Non-Binding Guiding Principles on Use of Battlefield Evidence in Civilian Criminal Proceedings[1]

I. *Introduction*

A. Context

Over the course of the armed conflict in Syria and Iraq, more than 40,000 foreign terrorist fighters (FTFs) from approximately 100 countries traveled to this region. While Syria and Iraq served as the epicenter in recent years, the terrorist "battlefield" remains transregional and global. During the last two decades, transnational terrorist organizations[2] have increasingly taken advantage of ungovernable or under-governed spaces to assert control of territory in various countries. As a result, military forces regularly engage in sustained armed conflict and other operational activities against transnational terrorist organizations. For this reason, countries may collaborate with local government and non-government forces in areas that may or may not be under sovereign control. This could result in the detention of individuals, who will be handled through the criminal justice system, rather than subject to a kinetic finish. Therefore, effective prosecutions and adjudications under these circumstances are critical to military mission success.

Transnational terrorist groups exploit conflict zones that are often urban, fluid, and noncontiguous, which further complicates the operating environment. During the course of conflicts, military forces may detain terrorists as well as seize documents, electronic media, and other materials. With the detention of terrorists, finding pathways to convictions and ensuring the effective use of information collected by military in civilian criminal investigations and prosecutions is vitally important.[3]

United Nations Security Council Resolution (UNSCR) 2396 underscores the importance of criminal justice tools in combatting terrorism. The resolution emphasizes the obligation of United Nations Member States, set forth in UNSCR 1373, "to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in support

[1]For the purposes of this document, the term battlefield evidence will be used to describe documents and objects collected by or given to military personnel. The drafters recognize that other terms are used, such as sensitive site exploitation (SSE), captured enemy material (CEM), or even collected exploitable materials. The drafters opted to use battlefield evidence because this term is used in multilateral and international fora. Furthermore, the focus of this document is on using materials or objects collected by the military as evidence in civilian investigations and prosecutions. These guidelines are non-binding and meant to be advisory to a range of countries that are interested in developing or amending their laws and policies concerning how to use battlefield evidence in terrorism-related cases.

[2] Could also be referred to as violent extremist organizations (VEOs)

[3] Some of these individuals may also be indigenous to these nations and face justice in domestic courts.

of terrorist acts *is brought to justice*." Furthermore, UNSCR 2396 stresses that Member States have the primary responsibility in countering terrorist acts. This responsibility necessarily includes the investigation, prosecution, and adjudication of their citizens for terrorism related crimes, as reflected in *inter alia*, UNSCR 2396's urging of Member States to develop and implement appropriate investigative and prosecutorial strategies regarding those suspected of committing foreign terrorist fighter-related offenses described in UNSCR 2178's paragraph 6.

The U.S. Integrated Strategic Plan to Defeat the Islamic State of Iraq and Syria also accentuates the importance of enabling law enforcement as a key effort towards achieving our national objectives.[4] Furthermore, the U.S. Counterterrorism Strategy highlights the significance of criminal justice and other tools in combating terrorism in this fluid, complex, and decentralized threat environment. The strategy notes that the United States is "enhancing the collection, discovery, and exploitation of identity information supporting the counterterrorism mission, particularly biometric data. Categories of identity information includes publicly available information, financial intelligence, and captured enemy material."

While many nations seek to develop and implement criminal justice solutions for dealing with terrorists, they face a myriad of challenges. One such challenge that countries have highlighted in a number of bilateral, regional, and multilateral fora is the use of information or materials collected on the battlefield in the civilian criminal justice system. For example, there are countries that do not have the legal authority to introduce information collected by non-law enforcement entities as evidence in a civilian criminal case. In addition, there are countries that do not have the legal mechanisms that allow for the protection of classified information in criminal proceedings such as the United States does.[5] Moreover, judges and prosecutors may lack knowledge and experience in dealing with battlefield evidence. For these practitioners, it is important to understand the conditions under which information is collected in a conflict zone.

There are also logistical issues that may hamper a country's ability to analyze and use information obtained by militaries in terrorism investigations and prosecutions. For instance, military personnel collect or obtain an enormous amount of documents, media, and other objects. The significant number of items that require analysis may put a strain on the military's human and financial resources. In addition to the sheer volume of the information collected, countries must contend with how to decipher encrypted material and translate multiple languages.

