POLICY BRIEF MAY 2026

TECH4TRACING

Detecting Violations

Computer Vision and Digital Evidence for Explosive Weapons Violations

Key findings

- Existing workflows for the use of camera-enabled drones and AI computer vision models for the detection, identification, and geolocation of UXO in the context of humanitarian and emergency mine action can also generate digital evidence for use in establishing facts on the ground in legal mechanisms for certain weapons-related crimes.
- Cases for which digital evidence based on AI computer vision are well suited include accountability for the use of prohibited weapons or, in some instances, the indiscriminate use of weapons that results in civilian harm under international humanitarian law.
- AI computer vision models could play an important role in treaty monitoring, even where the treaty does not provide for judicial enforcement. Such models can be a tool for states to identify breaches and provide evidence to other states parties to the treaty or to the treaty bodies tasked with monitoring violations.
- The admissibility of digital evidence generated using drones coupled with AI computer vision models and geolocation capabilities depends on the rigorous application of evidentiary chain of custody and data storage, management, and security guidelines.
- As AI computer vision models become more sophisticated and widely used, courts will increasingly need to grapple with the admissibility of the evidence they generate and must consider whether such models can in some circumstances be relied on as 'experts' in the same way as highly trained humans.
- AI computer vision object detection developers should play a role in ongoing discussions on battlefield forensics standards and guidelines, as the preservation of some military intelligence captured on the battlefield can also serve legal accountability objectives.

Introduction

Over the last few years, artificial intelligence (AI) capabilities have increased in sophistication and processing power and are now becoming widely integrated into a range of global business and military activities. At the same time, research and development and multi-year projects supported by donors such as the European Union are demonstrating that some types of AI can make significant contributions to humanitarian action, the rule of law, and criminal accountability.

One type of AI that can enhance humanitarian and rule of law outcomes is computer vision. This technology is already helping to automate the identification and recognition of threat objects and advancing emergency and humanitarian mine action in conflict-affected areas. The use of AI computer vision to identify and map unexploded ordnance (UXO) such as landmines and cluster submunitions using commercial drones with integrated cameras is no longer science fiction. Remote drone-based UXO detection, if conducted systematically, can speed up the work of marking contaminated mine fields, prioritizing areas for clearance, and ultimately returning the land to safe agricultural use. A key element of remote UXO detection systems is the geolocation of threat objects so that they can be automatically and accurately positioned in the real world for prioritization and clearance operations.

AI computer vision object detection for explosives and geolocation in orthomosaic maps has other potential humanitarian dimensions that have not yet been well described or implemented. One is the creation of digital evidence for use in legal mechanisms to hold perpetrators accountable for the deployment of prohibited weapons or for the use of certain weapons in an indiscriminate manner, in violation of international law. This Policy Brief describes several such use cases that will become feasible and efficacious as the deployment of AI computer vision detection of UXO becomes more widespread in emergency mine action contexts. In these cases, actors can create valuable evidentiary data that could, if handled in compliance with legal chain of custody and data security requirements, contribute to efforts to bring violators to justice.

The objective of this Policy Brief is thus to describe the applicability of the AI computer vision detection and geolocation of specific explosive ordnance objects for the creation of digital evidence in legal accountability mechanisms. It begins with a review of the two key technological components (computer vision and object geolocation), discussing how they work and their current deployment with emergency mine action actors focused on the remote detection of explosive ordnance in conflict-affected and post-conflict areas. It then discusses the core principles of digital evidence and the conditions under which accountability mechanisms could use mine-action-collected data under different bodies of law: international humanitarian law, international criminal law, and international human rights law. In doing so, it sketches the kinds of violations for which this data could be applicable, before concluding with a discussion of how to demonstrate the authenticity of the data.

Mine action AI computer vision basics

AI computer vision is an emerging technology in the emergency and humanitarian mine action community, one of many approaches to remotely detect and identify hazardous objects safely from the air. Actors use camera-fitted drones to review areas that are suspected of being contaminated with UXO. Target scenarios include areas that have been deliberately mined by physically burying explosive devices (e.g., anti-tank mines) or by dropping them from the air to rest on the surface (e.g., scatterable mines and cluster submunitions); former frontline areas where substantial exchanges of fired munitions have occurred; areas surrounding ammunition storage facilities that have been bombed, resulting in the widespread dispersal of explosive material; or urban and semi-urban bombing or occupation sites where live munitions may have been abandoned by retreating forces.

While many mine action actors use drones to simply visually review areas via a live video feed from the built-in camera, a full UXO remote detection workflow involves a much more sophisticated process, typically involving the systematic capture of images taken from the drone at a fixed altitude in a highly structured grid formation that are then run through computer vision algorithms (or models). The resulting detections are geolocated in an orthomosaic map image of the entire area.

The two key considerations for the purposes of this process are thus the detection and identification of the objects as specific weapons threats, and their geolocation. These represent two tasks that are fused into one workflow, discussed briefly below.

