INTELLIGENCE DISCOVERY EXPERIMENT: OPEN-SOURCE INTELLIGENCE SUPPORT TO TARGETING

by Ms. Lori A. Sieting

Introduction

In December 2022, the Intelligence Battle Lab at Fort Huachuca, Arizona, conducted an Intelligence Discovery Experiment on open-source intelligence (OSINT) support to targeting. The experiment focused on identifying issues and gaps in collection management and processing, exploitation, and dissemination (PED) for OSINT and their potential solutions. The experiment simulated a corps intelligence and electronic warfare battalion conducting collection management and PED related to OSINT as it supports targeting in multidomain operations.

Background

Commanders find using OSINT as a deep and persistent sensor integral to providing near real-time data-tracking of regional activities, patterns, and deviations from patterns in threat operations during both competition and conflict. During competition, OSINT can identify unusual deployments, movements, exercises, targets and dispositions, high-value target tracking, and unusual logistic patterns. OSINT use during competition supports information operations by identifying misinformation and disinformation campaigns, tracking sentiment and population atmospheric changes that signify the threat's attempt to influence a population into action, and detecting other indicators of our competitors' influence. During conflict, OSINT aids in identifying indicators, tracking troop movements and high-value targets, conducting battle damage assessment of lethal and nonlethal attacks, and providing other crucial intelligence.

The first Army doctrinal mention of OSINT as an intelligence discipline was in Change 1 to FM 2-0, *Intelligence*, dated 11 September 2008. However, the Army does not currently have OSINT-specific collection management, all-source analysis, PED, and the associated tactics, techniques, and procedures (TTP) for multidomain operations. An investigation through the Center for Army Lessons Learned and interviews with subject matter experts who previously worked or are currently working OSINT in real-world conflicts revealed that there are no established TTPs for OSINT integration into collection management and PED at echelons corps and below.

Methodology

The experiment focused on PED at the point of collection and collection management as they apply to OSINT, not on collection in general or all-source analysis. Participants executed intelligence operations in a simulated environment using real-world data. The Intelligence Battle Lab provided role players with an operations order (OPORD) that included priority intelligence requirements (PIR) and information requirements (IR), a high-payoff target list, initial intelligence preparation of the operational environment products, and hundreds of current real-world OSINT reports. Role players were divided between the collection management and the PED cells. They included a collection manager, OSINT-trained personnel, signals intelligence analysts, geospatial intelligence imagery analysts, and all-source analysts. Subject matter experts in special operations, electromagnetic warfare,

cyberspace operations, information operations, space operations, and fires served as liaisons to the collection management and PED cells in their specific areas of expertise. They included representatives from—

- Army OSINT Office.
- Fires Capabilities Development Integration Directorate (CDID).
- U.S. Army Special Operations Command.
- U.S. Army Civil Affairs and Psychological Operations Command (Airborne).
- Cyber CDID.
- Space and Missile Defense Center of Excellence.
- Intelligence CDID.

A white cell answered the role players' requests for information and requests for collection and stimulated the experiment with reports. Discussions following the experiment assessed individual and collective tasks, actions, and results. The observations were compared against hypotheses and learning demands.

The U.S. European Command's area of responsibility served as the basis of the scenario and provided real-world data for the experiment. Hundreds of real-world OSINT reports related to the master scenario event list were readily available. They were extracted from established OSINT repositories such as Think Analyze Connect and Protected Internet eXchange. The master scenario event list was multidomain-focused and included antiaccess and area denial efforts, troop movements, equipment and supply movements, battle damage assessment (physical and functional for desired lethal and nonlethal effects on targets), electromagnetic warfare, information operations, cyberspace operations, and space operations.

