Battlefield Evidence in the Age of Artificial Intelligence-Enabled Warfare

Winthrop Wells*

Abstract

A number of emerging technologies increasingly prevalent on contemporary battlefields—notably unmanned autonomous systems (UAS) and various military applications of artificial intelligence (AI)—are working a sea change in the way that wars are fought. These technological developments also carry major implications for the investigation and prosecution of serious crimes committed in armed conflict, including for an under-examined yet potentially valuable form of evidence: information and material collected or obtained by military forces themselves.

Such "battlefield evidence" poses various legal and practical challenges. Yet it can play an important role in justice and accountability processes, in which it addresses the longstanding obstacle of law enforcement actors' inability to access the conflict-torn crime scenes. Indeed, military-collected information and material has been critical to prosecutions of international crimes and terrorism offenses in recent years.

The present Article briefly surveys the historical record of battlefield evidence's use. It demonstrates that previous technological advances—including in remote sensing, communications interception, biometrics, and digital data storage and analysis—not only enlarged and diversified the broader pool of military data but also had similar downstream effects on the (far) smaller subset of information shared and used for law enforcement purposes.

The Article then examines how current evolutions in the means and methods of warfare impact the utility of this increasingly prominent evidentiary tool. Ultimately, it is argued that the technical features of UAS and military AI give rise to significant, although qualified, opportunities for collection and exploitation of battlefield evidence. At the same time, these technologies and their broader impacts on the conduct of warfare risk inhibiting the sharing of such information and complicating its courtroom use.

---

* Senior Manager for Programs and Policy Planning, and Programmatic Unit Officer-in-Charge, the International Institute for Justice and the Rule of Law. The author wishes to thank the editors of the *Chicago Journal of International Law* for the opportunity to contribute to this symposium and for their diligent work. The views expressed are those of the author alone.

Table of Contents

I. INTRODUCTION

Ever since the 1991 Persian Gulf War, policymakers and scholars have vigorously contested whether new technologies are ushering in a revolution in military affairs and rendering the struggle for information supremacy decisive in future warfare.[1] Recent and ongoing armed conflicts in theaters from Nagorno-Karabakh and Syria to Ukraine and Gaza have intensified this debate. While it remains to be seen whether and how technologies such as unmanned autonomous systems (UAS) and artificial intelligence (AI) will affect the determinants of military victory, it is clear that they are already working a sea change in the way that wars are fought. Battlefields now teem with sensors and echo with the buzz of UAS, which collect tremendous volumes of information. Military assets harvest, sift through, analyze, re-package, and disseminate this data at unprecedented speed, aided by increasingly sophisticated applications of machine learning (ML) and AI. At the same time, due to the near-omnipresence of personal digital devices, the evolution of social media, and improvements in commercial satellite imagery, conflict zones are not only more transparent to commanders and operators but more visible to interested audiences worldwide, albeit mis- and disinformation distort even careful observers' perspectives.

These technological developments also carry major implications for the investigation and prosecution of serious crimes committed in armed conflict, some of those implications still underexplored. A wealth of scholarship addresses the "accountability turn" in U.N. fact-finding and investigative missions, the professionalization of civil society documentation, and the emergence of open-source digital evidence. The opportunities for non-governmental and criminal justice actors alike to leverage technologies such as ML and AI for evidence analysis and presentation have also inspired a substantial literature.[2] Yet scholars have devoted relatively little attention to how the introduction of new technologies in the military domain affects another potentially valuable form of evidence: information and material collected or obtained by military forces themselves.

For several reasons, this gap in the literature is significant. Such "battlefield evidence" has been critical to prosecutions of international crimes and terrorism offenses in recent years.[3] Its burgeoning use can be credited in large part to previous technological advances, including in remote sensing,

---

1 *See*, *e.g.*, Andrew F. Krepinevich, *Cavalry to Computer: The Pattern of Military Revolutions*, 37 NATIONAL INTEREST (1994), Michel Mazaar, *The Revolution in Military Affairs: a Framework for Defense Planning,* U.S. ARMY WAR COLL, STRATEGIC STUD. INST. (1994); Eliot Cohen, *A Revolution in Warfare*, 74 FOR. AFF'S. (1996); Stephen Biddle, *The Past as Prologue: Assessing Theories of Future Warfare*, 8 SEC. STUD. (1998); Kenneth Payne, *Artificial Intelligence: A Revolution in Strategic Affairs?*, 60 SURVIVAL 7 (2018).

2 Separately, a vast amount of scholarship addresses issues related to the protection of military data and to such data's uses in warfare itself. *See generally* THE RIGHTS TO PRIVACY AND DATA PROTECTION IN TIMES OF ARMED CONFLICT (Asaf Lubin & Russell Buchan eds., 2022).

3 *See infra* Section III.B.

communications interception, biometrics, and digital data storage and analysis, which equipped militaries to collect more information and material than before and to more effectively exploit and analyze their collections, with (indirect) benefits for law enforcement. The present Article aims to examine how current evolutions in the means and methods of warfare impact the utility of this increasingly prominent evidentiary tool.

The Article is structured as follows. Section II begins by defining the concept of battlefield evidence and laying out some of the legal issues associated with its collection, sharing, and use (II.A). It then briefly surveys the historical record, describing how an increasing variety of such information and material, derived from militaries' growing repertoire of technical means, has proven valuable in justice processes (II.B).

Section III discusses new and emerging technologies employed in recent armed conflicts, notably UAS and military AI (III.A), and what they portend for battlefield evidence (III.B). Here, the Article argues that these technologies hold out the promise of further increasing the amount of potential evidence that militaries collect and further improving the prospects of effective exploitation and analysis—yet they also give rise to new obstacles to the collection and sharing of such information and new complications for its investigative and evidentiary use, some more susceptible to mitigation than others. Section IV concludes with a final observation.

II. INFORMATION FROM MILITARY OPERATIONS AS "BATTLEFIELD EVIDENCE"

This Section will explain why information collected by the military is potentially valuable as evidence in criminal proceedings, introduce some associated legal and practical issues, and demonstrate how the history of its law enforcement use has tracked previous technological improvements in military collection and exploitation capabilities.

A. Legal Issues Associated with Collection, Sharing, and Use

The present Article will use "battlefield evidence" to refer to information and material collected or obtained through military operations and subsequently used in criminal proceedings. Admittedly, while it enjoys broad currency, this is not a legal term of art. Other phrases are sometimes preferred, including "military evidence," "captured enemy material," or "collected exploitable material." More confusingly, "battlefield evidence" itself is sometimes used to refer to any information or material collected in a conflict zone, whether by military forces, law enforcement personnel, or even private actors. However, the term is increasingly understood in the way that this paper proposes to use it. U.N. Security Council Resolution 2617, adopted in 2021, observed that "information and materials collected or received by the military [are] also referred to as battlefield evidence," and surrounded "battlefield evidence" with quotation marks in each subsequent use, reiterating this

definition in a reference to "evidence collected by the military, also referred to as 'battlefield evidence.'"[4]

The working definition set forth above has several elements worth noting. First, the types of military forces that may be collectors and the legal and operational situations in which they may collect material both vary. Regular military and special operations personnel; militaries under national command as well those in multinational constructs; and those operating extraterritorially as well as those operating domestically—all collect potentially relevant material in the course of their missions and operations.

Second, from a criminal justice perspective, battlefield evidence is defined by the military *source* of the material and is thus a subset of the larger category of "evidence," which may have multiple sources. It is not restricted to a particular *type* of material, as, for example, "digital evidence" or "documentary evidence" are. As a practical matter, military forces collect or obtain a great variety of information and material. Individual personnel recover physical items, including documents; weapons and weapons components; electronic media, such as cell phones, laptops, and hard drives; and other objects. Technical exploitation of this material gleans further information, including biometrics and, in the case of devices, many forms of digital data. Military personnel also record statements when questioning detainees or other individuals they come across in operational theaters, and military intelligence services active in such areas obtain information from human sources, or human intelligence. Finally, a host of intelligence, surveillance, and reconnaissance (ISR) systems—satellites, manned aircraft and maritime vessels, unmanned autonomous systems, and airborne and ground-based sensors—intercept communications and generate geospatial intelligence, on-the-ground imagery and footage, and other signals intelligence.

From a military perspective, on the other hand, it is the material's *use* for criminal justice purposes that distinguishes it. In that sense, it is a subset of the larger category of "military data" (alternatively, "battlefield information" or "military intelligence"), which may have multiple uses. Battlefield evidence's usefulness for law enforcement is not limited to a certain type of jurisdiction nor a certain type of crime: such material has in fact been introduced both in international criminal fora and in domestic criminal proceedings related to core international crimes, to terrorism offenses, and to piracy.[5]

Finally, saying that the material is ultimately used for law enforcement is *not* to say that it was *collected* with that end in mind. Indeed, in most circumstances battlefield evidence was originally collected for other purposes. Military forces use information to improve their situational awareness and strategic decision-making, as well as to support a range of specific activities,

---

4 S.C. Res. 2617, preamble, ¶ 8 (Dec. 23, 2021).

5 It should also be recognized that military-collected information and material can serve to initiate or nourish an ongoing investigation, or otherwise support legal process. But this Article will restrict its focus to evidence actually introduced in court, which brings distinct legal issues into play.

most notably targeting and force protection. Other uses include access and border control, detention decisions, identification of the dead, and hostage rescue. In most circumstances, it is for these military purposes that defense officials devote their resources and military personnel prolong their time in dangerous environments to gather and preserve information and material.[6]

Nevertheless, although collected for non-law enforcement purposes, the information may be hugely valuable to criminal justice practitioners. This is primarily because it represents a means of responding to a longstanding obstacle to accountability for international crimes, as well as for terrorism offenses committed in armed conflict: law enforcement actors' inability to access the conflict-torn crime scenes.

Significant legal and practical challenges confront both military forces seeking to collect material on the battlefield and criminal justice authorities seeking to obtain and use that material for their own ends, however.

Military personnel regularly operate in non-permissive environments, under attack or threat of attack by hostile forces. They may be afforded as little as five to ten minutes of "time on target" before having to relocate, and during that brief window their overriding priorities are accomplishing their mission and ensuring force protection while doing so. They rarely enjoy the luxury of securing scenes and conducting searches in the meticulous fashion of law enforcement officers, who work in relatively controlled settings and for whom evidence-gathering is a core function.[7] Likewise, military means of collecting information at some remove from active hostilities must overcome determined foes' technical countermeasures and the general "fog of war," neither of which impede typical civilian criminal investigations. Multinational military operations involve an additional layer of complexity, as coalition partners must resolve questions about collected material's legal ownership and find practical solutions to bridge differences in domestic legal and policy approaches to information processing.