Object identification (AI computer vision)

Creating a custom object detection model (or algorithm) focuses on learning how that object appears in a specific context. Developers curate a training set of images that precisely mirror the target deployment conditions, including the lighting, camera angles, background clutter, and object scales the system will encounter. These images are meticulously annotated with bounding boxes to define the 'ground truth' and then subjected to data augmentation techniques—such as simulating different weather conditions or changes in lighting—to ensure that the model accurately and reliably learns to recognize objects even under different environmental conditions.

The detection model is then built using transfer learning, starting with a foundation of general visual knowledge, and is fine-tuned on this specialized dataset. This process allows the AI to adapt its understanding of edges and textures to the unique characteristics of the deployment area, effectively eliminating errors that occur when a generic model is applied to a niche environment. Once trained and validated against new (previously unseen) images from the same environment, the model is optimized and exported into a format compatible with the target hardware, resulting in a highly accurate, real-time detection system that understands not just the object, but the world it inhabits.

The performance of computer vision systems is measured by how well predictions align with reality, which can be categorized into four types of outcomes: true positives (correctly identified objects), false positives (objects incorrectly detected where none exist), false negatives (missed objects that were actually present), and true negatives. These measures are synthesized into two key metrics: precision, which measures the reliability of the system's alerts (how many detected objects are real), and recall, which measures the system's completeness (how many real objects are successfully found). To provide a single, comprehensive score of performance, the industry relies on the metric of mean average precision (mAP), which balances the trade-off between precision and recall. A high mAP score indicates that the system is both reliable (few false alarms) and thorough (few missed detections), making it a robust standard for determining whether a computer vision model is ready for real-world deployment in contexts where errors can have significant consequences.

Object geolocation

An orthomosaic is a high-resolution, geometrically corrected image of the Earth's surface that is compiled by stitching together hundreds (or thousands) of overlapping

1 This process can be performed by running the detections either in the orthomosaics or in the original images.

2 This discussion assumes that predications are generated using models such as YOLO, SSD, Faster-RCNN, and related models.

aerial photos. Unlike a standard photo, which suffers from perspective distortion (where objects closer to the camera appear larger and tilted), an orthomosaic is mathematically 'flattened'. Every pixel in the image has been adjusted to account for the camera's angle, the terrain's elevation, and lens distortion. The result is a seamless, map-like image where the scale is uniform across the entire picture; i.e., a pixel represents the exact same ground distance (e.g., 5 cm) whether it is in the centre of the image or at the edge. Essentially, it is a composite photo that behaves like a precise map.

In the context of AI computer vision geolocation, the orthomosaic serves as the critical bridge between digital detection and real-world coordinates. When an AI model analyses an orthomosaic to identify objects it has been trained to detect, it initially only knows the object's location in 'pixel space', e.g., row 500, column 1200. Because the orthomosaic is georeferenced—meaning every pixel is intrinsically linked to a specific latitude and longitude via a mathematical transformation—the system can instantly convert these pixel coordinates into precise GPS coordinates. This allows the AI to not just find that 'there is a submunition in the image', but to pinpoint it exactly, e.g., 'the submunition is at 52.36° N, 4.89° E', enabling its immediate integration into geographic information systems (GISs).

When a computer vision model identifies an object, it outputs bounding boxes defined in a 2D pixel coordinate system relative to the image canvas. However, these pixel coordinates can be mathematically inverted, because an orthomosaic is a georeferenced raster image where every pixel is intrinsically linked to a specific ground coordinate via a geotransform matrix (often derived from structure-from-motion photogrammetry and ground control points). By applying the inverse transformation, the system translates the discrete pixel indices of the detection directly into continuous real-world coordinates (eastings/northings or latitude/longitude), effectively anchoring the digital detection to a precise physical location on the Earth's surface.

In scenarios involving raw imagery rather than a pre-compiled mosaic, this process is termed 'back projection'. Here, the system utilizes the precise exterior orientation parameters (position and attitude) of the drone at the moment of capture to project a 3D ray from the camera's optical centre, through the specific pixel identified by the AI, down to the terrain surface defined by a digital surface model. The intersection of this ray with the ground model yields the object's exact geospatial footprint. This transformation bridges the gap between the semantic understanding of the AI computer vision (which recognizes what an object is) and the geospatial context (which dictates where it is), enabling the immediate integration of detection data into GISs for actionable intelligence, asset tracking, and spatial analysis.

The state of the art in 2026

Largely driven by evolving commercial technologies, AI, and the Russian war of aggression against Ukraine, humanitarian, emergency, and technology providers are developing and deploying AI computer vision technologies in drones for the detection of UXO to prioritize clearance operations. The orthomosaic and back-projection components of the workflow are mature and stable, and there are several off-the-shelf solutions for achieving accurate object geolocation in orthomosaics. The critical area where performance varies is in the underlying computer vision models (algorithms) themselves. Because there is not enough publicly available image data to create and train models, organizations like Tech 4 Tracing (T4T) have developed pipelines for generating the underlying digital and physical assets, like the 3D models and renders of the target objects and self-generated training data, to create models that can yield high-performance algorithms.

