

Explosive Ordnance Disposal & Intelligence: Exploring Gaps between Mutually Supporting Communities

BY Lieutenant Colonel Philip D. Cordaro

Introduction

A significant gap exists between the military intelligence and explosive ordnance disposal (EOD) communities that prevents the realization of each other's full potential. It lies in the area of science and technology under technical intelligence (TECHINT) where subject matter expertise and intelligence often overlap in a confusing gray area. The EOD community has information and expertise on foreign weapon systems that it does not know are valuable to military intelligence, and the military intelligence community has access to information on foreign weapon systems that it does not realize is vital to EOD. While the importance of the communities coordinating with one another has been recognized since EOD's establishment in the 1940s and has been captured in multiple versions of TECHINT field manuals, regulations, and publications over the years, a gap still exists.¹ It can only be closed through a concerted effort to update education, training, doctrine, and manning to reflect and codify this mutually beneficial relationship of increasing importance as we shift our focus to large-scale combat operations.

Operation-Dependent Integration

During the counterinsurgency operations in Iraq and Afghanistan, a link between the EOD and military intelligence communities emerged because the intelligence community required robust counter-improvised explosive device (C-IED) acumen to identify trends and assist with their predictive analysis. That expertise was only available through EOD preserving and exploiting components related to the manufacture and employment of improvised explosive devices. The concepts of "attack the network" and "counter threat network" were captured in multiple North Atlantic Treaty Organization (NATO), joint, and Service doctrinal publications, but they were still perceived to apply only to

C-IED. Because of the perception that EOD and exploitation are solely tied to C-IED, the military intelligence community still does not associate the EOD mission with traditional intelligence collection activities. As a result, EOD's level of integration with the intelligence community fluctuates greatly depending on the type of operation being conducted.

During EOD school, the EOD community does not teach its relationship with military intelligence. Additionally, it provides minimal follow-on training on intelligence, other than how to conduct a TECHINT report for first-seen ordnance, and it does not openly share its operational reporting. The *Generic Intelligence Requirements Handbook for Joint Service EOD*, which the Naval EOD Technology Division published in January 2004, contains best practices for recording first-seen materiel but only for the purposes of developing EOD render-safe procedures.² When deployed, EOD units are often approached by agencies from across the broader intelligence community that are looking for specific information on ordnance, weapon systems, and associated components. EOD units' support to those requests varies because the units often do not have visibility into what those agencies will do with the data, which results in the EOD units' lack of appreciation for the impact of their reporting.

Joint Exploitation

In the Universal Joint Task List, several tasks now link EOD to exploitation, battlefield foreign materiel acquisition, and scientific and technical intelligence.³ Additionally, JP 2-01, *Joint and National Intelligence Support to Military Operations*, Appendix F, describes supporting intelligence through joint multidiscipline exploitations.⁴ It underscores how critical information collected through EOD operations feeds the intelligence cycle.

Threats



**Defense
Intelligence
Agency**

Conventional

- Automated Systems
- Documents and Media
- C&E Equipment
- Medical Materiel
- Mobility Systems
- Munitions
- Weapons



**Defense
Threat Reduction
Agency**

Unconventional

- Chemical
- Biological
- Radiological
- Nuclear
- IEDs
- Modified Munitions and Weapons

Expeditionary Exploitation



Collect, Exploit, Analyze

DoD Exploitation Capabilities



Organized under a Joint Task Force with Reachback

Outcomes

- Force Protection
- Targeting
- Signature Characterization
- Component and Material Sourcing
- Support to Prosecution
- Support to RDT&E
- Support to Special Activities

Joint exploitation may be conducted simultaneously at all three levels of warfare. While DIA primarily addresses conventional threats and DTRA primarily addresses unconventional threats, they and other CSAs may address threats in both areas.

Legend

BCT	brigade combat team	GEOINT	geospatial intelligence
C&E	collection and exploitation	HUMINT	human intelligence
CLIC	company level intelligence cell	IED	improvised explosive device
CoIST	company intelligence support team	IMINT	imagery intelligence
CSA	combat support agency	INF	infantry
DIA	Defense Intelligence Agency	LEP	law enforcement professional program
DIV	division	MASINT	measurement and signature intelligence
DoD	Department of Defense	OBJ	objective
DOMEX	document and media exploitation	RDT&E	research, development, test, and evaluation
DTRA	Defense Threat Reduction Agency	SIGINT	signals intelligence
EAC	echelons above corps (Army)	WIT	weapons intelligence team
EOD	explosive ordnance disposal	WMD	weapons of mass destruction
FSB	forward support battalion		

