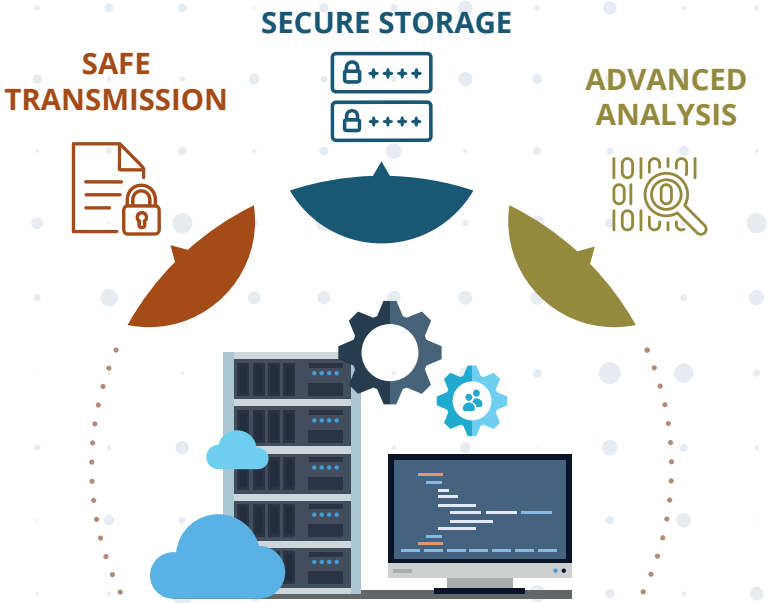
CICED

Cases to which Eurojust provides support may involve battlefield evidence that can prove beneficial to partners other than the one collecting it or with whom it was initially shared.

Where such cases concern CIC and related criminal offences, additional support in **preserving, analysing and storing evidence** can be offered.

Competent national authorities from EU Member States and countries with Liaison Prosecutors at Eurojust can submit evidence to Eurojust's Core International Crimes Evidence Database (CICED) via **secure file transfer**.

Evidence submission is **voluntary and the submitting authority remains in control** of how the evidence or information about the evidence is shared.



Cooperation with third countries and international organisations

As a facilitator of cross-border judicial cooperation, Eurojust plays an important role in promoting effective working relationships between the national authorities of Member States and non-EU countries and offers close cooperation with non-EU partner countries and international organisations, including the Office of the Prosecutor of the International Criminal Court (ICC-OTP) and the United Nations Office on Drugs and Crime (UNODC).

Agreements on cooperation

With 13 third countries

Liaison Prosecutors at Eurojust

From 12 countries

Contact Point network

Covering 70+ jurisdictions worldwide + 3 organisations

Working arrangements

With 9 countries + one regional association

This information is subject to change, please check the Eurojust website for the current state of play.

Victims' rights – Support through cooperation

The complexity inherent in investigating crimes and collecting evidence on the battlefield exacerbates the difficulties in protecting the victims at the scene of the event.

Getting access to victims, including those who are still in the conflict area and often heavily traumatised, **understanding their cultural background** and **maintaining regular contact** despite technical limitations represent some of the significant challenges faced by national authorities.

Providing support to the victims and ensuring the protection of their rights **can be facilitated by judicial cooperation** and **with the help of Eurojust**.

For more information, please see:
Eurojust support in the protection of victims of crime in cross-border cases.

Genocide Prosecution Network

The European Network for Investigation and Prosecution of Genocide, Crimes against Humanity and War Crimes (Genocide Prosecution Network), is comprised of national Contact Points, specialised prosecutors, investigators and officers for mutual legal assistance who provide operational support to their colleagues at the national and EU levels. The Member State national authorities are joined in the network by Observer States and associate organisations from, among others, the EU and the United Nations, along with CSOs. This platform allows for practitioners to share experience and best practice, i.a. through biannual meetings held at Eurojust.

The Genocide Prosecution Network has a wealth of experience in dealing with cumulative prosecution cases (terrorism and CIC), many of which have used battlefield evidence in criminal proceedings.