Experiment Findings

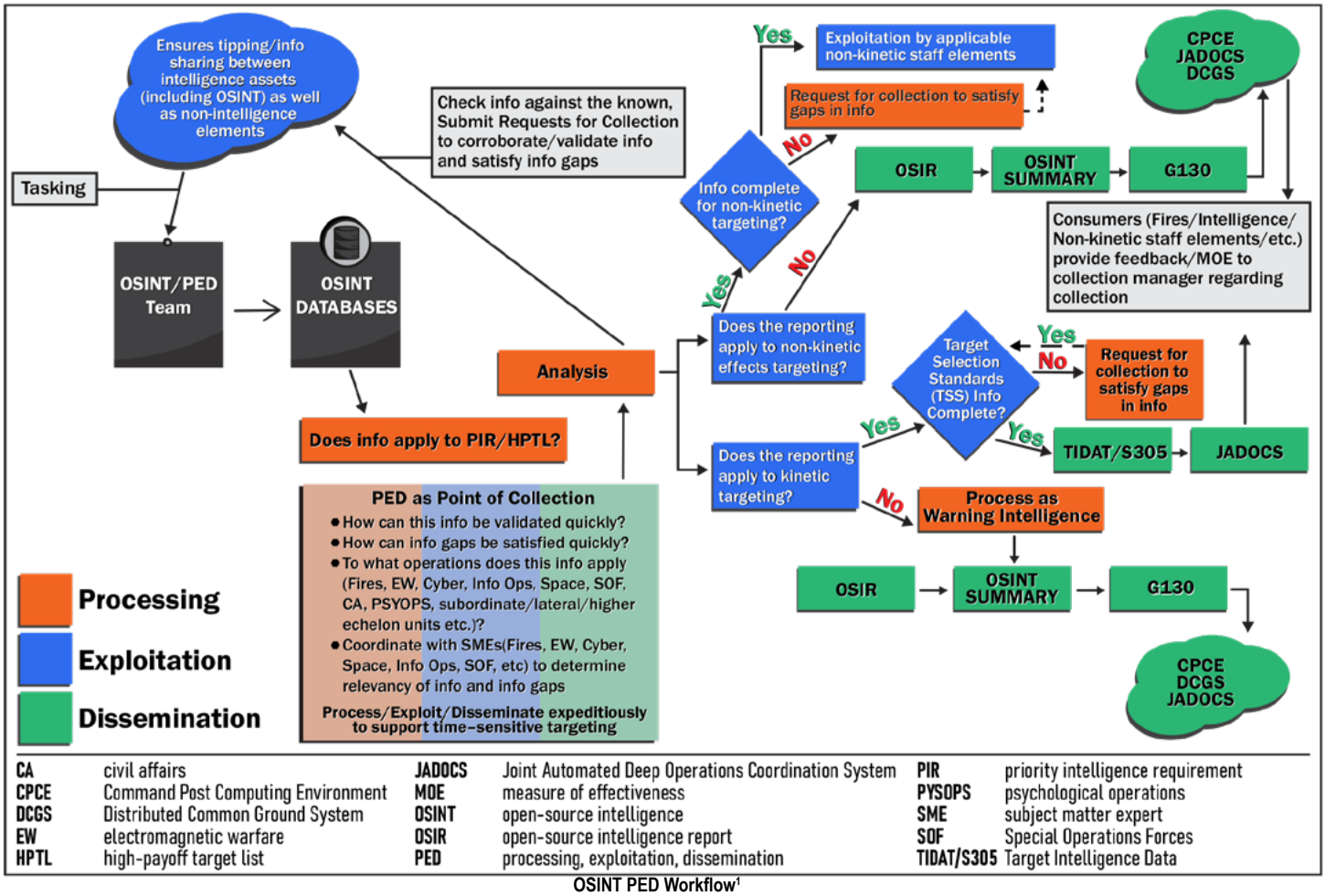
Need for an OSINT Integrator. OSINT teams and cells should have an OSINT integrator responsible for acquiring mission approval authorities, synchronizing OSINT collection efforts with higher and adjacent headquarters and subordinate OSINT elements, and ensuring the team has the required OSINT training certifications and tools. This integrator could also represent OSINT to the collection manager, translate PIRs, IRs, and indicators into OSINT-digestible requirements, be responsible for creating and updating Appendix 7 (OSINT) to Annex B (Intelligence) of the OPORD, and ensure incorporation of OSINT into Annex L (Information Collection). The OSINT integrator could look for opportunities to potentially exploit OSINT, assist in prioritizing OSINT collection efforts, and guide the analysis of OSINT reporting.