Over numerous deployments as part of EOD and C-IED task forces to Iraq and Afghanistan, I witnessed EOD teams identify a unique device or piece of ordnance that we thought would be of interest to someone in the intelligence community, but we did not know who. We had no familiarization training on intelligence requirements. The first time I detected a demand signal for EOD reporting was during a senior leader tour in Washington, DC, before an EOD battalion deployment to Afghanistan in 2013. Even then, the requirements were vague. No one provided a list of ordnance items that the intelligence community wanted to acquire, but we did at least come away with points of contact for when we had questions. Once deployed, our organic and contracted intelligence analysts at the battalion were extremely proficient at tracking trends but were disconnected from the larger intelligence collection apparatus. When we had questions about specific incidents, I would contact national-level intelligence agencies for answers because it seemed there was no intelligence organization at an echelon in between that understood the link between the communities. Since I arrived at the Defense Intelligence Agency's (DIA's) Joint Foreign Materiel Program Office (JFMPO) in 2017, intelligence community elements have started to leverage JFMPO as the primary link for tracking down EOD reports and points of contact. This was not by design but rather born out of necessity.

Congressional Support

Congressman Rick Crawford (who served as a U.S. Army EOD technician) included language in the FY20 National Defense Authorization Act requiring the Department of Defense (DoD) to conduct a study of the gap between the EOD and intelligence communities. He sent congressionally directed actions to the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), Foreign Materiel Program Director, requiring an analysis of the current EOD, Foreign Materiel Program, and intelligence relationship and the establishment of an explosive ordnance intelligence sub-discipline under TECHINT.⁶ He also sent action memorandums to the Army G-2 and OUSD(I&S) on specific aspects of the relationship between the communities.

These actions by Congress, OUSD(I&S), and the Joint Staff are driving a deeper study into the relationship gap that could result in a significant change in the way the two communities interact in the future. Although initial requests from Congressman Crawford focused on using EOD technicians as intelligence analysts, the recent FY20 National Defense Authorization Act language and congressionally directed actions to OUSD(I&S) centered on the establishment of explosive ordnance intelligence and increased coordination between the EOD and intelligence communities.

In March 2020, OUSD(I&S) directed the U.S. Navy to conduct a study on the current relationship between the two communities and to propose recommendations on how to improve collaboration.⁷ Following the 3-month study that canvassed combatant command (COCOM), combat support agency, and Service EOD and intelligence staffs, the U.S. Navy-led group sent OUSD(I&S) multiple recommendations to facilitate greater coordination between the communities. OUSD(I&S) recently forwarded the recommendations to Congressmen Crawford.

Role of the Joint Foreign Materiel Program Office

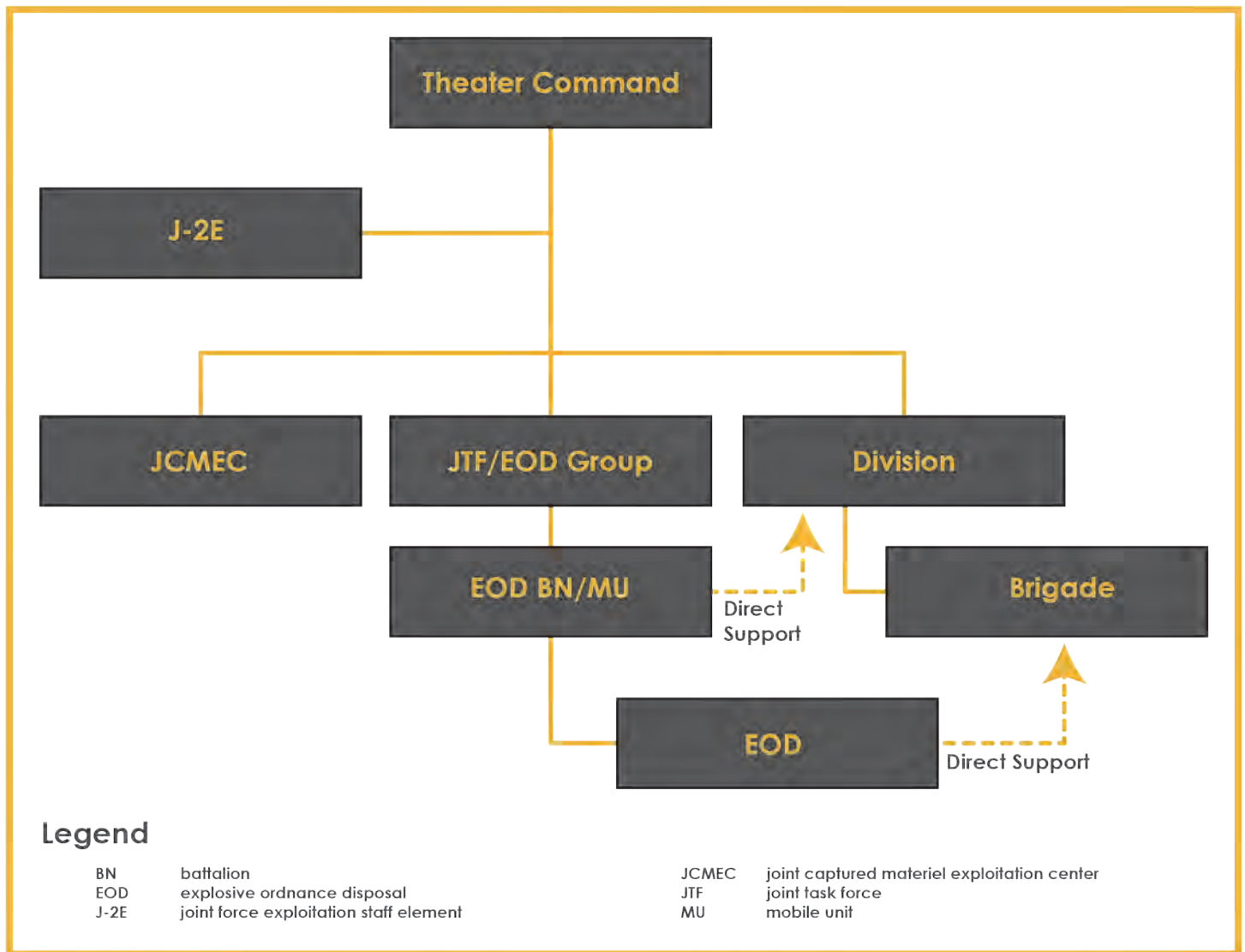
DIA's JFMPO is responsible for managing the DoD's foreign materiel enterprise. This responsibility includes—