Key jurisprudence of these cases can be found in the National jurisprudence database on core international crimes

See also the Genocide Prosecution Network's Reports on cumulative prosecutions

Europol and law enforcement cooperation

The European Counter Terrorism Centre (ECTC) serves as Europol's central information hub for counter-terrorism and international crimes, providing law enforcement authorities in EU Member States and elsewhere with advanced information and intelligence-sharing capabilities.

Through its Analysis Projects Travellers (AP Travellers) and Core International Crimes (AP CIC), Europol collects and analyses battlefield information to support the efforts of competent authorities in EU Member States and third countries in preventing and combating terrorism, as well as international crimes such as genocide, crimes against humanity, and war crimes. In doing so, the ECTC contributes to strengthening operational responses and enhancing overall security within the EU and the Schengen area.

CASE EXAMPLE – **PORTUGAL**

Two brothers, belonging to ISIL (Da'esh), escaped from Mosul, Iraq, and fled to Portugal. On a Facebook profile, the Portuguese authorities found 236 propaganda videos, which were collected by a resistance group called 'Free men of Nineveh'. One of the brothers was identified in one of the videos.

In this investigation, **open-source information** and **geospatial intelligence** were beneficial, as was the **international cooperation of the police and judicial authorities, including Europol, Interpol, UNITAD and Operation Gallant Phoenix**.

The two brothers were each sentenced to 10 years of imprisonment and expulsion from the national territory. In addition, one of the brothers was sentenced to another 13 years and four months of imprisonment for the commission of a **war crime** and aggravated threat, and ordered to serve a total of 16 years in prison. Both convictions set new legal precedents in Portugal.

The relevant judicial decision is not final yet as both the defence and the prosecution appealed to the Supreme Court.

International bodies with investigative mandates

Mechanisms and bodies with investigative mandates set up by the United Nations, among others, such as international commissions of inquiry, commissions on human rights, fact-finding missions and other investigations, gather information and evidence in relation to a specific armed conflict or situation and have analytical capabilities that can assist national authorities in their investigations and prosecution efforts. The mandates of these bodies are limited to cases that (also) concern CIC, which means that cases concerning terrorist offences alone fall outside their mandates.

Such international bodies and mechanisms include the International, Impartial and Independent Mechanism - Syria (IIIM), the Investigative Team to Promote Accountability for Crimes Committed by ISIL (Da'esh) (UNITAD) (now closed) and the Independent Investigative Mechanism for Myanmar (IIMM).

Also, the Office of the Prosecutor of the International Criminal Court (ICC) gathers information and evidence that can be beneficial to investigations carried out by EU Member States and other countries.

UNITAD

UNITAD collected **millions of pieces of ISIL (Da'esh)-related material**, which was consolidated into one central database. Responding to requests for assistance, UNITAD **enabled and facilitated** the use of this material in a number of national criminal **investigations and proceedings**.

However, UNITAD concluded its mandate on 17 September 2024 pursuant to Security Council Resolution 2697 (2023), and its archive has been delivered to the United Nations Secretariat. While the capacity to manage and provide access to this archive is currently limited, discussions are ongoing to assess possible solutions in this regard.

FOCUS
THE INTERNATIONAL, IMPARTIAL AND INDEPENDENT MECHANISM - SYRIA (IIIM)

Type of support

- **Sharing information and evidence** concerning CIC committed in Syria since 2011 collected by the IIIM and preserved in its repository, upon request or on its own initiative
- **Sharing analytical products** prepared on the basis of evidence collected, preserved and analysed by the IIIM
- Conducting **multilingual open-source research**
- **Geolocating** crime scenes and other locations of interest
- Identifying and locating witnesses for interviews by competent jurisdictions
- Introducing sources to competent jurisdictions
- Producing **translations** of high-value data
- **Conducting high-value interviews** for competent jurisdictions

Cooperation modalities

- Direct contact with States to gather their views on how the IIIM can best assist their prosecution efforts and work with them towards the adoption of legal frameworks to permit this cooperation
- Cooperation agreements or other forms of cooperation, depending on the applicable national legal framework
- Contact through the IIIM website

Civil society organisations

Local CSOs may have access to conflict areas in armed conflict situations before national or international authorities are able to access the location, and can therefore play a critical role in collecting and securing battlefield evidence (especially in the early stages of the conflict, as was the case in Syria and Iraq).