OSINT Reporting and Messaging Deficiencies. The Army must establish a standard message format for OSINT compatible with the Army's Command Post Computing Environment and respective systems, such as the Advanced Field Artillery Tactical Data System, the Electronic Warfare Planning and Management Tool, and other integrating systems to facilitate information sharing. This format must incorporate the various data types associated with multidomain operations, such as cyberspace, information, and space operations.

Lack of TTPs for Collection Management and Collection Specific to OSINT. The role players working collection management in this experiment had difficulty writing specific information requirements for OSINT. They did not have a clear understanding of the capabilities and limitations of OSINT. There was an inclination to write vague, wide-ranging specific information requirements. For example, find bad things on the Internet. We can obtain significant information from OSINT by focusing on the specifics of PIRs, IRs, the high-payoff target list, and single-source intelligence discipline objectives. We can also gain information by looking at *what OSINT tells us* about changes in the operational environment and threat intent that would otherwise be unknown and could affect decision making. OSINT can monitor pattern of life baselines and detect changes that affect operations. All this requires developing TTPs at echelons corps and below for OSINT collection methodology. OSINT collection is possible through several different approaches. OSINT can be directed at a specific region, for a specific period, using a specific source of information, and using keyword searches (related to a particular PIR, IR, high-payoff target, or other indicator). To conduct a keyword search, the collector needs an understanding of relevant keywords associated with specific targets.

Lack of PED TTPs for OSINT. Collectors must ensure the isolation of pertinent data for further exploitation. This generally applies to application programming interface calls from specific repositories. Collectors must verify sources to mitigate disinformation risks and apply credibility ratings. After isolating the data and establishing veracity, collectors may exploit the data in several ways, including location verification (either through metadata, background, or landmark exploitation), date and time verification (by metadata or other source), source network characterization, source activity characterization, or a pivot to related collection activities (such as pattern of life characterization).

The Army must establish systems, architecture, databasing, and dataflow for OSINT to ensure dissemination of information to all applicable organizations and elements and to enable stakeholders' access to the data relevant to their operations. OSINT requires a cross-domain solution to collect information at the unclassified level and then send information to mission command systems. The Intelligence Battle Lab analysts created an OSINT PED workflow for the experiment. (See Figure, on the next page.)



OSINT PED Workflow[1]

Target Selection Standards Not Considered in Collection. It is common for the collection plan to be based on PIRs and IRs. However, it is also necessary for OSINT teams (and the entire intelligence staff, for that matter) to have the target selection standards for high-payoff targets in advance. Having the information in advance informs the collection strategy. It helps determine if the collected information satisfies the target selection standards and is sufficient to submit as target intelligence data to the Advanced Field Artillery Tactical Data System or the Joint Automated Deep Operations Coordination System. Knowing the required information for targeting up-front makes PED more efficient, effective, and timely. The target selection standards for high-payoff targets are usually in a spreadsheet published in Annex D (Targeting) of the OPORD and are available to the intelligence staff.

Addressing OSINT in the OPORD. Appendix 7 (OSINT) of the OPORD, if included, is often a cut and paste of current regulations without specific thought given to how to conduct OSINT collection and PED and to the coordination required with other staff elements, collection management, and other organizations. Units also frequently refrain from including targeting information for nonlethal effects in Annex D (Targeting). OSINT units should practice and refine including OSINT in orders production; something as simple as using a Mardam-Bey Internet Relay Chat (more commonly known as MIRC) chat room to push, tip, or cue information between OSINT and other intelligence disciplines, organizations, and elements. Cementing this technique across the intelligence disciplines and throughout organizations and elements will assist with exploiting the information environment. It should be included as part of the pre-execution checklist for OSINT collectors and other intelligence disciplines.