- ◆ Validating all foreign materiel requirements.
- ◆ Deconflicting acquisitions.
- ◆ Coordinating exploitations.
- ◆ Maintaining visibility of all subsequent countermeasures developed by the test and evaluation community.

JFMPO's Expeditionary Operations section contains a joint captured materiel exploitation center (JCMEC), which stands up at the behest of a COCOM commander during named operations for the exploitation of materiel recovered or captured on the battlefield and the coordination to transport it back to national-level exploitation laboratories. If a COCOM commander requires an in-theater foreign materiel exploitation capability, JFMPO deploys the JCMEC under the J-2X, J-2E, or J-23. A deployed JCMEC includes experts from across the intelligence community and a company from the 203rd Military Intelligence Battalion (TECHINT) to collect foreign materiel from across the battlefield. JP 3-42, *Joint Explosive Ordnance Disposal*, explains the relationship between a JCMEC and an EOD headquarters. Every JCMEC level-one collection team requires EOD support to conduct its mission.

JFMPO is also responsible for establishing and deploying expeditionary exploitation teams in as little as 24 hours to support requirements from the defense attaché office and COCOM commander. JFMPO tailors the teams based on the target and location. It can leverage subject matter experts from more than 25 organizations and agencies to support those requests. Regardless of the target, the team will always incorporate EOD support and capture reporting in DIA-published intelligence information reports.

When not deployed, JFMPO's expeditionary operations team coordinates with either the J-2X or the J-23 section in each COCOM to disseminate requirements to the operational forces. In 2018, JFMPO recognized the classification of the list was limiting its dissemination to the EOD teams and worked with the Service intelligence centers to develop an unclassified list of requirements that EOD teams could



Explosive Ordnance Disposal and Captured Materiel Relationships⁸

carry with them on missions. The list also includes contacts for JFMPO and experts at the Service intelligence centers. Initially titled the “do not destroy” list, it is now referred to as the “most wanted ordnance” list. Administrators for the EOD Information Management System (EODIMS), which is the joint system of record for all EOD reporting, also plan to add it as a reference.

In support of its wider Foreign Materiel Program governance role, JFMPO also canvasses more than 20 Service, COCOM, and combat support agency-level organizations for each one’s top 50 foreign materiel acquisition priorities. Although JFMPO primarily collects that data to aggregate into the DoD’s top 50 foreign materiel acquisition priority list, each submission can also be used by military intelligence personnel preparing EOD units to deploy in support of a specific command or to a particular region. JFMPO is also coordinating foreign materiel acquisition requirements and opportunities with the COCOMs to integrate them further into the Foreign Materiel Program activities that directly align with their priorities. Because of the way most

COCOMs develop their priorities in the J-3, J-5, and J-58 sections, it is critical for the J-2X or J-23 section to synchronize Foreign Materiel Program activities across the COCOM. Although foreign materiel acquisition activities are an intelligence function, the priorities, funding, and resulting exploitation are relevant and of significant interest to many other offices.