Prior to T4T's innovative methodology for creating UXO detection algorithms (Harvey and LeBrun, 2023), high-performance prediction models could not be created for such objects because of insufficient quantities and diversity of open-source images to train the model. T4T's solution involves partnering with national explosive ordnance disposal schools to acquire real examples of the target objects. Using a combination of photography, photogrammetry, 3D rendering, 3D printing, custom software, and artistic replication, high-resolution, high-fidelity 3D and physical models are developed to generate almost unlimited training data. As

3 Depending on the system used, AI model predictions can occur before or after the photos have been used to create the orthomosaic.

Figure 1. T4T Vulture software showing geolocations of anti-tank landmines in a field (Tech 4 Tracing)

of mid-2026, T4T's models are deployed on a workstation (desktop or laptop) to which drone images are uploaded for prediction processing.

T4T's models are built and customized for deployment by government or humanitarian demining agencies using specific drone deployment configurations. In the standard use case, a user flies a camera-enabled drone over an area that is suspected of being contaminated with UXO. In such a survey, the drone flies in a pre-programmed pattern at a fixed altitude taking photos at designated intervals. Once the pattern is completed, images are downloaded to a workstation containing the AI computer vision models. The individual drone images include the time, date, and location in the EXIF data accompanying each image. Predicted detections of hazardous objects are then displayed in an orthomosaic following the process described above. The orthomosaic can be displayed and reviewed in T4T's software interface, called Vulture (see Figure 1).

In scenarios like this, AI computer vision models identify objects that have been deployed but have not exploded, whose physical integrity is sufficient for recognition using the data on which the models are trained (the system will not recognize the use of weapons that have completely detonated). For this reason, the system is particularly well suited to locate objects that have been emplaced by hand or mechanical process, such as anti-tank landmines, and explosive objects delivered by air that have a significant failure rate, such as submunitions.

What has not been well recognized is that this emerging prototypical system for detecting and geolocating UXO can be leveraged to create digital evidence for legal accountability mechanisms, e.g., in cases where certain kinds of prohibited weapons (such as cluster submunitions) have been deployed in violation of treaty law, or where weapons have been used indiscriminately in populated areas in violation of international law. Furthermore, because in conflict scenarios emergency or military actors may move quickly to remove threat objects once they have been detected, they are unlikely to take the steps needed to create evidence that could later be used in legal accountability mechanisms. Therefore, initial drone-based surveys may represent a unique source of not only intelligence, but digital evidence.

To understand the applicability of these systems and the requirements for their effective use in legal accountability mechanisms, it is necessary to understand what digital evidence is, its position in the legal landscape, and the requirements for its admissibility in a court.

4 In typical current scenarios, the end user retains the original photos on the drone's SD card; copies are uploaded to a secure server for T4T to access and process.

Digital evidence landscape

The *Leiden Guidelines on the Use of Digitally Derived Evidence* defines digital evidence as information that "originates from electronic or digital technology, as well as evidence that would normally fall under another category of evidence but has been copied or preserved by being converted into a digital form" (Aalto-Setälä et al., n.d., p. 4). This definition therefore includes information created in digital format and information that has been transferred to a digital format (digitized). The photos captured by demining actors for analysis by AI computer vision models fall within this definition.

The lifespan of digital evidence includes several stages that are described slightly differently depending on whether the actors involved are professional law enforcement agencies or civil society organizations.

Stakeholders may place these stages in different order or use different terminology, but the core stages are:

1. *Identification*: finding or discovering the information.
2. *Collection:* extracting the information from where it was found.
3. *Authentication*: verifying the accuracy and integrity of the information.
4. *Analysis*: filtering data, aggregating similar data, identifying patterns, compiling timelines, etc.
5. *Storage/preservation/archiving*: saving the information in a secure environment that ensures that its integrity remains intact for an extended period and it can be easily found and retrieved in the future for use in investigations and trials.
6. *Transfer/sharing*: exporting the data to relevant stakeholders, such as law enforcement or other investigative mechanisms.
7. *Presentation/visualization:* visualizing the information in an understandable way, e.g., multimedia reconstructions or interactive platforms used in a trial (see Figure 2).

What role drone-sourced photos collected by demining actors can play as potential evidence that international crimes have been committed depends on whether they are collected, authenticated, analysed, stored, transferred, and presented in accordance with evidentiary standards. While analogue photos have long been used as evidence in legal proceedings, the ease with which digital photos can be altered and shared makes them especially vulnerable to tampering. Often, by the time they reach the hands of investigators, the images may be far removed from their original source. These issues can pose unique challenges for authentication. To eventually be admissible as evidence in a trial, images must be both relevant to an investigation or case and demonstrably authentic. The next two sections will address each of these issues in turn.

Legal framework

To examine the role that photos identified by AI computer vision models can play as evidence in weapons-related accountability processes, it is necessary to understand the basic international legal framework governing weapons use, specifically what conduct is prohibited, who can be held responsible, and in what forums. This foundation is important, because it determines what information is relevant.

Regarding what conduct is prohibited, the relevant bodies of law are international humanitarian law (IHL), international criminal law (ICL), and international human rights law (IHRL).