Besides the legal and logistical obstacles affecting the use of battlefield evidence, there is considerable misunderstanding and misinformation about the use of information. There appears

[4] U.S. Integrated Strategic Plan to Defeat the Islamic State of Iraq and Syria, February 2018.

[5] For example, in the United States the Classified Information Procedures Act, 18 U.S.C. App. III., may be used to protect certain aspects of classified information from disclosure while ensuring the defendant's right to a fair trial, including all necessary disclosure of information from the government.

to be widespread misperception among countries that if they simply had access to battlefield evidence, they could secure the convictions of those charged with terrorist offenses. In reality, under some civilian criminal justice systems, battlefield evidence is likely to provide an investigative lead, which would need authentication and probably corroboration with additional, independent evidence.

B. Background

In September 2017, the Department of State (DOS), Department of Justice (DOJ), and Department of Defense (DoD) launched a battlefield evidence initiative to address some of these issues. This initiative seeks to assist partner nations in using battlefield evidence effectively in civilian criminal justice proceedings. As a part of this initiative, representatives[6] from these three agencies formed a core interagency working group. Since the United States convicted terrorists using information collected by the U.S. military, the interagency working group determined that an initial review of DoD procedures may illuminate best practices, highlight lessons learned, and shape the guiding principles framework. This interagency team conducted roundtable discussions at each of the six U.S. Geographic Combatant Commands (GCC)[7] with participation from a wide range of civilian and military stakeholders. These fact-finding roundtable discussions focused on understanding how each respective GCC collects, analyzes, and shares battlefield evidence. Based on the key issues and themes highlighted during these discussions, DOS, DOJ, and DoD collectively developed fourteen non-binding guiding principles.

These non-binding principles can assist foreign partners as they review, revise, or develop their own approaches to using evidence derived from the military in their domestic civilian terrorism investigations and prosecutions. Where appropriate, the U.S. could offer training and technical assistance using these guidelines to shape those efforts. Moreover, these non-binding principles may complement and augment similar battlefield evidence efforts undertaken by the United Nations Counterterrorism Executive Directorate[8] and the Global Counterterrorism Forum.[9]

---

[6] Representatives came from the DOS's Counterterrorism Bureau, DOJ's Counterterrorism Section and the Office of Overseas Prosecutorial Development Assistance and Training, DoD's Special Operations Command Special Operations Support along with the Office of the Secretary of Defense for Policy and the Joint Staff.

[7] The interagency core group held roundtables at United States Africa Command (USAFRICOM), United States European Command (USEUCOM), United States Central Command (USCENTCOM), United States Indo-Pacific Command (USINDOPACOM), United States Southern Command (USSOUTHCOM), and United States Northern Command (USNORTHCOM) respectively.

[8] The United Nations Counter Terrorism Executive Directorate with assistance from the International Counter Terrorism Centre – the Hague drafted UN guidelines to facilitate the use and the admissibility of information and evidence preserved, collected and shared by the military.

[9] The Global Counterterrorism Forum's Criminal Justice and Rule of Law Working Group in partnership with ICCT developed *Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects.*

II. *Non-Binding Guiding Principles*

A. Summary of Principles

• Ensure clear legal authorities and practices for military operations exist that allow for the collection and use of information.
• Develop legal frameworks that allow for the admissibility of battlefield evidence, including protection of classified information, as well as sharing information with non-military actors.
• Develop clear guidelines or policies addressing the security classification of battlefield evidence and its ability to be unclassified, where possible.
• Develop policies and procedures for the creation and maintenance of a chain of custody and the integrity of the information and/or materials as a way to ensure authentication
• Create a systematic process to preserve information and objects that are collected and/or obtained by military personnel so that they are accessible and useable over the long term
• Exploit military collected or obtained information and materials for identifying data
• Establish processes for reviewing and downgrading the classification of information collected or obtained through military operations
• Recognize that battlefield evidence can have a multitude of civilian counterterrorism-related uses.
• Use multilateral and/or regional platforms to share battlefield evidence with partner nations
• Educate relevant government officials, particularly in the military, on the value of criminal prosecution
• Conduct joint trainings, as appropriate, that includes military and law enforcement officers.
• Provide training to key interlocutors, such as judges and investigating magistrates, on the unique nature of battlefield evidence and the nature of the environment in which the military collects and obtains information and materials

• Improve policymakers and practitioners' understanding that battlefield evidence will often require the need to develop independent, corroborating evidence
• Advance the basic knowledge, understanding, and training of designated military forces to handle battlefield evidence.