EOD Reporting

In early 2020, EODIMS administrators coordinated with JFMPO to reclassify the database from a Defense Warfighting Mission Area to a Defense Intelligence Mission Area.⁹ This change took effect in June 2020 and will lead to changes that will allow intelligence analyst search engine tools on Secret and Top Secret networks to query EODIMS data and reporting. EOD TECHINT reports provide actualities on foreign materiel that can be used to positively confirm or deny assessments. The analysts will not have access to render-safe procedures or disposal details but will be able to find EOD reports to use as sources and provide more depth to their analysis. This is a crucial step toward getting the wider

intelligence community to recognize the unique value EOD reporting provides to satisfy the intelligence community's collection requirements.

JFMPO engages in more direct messaging efforts to the joint Service EOD community during technical conferences, predeployment training, professional military education courses, leader development opportunities, and deployments. These efforts have expanded the EOD community's understanding of its symbiotic relationship with the intelligence community. To capitalize fully on the relationship, military intelligence officers who are integrated with these units still need a better understanding of how EOD exploitations are useful to the intelligence community as raw reporting. If the national-level intelligence community understands and values EOD's access and reporting, but the military intelligence units on the battlefield with EOD do not understand its value, the communities will continue to have a significant gap. JFMPO's current engagement strategy focuses on reaching the intelligence professionals assigned to joint Service EOD units. These personnel are the true lynchpins who, with greater understanding, can best champion the relationship between the military intelligence and EOD communities.

Unified Exploitation Community of Interest

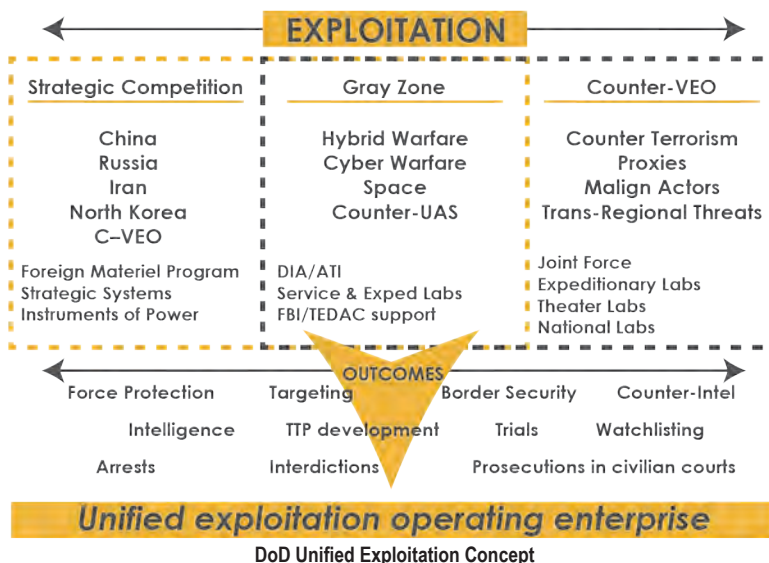
Unified exploitation is a concept that has existed at least since the 2012 West Point study on Combined Joint Task Force Paladin's Exploitation Systems,¹⁰ but it did not gain traction until DoD senior leaders attending a U.S. Special Operations Command (SOCOM) seminar in 2018 recognized the gap and recommended combining the various DoD exploitation efforts into one cohesive community. Since then, OUSD(I&S) and the Joint Staff J-5 have led an effort to establish the DoD unified exploitation community of interest. With an understanding of all the desired outcomes of exploitation, the community of interest developed the term "collected exploitable material" (CEM) to encompass: *all material and/or materiel in the possession of the Department of Defense (DoD), regardless of its classification or how it was obtained, that could be exploited in support of Department and national interests.*¹¹

The community of interest is coordinated around five lines of effort (LOEs):¹²

- ◆ LOE 1: Policy and Doctrine.
- ◆ LOE 2: Processes.
- ◆ LOE 3: Technology and Architecture.
- ◆ LOE 4: Capabilities and Resources.
- ◆ LOE 5: Information Sharing.

The unified exploitation community of interest's two desired end states are¹³—

- ◆ Under the umbrella of a unified exploitation architecture, all collected exploitable material is fully exploited in a timely and accurate manner to be discoverable by, and shareable with, all authorized customers.
- ◆ The processes for unified exploitation of collected exploitable material are transparent and collaborative, resulting in efficient, effective, and sustainable mission activities regardless of their location in the unified exploitation enterprise.