International humanitarian law

IHL is the branch of law that seeks to limit the destruction and suffering during armed conflict and is found in treaties, including the Geneva Conventions, and customary international law (ICRC, 2004). IHL is based on four fundamental principles: humanity, distinction, proportionality, and military necessity (ICRC, n.d.a). The principle of *humanity* entails a prohibition against the infliction of "superfluous injury or unnecessary suffering" and the obligation to treat humanely those who are not active participants in the hostilities (Corn, 2013). The

5 See, e.g., Eurojust and OTP ICC (2022); Aalto-Setälä et al. (n.d).

6 The field of digital forensics is dedicated to detecting such tampering.

7 See, e.g., Aalto-Setälä et al. (n.d.) and ENFSI (2021). However, it is important to note that even if information does not reach the standards of trial evidence, it can still serve as lead evidence—i.e., pointing investigators towards what they should look at—or corroborating evidence.

Figure 2.
Digital evidence lifespan

principle of *distinction* means that those individuals and objects involved in the fighting must be distinguished from civilians and civilian objects that are not (ICRC, n.d.b). The principle of *proportionality* prohibits attacks on military objects that will cause incidental harm to civilians or civilian objects that is excessive in relation to the military advantage that is sought (ICRC, n.d.c). The principle of *military necessity* is a counter-balance to the previous principles that allows parties to a conflict to take measures necessary to achieve a legitimate military aim, provided that these measures do not violate other IHL provisions (ICRC, n.d.d).

These principles are reflected in a wide constellation of treaties and agreements between states that address weapons, as well as political declarations of principles. Examples of these documents include:

- Geneva Conventions and Additional Protocols (see ICRC, 1977);
- Convention on Certain Conventional Weapons (1996), Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby-Traps, and Other Devices as amended on 3 May 1996;
- Convention on the Prohibition of Anti-Personnel Mines (1997);
- Convention on Cluster Munitions (2008);
- Political Declaration on Strengthening the Protection of Civilians from the Humanitarian Consequences Arising from the Use of Explosive Weapons in Populated Areas (UNODA, n.d.).

The prohibitions on the use of weapons in these treaties fall primarily into two categories. The first includes *absolute bans* on using weapons that by their nature and design are indiscriminate or cause unnecessary suffering or superfluous injury. In other words, these weapons cannot be precisely targeted, are designed to cause excessive damage, or both. Examples of these types of weapons include cluster submunitions and anti-personnel landmines.

The second category focuses on weapons that are not subject to outright bans, but which may be deployed in an indiscriminate manner (e.g., see Geneva Convention, Protocol I, 1977, art. 51.4 (ICRC, 1977); Convention on Certain Conventional Weapons, Protocol II, 1996, art. 3.8) or otherwise violate the requirement to take all feasible precautions to minimize the loss of civilian life, injury to civilians, and damage to civilian objects (Geneva Convention, Protocol I, 1977, art. 57 (ICRC, 1977)). The emphasis here is on targeting as opposed to the type of weapon used. Examples of indiscriminate use include targeting a civilian object or deploying weapons in an area where there would be excessive incidental loss of civilian life or damage to civilian objects (e.g., see Geneva Convention, Protocol I, 1977, art. 51.5(b) (ICRC, 1977); Convention on Certain Conventional Weapons, Protocol II, 1996, art. 3.8). Bombing a church, hospital, or school where civilians have taken shelter and which serves no military purpose would be prohibited under this category, regardless of the type of munition used.

While AI computer vision models are relevant to both categories, they are particularly applicable to the first category of prohibitions because they are ideally suited to identifying specific prohibited weapons in images. The crimes included in the second category stem less from the type of weapon than from the selection of target, method of delivery, and circumstances on the ground at the time of the attack, which lie beyond the technology's capacity to assess. Even though the type of weapon used in these situations is not solely dispositive, it can help inform the analysis.

AI computer vision models are particularly relevant for identifying the use of prohibited weapons and can contribute to analyses of whether weapons were deployed in an indiscriminate manner

Under IHL, states rather than individuals are accountable, and each treaty contains its own instructions for enforcement and addressing violations. The options range from raising alleged violations at the treaty's meetings of states parties (Convention on the Prohibition of Anti-Personnel Mines, 1997) to bringing charges against a state before the International Court of Justice (ICJ) (Convention on Cluster Munitions, 2008). AI computer vision models can play an important role in treaty monitoring, even where the treaty does not provide for judicial enforcement. Such models can be a tool for states to identify breaches and provide evidence to other states parties to

8 Because this Policy Brief focuses on the types of weapons that can be detected by T4T's technology, agreements addressing nuclear, chemical, or biological weapons, incendiary devices, and certain types of small arms ammunition, among others, are not discussed here.

9 The present discussion focuses on prohibitions on the use of these weapons rather than those covering their stockpiling, production, transfer, and destruction. However, the application of AI computer vision in these other contexts deserves exploration.

10 The Convention on Cluster Munitions (2008), Article 1.1(a) states, "Each State Party undertakes never under any circumstances to: (a) Use cluster munitions …".

11 The Convention on the Prohibition of Anti-Personnel Mines (1997), Article 1.1(a) states, "Each State Party undertakes never under any circumstances: (a) To use anti-personnel mines …".

the treaty or to the treaty bodies tasked with monitoring violations.