OSINT Support to Time-Sensitive Targeting. OSINT support to targeting in large-scale combat operations is more complex than support to targeting against an unconventional threat, such as ISIS, Al-Qaida, or the Taliban. In the Middle East, the U.S. Armed Forces could persistently watch targets for days at a time with an unblinking eye prior to placing rounds or operators on target. Intelligence support to targeting against a conventional threat will be more time-sensitive because the targets will be constantly moving, fleeting targets of opportunity, and in an evolving battlefield environment that could adversely affect U.S. forces and missions. For these reasons, commanders may engage a target with less data resolution than target selection standards require. For these same reasons, it is understood that targeting with partial information could lead to extensive expenditure of finite munitions. Time-sensitive reporting and the associated processes will quickly enable dynamic, follow-on activities, such as tipping other assets for collection and expeditious reporting to

inform targeting, intelligence preparation of the operational environment, and the intelligence running estimate. Corps and divisions must develop TTPs for OSINT PED that adapts its intelligence support to the current yet varied operational environment and reduces latency to support time-sensitive targeting.

Validation of OSINT Information. Confirmation from other sources (another discipline, source, or multiple sources) validates OSINT information. Multiple reports obtained though publicly available information on the same target could offer more credibility. For example, several armored vehicle reports with images rectified to the specific location received within a precise temporal window could offer more credibility. Conversely, multisource publicly available information about the same event but without supporting imagery or other corroborating reporting (or within a broad temporal window) would likely not meet validation requirements for targeting. An analyst should assess each OSINT report for source reliability, credibility, and quality of the information in accordance with ICD 203, *Analytic Standards*.[2] The OSINT team/cell outputs should feed into the fusion cell where the G-2/S-2 staff can corroborate or confirm the OSINT reports. Staff elements outside of intelligence should also receive OSINT outputs for corroboration or confirmation (e.g., electromagnetic warfare, cyberspace operations, information operations, space operations) where applicable. The Army must develop standards to assess credibility of OSINT reporting and sources. Such standards could include—

- Account history: How long has the account existed?
- Information accuracy: Does the individual posting have a history of posting things known to be accurate?
- Timeliness: How quickly does this individual post after an event occurs?
- Location: Is this individual taking pictures or just reposting?
- Verification: Does this individual have a verified account?[3]

Conclusion

Although OSINT has been used by military intelligence for decades, only recently was it identified as an intelligence discipline. OSINT does not have a specific military occupational specialty (MOS) or additional skill identifier. Any military intelligence MOS can conduct OSINT if they receive mission authority, use approved tools with managed attribution, and meet the security and training requirements. However, TTPs for collection management and PED still require development. The current force design does not include a senior OSINT cell integrator. OPORDS do not effectively address OSINT requirements. Further study is necessary to determine all-inclusive artificial intelligence and machine learning requirements for OSINT. In-depth studies are essential to explore the details of these gaps and inform DOTMLPF-P[4] decisions for the future force.

Endnotes

1. Figure adapted from author's original.

2. Office of the Director of National Intelligence, Intelligence Community Directive 203, *Analytic Standards* (Washington, DC: Office of the Director of National Intelligence, 2 January 2015), https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

3. See "Verified," Social Media Glossary, Later, https://later.com/social-media-glossary/verified/. Verified refers to the process of confirming an account or profile on social media as authentic. Verification is typically denoted by a blue checkmark or similar symbol beside the account name or profile. Verification serves as a means of establishing credibility and trustworthiness on social media platforms. It helps users differentiate between authentic accounts and potential impersonators or fake accounts. The verification process varies across social media platforms, but generally it involves confirming the account holder's identity through documentation, official records, or other verification methods.

4. DOTMLPF-P: doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

Ms. Lori Sieting is an intelligence specialist at the Intelligence Battle Lab, Fort Huachuca, AZ. For the past 15 years, she has served as a Department of the Army Civilian. She currently conducts planning and experimentation focused on intelligence support to multidomain operations. Previously, she was an instructor/course chair at the Human Intelligence Training-Joint Center of Excellence. Ms. Sieting retired after a 21-year career as a U.S. Army military intelligence warrant officer.