Information and material collected by the military is presumed to implicate national security interests almost as a matter of course, and therefore almost invariably classified. This practical reality greatly complicates domestic, let alone international, interagency sharing. In most circumstances, there is no legal obligation to make information of such sensitivity available for law enforcement use; even when criminal justice authorities are empowered to request or receive the information, defense and security agencies can lawfully

---

6 *Cf.* Letter from George Washington to Colonel Elias Dayton, July 26, 1777, *in* THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745–1799 479 (John C. Fitzpatrick ed., 1931) ("The necessity of procuring good Intelligence, is apparent and need not be further urged.").

7 *See* Michael N. Schmitt, *Investigating Violations of International Law in Armed Conflict*, 2 HARV. NAT'L. SEC. J. 31, 54–55. (2011).

withhold it based on some form of public interest or state secrets privilege.[8] The decision to share military-collected information—and, as may be necessary, to declassify it—is therefore at the discretion of officials notoriously incentivized toward caution. Moreover, in cases where the information was not collected by the state's own military forces but rather received from a foreign state, the recipient state agency ordinarily abides by a "third party rule," or "originator control principle," whereby it refrains from sharing the information onward or divulging it publicly without the express authorization of the state that provided it.[9]

The just-described complications associated with collecting and sharing such information and material also make it more challenging to use as legal evidence.

Military forces' distinct—i.e., from law enforcement—institutional competence and the practical circumstances with which they contend elevate the real risk that any material collected will be contaminated during preservation and processing. They also mean that the documentation even of actually uncontaminated material falls far short of the thoroughness expected in criminal justice contexts. Important elements like photographs and descriptions of precise collection locations and conditions, as well as collectors' identities, may be omitted. Chains of custody may be marred by gaps. Additionally, some technical means of collection may require expert explanation. All of this makes it more difficult to establish battlefield evidence's authenticity and reliability in a court of law, and more likely that judges will exclude it from consideration or refuse to rely on it. Statements that military personnel take during the course of missions and operations or in detention settings may also raise voluntariness issues, even if criminal procedural safeguards, such as the rights to remain silent, to be provided with counsel, and to be informed of these rights, are deemed inapplicable.

Further difficulties flow from the need to introduce the evidence in court in a manner that protects the national security interests in play, including the sources and methods of its collection. Indeed, security officials will only share sensitive information if confident that measures will be put in place to prevent any harm that its fulsome disclosure to the public or even the defense might cause. Yet the modes of protecting such information most palatable to providers may be in tension with the defendant's rights to receive a public hearing, to be present throughout, to examine the evidence against them, and to obtain disclosure of exculpatory material the prosecution possesses. And defense and security agencies may likewise condition the availability of military personnel and other sensitive witnesses for testimony on procedural

---

8 *See, e.g.*, Conway v. Rimmer [1968] A.C. 910 (U.K. H.L.). In some jurisdictions, executive authorities are required to affirmatively invoke such a privilege to withhold material that would otherwise be disclosable to criminal justice authorities; in others, decision-makers can withhold the material by simply refusing to lift a privilege which operates automatically.

9 *See* HANS BORN ET AL., MAKING INTERNATIONAL INTELLIGENCE COOPERATION ACCOUNTABLE 152–53 (2015).

protections that, in accommodating security concerns, restrict the defendant's ability to exercise the full range of their rights. In either scenario, the risk arises that the trial's fairness will be compromised.

B. Brief History of Use

Despite the challenges, over the years numerous courts both domestic and international have admitted and relied on military-collected information and material as evidence. A brief look at the past gives a sense of the panoply of military forces that originally collected that information, the breadth of criminal charges it has supported, and the impact of technological advances.

The earliest modern instance worth noting is Nuremberg. In the aftermath of Germany's unconditional surrender, when the Allied powers decided to hold Nazi leaders individually responsible for their crimes, the prosecutors at the International Military Tribunal established for that purpose benefited from the full military occupation of German territory by the U.S., U.K., Soviet Union, and France. At the prosecution team's instruction, "[A]llied forces could act swiftly to seize evidence and to make arrests at any place, at any time, within the areas under their control."[10] German bureaucrats, never imagining future accountability, had recorded the regime's criminality in painstaking detail, and the "hundreds of tons of official German documents"[11] that Allied personnel seized represented the principal evidence introduced at Nuremberg, as well as in subsequent post-World War II war crimes trials held in German courts. Prosecutors also screened in the courtroom a "chillingly graphic" film assembled from footage shot by military photographers of Allied troops' arrival in the concentration camps, to striking effect.[12]

For decades following the immediate postwar period, the record of international crimes prosecutions remained sparse. At the same time, attacks plotted and conducted by terrorist groups were for the most part unconnected with armed conflict situations, and governments considered this threat primarily a matter for law enforcement and intelligence responses, with little role for the military. One notable exception was the U.K.'s approach to terrorism in Northern Ireland. The U.K. government regularly dispatched military and paramilitary forces on British territory to secure potential targets, patrol areas believed at risk of attack, conduct disruption operations, and respond to attacks. After initially relying on a security detention regime, it eventually came to try individuals arrested in Northern Ireland in connection

---

10 Mark Harmon & Fergal Gaynor, *Prosecuting Massive Crimes with Primitive Tools: Three Difficulties Encountered by Prosecutors in International Criminal Proceedings*, 2 J. INT'L CRIM. JUSTICE 403, 404 (2004).

11 *See* Justice Robert H. Jackson, *Opening Statement before the International Military Tribunal* (Nov. 21, 1945), https://perma.cc/D7FG-WRLD.

12 *See* TELFORD TAYLOR, ANATOMY OF THE NUREMBERG TRIALS: A PERSONAL MEMOIR 186 (1992).

with terrorism before non-jury "Diplock courts" equipped with special rules of procedure and evidence adapted for that purpose.[13]

Another exception warranting mention is Israel's longtime struggle against terrorist plots and attacks mounted in the context of military occupation or otherwise connected with active armed conflict. Unsurprisingly, the Israeli response to this threat has been and remains highly militarized. While Israel has primarily opted for law of armed conflict (LOAC) or other forms of security detention, it also tries terrorism suspects before both regular criminal courts (in Israel proper) and in military courts (in the West Bank and, until its 2005 withdrawal, in Gaza). Israeli courts, like the Diplock courts, have regularly based terrorism convictions on information provided by military personnel, particularly testimonial evidence.[14]

The U.N. Security Council revitalized international criminal justice in the early 1990s, creating the International Criminal Tribunals for the Former Yugoslavia (ICTY) and for Rwanda (ICTR). Prosecutors could only regard their Nuremberg counterparts' investigative advantages wistfully: the *ad hoc* tribunals had jurisdiction over crimes committed with state involvement in areas where security conditions remained hazardous and much evidence in the hands of interested actors, while lacking their own enforcement machinery.[15] Then-Chief Prosecutor Richard Goldstone later observed that, given these constraints, upon arrival in his post he quickly "concluded that it would be very helpful to have access to [military] intelligence information," and thus embarked on "lengthy, complex and detailed negotiations" with multiple states to that end.[16] Goldstone and his successors' diplomacy ultimately bore fruit in states' provision of various types of sensitive information relevant to the ICTY's work, including military video footage, intercepted communications, and satellite imagery.[17] Tribunal Judge Patricia Wald later commented that the "most astounding" evidence in the Srebrenica genocide case was "the satellite aerial image photography furnished by the U.S. military intelligence which

---

13 *See* JOHN JACKSON & SEAN DORAN, JUDGE WITHOUT JURY: DIPLOCK TRIALS IN THE ADVERSARY SYSTEM (1995).

14 *See* EMANUEL GROSS, THE STRUGGLE OF DEMOCRACY AGAINST TERRORISM: LESSONS FROM THE UNITED STATES, THE UNITED KINGDOM, AND ISRAEL (2006).

15 *See First Annual Report of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the former Yugoslavia Since 1991*, U.N. GAOR, 49th Sess., U.N. Doc. A/49/342-S/1994/1007 (Aug. 29, 1994), ¶ 84.

16 *See* Richard Goldstone, *Remarks by Richard Goldstone*, 98 PROC. ANN. MEETING AM. SOC'Y INT'L L. 148 (2004); Richard Goldstone, *A View from the Prosecution*, 2 J. INT'L CRIM. JUST. 380, 380–81 (2004).

17 *See* Carla Del Ponte, *Investigation and Prosecution of Large-Scale Crimes at the International Level: The Experience of the ICTY*, 4 J. INT'L CRIM. JUST. 539, 554 (2006) ("A second set of contemporaneous records that have been found to be useful are intercepted communications, [including] recordings of intercepted communications from the intelligence or other branches of armed forces.").

pinpointed to the minute movements on the ground of men and transports in remote Eastern Bosnian locations."[18]

With respect to the former Yugoslavia, prosecutors also received crucial assistance from North Atlantic Treaty Organization (NATO)–led international peace enforcement missions,[19] which not only detained numerous defendants but seized key evidence on the ICTY's behalf, enabled exhumations of mass graves, and permitted prosecutors to search their own databases. The ICTR, while relying far more heavily on witness testimony,[20] also admitted military intercepts as well as documents provided by the U.N. peacekeeping mission in Rwanda. And both *ad hoc* tribunals heard testimony from military officers who had commanded or served in peacekeeping missions active in the relevant territories. The International Criminal Court (ICC) and other tribunals established since have followed their example in seeking military- and intelligence-derived information both from states and from international peace operations, albeit with mixed success.[21]

Separately, the military took on a leading role in the fight against terrorism following the Al-Qa'ida attacks of September 11, 2001, the U.S.'s assertion of a "global war on terror," and the ensuing launch of the Afghanistan and Iraq wars, along with the persistent use of armed force by the U.S. and its allies and partners in Pakistan, Yemen, and elsewhere. Concerns around the evidentiary viability of military-collected material figured large in U.S. legal and policy debates about the proper disposition option for captured Al Qa'ida combatants. Senator Strom Thurmond, pressing the case for President George W. Bush's preferred solution in Senate Oversight Hearings, asserted that:

> Military commissions are preferable to trial in civilian courts because of the unique conditions of war. For example, these commissions would allow for the more flexible use of classified information . . . Additionally, more flexible rules would allow for the use of evidence collected during war. Rules governing the gathering of evidence for use in trial courts in

---

18 Patricia Wald, *The International Criminal Tribunal for the Former Yugoslavia Comes of Age: Some Observations on Day-to-Day Dilemmas of an International Court*, 5 WASH. U. J. OF L. AND POL'Y 101 (2011).