International criminal law

Under ICL, responsibility for violations attaches to individuals. The International Criminal Court (ICC) is the primary forum for individual criminal responsibility at the international level in relation to violations of IHL. The founding Rome Statute of the ICC sets out the crimes for which individual perpetrators may be tried. Similar to the treaties discussed above, the prohibitions related to weapons address both the type of weapon used (UN, 1998, art. 8.2(b)(xx)) and the way weapons are used (art. 8.2(b)(i), (ii), (iv)).

Of most relevance to this discussion, the Rome Statute refers to allegations of:

> *Employing weapons, projectiles and material and methods of warfare which are of a nature to cause* ***superfluous injury or unnecessary suffering*** *or which are* ***inherently indiscriminate*** *in violation of the international law of armed conflict, provided that such weapons, projectiles and material and methods of warfare are the subject of a comprehensive prohibition and are included in an annex to this Statute …* (UN, 1998, art. 8.2(b)(xx); emphasis added).

This annex was never adopted; however, in 2017, amendments to the Rome Statute were adopted to add certain weapons. Landmines and cluster submunitions were not included in this amendment, and the use of these weapons must be tried under the provisions of the statute related to targeting civilians or causing excessive civilian casualties. These provisions include Article 8.2(b)(i), which deals with allegations of "Intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities", and Article 8.2(b)(iv), which deals with allegations of

> *Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated* (UN, 1998).

Images identified by AI computer vision models are relevant to allegations of attacks on civilians or civilian objects by demonstrating that the weapons deployed were indiscriminate in nature or designed to cause excessive damage and would therefore be likely to cause excessive loss of life and injury to civilians or damage to civilian objects. Again, this crime is a targeting violation rather than a weapons violation, but the type of weapon used can help demonstrate the requisite knowledge or intent.

AI computer vision models can help establish when attacks used weapons likely to cause excessive loss of life or injury to civilians or damage to civilian objects

Individuals can also be held criminally liable for international crimes in domestic courts. In such cases, domestic law will apply. Presuming that the domestic legislation similarly prohibits the use of weapons that are indiscriminate or designed to cause excessive damage, UXO identified by AI computer vision technology is also relevant in this context.

International human rights law

IHRL is a separate body of law that applies in times of both conflict and peace. It does not address the conduct of war or the use of weapons per se, but human rights provisions can be violated when prohibitions on weapons use are breached. For example, the International Covenant on Civil and Political Rights (UNGA, 1966) obligates states to protect the right to life (art. 6.1), and refrain from subjecting people to torture and cruel, inhuman, or degrading treatment (art. 7).

Breaches of IHL or ICL involving prohibited weapons can also violate IHRL provisions such as the right to life or freedom torture and cruel, inhuman or degrading treatment

Each treaty has a committee charged with its oversight and provides for states and/or individuals to report alleged breaches of a state's obligations. While no cases have appeared before such committees related specifically to banned weapons, they represent forums where evidence of the use of indiscriminate weapons or weapons that cause excessive damage could be relevant.

12 In Ukraine, the Special Tribunal for the Crime of Aggression will also provide for individual criminal responsibility. This tribunal will adjudicate leaders' decisions to use armed force against another state in violation of the UN Charter. Because the focus is on the decision to go to war rather than the conduct of the war, it is less relevant to the present discussion.

13 There is some variation in this framework as to which laws apply, depending on the nature of the conflict (international or non-international armed conflict). However, this level of granularity is not necessary for the scope of the present discussion.

14 According to the Progress Report of the Thirteenth Meeting of States Parties to the Convention on Cluster Munitions, 67 states have enacted national legislation to implement the convention (UN, 2025). Comparable data is not available for national implementing legislation related to anti-personnel mines.

Information about the use of prohibited weapons could also be used indirectly against states that deploy them. In 2020, a group of human rights organizations and the VFRAME technology project (which became part of T4T), sought to demonstrate that cluster submunitions were being used in the war in Yemen. Their objective was to demonstrate that arms sales by third countries to these parties were contributing to human rights violations (Hao, 2020). In this situation, evidence of the use of prohibited weapons targeted states enabling and facilitating human rights violations.

In summary, field imagery processed by AI computer vision models can serve as evidence in state claims against other states for treaty violations; state or individual complaints to non-judicial mechanisms, such as human rights treaty bodies; cases against states before the ICJ; and trials of individuals at the ICC or in domestic courts. In the latter scenarios, if it is to be used as evidence in a trial setting, digital evidence must be deemed admissible, which entails a higher burden of proof than what is needed for non-judicial forums. As noted above, to serve as trial evidence, the authenticity of the images must be demonstrated. The next section discusses the admissibility requirements to confirm such authenticity.