B. Legal and Policy Frameworks

- ***Ensure clear legal authorities and practices for military operations exist that allow for the collection and use of information.*** States should have legal authorities[10] or mandates for military activities. This authority typically covers the specific military operations or its jurisdiction. These authorities are important because they may detail the military's legal ability to collect, use, and share information or materials with non-military entities.

- ***Develop legal frameworks that allow for the admissibility of battlefield evidence, including protection of classified information, as well as sharing information with non-military actors.*** Some States' legal authorities expressly prohibit the military from sharing information with non-military actors, thus precluding the use of battlefield evidence in prosecutions. Therefore, countries should review and amend, if needed and appropriate, their legal frameworks so that information or objects collected by or given to the military could be admissible in court, provided that they meet domestic evidentiary rules, if they exist, and fair trial guarantees. Furthermore, States should have a legal framework as well as administrative policies and procedures in place to safeguard classified sources and methods of collection in the context of military operations, as necessary. Additionally, it would be beneficial if a country's legal framework includes provisions to allow for sharing and accepting battlefield evidence with and from domestic and foreign government agencies[11] as well as non-governmental entities.

[10] For example, Title 10 of the United States Code outlines the role of armed forces. This section provides the legal basis for the roles, missions and organization of each of the services as well as the overall United States Department of Defense. Also, the USA PATRIOT Act, P.L. 107-56, 115 Stat. 272 (2001), broadened the permissible circumstances for the use of the military to assist law enforcement agencies in countering terrorism.

[11] 10 U.S.C. §§ 271 specifically permits the U.S. Armed Forces to share information acquired during military operations with civilian law enforcement. It provides: (a) The Secretary of Defense may in accordance with other applicable law, provide to Federal, State or local civilian law enforcement officials any information collected during the normal course of military training or operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials; (b) The needs of civilian law enforcement officials for information shall, to the maximum extent practicable, be taken into account in the planning and execution of military training or operations; and (c) The Secretary of Defense shall ensure, to the extent consistent with national security, that intelligence information held by the Department of Defense and relevant to drug interdiction or other civilian law enforcement matters is provided promptly to appropriate civilian law enforcement officials.

- ***Develop clear guidelines or policies addressing the security classification of battlefield evidence and its ability to be unclassified, where possible.*** While the sources and methods of collection are often classified, the actual objects or information generally do not need classification. Government policies or guidelines clearly articulating this principle would help to prevent unnecessary complications at later stages when there is a need for information to support either domestic or foreign criminal proceedings.

C. Usage, Exploitation & Distribution

- ***Develop policies and procedures for the creation and maintenance of a chain of custody and the integrity of the information and/or materials as a way to ensure authentication.*** Chain of custody typically refers to the chronological history of the handling of physical evidence and is typically an element in determining the admissibility of that evidence. [12] Chain of custody is important in certain instances because it authenticates an item's origin, ensures evidence has not been contaminated or altered, and the evidence is what the government, or the party offering the evidence, purports it to be. Because of the dangerous and fast-paced nature of military operations, it may be difficult for military personnel to secure, label, and seal information at the scene in the same manner as law enforcement agencies execute their duties in criminal cases. Recognizing these circumstances, militaries should develop processes for the labeling and securing of battlefield evidence. When the situation permits and it is safe to do so, it is important to document the following information at a minimum: (1) identification of who collected the material(s); (2) brief description of what was collected; (3) location of where the material(s) collected; (4) date and time the material(s) collected; and (5) photographs of the material at the collection point. Furthermore, there should be established procedures to track who maintained custody of the evidentiary material. If a country's military follows these practices, there is a better chance of complying with evidentiary rules for authentication, if such rules exist.