19 NATO's Bosnia Implementation (IFOR) and Stabilization Forces (SFOR) and Kosovo Force (KFOR) facilitated the ICTY's work, as did the U.N. temporary administrations of Croatia (UNTAES) and Kosovo (UNMIK). *See Fifth Annual Report of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the former Yugoslavia Since 1991*, U.N. GAOR, 53rd Sess., U.N. Doc. A/53/219-S/1998/737 (Aug. 10, 1998), ¶¶ 56, 123; *Sixth Annual Report of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the former Yugoslavia Since 1991*, U.N. GAOR, 54th Sess., U.N. Doc. A/54/187-S/1999/846 (Aug. 25, 1999), ¶¶ 134, 137.

20 *See* Nancy Amoury Combs, *Deconstructing the Epistemic Challenges to Mass Atrocity Prosecutions*, 75 WASH. AND LEE L. REV. 223, 236 (2018).

21 *Compare* Charlie Savage, *Biden Orders U.S. to Share Evidence of Russian War Crimes With Hague Court*, N.Y. TIMES (July 26, 2023), *with* Ellen Nakashima, *Trump Administration Unwinds Efforts to Investigate Russian War Crimes*, WASH. POST (Apr. 22, 2025).

> the United States do not necessarily apply to evidence gathered on the battlefield.[22]

The Bush administration designed, and subsequently reworked, the Guantánamo military commissions' procedures in part for the express aim of enabling the use of such evidence. When President Barack Obama decided to continue trying some captured combatants through the commissions, he publicly explained the decision in the same terms, declaring in mid-2009 that:

> Military commissions . . . are an appropriate venue for trying detainees for violations of the laws of war. They allow for the protection of sensitive sources and methods of intelligence-gathering . . . and for the presentation of evidence gathered from the battlefield that cannot always be effectively presented in federal courts.[23]

With time, however, as proceedings at Guantánamo encountered difficult legal issues and the prolongation of detentions there attracted widespread international opprobrium, the U.S. came to try the overwhelming majority of terrorism suspects in federal criminal courts. In doing so it made ample use of information and material collected by U.S. forces on foreign battlefields, particularly in Afghanistan and Iraq. The military's recently improved biometrics capabilities yielded information that proved of great value in these cases.[24] Investment in facilities for in-theater exploitation and the preservation of millions of records against which newly collected data could be checked in near-real time had made biometrics a critical tool for a range of military purposes. Perhaps its most noteworthy function was to "attack the networks" of terrorist group members financing, fabricating, and emplacing improvised explosive devices (IEDs), including through criminal prosecutions.[25]

In some instances, the U.S. even shared biometric data with other states for use in prosecutions of bombmakers arrested on foreign soil. An oft-cited example is the case of Anis Sardar, a British citizen who, while living near Baghdad in 2007, planted several IEDs with the intent of killing U.S. soldiers. In so doing, he inadvertently left fingerprints on the sticky tape that bound together two devices' components. Forensic scientists did not identify the prints as Sardar's until nearly a decade later, but when they did, the match led

---

22 Strom Thurmond, *Statement of Hon. Strom Thurmond, a U.S. Senator from the State of South Carolina, Department of Justice Oversight: Hearing Before the United States Senate Committee on the Judiciary* (Nov. 28, 2001), https://perma.cc/B7N8-34N934N9.

23 Barack Obama, *Remarks by the President on National Security*, THE WHITE HOUSE (May 21, 2009), https://perma.cc/EC8V-J5CK.

24 Military biometrics also became a useful tool in national and multinational efforts to support piracy prosecutions. *See*, *e.g.*, David Axe, *CSI Somalia: Interpol Targets Pirates*, WIRED (June 18, 2009), https://perma.cc/LCT8-JV7P.

25 *See generally* GLENN VOELZ, THE RISE OF IWAR: IDENTITY, INFORMATION, AND THE INDIVIDUALIZATION OF MODERN WARFARE (2015).

to Sardar's arrest and conviction by a British jury on charges of murder and conspiracy to murder.[26]

U.S. and allied forces also systematically provided collected material to Iraqi and Afghan criminal justice authorities to support terrorism trials. In what was termed "warrant-based targeting" in Iraq and "evidence-based operations" in Afghanistan, coalition forces supported local rule of law by transferring detainees to host state judicial authorities along with evidence packages that could substantiate criminal charges.[27]

The following decade, worldwide alarm at the threat posed by foreign terrorist fighters (FTFs) traveling to join the Islamic State in Iraq and the Levant (ISIL), among other parties to the civil war in Syria, inspired the broadest multilateral effort yet to share and use battlefield evidence for terrorism prosecutions at the national level. In Resolution 2396, adopted in 2017, the U.N. Security Council called upon member states as well as U.N. entities:

> [T]o share best practices and technical expertise . . . with a view to improving the collection, handling, preservation and sharing of relevant information and evidence . . . including information obtained . . . in conflict zones, in order to ensure foreign terrorist fighters who have committed crimes, including those returning and relocating to and from the conflict zone, may be prosecuted.[28]

This exhortation—which the U.N. Secretary-General clarified as referring in great part to information obtained by the military[29]—helped lead to a concerted increase in the provision of such information, chiefly collected by Global Coalition to Defeat ISIL forces, to criminal justice authorities, including through international mechanisms such as INTERPOL and the European Union Schengen Information System. ISIL's bureaucratic penchant for extensive record-keeping was a boon for investigators and prosecutors, who made effective evidentiary use of various types of documents issued by the group, e.g. membership rosters, registration forms, and financial or hospital records. Much of this material was obtained in electronic form, on hard drives or thumb drives recovered on the battlefield and subsequently decrypted. Digital media more vividly documenting atrocities also abounded in the Syria/Iraq conflict zone, in which victims, perpetrators, and bystanders

---

26 *See* Steve Swann, *Anis Sardar Trial: Iraq Bombmaker Trapped By Sticky Tape*, BBC NEWS (May 21, 2015), https://perma.cc/ZA6H-XEGR; Haroon Siddique, *London Cab Driver Jailed For Life For Making Bombs to Kill US Soldiers in Iraq*, THE GUARDIAN (May 22, 2015), https://perma.cc/9QEN-JNDR.

27 *See* Kevin Govern, *Warrant-Based Targeting: Prosecution-Oriented Capture and Detention as Legal and Moral Alternatives to Targeted Killing,* 29 ARIZ. J. INT'L & COMP. L. 477 (2012); Joop Voetelink, *Evidence-Based Operations: How to Remove the Bad Guys from the Battlefield*, 4 J. INT'L L. PEACE & ARMED CONFLICT 194 (2013).

28 S.C. Res. 2396, ¶ 20 (Dec. 21, 2017).

29 U.N. Secretary-General, *Seventh report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat*, U.N. Doc. S/2018/770, ¶ 69 (Aug. 16, 2018).

alike carried smartphones, and images and videos that the military extracted from seized devices proved crucial for law enforcement as well.

In numerous European and other domestic courts with jurisdiction, battlefield evidence has come to play an increasingly important role in prosecutions of atrocities committed in Syria and Iraq, including to substantiate international crimes charges against both terrorist group members and agents of Bashar al-Assad's government. Such cases continue to this day, as do prosecutions of serious crimes committed in other conflicts, in both national and international fora, that similarly rely on military data.[30]

Before proceeding any further, several general points regarding battlefield evidence's historical availability and legal viability are in order.

First, technological improvements in collection and exploitation capabilities—including in remote sensing, communications interception, biometrics, and digital data storage and analysis—have not only enlarged and diversified the broader pool of military data but also had similar downstream effects on the (far) smaller subset of information shared and used for law enforcement purposes.[31] This development reflects a wider trend in criminal law, in which "[a]dvances in technology over the past fifty years have resulted in improvements in the types of evidence which can be brought before the court."[32]

Second, in practice, defense and security agencies have shared military data with and made military witnesses available to criminal justice authorities not from an altruistic commitment to justice but due to their own pragmatic policy considerations. For example, NATO allies provided the ICTY with information documenting Slobodan Milošević's crimes only after concluding that the Bosnian Serb leader represented an obstacle to the peaceful settlement they sought; so long as they still viewed him as a potential contributor to such a settlement, they withheld that evidence. U.S. and allied forces shifted from a security detention regime in Iraq to broad-scale support for prosecutions through a reformed host state criminal justice system years before making a similar effort in Afghanistan not due to differing demands of criminal accountability but because changes in strategic circumstances necessitated this shift years earlier in the former situation.[33]

---

30 Already in 2020, "[t]he experience of national authorities in obtaining and using battlefield evidence ha[d] increased over the past years. Courts in several Member States have rendered convictions in cases in which significant evidence originated from the battlefield." EUROJUST, SEPTEMBER 2020 MEMORANDUM ON BATTLEFIELD EVIDENCE 21 (2020).

31 *Cf.* Laura Moranchek, *Protecting National Security Evidence While Prosecuting War Crimes: Problems and Lessons for International Justice from the ICTY*, 31 YALE J. INT'L L. 476, 479 (2006) ("Advances in intelligence technology, particularly signals surveillance and satellite reconnaissance, have given prosecutors new tools to document war crimes and command responsibility where the paper trail leaves off.").

32 Richard May & Marieke Wierda, *Trends in International Criminal Evidence: Nuremberg, Tokyo, The Hague, and Arusha*, 37 COLUM. J. TRANSNAT'L L. 725, 734 (1999).

33 Robert Chesney, *Iraq and the Military Detention Debate: Firsthand Perspectives from the Other War, 2003-2010*, 51 VA. J. INT'L L., 51 (2011), 553; *see also* Voetelink, *supra* note 28, 195–97.

In this connection, it is also worth recalling that Resolution 2396's main thrust was to urge states to address the *security* threat posed by foreign terrorist fighters.[34] The U.N. Security Council called upon states to share information not just for law enforcement but also for other uses including border security, and it urged criminal prosecution primarily as one way of stanching the flow of FTFs across borders, and not in order to achieve justice as such.[35]

Finally, observing that battlefield evidence has been used in this range of contexts is not to advance a normative argument about the consistency of such use with applicable international or domestic law.[36] In any given jurisdiction, the viability of military-collected information and material as legal evidence is a complex, case-specific issue. But for present purposes, it bears mention that the 2020 Eurojust Memorandum on Battlefield Evidence, based on a survey of twenty-seven national judicial authorities,[37] concluded that, as a general matter, "use of battlefield evidence is not excluded under national law."[38] The Council of Europe's 2024 Comparative Practices on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings echoed this conclusion.[39] Moreover, in spite of the legal challenges outlined above, practitioners have successfully availed themselves of various procedural mechanisms and techniques to admit the evidence at trial while protecting security interests, and to corroborate its authenticity and reliability and support its probative value.