Authenticity

Digital media proffered as evidence in judicial accountability mechanisms must meet established standards for admissibility, and these standards apply to individual photos or orthomosaics featuring geolocated objects of interest. In addition to *relevance*, as explained above, such evidence may be admitted if its *authenticity* can be demonstrated. In other words, the party tendering the evidence must demonstrate that it shows what the tendering party claims it shows. According to the *Leiden Guidelines on the Use of Digitally Derived Evidence*, authenticity can be demonstrated by providing information about the author/source, date, location, events depicted, and/or chain of custody (Aalto-Setälä et al., n.d., sec. B2). How this information can be demonstrated depends on whether the photographer or source of the images is known. Traditionally, witnesses testify as to the source of a photo or video (TRUE Project, 2024, p. 19).

The following discussion applies to cases where non-technical mine action survey teams or emergency services reconnaissance teams deploy drones to capture images of contaminated areas. In these scenarios, the teams, as the source of the images, would provide testimony to help demonstrate the images' authenticity.

Date and location information can be provided in two corroborating ways. First, the metadata collected by the drone-mounted camera and stored in the individual drone images' EXIF data, as well as in the complete geolocated orthomosaic, can provide information about where and when the images were taken. Secondly, the drone operator can testify as to where and when they captured the photos.

The verification of the **events depicted** has two aspects: (1) confirmation that the image is a true and accurate representation of the scene filmed; and (2) confirmation that the objects in the image represent specific weapons. Regarding the first aspect, the drone operator can testify that the image is a true likeness of the scene. Regarding the nature of the objects filmed, the AI detection model recognizes that an object is likely a specific landmine, cluster submunition, or other kind of object for which the AI model was developed and deployed to detect. As described above, the classification technology recognizes the external geometry and dimensions of an object, categorizes it based on these features, and generates a prediction score based on them.

Although the model can classify the object in the image, in a trial a weapons expert likely would be called to review the image and present their conclusion as to the nature of the object in the image. This approach is more practical, because a weapons expert, who can explain their expertise and the logic of their opinion, may be more understandable to all parties, including the judges, than a technologist explaining the workings of a complex and innovative AI model. However, the evolution of AI computer vision models increasingly raises the question of whether the AI itself could become the expert. As AI models become more sophisticated and widely used, courts will

15 As discussed above, geolocation can also be established from the resulting orthomosaic, which can also be admissible. For the sake of simplicity, this discussion focuses on geolocation derived from individual images.

16 Computer vision in the RGB (visual) spectrum cannot prove that objects in images contain explosives, only that they conform to the appearance of known explosive objects.

increasingly need to grapple with the admissibility of AI conclusions.

Chain of custody refers to the process of tracing the lifespan of a piece of information to ensure that its integrity remains intact. In this context, the key question is: Who had access to the data and the ability to manipulate it (e.g., an individual digital image and EXIF files) from the time the images were captured until they were provided to investigators? It is not a function of an AI computer vision model to protect the integrity of the photos provided to it for analysis. Demonstrating that the data has not been manipulated will rely on testimony by the agency that captured and stored the original photos as to its data-handling procedures. If necessary, images could be subject to forensic analysis. However, this approach is time and resource intensive. Building functions such as hashing or encryption into the image-capture process could help safeguard the integrity of photos.

AI computer vision and battlefield forensics

Battlefield forensics has been defined as the adaptation of scientific methods to collect, analyse, and disseminate information, intelligence, and evidence during crises or in conflict zones (Rietveld, 2025). Information identified by AI computer vision models, e.g., what weapons have been used on the battlefield, serves both intelligence and evidentiary purposes during crises or in conflict zones, bringing the technology into the field of battlefield forensics. As intelligence, the models can in some cases identify what weapons have been deployed and where. Additionally, as discussed throughout this Policy Brief, the information identified by the AI models can be evidence of international law violations. Preserving evidence of potential atrocity crimes captured on the battlefield poses unique challenges, because this information is often captured by military or humanitarian actors rather than law enforcement agents. Humanitarian and military experts have identified the need for further development of this field of study (Rietveld, 2025). Developers and users of AI computer vision models are emerging as important stakeholders in battlefield forensics and should play a role in these discussions to ensure that their tools and data collection procedures are aligned with forensic and legal requirements.

Conclusion

This Policy Brief has described how AI computer vision detection and classification technology such as that developed by T4T is changing the landscape of demining in conflict-affected areas. AI computer vision detection and geolocation in orthomosaics can rapidly and accurately identify and map UXO such as landmines and cluster submunitions. In the process, this technology can help identify and generate information of relevance to proving violations of IHL, ICL, and IHRL.

AI detection models are particularly relevant to demonstrating the use of weapons that are prohibited under international law. They can also contribute to analyses of whether attacks may have been indiscriminate or likely to cause excessive loss of civilian life or damage to civilian objects. This information not only is relevant for legal accountability efforts but can also support treaty monitoring.

However, for the imagery processed by AI detection models to be used in trial contexts, its authenticity must be demonstrated. While ensuring the integrity of the images falls outside the functionality of the models, rigorous data-handling practices and testimony from users will increase the likelihood of meeting the required admissibility standards. As these tools continue to develop, there is an opportunity to build in features to further strengthen the evidentiary value of this information. ■

Abbreviations and acronyms

AI	artificial intelligence
GIS	geographic information system
ICC	International Criminal Court
ICJ	International Court of Justice
ICL	international criminal law
IHL	international humanitarian law
IHRL	international human rights law
mAP	mean average precision
RGB	red, green and blue (light)
T4T	Tech 4 Tracing
UXO	unexploded ordnance

17 Once in the hands of investigators, chain of custody procedures to safeguard the integrity of the information will generally be established.