- ***Create a systematic process to preserve information and objects that are collected and/or obtained by military personnel so that they are accessible and useable over the long term.*** The evidentiary value of information and materials collected or received by military personnel may not be immediately evident. Therefore, States should consider having some system in place to store and analyze information and materials that could be easily accessible for investigation and potential use in future prosecutions.[13]

[12] In the US, defects in the chain of custody go to the weight of the evidence, not its admissibility.
[13] For instance, in the United States, the National Media Exploitation Center (NMEC) analyzes documents and hard drives seized on the battlefield. In 2017, NMEC received over 300 terabytes of data from ground forces for processing. In addition, the FBI's Terrorist Explosive Device Analytical Center (TEDAC) serves as the single interagency organization to receive, analyze, and exploit all terrorist improvised explosive devices. TEDAC has

- ***Establish processes for reviewing and downgrading the classification of information collected or obtained through military operations.*** As noted in a prior principle, the sources and methods of obtaining, analyzing, or exploiting materials and information require protection. While the actual content, such as a list of names, or physical objects, like a telephone, do not need to be classified, there is still a tendency for military personnel to classify items or information. Therefore, it would be useful for States to establish processes so there can be a review of classified information to ensure the material does require classification because it deals with sources and methods. If the material does not need to be classified, then there should be procedures in place to downgrade the information so that it is shareable with appropriate stakeholders.

- ***Exploit military collected or obtained information and materials for identifying data.***[14] Biometric data, such as fingerprints, is a critical element in terrorist related investigations and prosecutions. Information and/or materials collected or received by military personnel is limited in value when it cannot be compared to known samples and/or when it is labelled improperly. Therefore, it is important for States to consider gathering and analyzing biometric data from battlefield evidence.[15] This principle is in line with UNSCR 2396, requiring States to develop and implement systems to collect biometric data. It is important for States to respect privacy and human rights when collecting, analyzing, and sharing biometric data.[16]

---

received more than 100,000 IED submissions from more than 50 countries. TEDAC has been successful in obtaining latent fingerprints from unexploded IEDs, however, those prints must then be matched to known prints in order to obtain a match. Often these matches are identified years after the IED was recovered. For example, in United States v. Alwan, FBI's TEDAC was able to match the fingerprints from an IED recovered in Iraq in 2005 to an individual that was living in Bowling Green, Kentucky. That match, however, occurred in 2011. The fingerprint match was instrumental in obtaining a guilty plea from the defendant who is serving a sentence of 40 years in prison.

[14] The Defense Forensic Center (DFSC) has the mission to increase the military's readiness through full-service support. For the first eight months of 2018, the DFSC labs received and exploited over 150,000 IED and non-IED submissions. Unique biometric data identifications of known and suspected terrorists developed by these laboratories resulted in court convictions, contributed to investigative leads, and issuance of INTERPOL Blue Notices.

[15] It is important to try to get biometric data from an object as soon as feasible, so individuals should seek to get any objects collected or obtained from the military to a lab for exploitation.

[16] The Sixth Report of the United Nations 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 notes that "[b]iometric identification of suspicious individuals can be an effective tool to counter the threat of terrorists attempting to travel internationally using false, forged or altered travel documents. Therefore, the inclusion of biometric data, high quality pictures and fingerprints of such fighters in various regional and international databases, including the INTERPOL database on foreign terrorist fighters, remains important."

- ***Recognize that battlefield evidence can have a multitude of civilian counterterrorism-related uses.*** Information or objects collected or obtained by the military may be used to address a broad range of counterterrorism objectives. In addition to criminal investigations and prosecutions, battlefield evidence can also be used in watch-listing, border screening, visa adjudications, immigration proceedings, and other functions. If the information or materials meet the high evidentiary thresholds required in most civilian prosecutions, it is likely that it will also meet the necessary standards for these other uses as well.