III. IMPLICATIONS OF NEW AND EMERGING TECHNOLOGIES IN WARFARE

This Section will turn to several emerging technologies in the military domain and examine the potential consequences for battlefield evidence. It

---

34 *See* S.C. Res. 2396, preamble (Dec. 21, 2017).

35 *See id.*, ¶¶ 2–16 (on border security and information sharing) and preamble ("*Underlining* the importance of strengthening international cooperation to address the threat posed by foreign terrorist fighters, including on information sharing, border security, investigations, judicial processes, extradition . . . and prosecution").

36 For instance, the great domestic and international contention generated by Diplock courts' and Israel courts' admission of statements taken by military and (more commonly) intelligence personnel for security purposes—in addition to the harsh and in some cases unlawful interrogation tactics employed—should be acknowledged. *See*, *e.g.*, Paul Hunt & Brice Dickson, *Northern Ireland's Emergency Laws and International Human Rights*, 11 NETH. Q. HUM. RTS. 173 (1993); Adrian Zuckerman, *Coercion and the Judicial Ascertainment of Truth*, 23 ISRAEL L. REV. 357 (1989).

37 The twenty-seven included those of EU Member States and of non-EU countries represented by a liaison prosecutor at Eurojust and the Genocide Network.

38 Eurojust, *supra* note 31, at 21.

39 I authored the Comparative Practices, based primarily on information provided by the competent authorities of states that are members of the Council of Europe Committee on Counter-Terrorism (CDCT), within the framework of a joint project of the CDCT Secretariat and the International Institute for Justice and the Rule of Law. *See* COUNCIL OF EUROPE, COMPARATIVE PRACTICES ON THE USE OF INFORMATION COLLECTED IN CONFLICT ZONES AS EVIDENCE IN CRIMINAL PROCEEDINGS (2024).

will be argued that from a criminal justice standpoint this technological leap, like its predecessors, presents both benefits and challenges.

A. Technologies Introduced in Recent Armed Conflicts

Among other new technologies, unmanned autonomous systems and artificial intelligence have seen particularly rapid military adoption and already effected notable changes—including in the collection and processing of information—in conflicts ranging from Ukraine to Gaza.

1. Unmanned autonomous systems

UAS have long been present on the battlefield, but steep increases in lethality and decreases in cost have made them especially prevalent in recent civil wars in Syria, Yemen, Libya, and Ethiopia, in the 2020 Armenia-Azerbaijan conflict over Nagorno-Karabakh, and in the Russia-Ukraine and Israel-Hamas conflicts. Despite questions about their actual military decisiveness,[40] the continuation of these trends and general perceptions of their usefulness make it likely that their role will only increase in future warfare.[41]

Beyond their much-discussed use in kinetic targeting, UAS have greatly enhanced military ISR capabilities. Some of these systems combine powerful remote sensors that can generate broad landscape overviews and long-range images with the maneuverability to capture on-the-ground footage. They can provide visibility into the movements of adversary forces, the actions of individual soldiers and civilians, and the use of specific types of weaponry, as well as other situational context.

These attributes are on full display in the current Russia-Ukraine conflict, the first protracted, high-intensity interstate hostilities in which UAS have featured so prominently. While drones' kinetic uses have attracted the lion's share of attention, arguably their "largest impact has been their use in *reconnaissance* and guiding artillery fire" in what is still primarily an artillery war.[42] As of mid-2023, UAS reconnaissance was reportedly responsible for identifying a staggering 86% of all Ukrainian targets.[43]

ISR was in fact the principal function of UAS historically, and in some ways remained so even after wide-ranging, high-tempo drone strike campaigns

---

40 *See* Antonio Calcara et al., *Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare*, 46 INT'L SEC. (2022).

41 *See*, *e.g.*, Dominika Kunertova, *The Ukraine Drone Effect on European Militaries*, 10 CSS POL. PER'V. (2022).

42 Jean-Marc Rickli & Federico Mantellassi, *The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare*, 34 GENEVA CENTRE FOR SECURITY POLICY 4 (2024).

43 Shashank Joshi, *The War in Ukraine Shows How Technology is Changing the Battlefield*, THE ECONOMIST (July 3, 2023). It has also been suggested that a dearth of ISR drones was a major factor in Russia's lack of situational awareness (and ensuing high casualties) in the initial days following the February 24, 2022 full-scale invasion. *See* Samuel Bendett, *Where Are Russia's Drones?*, DEFENSE ONE (Mar. 1, 2022), https://perma.cc/CFT3-SR48.

became the centerpiece of the U.S.'s and other states' post-9/11 counterterrorism and counterinsurgency operations.[44] To be sure, the use of UAS for ISR purposes cannot be cleanly disentangled from the targeting process, since the primary immediate use of the information that UAS gather is for target development and validation.[45] For present purposes, however, what is pertinent is that UAS are not simply a tool for engaging targets, but an increasingly vital source of military data which would otherwise go uncollected and which can be valuable for a range of uses.

2. Military applications of artificial intelligence

No authoritative definition of artificial intelligence exists in international law, but for present purposes reference can be made to an influential International Committee of the Red Cross (ICRC) position paper, which defined AI as "the use of computer systems to carry out tasks—often associated with human intelligence—that require cognition, planning, reasoning or learning."[46] The same paper defined machine learning systems as "AI systems that are 'trained' on and 'learn' from data, which ultimately define the way they function."[47]

Military uptake of AI, mooted for decades, has burst into full view in Gaza and Ukraine, and ethical and prudential concerns notwithstanding, policymakers' enthusiasm seems set to accelerate its adoption going forward. Much ink has been spilled on the opportunities and dangers of AI's capacity to power fully autonomous lethal weapons systems. The technology's most dramatic armed conflict application to date, however, has been on belligerents' ability to gather and analyze information.[48]

Partly thanks to AI-driven autonomy, militaries are now hoovering up ever more massive amounts of data from the battlefield through an increasing diversity of technical means. Advanced sensors mounted on drones and satellites today capture images, audio, and video that would have previously remained beyond military intelligence assets' reach. AI and ML tools enable the processing and analysis of hitherto unmanageable volumes of information, and at hitherto unimaginable speed, discerning intricate connections and generating compelling predictions. Information management systems that integrate military data with commercial satellite images, social media posts, and

---

44 *Cf.* Michael N. Schmitt, *Drone Attacks Under the Jus ad Bellum and Jus in Bello: Clearing the "Fog of Law"*, 13 Y.B. INT'L HUM. L. 311, 313 (2010) ("The nature and use of drones varies widely. Most are unarmed and used for intelligence, reconnaissance and surveillance (ISR) functions").

45 *See generally* NATO, NATO STANDARD ALLIED JOINT PUBLICATION-3.9 ALLIED JOINT DOCTRINE FOR JOINT TARGETING (ed. B, version 1) (Nov. 2021).

46 ICRC, *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*, 102 INT'L REV. RED CROSS 463 (2021).

47 *Id.*

48 *See* Steven Hill & Nadia Marsan, *Artificial Intelligence and Accountability: A Multinational Legal Perspective*, *in* BIG DATA AND ARTIFICIAL INTELLIGENCE FOR MILITARY DECISION MAKING (2018); Anthony King, *Digital Targeting: Artificial Intelligence, Data, and Military Intelligence*, 9 J. GLOB. SEC. STUD. (2024).

other digital open-source information can enhance analytical outputs' verifiability and reliability, whether relating to the identification of an individual, for instance, or the assessment of harm to civilians and damage to civilian objects an attack is expected to cause. Such analyses can support military decision-making with regard to both human-controlled and autonomous kinetic targeting, as well as detention, navigation, damage assessment, force protection, planning, logistics, equipment maintenance, supply chain management, training design, information warfare, and even the formulation of wider wartime strategy.[49]

One exemplar of AI's potential for military data integration and analysis is the Algorithmic Warfare Cross-Functional Team, or Project Maven, which the U.S. Department of Defense announced in 2017 as an effort to automate the exploitation of full-motion video collected in conflict zones, using sophisticated object detection technology to identify threats and potential targets.[50] The initiative developed algorithms used just months after its launch to process drone footage in support of actual counter-ISIL missions.[51] It has since been expanded to embrace analysis of data from additional sources and operationalized in multiple theaters.[52]

Ukraine has striven to emulate this model in its conflict with Russia. Much of the data that Ukrainian personnel collect or derive from exploitation is preserved in DELTA, a digital battlespace management system that Kyiv has developed and refined, in coordination with NATO, since 2014. DELTA fuses and analyzes data from satellites, ground-based sensors, UAS, and social media feeds, among other sources, to support various military purposes.[53]

Israel has harnessed similar technologies for data fusion and analysis in its wars against Hamas in 2021—Operation Guardian of the Walls—and in 2023–2025—Operation Iron Swords.[54] While most legal commentary on the

---

49 *See* Robin Geiß & Henning Lahmann, *The Use of AI in Military Contexts: Opportunities and Regulatory Challenges*, 59 MIL. L. & L. WAR REV. 165, 172–75 (2021).

50 Kelley M. Sayler, *Artificial Intelligence and National Security*, CONGRESSIONAL RESEARCH SERVICE 10, 18 (Nov. 10, 2020).

51 Marcus Weisgerber, *The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS*, DEFENSE ONE (May 14, 2017), https://perma.cc/NG85-DZBR; Gregory Allen, *Project Maven Brings AI to the Fight Against ISIS*, BULL. ATOMIC SCIENTISTS (Dec. 21, 2017), https://perma.cc/8JE5-A88C.

52 Brenda Marie Rivers, *Air Force to Integrate 'Project Maven' AI Scope Into ABMS; Will Roper Quoted*, EXEC. GOV. (Aug. 11, 2020), https://perma.cc/CFU2-Y9PQ; Richard Shultz & Richard Clarke, *Big Data at War: Special Operations Forces, Project Maven, and Twenty-First Century Warfare*, MOD. WAR INST. (Aug. 25, 2020), https://perma.cc/JZW6-9D3P.

53 *See*, *inter alia*, *Ukraine Unveiled Its Own Delta Situational Awareness System*, MILITARNYI (Oct. 27, 2022), https://perma.cc/9RRK-5VKF; Lara Jakes, *For Western Weapons, the Ukraine War Is a Beta Test*, N.Y. TIMES (Nov. 15, 2022); NATO Allied Command Transformation, *Battlefield Innovation: Ukraine's DELTA System Paves the Way for Allied Interoperability at CWIX24* (July 12, 2024), https://perma.cc/FT2W-SY74.