Type of support

Beyond their role as information providers, CSOs may assist national authorities in other ways, including by:

- **documenting crime scenes**
- facilitating the **identification and access to witnesses**, taking first general accounts for potential witnesses
- providing **psychological/social support to victims and witnesses** and, if relevant, facilitating their travel to EU Member States for testifying at trial
- providing **contextual elements** and support in dealing with historical, cultural, social and religious sensitivities
- providing **analytical products** (e.g. reports on ISIL (Da'esh) bureaucracy and recruitment pathways)
- facilitating the **identification of suspects** residing in or transiting through European jurisdictions
- providing **case(-building) support**

Cooperation modalities

Cooperation modalities will vary depending on the CSO in question and applicable laws of the requesting State.

Experts and academic researchers

Provide specialised knowledge of, for example, the historical, political or cultural context in which the alleged crimes took place and which may be needed to assess the available battlefield evidence and put it into context.

News media and other actors

Journalists and other media actors may:

- have collected information in a conflict area that is relevant to the investigation/prosecution (in particular as leads).

Private companies and contractors may:

- hold information that they have collected, for their own use, in conflict areas. Such information may have potential evidentiary value in civilian court proceedings and has already been used in cases against suspected terrorists.

Potential cooperation should be considered in light of challenges such as the confidentiality of the judicial proceedings. In relation to journalists, additional challenges include the protection of their sources, the scope of information they are likely to publish and how this may affect the investigation/prosecution. Requests for financial compensation in return for assistance could also cause concerns.

STEPS TO ACCESS BATTLEFIELD EVIDENCE

1.

At the national level, contact relevant stakeholders (authorities/ CSOs) to identify available battlefield evidence

2.

Request support bilaterally from EU or non-EU country partners by:

- exchanging information between experts
- sharing information at the law enforcement level (including through Europol and Interpol)
- submitting formal MLA requests

3.

Request judicial cooperation support from Eurojust

- Engage Eurojust as early as possible in your case, to benefit from the support and services offered, including CICED

4.

Request support from other relevant stakeholders investigating or documenting crimes in the battlefield, including:

- international bodies with investigative mandates
- international CSOs

HOW TO ENSURE SUCCESSFUL USE OF **BATTLEFIELD EVIDENCE** IN COURT?

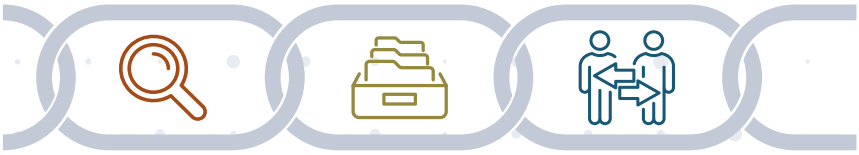
While information collected in conflict zones can be crucial in terrorism and CIC cases, the use of battlefield evidence **may raise evidentiary issues** in court proceedings. The value of this type of evidence or, in some countries, its admissibility, may be questioned. Additionally, **human rights considerations** may be an obstacle to using battlefield evidence collected and obtained in a manner that differs from common domestic cases.

Over the years, many countries have gained experience through cases brought before their courts. This expertise allows for **best practice** to be extracted, which shows that national authorities can overcome challenges by taking certain measures and by learning from previous experience and case law. Also in this respect, EU Member States and partner countries benefit from looking beyond their borders and making use of the **experience gained at regional and international level**.