In the last 15 years, Services and combatant commands have stood up their own exploitation laboratories to meet their various mission requirements. There are currently separate U.S. Army, U.S. Navy, U.S. Marine Corps, SOCOM, and DIA exploitation laboratories; however, there are no exploitation or reporting standards across the laboratories, and they do not use a common database. This approach does not allow for a DoD common operational picture of all exploitable material collected by DoD elements. Additionally, problems often arise between exploitation entities because of the classification of collected material and some organizations' inability to share data because of the classification associated with how they collected it.

The Secretary of Defense signed a memorandum in January 2020 to eliminate issues with the over-classification of collected exploitable material. According to the memorandum, all newly acquired raw and unexploited collected exploitable material that the U.S. Armed Forces capture, collect, or handle during military operations is to be unclassified unless sensitive sources, methods, or activities were used to acquire the collected exploitable material.¹⁴ The DoD unified exploitation community of interest is also embedded within the larger U.S. Government battlefield evidence community of interest, the NATO Technical Exploitation Group, and the NATO Battlefield Evidence Working Group.

Conclusion


The fact that we are having the conversation and looking for ways to better integrate the EOD and military intelligence communities is a step in the right direction. The issue is starting to receive the level of visibility required to drive the necessary institutional changes. As integration efforts continue to move forward, it will be crucial for the EOD and military intelligence communities to establish regular opportunities for greater communication. Large-scale combat operations are the driver to better coordinate our efforts. EOD should start training Soldiers on their roles within intelligence earlier in their careers, and the intelligence community should recognize the value EOD Soldiers can provide to intelligence collection and analysis efforts. Only when the communities start to gain a better appreciation for their mutually supporting capabilities will we be able to build a bridge over the gap to tighten our collaborative efforts. ✨

Endnotes

1. Department of the Army, Field Manual 30-16, *Technical Intelligence* (Washington, DC: U.S. Government Publishing Office, 31 August 1972 [obsolete]).
2. Department of the Navy, *Generic Intelligence Requirements Handbook for Joint Service EOD* (16 January 2004).
3. Office of the Chairman of the Joint Chiefs of Staff, Universal Joint Task List, accessed 19 August 2021, <https://www.jcs.mil/Doctrine/Joint-Training/UJTL/>.
4. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, 5 July 2017).
5. Ibid., F-2, adaptation of original figure.
6. Representative Rick Crawford letters to Office of the Under Secretary of Defense for Intelligence and Security, Foreign Materiel Program Director, 3 February 2020.
7. Office of the Under Secretary of Defense for Intelligence and Security memorandum for the Director of Navy Staff, Subject: Explosive Ordnance Disposal Intelligence Gaps, 25 March 2020.
8. Office of the Chairman of the Joint Chiefs of Staff, JP 3-42, *Joint Explosive Ordnance Disposal* (Washington, DC: The Joint Staff, 9 September 2016), II-18, adaptation of original figure.
9. The Explosive Ordnance Device Information Management System requested a mission area change from the Warfighter Mission Area to the Department of Defense (DoD) portion of the Defense Intelligence Mission Area supporting the following domains: exploitation, mission management, dissemination, collection, analysis, and production. The change, in accordance with DoD Information Technology Portfolio Repository Guidance and Secretary of the Air Force, was approved and is effective as of 24 June 2020.
10. Department of the Army, *CJTF Paladin Exploitation Systems: The Evolving Role in Unified Exploitation* (Annapolis, MD: West Point, 19 October 2012).
11. Department of Defense, *Implementation Plan to the Department of Defense Strategy for Unified Exploitation* (August 2020).
12. Ibid.
13. Ibid.
14. Ibid.


LTC Philip Cordaro is the Commander, 303rd Explosive Ordnance Disposal Battalion, at Schofield Barracks, HI. Before taking command, he was assigned to the Defense Intelligence Agency's Joint Foreign Materiel Program Office where he was the Deputy Director for Enterprise Operations and the U.S. Foreign Materiel Program Head of Delegation.


CW2 CHRISTOPHER G. NASON




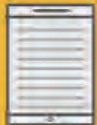
MILITARY INTELLIGENCE LIBRARY


Options Available

LIBRARY CATALOG

DATABASES

USAICoE WRITING PROGRAM

EBOOKS

RESEARCH GUIDES

The MI Library website is located at:
<https://auls.insigniaalls.com/Library/Home?LibraryID=0010&Language=English>