54 *See* Anna Ahronheim, *Israel's Operation Against Hamas Was the World's First AI War*, THE JERUSALEM POST (May 27, 2021), https://perma.cc/DM74-PGXE; Avi Kahlo, *AI-*

Israel Defense Forces' (IDF) wartime use of artificial intelligence has focused on issues of compliance with LOAC arising from AI–enabled targeting, one of AI's most important functions in Operation Iron Swords has been to assist in developing intelligence on the locations of individuals taken hostage in the attacks of October 7, 2023. To that end, Israel reportedly employs cutting-edge algorithmic tools to uncover patterns in enormous aggregations of data from sources including recovered documents, digital material from seized devices, human intelligence from captured Hamas fighters, and Israeli sensors, as well as U.S. Reaper drones flown over Gaza.[55] This multi-source big data analysis has yielded intelligence leading in several instances to IDF raids that freed hostages.[56]

B. Implications for Battlefield Evidence

The foregoing developments give rise to various opportunities and challenges for military collection and analysis of potential evidence and for that information's sharing and eventual law enforcement use. This paper will highlight a few particularly significant implications, without purporting to be exhaustive.

1. Military data collection and exploitation

On the one hand, the advantages for collection and exploitation already touched on can hardly be overstated. Drone footage alone is a highly promising evidentiary source. Unmanned systems have a unique vantage point on battlegrounds not only before and after combat but while it is ongoing; in many situations they are themselves involved in the conduct of hostilities. The information they gather that may document crimes committed there often has no practical substitute.

More broadly, AI-enabled systems' ability to preserve huge troves of data from various military sources to which civilian investigators lack access, integrate data from non-military sources, and swiftly conduct complex technical exploitation could have clear subsidiary benefits for law enforcement. Machine learning algorithms can execute mundane tasks like translating text or spoken words with rapidity that far outstrips what is humanly possible. To put this in perspective, it should be recalled that much of the information collected by the U.S. military in Afghanistan since 2001 has

---

Enhanced Military Intelligence Warfare Precedent: Lessons from IDF's Operation "Guardian of the Walls", FROST & SULLIVAN (June 9, 2021), https://perma.cc/HD7R-D6JH; Omar Yousef Shehabi & Asaf Lubin, *Israel–Hamas 2024 Symposium – Algorithms of War: Military AI and the War in Gaza*, ARTICLES OF WAR (Jan. 24, 2024), https://perma.cc/K8LN-HAD2; Tal Mimran et al., *Israel–Hamas 2024 Symposium – Beyond the Headlines: Combat Deployment of Military AI-Based Systems by the IDF*, ARTICLES OF WAR (Feb. 13, 2024), https://perma.cc/V6CD-PLMH.

55 *See* Riley Mellen & Eric Schmitt, *U.S. Drones Are Flying Over Gaza to Aid in Hostage Recovery, Officials Say*, N.Y. TIMES (Nov. 2, 2023); Mark Mazzetti et al., *Israel's Hunt for the Elusive Leader of Hamas*, N.Y. TIMES (Oct. 18, 2024).

56 *See* Julian Barnes et al., *U.S. Intelligence Helped Israel Rescue Four Hostages in Gaza*, N.Y. TIMES (June 8, 2024).

yet to be translated, let alone analyzed. AI can also perform functions that humans cannot, like precise recognition of momentarily-apparent symbols (like flags and military insignia) and objects (like weapons) in fast-moving video sequences.

Not only could analyses for military purposes have the side effect of revealing material with investigative or evidentiary value, but battlefield information systems' processes could be adapted to incorporate analyses that actively seek to identify such material. Consider how well-suited an AI–powered system might be to comb through multi-source datasets recording attacks on civilian infrastructure, movements of troops, and orders traveling up and down chains of command and to pinpoint patterns and correlations that would evade human scrutiny. By way of example, Ukraine has already created a data layer within the DELTA system that catalogues destroyed or damaged cultural heritage sites and cultural property.[57]

Relying on AI and ML to process data also entails considerable risks, however.[58] As should be apparent, algorithms programmed on the basis of incorrect assumptions or misguided analytical approaches or deployed in environments for which they are not adequately prepared will often deliver erroneous outputs.[59] More perniciously, the complexity of the most sophisticated deep ML-based systems may render their decision-making "inherently unpredictable" to a certain extent.[60] Those systems' related lack of explainability—their "black box" character—makes it difficult to detect subtle, yet still consequential, errors, to say nothing of diagnosing their cause.[61] And even algorithms functioning "properly" and predictably on their own terms will reproduce the biases of discriminatory or otherwise faulty training data.[62]

Several of these risks may be more likely to eventuate in armed conflict environments. Large, high-quality training datasets "representative of the intended context of use (if there even is a stable 'context' in an adversarial environment such as the battlefield)" are more demanding to compile.[63] Opportunities to validate models' predictability and hone their accuracy in

---

57 Gyunduz Mamedov & Vitaliy Tytych, *Як зменшити наслідки війни для культурної спадщини: можуть допомогти ЗСУ* [*How to Reduce the Effects of War on Cultural Heritage: How the Ukrainian Armed Forces Can Help*], ДЗЕРКАЛО ТИЖНЯ [MIRROR OF THE WEEK] (Jan. 8, 2024) (Ukr.), https://perma.cc/566S-YZ29.

58 *See* Nema Milaninia, *Biases in Machine Learning Models and Big Data Analytics: The International Criminal and Humanitarian Law Implications*, 102 INT'L REV. RED CROSS 199, 203–16 (2020).

59 *See* Arthur Holland Michel, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision-Making*, INTERNATIONAL COMMITTEE OF THE RED CROSS 31–44 (Apr. 2024).

60 *See* Geiß & Lahmann, *supra* note 50, at 181–83.

61 *See* Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, HARV. J. L. & TECH. 889 (2018).

62 *See* ICRC, *Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control* (2019), https://perma.cc/HFG5-CDQ8.

63 United Nations Institute for Disarmament Research (UNIDIR) Security and Technology Programme, *Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies: A Primer*, 9 UNIDIR RESOURCES 3 (2018).

actual conflict settings are relatively scarce. Wartime pressure to utilize every tool available may lead to algorithms' premature deployment, further exacerbating the likelihood of mistakes.

Military opponents' employment of countermeasures can also blinker or blind ISR assets. Electronic warfare systems can flood the electromagnetic frequencies used by a UAS, jam GPS signals, and disrupt or disable sensors.[64] AI–specific countermeasures could have even more deleterious effects. Whether by "poisoning" datasets used to train algorithms with manufactured or corrupted information, "spoofing" AI systems with fake information after deployment, or feeding them with operational inputs tailored to exploit identified weaknesses, adversaries could elicit outputs that are not just incorrect but self-defeating, and without necessarily alerting the AI system's operators.[65]

Confounding all these difficulties is the fog of mis- and disinformation which envelops contemporary conflicts. Advances in deepfake video and spoof audio, automated bots, and tech-enabled micro-targeting have supercharged both state and non-state information operations even in peacetime.[66] During armed conflict, inaccurate information about battlefield developments—conveyed through synthetic media, auto-generated text, doctored data, and traditional propaganda—proliferates with rapid and far-reaching effects.[67] As observed, ISR systems combine military data with large volumes of publicly available information such as social media posts in order to produce more valuable analytical outputs.[68] Faked or manipulated open-source data, if integrated into AI-enabled analyses, could thus lead to faulty outputs.

Parties may engage in such information warfare tactics for direct military gains or to shape the information space surrounding the conflict for strategic advantage.[69] They may even do so with the deliberate intention of obstructing or diverting justice processes themselves. Recently, following France's 2022 military withdrawal from Mali, Wagner Group fighters sought to frame the

---

64 *See*, *e.g.*, Thomas Gibbons-Neff & Yurii Shyvala, *"Jamming": How Electronic Warfare Is Reshaping Ukraine's Battlefields*, N.Y. TIMES (Mar. 12, 2024).

65 *See* Jonathan Kwik, *Is Wearing These Sunglasses An Attack? Obligations Under IHL Related to Anti-AI Countermeasures*, 106 INT'L REV. RED CROSS 732 (2024).

66 S*ee* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019).

67 *See* Eian Katz, *Liar's War: Protecting Civilians from Disinformation During Armed Conflict*, 102 INT'L REV. RED CROSS 659 (2020); Tilman Rodenhäuser, *The Legal Boundaries of (Digital) Information or Psychological Operations Under International Humanitarian Law*, 100 INT'L L. STUD. 541 (2023).

68 *See* Hannah van Beek & Sebastiaan Rietjens, *Open-Source Intelligence in the Russia-Ukraine War, in* REFLECTIONS ON THE RUSSIA-UKRAINE WAR 62–63 (Maarten Rothman et al. eds., 2024).

69 Terrorist groups may also use such information tactics outside zones of active hostilities. Within days of the March 2024 ISIL-Khorasan attack at the Crocus City Hall concert venue in Moscow, Islamic State supporters spread AI-generated propaganda videos to amplify and justify the attacks, and to draw attention to ISIL affiliates' activities in theaters ranging from Iraq to West Africa. Pranshu Verma, *These ISIS News Anchors are AI Fakes. Their Propaganda is Real*, WASH. POST (May 17, 2024).

departed forces for a "massacre of civilians" by re-burying a dozen Malian dead in a shallow mass grave outside a recently abandoned French base, while in coordination fake or sympathetic social media accounts decried the "French" crime.[70]

In the latter example, notably, it was in fact a French military drone that captured the surreptitious re-burial on overhead video, which when subsequently released to the public gave the lie to Wagner's attempted deception.[71] The footage moreover arguably constitutes potential evidence of the Wagner fighters' own commission of the war crime of outrages upon personal dignity.[72] This attempt to "plant" fake evidence and to amplify the staged atrocity online thus underlines not only the challenges associated with collection on the battlefield, but also the opportunities for law enforcement attendant on technology's introduction into warfare. Whether the benefits outweigh the risks, only time will tell.

2. Sharing for law enforcement purposes

If emerging technologies are having equivocal effects on military data collection and analysis, on the whole they appear likely to inhibit its sharing for law enforcement purposes.

In quite a few contexts, criminal justice actors' efforts to obtain information derived from new military technologies will immediately encounter legal and procedural roadblocks. Many existing authorities and processes are only geared toward the transmission of certain types of information, and will require adaptation. NATO's intelligence sharing practices are a case in point. Allies have adopted several NATO-wide policies to regulate sharing of biometric data, including for law enforcement use, and have established corresponding information systems and coordination mechanisms.[73] There are as yet no equivalent policies or structures to facilitate sharing of UAS footage for law enforcement ends.