- ***Use multilateral and/or regional platforms to share battlefield evidence with partner nations***. International Criminal Police Organization (INTERPOL), European Union Agency for Law Enforcement Cooperation (EUROPOL), North Atlantic Treaty Organization (NATO) and other multilateral information sharing platforms such as OPERATION GALLANT PHOENIX (OGP) are potentially useful organizations to distribute relevant information collected through military operations, with civilian investigators and prosecutors. UNSCR 2396 highlighted the importance of multilateral and regional organizations in sharing information. Specifically, it "noted with appreciation the efforts of INTERPOL, to address the threat posed by foreign terrorist fighters, including through global law enforcement information sharing enabled by the use of its secure communications network, databases, and system of advisory notices and procedures to track stolen, forged identity papers and travel documents, and INTERPOL's counter-terrorism fora and foreign terrorist fighter programme."

D. Outreach & Education

- ***Educate relevant government officials, particularly in the military, on the value of criminal prosecution.*** Military officials focus on ensuring the success of their counterterrorism military operations when they are operating in conflict zones. Prosecution of terrorists is a viable and useful option for dealing with terrorists. It is important to conduct outreach and awareness-raising activities on how civilian criminal justice prosecution can be a complementary tool to military action in the fight against terrorism.

- ***Conduct joint trainings, as appropriate, that includes military and law enforcement officers.*** States may want to consider implementing joint, battlefield evidence training programs with military and civilian law enforcement counterparts. Military and civilian officials generally train separately. Therefore, joint trainings could help overcome some of the institutional impediments to the sharing of battlefield evidence. Some potential

topics of mutual interest could include developing reliable chain of custody procedures and/or maintaining or sharing information between military and civilian agencies.[17]

- ***Provide training to key interlocutors, such as judges and investigating magistrates, on the unique nature of battlefield evidence and the environment in which the military collects and obtains information and materials.*** States may wish to conduct specific training efforts on battlefield evidence for judges, investigating magistrates, prosecutors and other officials within their respective criminal justice system. Tailored training should highlight the unique and complex operating environment in which militaries work and focus on specific steps they take to preserve information and objects, which may have different purposes. Training programs should highlight and review cases from different operating areas where battlefield evidence was deemed credible and admissible.

- ***Improve policymakers and practitioners' understanding that battlefield evidence will often require the need to develop independent, corroborating evidence.*** Battlefield evidence can often be fragmentary in nature, or not easily corroborated. It will often be difficult, if not impossible, to develop a prosecutable case based entirely on the information collected from the battlefield. This type of information can often be more valuable as a lead for law enforcement to start an investigation. Given that judges may have questions about battlefield evidence and the associated authentication claims, where possible, investigators should strive to obtain separate, independent information that confirms the facts associated with the battlefield evidence. This may also help to support the reliability and relevancy of the information collected or received by the military. Improving policymakers and practitioners' understanding of battlefield evidence, its limitations, and what can be done to address constraints, should reduce misconceptions and improve how this information is used in terrorism investigations.

- ***Advance the basic knowledge, understanding, and training of designated military forces to handle battlefield evidence.*** To ensure the usability of received or collected information and objects, militaries should have units trained and prepared to create a chain of custody regarding the collection and preservation of battlefield evidence. Militaries should consider establishing practices that are recognized and approved by their respective law enforcement counterparts. For example, States may consider developing formal training curricula recognized by law enforcement organizations to teach standardize practices for collection and preservation of objects to enhance the integrity and reliability of the process. States that do have specialized units or opt not to

[17] For example, DoD/USSOCOM has implemented a Joint Exploitation Training Course (JETC) in close collaboration with the Federal Bureau of Investigations (FBI) in order to enable joint operations that result in reliable chain of custody procedures.

develop such units, may wish to consider embedding civilian law enforcement individuals with their military.

III. Conclusion

It is every State's responsibility to hold its citizens accountable for acts of terrorism. Critical components of accountability include the prosecution of individuals where there is credible information regarding their criminality and the actual retrieval of information and/or materials that prove the elements of the crime. In an environment where FTFs have traveled to a conflict or ungoverned regions, the collection of necessary information or objects is even more challenging because of the unstable and chaotic nature of the battlefield. These non-binding guiding principles may assist States in their efforts to address some of these challenges by providing guidance in how to use battlefield evidence effectively in civilian terrorism cases. These principles, when used in conjunction with other similar thematic documents, may assist States developing or amending laws, policies, procedures, and training programs.