MAIN LEGAL CHALLENGES

Integrity and accountability of processes (chain of custody)

- Chaotic and highly insecure situations on the battlefield make it challenging to collect, label and seal information at the scene.
- Improper collection, handling, preservation and sharing of evidence may render evidence inadmissible or reduce its evidentiary value in subsequent prosecutions.
- Preserving the chain of custody may be difficult, but it is crucial to authenticate an item's origin and to ensure evidence has not been contaminated or altered.

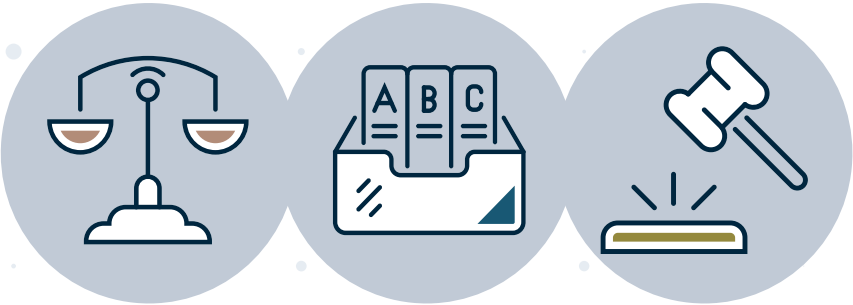


The **chain of custody** of physical items collected (weapons, phones, etc.) may raise particular concerns. Contrary to documentation which can be more easily identified based on its content, physical items can appear indistinguishable.

The same applies to **electronic evidence**: metadata (e.g. timestamps, GPS locations, camera details and original file history) can be lost when the files are handled and data may be altered when digitally transferred (via emails, USB, unsecured cloud storage, etc.), thereby calling into question its integrity and authenticity.

Admissibility, reliability and evidentiary value of battlefield evidence

- While, in general, the use of battlefield evidence is not excluded under national law – and is even allowed in many civil law jurisdictions under the principle of freedom of evidence – it has a relative probative value, and corroborating evidence will often be needed for a conviction.



FOCUS
NON-EU-COUNTRY PERSPECTIVE

The use of evidence obtained through international cooperation does not raise major issues in North Macedonia. It is admissible in domestic proceedings as long as it has been **collected in accordance with the rules of the requested country**.

CASE EXAMPLE – NETHERLANDS

Challenges using witness statements concerning a defendant's role in the conflict area

In a case concerning a female defendant who had travelled to Syria in 2013, the prosecution wanted to use a statement by the husband of the defendant, which could have established the active role of the defendant in combat training.

However, the first instance **court decided not to use this evidence as there was no way to test the reliability of the statement** – for example, by hearing the husband, because of his captivity in Iraq. In addition, this statement was not supported by other evidence.

On appeal, an FBI agent, who was present during the interview with the husband, was heard by the court. Nevertheless, the appeal court considered that it was still not sufficient to allow the statement to be used as evidence.

The defendant was convicted of membership in a terrorist organisation and acts of preparation and facilitation of the commission of terrorist offences, but was acquitted on the charge of participation in ideological and combat training and the armed jihad struggle (48 months imprisonment, of which 12 were suspended).

Compliance with human rights standards

- Reliance on information collected by external partners may raise questions regarding:
  - the **oversight and control** of the collection process
  - the **compatibility** of this process with the States' international human rights obligations, including in relation to the absolute prohibition of torture
  - **possible violations** of the fair trial requirements, and in particular of the rights of the defence and the principle of equality of arms, for instance in cases where the defence cannot question the collecting authorities or when the material shared is classified information

HOW CAN THESE CHALLENGES BE OVERCOME?

KEY CONSIDERATIONS AND BEST PRACTICES

Provide contextual information about the battlefield evidence collection process and handling

- Set up **standard procedures and practices** for handling, storing, exploiting and analysing material, in accordance with the relevant national and international legal standards, with a view to preserving its integrity and ensuring it can be included in subsequent stages of the criminal justice process.
- In particular with respect to the collection and storing of evidence and whenever possible, **obtain the unique identifiers/serial numbers** of physical items and the **hash value** of digital evidence to facilitate their authentication and use as evidence.