Such issues are resolvable. As described, however, history indicates that states will only make use of available information-sharing mechanisms, much

---

70 *See* Wassim Nasr, *Mali: L'Armée Française Affirme Avoir Filmé des Mercenaires Russes En Train D'Enterrer des Corps* [*Mali: French Army Claims to Have Filmed Russian Mercenaries Burying Bodies*], FRANCE 24 (Apr. 22, 2022) (Fr.), https://perma.cc/A5QJ-FNLF; Amy Mackinnon & Robbie Gramer, *Russian Mercenaries Staged Atrocities in Mali, France Says*, FOR. POL'Y (Apr. 26, 2022), https://perma.cc/M28Q-2SQ5.

71 *See* Mackinnon & Gramer, *supra* note 72.

72 *See* Rome Statute of the International Criminal Court, adopted July 17, 1998, entered into force July 1, 2002, U.N. Doc. A/CONF.183/9 [hereinafter Rome Statute] arts. 8(2)(b)(xxi), 8(2)(c)(ii). The exhumation for disinformation purposes also manifestly violated the obligation under customary LOAC to afford the dead a dignified burial. *See* ICRC, CUSTOMARY INT'L HUMANITARIAN LAW, VOL. I: RULES 414 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

73 *See* Chris Burt, *NATO Announces In-house Biometrics System for Secure Data-Sharing*, BIOMETRIC UPDATE (Nov. 18, 2020), https://perma.cc/Q7A4-FJDF; *NATO Allies Agree Policy on Battlefield Evidence from Operational Theatres to Boost Efforts Against Terrorism*, NATO (Oct. 23, 2020), https://perma.cc/V2G3-85N6.

less fashion new ones, if doing so furthers their policy goals. Here lies the problem: changes in the current strategic context, to no small degree attributable to emerging technologies themselves, may significantly weaken their incentives to share military data for law enforcement use.

In the first place, officials may consider that information, long critically important in armed conflict, is becoming *even more* important given the nature of contemporary and future warfare. Such a position need not rest on the still-controversial claim that achieving cognitive superiority will soon be the chief determinant of overall strategic success in warfare. It is enough to recognize how big data enables the range of tactical and operational applications in armed conflict mentioned above—most of which depend for their effectiveness, at least to a certain degree, on the information's secrecy. If an adversary is aware of what specific information the military possesses, it may respond either with defensive actions, like redeploying its forces or changing its tactics, or offensive actions, like expediting attack plans. The adversary may also identify the source of the information more precisely and seek to neutralize it, and thus to prevent future ISR activities, more effectively than it could otherwise.

Additionally, decision-makers may espouse the view that the way in which AI functions increases not just the importance of information generally but the potential importance of each discrete piece of information. That is to say that the more complex and the less explainable the processes by which AI-enabled military systems reach their conclusions, the less confidently one can dismiss the potential value of any individual piece of information to those processes. On this logic, it will become increasingly difficult to gauge the impact a particular datum may have on the calculations of one's own AI system not only in advance but even after the fact—let alone that datum's value for an enemy's AI system. Such an argument militates in favor of safeguarding battlefield information's secrecy to the greatest extent possible, to avoid either shedding light on one's own calculations or unwittingly supplying an adversary with a key input for their own.

These inclinations are only likely to be encouraged by shifts in the international security landscape. Great power competition has intensified with the Ukraine and Gaza conflicts, in which major and middle powers have diplomatically aligned with, and provided security assistance to, opposing parties. Military planners must give more credence than before to the prospect of a major-power war, in which achieving an information edge could be essential.[74] Today, in contrast to 2017 (the year of Resolution 2396's passage),

---

[74] Merel Ekelhof, in discussing NATO's joint targeting process, has argued that current limitations on human targeteers' capacity to conduct the extensive target system analyses required in asymmetric conflicts "would be even more problematic in a scenario in which NATO was at war against a near-peer opponent," making AI (and ML) support all the more vital. *See* Merel A.C. Ekelhof, *Lifting the Fog of Targeting: "Autonomous Weapons" and Human Control through the Lens of Military Targeting*, 71 NAVAL WAR COLL. REV. 61, 79 (2018) (citing an e-mail from Lieutenant General John N.T. Shanahan, previously Director of Project Maven and then

the U.N. Security Council is deadlocked, and international cooperation has fallen victim to stark polarization.[75] With the overall security stakes elevated, and geostrategic adversaries boasting far more significant intelligence and counterintelligence capabilities than did ISIL, even states that have already shared battlefield evidence of crimes in Syria and Iraq with foreign judicial authorities may be less willing to run any risk of exposing sources and methods, minimal as it may be, by sharing similarly sensitive information going forward. More fundamentally still, states may consider criminal prosecution a less impactful tool for meeting this security environment's chief threats, compared to periods when terrorism was a preeminent concern. Simply put, the potential upsides of information sharing may appear less meaningful and the potential downsides more damaging.

Experts have also warned that relying on algorithmic data processing to make determinations about who may be detained under LOAC or domestic administrative legal regimes could lead to more liberal security detention policies.[76] If that in fact transpires, it could also reduce one form of pressure to provide sensitive data to law enforcement authorities, including in terrorism cases, since states could incapacitate more individuals they see as potentially dangerous without resorting to criminal prosecution.

Finally, it bears mention that providing material to criminal justice authorities merely for "lead" purposes (i.e. to launch or advance an investigation), and not for introduction as evidence per se, often obviates the requirement that it be shared with the defense. But states contemplating this option may be given pause by another factor: the profusion and democratization of AI-enabled and other advanced cyber-hacking capabilities. Both governments and non-state actors possess increasingly sophisticated technical means of compromising information systems, and deploy them with increasing frequency. The potential perils were vividly illustrated when in September 2023 the ICC suffered what it called a "targeted and sophisticated [cyber] attack with the objective of espionage."[77] Such cyber threats will certainly enter decision-makers' calculus, and many will reasonably hesitate to

---

Director for Defense Intelligence (Warfighter Support) at the Office of the Under Secretary of Defense for Intelligence in the U.S. Department of Defense).

75 *See, e.g.*, Richard Gowan, *The UN is Another Casualty of Russia's War: Why the Organization Might Never Bounce Back*, FOR. AFF'S. (Mar. 10, 2012), https://perma.cc/L8ML-WDDS. Global polarization does not take a straightforward bilateral shape. Significant rifts plague major alliances and partnerships: consider China's reported disquiet at North Korea's provision of troops to fight with Russia in Ukraine, the at-times intense disagreements between NATO members over security assistance to Kyiv, or the hedging behavior of India, Türkiye, Saudi Arabia, and the United Arab Emirates.

76 *See, e.g.*, Ashley Deeks, *Predicting Enemies*, 104 VA. L. REV. 1529 (2018); Tess Bridgeman, *The Viability of Data-Reliant Predictive Systems in Armed Conflict Detention*, ICRC HUMANITARIAN LAW & POL'Y BLOG (Apr. 8, 2019), https://perma.cc/D7X4-PNGX; Dustin A. Lewis, *AI and Machine Learning Symposium: Why Detention, Humanitarian Services, Maritime Systems, and Legal Advice Merit Greater Attention*, OPINIO JURIS (Apr. 28, 2020), https://perma.cc/LU6R-LW67.

77 *Measures Taken Following the Unprecedented Cyber-Attack on the ICC*, INT'L CRIM. COURT (Oct. 20, 2023), https://perma.cc/YX2V-NA72.

share information that is not publicly disclosable if they lack confidence in the recipients' information security practices.

To be sure, there are counter-incentives that should not be minimized. Fierce contestation over the broader information space surrounding armed conflicts may increasingly impel states to declassify and publish sensitive material, both to proactively shape that environment and to counter adversaries' information warfare. The extraordinary steps by the U.S., U.K., and others to "pre-bunk" Russia's attempt to contrive a *casus belli* for the 2022 full-scale invasion of Ukraine by releasing declassified intelligence of Russian military preparations—and those steps' perceived success in helping forge a stronger coalition in support of Ukraine—serve as an object lesson here. But an increased appetite for strategic disclosures directly to the public will not necessarily translate to a readiness to provide *even that same information* to law enforcement actors (as the ICTY discovered).[78] Policymakers will more likely remain reluctant to do so if they do not see criminal processes as instrumentally valuable—particularly if wary of courtroom complications, to which the analysis now turns.

3. Use as evidence

Information and material derived from emerging military technologies can strengthen serious crimes cases in a range of ways.

To begin with, it can prove the *actus reus*, or material element, of a crime. Object detection tools can record uses of prohibited weapons, for example, or intentional attacks on civilian targets. Battlefield sensors can track the flight paths of individual projectiles or geolocate large-scale movements of troops or of forcibly displaced civilians.

Indeed, such data may in some instances be the *only* crime base evidence available. As noted, unmanned systems' maneuverability and sensing capabilities can give them an unrivalled ability to operate in especially hard-to-access conflict-impacted areas. Likewise, investigation of cyberattacks against civilian infrastructure constituting war crimes necessarily depends heavily on sophisticated digital forensics.[79]

Technology-derived military data can also establish individual perpetrators' liability for the criminal conduct, and prove the *mens rea*, or mental element, of the crime. Facial and voice recognition software can help identify individual suspects in military video and audio footage (or in open-source material checked against massive military databases) and confirm their precise physical location at a given moment. Automated translation of intercepted communications can reveal suspects discussing plans to commit crimes beforehand or describing their commission after the fact. ML

---

78 *See* Goldstone, *supra* note 16, at 149.

79 *Cf.* Katrin Nyman Metcalf, *Katrin Nyman Metcalf on: Can Cybercrimes Be War Crimes?*, RAOUL WALLENBERG INSTITUTE (Feb. 27, 2023), https://perma.cc/EGT9-ASXG ("For attacks in cyberspace, evidence will also be at least partially in cyberspace.").

algorithms can unearth nuggets of inculpatory information in mountains of data extracted from seized devices.

Finally, such battlefield evidence can bring arguably its greatest added value by connecting physical perpetrators to senior military commanders or political leaders who ordered the crimes but may have never themselves set foot on the crime scenes. Proving this linkage, commonly cited as the most difficult aspect of international crimes prosecutions, will often "rest heavily upon documentation generated by the perpetrating institutions,"[80] which is less likely than crime base evidence to be available from open sources. Documentary and digital material gathered by military personnel, in addition to data obtained by military intelligence capabilities, may be indispensable. Building a picture of chains of command or informal hierarchies so as to demonstrate higher-ups' authority and control over crimes' direct authors requires the painstaking assembly of discrete items of evidence, none of which in isolation is dispositive. Military data that AI systems have collected and/or analyzed at faster-than-human speed could supply the final piece of many such puzzles.