18 This approach would follow the example of controlled capture tools, such as eyeWitness to Atrocities (www.eyewitness.global/Using-metadata), which hash the image files at the point of capture, in essence creating a digital fingerprint unique to that image at that point in time. Any subsequent changes would be detectable because they would change the hash value.

References

Aalto-Setälä, S., L. Caroli, J. Freytag, M. F. Jaramillo Gomez and J. Lim. n.d. *Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals*. Leiden: Kalshoven-Gieskes Forum on International Humanitarian Law and Universiteit Leiden Grotius Centre. <https://leiden-guidelines.com/assets/Leiden%20Guidelines%20on%20the%20Use%20of%20DDE%20in%20ICCTs_20220404.pdf>

Convention on Certain Conventional Weapons (Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects). 1996. *Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996* (Protocol II to the 1980 Convention as amended on 3 May 1996). <https://treaties.un.org/doc/source/docs/CCW_CONF.I_16_Part%20I-E.pdf>

Convention on Cluster Munitions. 2008. Dublin, 30 May. <https://www.clusterconvention.org/files/convention_text/Convention-ENG.pdf>

Convention on the Prohibition of Anti-Personnel Mines (Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction). 1997. Oslo, 18 September. <https://treaties.un.org/doc/Treaties/1997/09/19970918%2007-53%20AM/Ch_XXVI_05p.pdf>

Corn, G. S. 2013. 'Principle of Humanity.' Oxford Public International Law. <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1810>

ENFSI (European Network of Forensic Science Institutes). 2021. *Best Practice Manual for Digital Image Authentication*. ENFSI-BPM-DI-03. April. <https://enfsi.eu/wp-content/uploads/2021/10/BPM_Image-Authentication_ENFSI-BPM-DI-003-1.pdf>

Eurojust (European Union Agency for Criminal Justice Cooperation) and OTP (Office of the Prosecutor of the) ICC (International Criminal Court). 2022. *Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations*. <https://www.icc-cpi.int/sites/default/files/2022-09/2_Eurojust_ICC_CSOs_Guidelines_2-EN.pdf>

Hao, K. 2020. 'Human Rights Activists Want to Use AI to Help Prove War Crimes in Court.' *MIT Technology Review*, 25 June. <https://www.technologyreview.com/2020/06/25/1004466/ai-could-help-human-rights-activists-prove-war-crimes>

Harvey, A. and E. LeBrun. 2023. 'Computer Vision Detection of Explosive Ordnance: A High-Performance 9N235/9N210 Detector.' *Journal of Conventional Weapons Destruction*, 27(2), June, pp. 60–68. <https://static1.squarespace.com/static/6081e2a18f1c88179800e119/t/6493cf-1ca64b3c41a45baa8a/1687408412548/Harvey_LeBrun_JCWD27.2_June_2023-final.pdf>

ICRC (International Committee of the Red Cross). 1977. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>

—. 2004. 'What Is International Humanitarian Law?' July. <https://www.icrc.org/sites/default/files/document/file_list/what-is-ihl-factsheet.pdf>

—. n.d.a. 'Fundamental Principles of IHL.' ICRC Casebook. <https://casebook.icrc.org/a_to_z/glossary/fundamental-principles-ihl>

—. n.d.b. 'Distinction.' ICRC Casebook. <https://casebook.icrc.org/a_to_z/glossary/distinction>

—. n.d.c. 'Proportionality.' ICRC Casebook. <https://casebook.icrc.org/a_to_z/glossary/proportionality>.

—. n.d.d. 'Military Necessity.' ICRC Casebook. <https://casebook.icrc.org/a_to_z/glossary/military-necessity>

Rietveld, R. M. 2025. 'Towards a Future Battlefield Forensics Framework: A NATO Action Research Case Study.' *Scandinavian Journal of Military Studies*, 8(1), pp. 451–465. <https://doi.org/10.31374/sjms.333>

TRUE Project. 2024. *Evaluating Digital Open Source Imagery: A Guide for Judges and Fact-Finders*. <https://www.trueproject.co.uk/osguide>