FOCUS
EXAMPLE OF GOOD PRACTICE

As reported by the UN Counter-Terrorism Committee Executive Directorate (CTED), some authorities have developed a **screening form** to collect and capture key information (including circumstances of arrest or surrender of a suspect, possession of weapon, etc.) at the initial point of contact on the battlefield between the authorities and individuals allegedly associated with terrorist organisations.

For more information, see Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences.

- When appropriate, for instance when the information has been collected by a commission of inquiry or an international organisation, consider inviting them to **testify about their methodology and chain of custody**.

Confirm the authenticity of battlefield evidence

- Authenticate battlefield evidence, for example, **through cooperation with international organisations with an investigative mandate** having the expertise and capacity to support national authorities in the process of authentication of battlefield evidence (e.g. looking into chain of custody issues, forensic analysis).

Regard battlefield evidence as part of the chain of evidence

- **Complement and corroborate battlefield information** through obtaining additional independent information that confirms the facts associated with the battlefield evidence. In particular, depending on the individual circumstances of each case, national authorities may:

- conduct their **own independent analysis** and exploitation of the material, notwithstanding previous analysis and exploitation that may have been conducted by the entity (States, commissions of inquiry, CSOs, etc.) that collected it
- collect **corroborating open-source** (electronic) **material**
- use **supporting testimony** (e.g. from the persons who collected, analysed and exploited the information; from experts providing background information; from law enforcement officers present during witness interviews conducted in the conflict area)
- generate **evidence from additional sources** (e.g. local police, border patrol, relatives of the witness, friends, local community, church, mosque)
- **cooperate with key stakeholders in the field** to gather corroborating testimonial evidence from witnesses or to ask them to produce analytical reports

Additional tool

The Berkeley Protocol on Digital Open Source Investigations identifies international standards for conducting online research of alleged violations of international criminal, human rights, and humanitarian law.

Explore the full range of procedural, technological and cooperation means to collect witness testimonies while addressing their rights and protection needs

- Cooperate with recognised CSOs operating in the field that can **facilitate access to and exchanges with the witnesses** that need to be interviewed

FOCUS
CSOs IN IRAQ AND SYRIA

In Iraq and Syria, some well-recognised CSOs working in the accountability field can channel outreach efforts towards victims and witnesses.

They can **build a trust relationship** with the local community and **ensure contact with the victims/witnesses after the interview**, notably for them to be updated of the progress and outcome of the proceedings.

- Cooperate with relevant international organisations and national authorities to **enable remote interviews of at-risk witnesses** living in conflict zones, ensuring their anonymity throughout the process.

EXAMPLE

Depending on national legal frameworks and on the circumstances of the case**, witness protection and anonymity measures** may include:

- redacting the witness' name and address from written statements
- arranging testimony via closed-circuit television or audiovisual links, such as videoconferencing
- shielding the identity of the witness by using a pseudonym, light disguise and/or voice alteration
- holding a closed session in the courtroom

- When witnesses may be relevant to investigations and prosecutions conducted in several Member States, consider cooperation in the framework of a JIT to facilitate the **coordination of witness interviews** and minimise the risk of secondary victimisation.

Victims' rights – Secondary victimisation

Conducting **multiple interviews of victims of crimes may lead to secondary victimisation**. This is especially true for victims in the battlefield who may suffer from multiple, long-lasting, repeated or continuous traumas.

To mitigate, as much as possible, the risks of secondary victimisation in cross-border cases, national authorities in the Member States concerned should avoid sending multiple cross-border requests for interviews with the same victim. International cooperation, within the framework of a JIT, may facilitate streamlined coordination and witness interviews, in particular by allowing participating countries to add their questions to those prepared by the country that will interview the witness.

For instance, Sweden, France, Belgium and the Netherlands are currently joining efforts, in the framework of a JIT, to identify and potentially prosecute FTFs who targeted the Ezidi/Yazidi minority during the armed conflict in Syria and Iraq. This JIT, supported by Eurojust, enabled the swift sharing of information and evidence, preventing victims – who have endured dire circumstances – from being subjected to multiple interviews.