It bears emphasizing that evidence is subject to different legal standards and rules in different jurisdictions, and determinations of admissibility and probative value are highly context-specific. And as explained above, national and international criminal justice practitioners have found procedural ways to successfully introduce battlefield evidence in many previous cases. Information and material in military holdings that was originally obtained through more traditional methods, albeit later identified as potentially valuable for law enforcement by AI analysis, is likely amenable to introduction through similar techniques. But data collected by UAS and autonomous sensors or generated by military AI-driven analysis poses several novel issues.

Some issues are endemic to all evidence derived from emerging technologies. For one thing, courts might underweight or even outright reject material of such provenance due to its sheer unfamiliarity. Indeed, the recency of their widespread use means there is little record of drone footage or AI-derived data in core international crimes cases.

In many respects, though, UAS' role as a source of evidence mirrors that played by satellites, which have yielded information admitted and relied on by a number of international criminal courts; in technical terms, UAS may gather information that is actually more verifiable.[81] As early as 1999, Louise Arbour, then Chief Prosecutor of the ICTY, asked some members of the NATO

---

80 William H. Wiley, *Effective Leadership, Management and Integrity in International Criminal Investigations, in* INTEGRITY IN INTERNATIONAL JUSTICE 423 (Morten Bergsmo & Viviane E. Dittrich eds., 2020).

81 *Cf.* Cono Giardullo, *Surveillance Drones as Tools to Enhance Accountability for Human Rights and Humanitarian Law Violations*, 166 RUSI J. 20, 21 n.10 (2021) ("Drones can often capture more detail than satellites, as UAV imagery is essentially a hybrid of standard on-the-ground photography and satellite imagery.").

Implementation Force deployed in Bosnia "to fly special missions with . . . drones in order to collect information of value for the tribunal."[82]

Moreover, civilian criminal justice practitioners have themselves begun to utilize both UAS and AI/ML tools. The United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/Islamic State in Iraq and the Levant (UNITAD) used drones to survey mass grave sites and other potential crime scenes, then integrated the resulting footage with terrestrial laser scans and satellite imagery for presentation in interactive virtual formats.[83] UNITAD also developed a custom "Zeteo" platform that performed AI and ML-based enrichments to facilitate investigators' search and analysis of huge datasets.[84] The Office of the Prosecutor (OTP) of the ICC has followed suit, incorporating AI and ML capabilities into its Project Harmony evidence management platform (launched in 2022) and OTPLink evidence submission portal (in 2023). The OTP's most recent strategic plan, in setting the ambition "to become a global technology leader" as one of its highest-priority goals, resolved to "apply AI and ML across all situations" for accelerated and improved evidence collection and analysis—indicating that it clearly expected ICC chambers will be receptive to AI-generated or -analyzed material.[85] In a number of atrocity crimes cases, in fact, not only the ICC but other international and domestic courts have already admitted such material, even when provided by third parties.

Such developments point up the alternative possibility that, rather than taking overly skeptical views, courts might fall prey to so-called automation bias when faced with evidence collected or generated by AI systems. This vulnerability can lead decision-makers to over-trust the products of algorithmic processes that they do not fully understand, without having examined them as carefully as they do other data.[86] Yet the risk of automation bias can be mitigated, at least somewhat, by training judges to remain alive to it and to deliberately subject technology-derived evidence to the searching scrutiny that is warranted.[87]

When obtained from *military* sources, however, this type of information presents distinct concerns. The first has to do with corroborating its

---

82 Marlise Simons, *Crisis in the Balkans: War Crimes Investigators Prepare for Kosovo*, N.Y. TIMES (June 7, 1999).

83 *Harnessing Advanced Technology in International Criminal Investigations: Innovative Approaches in Pursuit of Accountability for ISIL Crimes*, UNITAD (2021), https://perma.cc/3YP3-3HY8.

84 *Id.*

85 INTERNATIONAL CRIMINAL COURT, STRATEGIC PLAN 2023-2025 (2023), https://perma.cc/7KEE-ENGT.

86 *See* Linda J. Skitka et al., *Does Automation Bias Decision-Making?*, 51 INT'L J. HUM.-COMPUT. STUD. 991 (1999); Danielle Keats Citron, *Technological Due Process*, 85 WASH U. L. REV. 1249 (2010); Raja Parasuraman & Dietrich H. Manzey, *Complacency and Bias in Human Use of Automation: An Attentional Integration*, 52 HUM. FACTORS 381 (2010).

87 *See* Parasuraman & Manzey, *supra* note 86, at 387; Milaninia, *supra* note 58, at 215–16, 233; Ashley Deeks, *The Judicial Demand for Explainable Artificial Intelligence*, 119 COLUM. L. REV. 1829, 1846–47 (2019).

authenticity and reliability. Even when not strictly required for admissibility, testimony from the party that collected digital evidence is often crucial to authenticating it and demonstrating its reliability—and this may be all the more true for AI-sourced evidence, which is still unfamiliar to non-specialists.[88] As with other evidence from technical sources, specialized experts could explain the information's significance, describe the AI and ML collection and analysis processes that produced it, attest to its integrity and chain of custody, and otherwise corroborate its authenticity and support its probative value.[89]

Prosecutors seeking to introduce data produced by the battlefield layering of multiple AI and ML systems bear an even heavier burden. They must explain the operation and interaction of varied algorithmic systems of great complexity and confidentiality, with "humans who can provide direct testimony more and more distant from the evidence sought to be used."[90] Chris Jenks and Eric Talbot Jensen have posited a scenario in which a war crimes prosecutor might seek to use as evidence:

---

88 *See* Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 FORDHAM INT'L L.J. 283 (2018); Matthew Gillett & Wallace Fan, *Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom*, 21 J. INT'L CRIM. JUSTICE 661 (2023).

89 Former U.S. District Court Judge Paul W. Grimm has suggested that "the proponent of AI evidence [can] show that it was the product of a system or process that produces accurate results . . . [in other words,] that the AI technology has sufficient validity and reliability when used for the task to which it was applied, taking into consideration the danger of unfair prejudice to the party against which the evidence was admitted, [by] borrow[ing] the methodology for assessing the admissibility of scientific and technical evidence set out in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*" Paul W. Grimm, *Practical Considerations for the Admissibility of Artificial Intelligence Evidence*, 2 MD. BAR J. 39, 41 (2021) (citing Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)). Sabine Gless, Frederic Lederer, and Thomas Weigend similarly recommend (at least for the moment, in lieu of technological solutions to assess and certify the authenticity of AI evidence) "the appointment of experts by the court and . . . a procedure whereby the judge calls and neutrally examines the court-appointed expert when there are questions about the validity of scientific or technological evidence." Sabine Gless et al., *AI-Based Evidence in Criminal Trials?*, 59 TULSA L.J. 1, 35 (2024). Grimm, Maura Grossman, and Gordon Cormack have also argued that "a judge cannot make the determinations [that an AI system's outputs are valid and reliable] unless the party offering the AI evidence is prepared to disclose underlying information concerning, for example, the training data and the development and operation of the AI system sufficient to allow the opposing party (and the judge) to evaluate it." Paul W. Grimm et al., *Artificial Intelligence as Evidence*, 19 NW. J. TECH. & INTELL. PROP. 9, 89 (2021). However, Grimm and Maura Grossman have elsewhere argued persuasively that "[a] judge need not see or even understand every nuance of how the AI system operates, so long as the proponent can explain the process by and circumstances under which it has been developed, trained, and—most importantly—tested . . . AI that has been properly designed, developed, and deployed can be relied on for many legal purposes if exacting and independent auditing and validation of the system have occurred. Thus, the notion of 'explainability' may more usefully be thought of as the ability to demonstrate that the AI system unequivocally meets the requirements of validity, reliability, and equity, lack of bias, and/or fairness, rather than as a description of its technical inner workings." Paul W. Grimm et al., *AI in the Courts: How Worried Should We Be?*, 107 JUDICATURE 71 (2024).

90 Makayla Beitler & Eric Talbot Jensen, *Battlefield Artificial Intelligence and War Crimes Prosecutions*, 56 TEX. TECH L. REV. 689, 704 (2024).

> visual data . . . captured by an unmanned and unmonitored AI sensor such as a drone. That drone is directed by another AI 'control' system that, based on other AI sensors on the battlefield, determines the drone's flight path and when it captures visual data. The 'control' AI system then analyzes the visual data, applying pre-determined enhancements that increase its intelligence value[, which] might include visual resolution clarity, use of facial recognition technology, and the application of biometric data (perhaps collected by other non-human sensors in the area).[91]

Makayla Beitler and Jensen have suggested persuasively that recourse to multiple expert witnesses, each qualified to speak to one aspect of this "interweaving" of disparate systems, could suffice to establish the authenticity and reliability of such evidence[92]—but this solution remains to be tested in practice.

Relatedly, in some instances military personnel or security officials may be best positioned to offer corroborative testimony regarding UAS footage or AI-based analytical products, but only willing to do so given appropriate safeguards. In such cases, courts must ensure that the witnesses' own safety and security are protected and that questioning avoids national security matters that cannot be discussed in open court, while still respecting the rights of the defense. This complication has arisen in previous cases involving battlefield evidence, however, and several procedural techniques have proven effective in addressing it. When necessary, both domestic and international courts have used procedural devices including physical screening and voice scrambling, anonymity, and/or out-of-court hearings to protect sensitive witnesses while permitting the defendant to challenge their testimony.

Such issues are not simply hypothetical. An extraordinary war crimes case recently brought in Ukrainian court is instructive.[93] In June 2022, a quadcopter that the Ukrainian military had raised for reconnaissance purposes captured on video a Russian artillery attack on a civilian Ukrainian couple's car near Izium, and the aftermath in which several Russian infantrymen emerged from a concealed firing position and picked up the injured husband's prone form only to unceremoniously throw him into a roadside ditch. The Ukrainian military provided the UAS footage to the Kharkhiv National Police, which launched an investigation after Izium's recapture in Ukraine's September 2022

---

91 Chris Jenks & Eric Talbot Jensen, *Year Ahead: Emerging Technologies and the Collection of Battlefield Evidence*, ARTICLES OF WAR (Jan. 13, 2023), https://perma.cc/6L9D-UXLS.