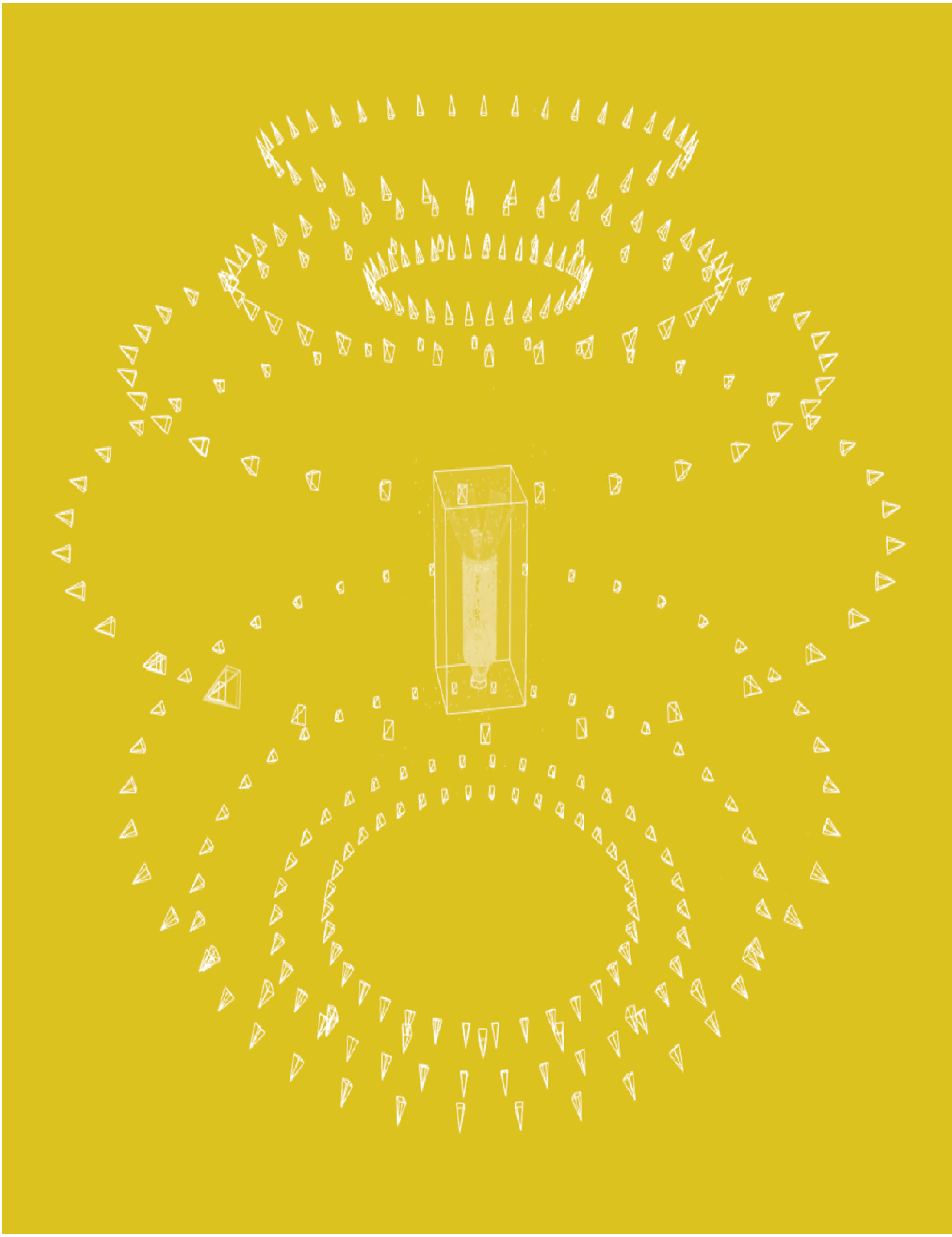
UN (United Nations). 1998. Rome Statute of the International Criminal Court. A/CONF.183/9 of 17 July. <https://docs.un.org/en/a/conf.183/9>

—. 2025. *Convention on Cluster Munitions 13MSP Progress Report: Monitoring Progress in Implementing the Lausanne Action Plan.* CCM/MSP/2025/8 of 9 September. <https://www.clusterconvention.org/files/meetings/13msp/CCM-MSP-2025-8-Advance%20Copy.pdf>

UNGA (United Nations General Assembly). 1966. International Covenant on Civil and Political Rights. Resolution 2200A (XXI) of 16 December. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

UNODA (United Nations Office on Disarmament Affairs). n.d. Political Declaration on Strengthening the Protection of Civilians from the Humanitarian Consequences Arising from the Use of Explosive Weapons in Populated Areas. <https://ewipa.org/the-political-declaration>

All links were accessed on 27 May 2026.



tech4tracing.org

TECH 4 TRACING

About Tech 4 Tracing

Stichting Tech 4 Tracing Europe is a non-profit AI computer vision lab based in the Netherlands that develops tools and assets to address the proliferation of illicit weapons, munitions, and unexploded ordnance in crime- and conflict-affected contexts, and advises policymakers on the safe and secure development of AI for counter-proliferation efforts.

Partners and supporters

This Policy Brief was supported by the European Union under the project Automated Arms and Ammunition Mapping Phase 2, part of the EU Global Threats programme.

Funded by the European Union

EU GLOBAL THREATS PROGRAMME

Contact

Stichting Tech 4 Tracing Europe

NDSM-Plein 89
1033 WC Amsterdam
The Netherlands

www.tech4tracing.org
info@tech4tracing.org

Disclaimer

Credits

This Policy Brief was prepared by Wendy Betts and Emile LeBrun. Wendy Betts is legal advisor to Stichting Tech 4 Tracing Europe and Emile LeBrun is Stichting Tech 4 Tracing Europe's Chief Operations Officer.

Copy-editor: Alex Potter
Proofreader: Stephanie Huitson
Design and layout: raumfisch.de/sign