NEW TECHNOLOGIES: CHALLENGES AND OPPORTUNITIES

New technologies such as electronic information and communications technologies have become **an established part of the investigation and prosecution** of different forms of criminality.

However, **when crimes are committed in the context of an armed conflict**, the investigating and prosecuting authorities often need to rely on battlefield evidence that was collected, preserved and transmitted from outside the crime scene or territory in which the national authorities usually act. In such situations, the **impact of new technologies used by all parties involved is particularly manifest**.

While the use of new technologies presents a number of risks and challenges, it also offers extensive opportunities.

Challenges

Broader capabilities for criminals to conduct their activities

- recruitment and training for, along with financing, coordination, planning and execution of terrorist offences and CIC.

Inherent limits to the use of the new types of data generated by digital means as evidence, leading to risks and concerns related to:

- preservation, management and archiving (digital materials are volatile and may be damaged or destroyed)
- verification and authentication (digital materials may be altered or manipulated)
- compliance with fair trial rights (equality of arms) and data protection requirements

Opportunities

Broader capabilities facilitating the collection and analysis of data, for example:

- new tools and specialised software allowing for the recording of photos and videos and packaging items with relevant metadata for the purpose of demonstrating their authenticity in court.
- new technologies, such as artificial intelligence, may be used:
  - to analyse large amounts of data and
  - identify patterns difficult to detect manually for authentication purposes (deep fake detection).

Greater availability of data of potential relevance to terrorism and CIC cases:

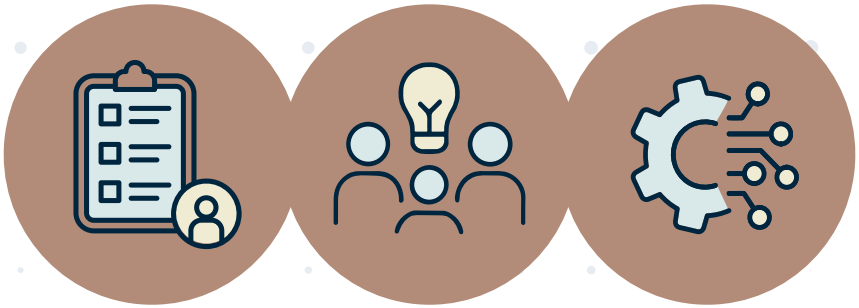
- by abusing new technologies, criminals leave behind digital traces that document their activities
- new technologies allow for the diversification of sources of evidence
- publicly available data can be collected by more accountability stakeholders, such as CSOs, thus providing further opportunities to capture the commission of crimes

Best practices to overcome challenges relating to the use of new technologies in criminal cases include:

- **developing and implementing authentication protocols** to ensure and assess at every stage of proceedings the integrity and reliability of digital information

- **strengthening legal practitioners' knowledge** on the specificities of electronic evidence, through appropriate training sessions and the dissemination of relevant tools (see, in particular, Evaluating Digital Open Source Imagery: A Guide for Judges and Fact-finders and the previously mentioned Berkeley Protocol on Digital Open Source Investigations)

- **carefully designing algorithms and machine-learning tools** to minimise biases, and subjecting them to frequent rigorous evaluations to ensure they remain as objective as possible.



ADDITIONAL RESOURCES

2020 Eurojust Memorandum on Battlefield Evidence

Eurojust Guidance on the identification of victims and witnesses of core international crimes

Council of Europe Recommendation CM/Rec(2022)8

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

Non-binding guiding principles on use of battlefield evidence in civilian criminal proceedings

PDF: Catalogue number: QP-01-25-018-EN-N
• ISBN: 978-92-9404-473-0 • DOI: 10.2812/2649038

Print: Catalogue number: QP-01-25-018-EN-C
• ISBN: 978-92-9404-474-7 • DOI: 10.2812/9397960

Eurojust is an agency of the European Union.


EUROJUST