92 Beitler & Jensen, *supra* note 90, at 705.

93 This account of the Kerzhaev case is based on Lyubomyr Levytsky, *SHOCKING DOCUMENTARY FILM "FOLLOW ME" On the military rescue operation in Ukraine 2023*, YOUTUBE (Jan. 18, 2023), https://perma.cc/ZQE6-LBJ9; Rebecca Wright et al., *'I Killed A Man Today': Russian Soldier Accused of War Crimes In Absentia After Audio Files Intercepted*, CNN (Mar. 21, 2023), https://perma.cc/DSA3-DJAL; Christine Chraibi, U*krainian Military Drone Leads Woman to Safety Amidst Enemy Fire*, EUROMAIDAN PRESS (Apr. 7, 2023), https://perma.cc/KR3D-FMDT; Iryna Domashchenko, *Ukraine: Saved by a Drone*, INST. FOR WAR & PEACE REPORTING (Aug. 22, 2023), https://perma.cc/ZS53-LDFS; Vladyslava Kobko, *The Ukrainian Drone that Said "Follow Me"*, JUSTICE INFO (Feb. 26, 2024), https://perma.cc/38RL-2GCJ.

counteroffensive. Investigators interviewed the victims and witnesses, conducted a forensic examination of the site and collected shell casings from large-caliber weapons, and searched through intercepted communications—which turned up phone calls from the week in question in which a Russian soldier admitted to his wife and to a friend, "I fucking killed a man today," and described the same set of circumstances as the drone footage depicted. Further investigation, including information from a Russian prisoner of war, identified the speaker as Klim Kerzhaev, commander of a motorized rifle company stationed in the exact area of the shooting on the relevant date. Taken together, this evidence—along with testimony at trial from a member of the Ukrainian mechanized brigade involved in the incident—led the Krasnograd District Court of Kharkiv to convict Kerzhaev *in absentia* for the war crimes of attempted murder and the cruel treatment of civilians and sentence him to fifteen years imprisonment.

A thornier question than corroboration may be the impact of technology-derived battlefield evidence on the prosecution's disclosure requirements. International law generally recognizes that, as part of the right to a fair hearing, criminal defendants must be afforded "access to documents and other evidence, [including] all materials that the prosecution plans to offer in court against the accused or that are exculpatory."[94] As a rule, such obligations are limited to material in the prosecution's possession. In civil law jurisdictions, however, the prosecutor (or investigative judge, as the case may be) typically has a duty to investigate exonerating as well as incriminating circumstances[95]—which arguably requires them to request exculpatory material from government agencies cooperating with an investigation, perhaps even from non-cooperating agencies reasonably likely to possess such material. Even in a common law system like the U.S., with adversarial safeguards in place, prosecutors have obligations not just to provide the defense with evidence favorable to the accused but to make efforts to search for such material in the first place, in some cases by requesting it from certain other government agencies, if not necessarily from foreign partners.

Holders of military data may react to such requests with consternation, and not just because they lack motivation to assist defendants accused of atrocities. As already noted, one of the principal reasons for their hesitance to share information in the first place is the need to maintain the secrecy of sources and methods of collection and of other contextual or related material, not the sensitivity of the relevant information as such.[96] In addition, even if

---

94 U.N. Human Rights Committee, General Comment No. 32, Article 14: Right to Equality Before Courts and Tribunals and to Fair Trial, U.N. Doc. CCPR/C/GC/32, ¶ 33 (Aug. 23, 2007).

95 *See* International Association of Prosecutors, Standards of Professional Responsibility and Statement of the Essential Duties and Rights of Prosecutors (Apr. 23, 1999) art. 3(5), https://perma.cc/2YGN-KKBH (Prosecutors shall "seek to ensure that all necessary and reasonable enquiries are made and the result disclosed, whether that points towards the guilt or the innocence of the suspect."). *See also* Rome Statute, *supra* note 73, art. 54(1)(a).

96 *See* Goldstone, *supra* note 16, at 148.

they did accede to some defense requests, AI systems' nature would make it trickier technically speaking to modify their analytical processes to conduct searches for exculpatory information.[97]

Many of the abovementioned factors likely to decrease decision-makers' practical willingness to share military data with criminal justice actors also reinforce their *legal* justification for withholding that data. In most national jurisdictions, a public interest or state secrets privilege protects information if its disclosure might harm national security. A similar principle operates at the international level, as an ICTY Appeals Chamber recognized in *Prosecutor v. Blaškić*.[98] Many courts will likely accept that the growing importance of information in warfare and the nature of AI analysis bolster the validity of such privilege claims.[99]

At the same time, technological developments could have the opposite effect on courts' interpretation of another "fundamental aspect of the right to a fair trial"[100]: equality of arms. This principle requires that each party "be afforded a reasonable opportunity to present [their] case in conditions that do not place [them] at a disadvantage vis-à-vis [their] opponent."[101] Most courts construe the principle as applying to criminal proceedings holistically, taking developments at the pre-trial and investigation stages into account in their assessments, although they rarely find violations absent a violation of another discrete fair trial right, such as the right to disclosure.[102]

Quite conceivably, future defendants will argue that military authorities' unilateral cooperation with the prosecution widens the gap in investigative

---

97 *See* Bart Custers & Lonneke Stevens, *Data as Evidence in Criminal Courts: Comparing Legal Frameworks and Actual Practices*, *in* HUMAN-ROBOT INTERACTION IN LAW AND ITS NARRATIVES 242–43 (Sabine Gless & Helena Whalen-Bridge eds., 2024).

98 Prosecutor v. Tihomir Blaškić, Case No. IT-95-14-AR108, Judgment on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997 (Oct. 29, 1997).

99 The logic is similar to that underpinning the longer-standing "mosaic theory," to which U.S, federal courts have been traditionally deferential, that the "bearing of [an individual piece of] information is not susceptible of intelligent estimate until it is placed in its setting, a tile in the mosaic." Christina Koningisor, *Secrecy Creep*, 16 U. PA. L. REV. 1751, 1785–87 (2021) (citing In re Edge Ho Holding Corp., 176 N.E. 537, 539 (N.Y. 1931)). The mosaic theory, which may also be defined as "the idea that individual pieces of data assembled together may reveal more than the sum of their parts," in fact "originated . . . as a way for the government to shield information, especially national security information, from the public." *Id.* at 1785. Even prior to the widespread advent of AI, Koningisor showed that this concept's "salience ha[d] grown in recent years as technological advances have allowed for ever-larger datasets and increasingly sophisticated data analyses." *Id.*

100 Rowe v. United Kingdom, 2000-II Eur. Ct. H.R. at ¶ 15 (Feb. 16, 2000).

101 Bulut v. Austria, 1996-II Eur. Ct. H.R., ¶ 47 (Feb. 22, 1996). *See also* Decision on Prosecutor's Appeal on Admissibility of Evidence, Prosecutor v. Aleksovski, Case No. 1-95-14/1-A, Appeals Chamber, International Criminal Tribunal for the Former Yugoslavia, ¶ 24 (Feb. 16, 1999) ("[E]ach party must be afforded a reasonable opportunity to present his case—including his evidence—under conditions that do not place him at a substantial disadvantage *vis-à-vis* his opponent").

102 *See* AMAL CLOONEY & PHILIPPA WEBB, THE RIGHT TO A FAIR TRIAL IN INTERNATIONAL LAW 748–49 (2020).

resources between prosecution and defense so dramatically that the proceedings' fundamental equality is fatally undermined. Courts have not been receptive to such arguments in the past, but military AI systems' unprecedented processing and analytical power could give such arguments greater purchase in the future.

In the present author's view, the aforementioned hurdles are surmountable in many, perhaps most instances, even if this suggestion can only be tentative. Procedural mechanisms allow for testimony from experts who can elucidate technology-derived military data's evidentiary significance, yet expert witnesses will need to overcome many unfamiliar courts' skepticism. Given judicial deference in matters of national security, successful defense challenges based on non-disclosure of material covered by a type of state secrets privilege appear unlikely. Still, few courts have been presented with the issue in the form in which it is likely to arise in future. It is likewise submitted that an interpretation of equality of arms so broad as to call battlefield evidence's viability into question would be out of step with the preponderance of judicial precedent.[103] However, the very point is that the issue has not been extensively litigated to date and that, going forward, technological developments may cast it in a new light which makes courts' views less predictable.

IV. CONCLUSION

To sum up, this Article has argued that emerging technologies employed in recent and ongoing armed conflicts will enhance the potential value of battlefield evidence but make realizing that potential more difficult. Section II demonstrated that previous technological advances have been key drivers of battlefield evidence's use to date, as improvements in militaries' ability to collect and exploit data for their own purposes have indirectly redounded to the benefit of law enforcement. Section III made the case that the technical features of UAS and military AI may likewise deliver significant, although qualified, opportunities for collection and exploitation. At the same time, the analysis showed that these technologies and their broader impacts on the conduct of warfare risk inhibiting information sharing and complicating courtroom use, with effects that will reverberate differently in different contexts.

Having examined issues that may complicate the evidentiary use of technology-derived military data, it is worth noting in conclusion that an *over*reliance on such evidence could be problematic in other ways. Truth-finding in any given case optimally involves combining multiple types of evidence from multiple independent sources. And beyond epistemic considerations, depending on technology-derived data may, as Alexa Koenig and Ulic Egan have argued, lead to "certain crimes becoming hypervisible, such as chemical weapons attacks or the bombing of hospitals, potentially

---

103 *See id.*, at 748–53.

drawing attention to those crimes like shiny objects, while detracting from other . . . information, such as that related to sexual violence, which may not as easily be captured by machines."[104] Furthermore, in international criminal law specifically, giving victims and other witnesses a voice in court advances important separate purposes such as creating a historical record, promoting societal healing, and expressing legal and moral values—which an exclusive focus on any form of non-testimonial evidence may not fulfil.[105]

Such risks are less than immediately concerning, due to the complications that this paper reviewed, but worth bearing in mind all the same. As with the future of warfare, the shape that criminal justice may take years from now cannot be anticipated with certainty. But while emerging technologies may or may not transform the underlying nature of war and the determinants of victory, they should not alter the fundamental character or objectives of the law. AI can help facilitate the collection and analysis of evidence, but the criminal enforcement of the law of armed conflict, like the use of AI in armed conflict itself, should remain centered on humanity.

---

104 Alexa Koenig & Ulic Egan, *Hiding in Plain Site: Using Online Open Source Information to Investigate Sexual Violence and Gender-Based Crimes, in* TECHNOLOGIES OF HUMAN RIGHTS REPRESENTATION (Alexandra Moore & James Dawes, eds.) 120 (2022).

105 *See, e.g.*, Mirjan Damaška, *What Is the Point of International Criminal Justice?*, 83 CHI.-KENT L. REV. 329 (2008).