OSINT

The need for an open source intelligence workforce

by Heather A. Barrows

>Ms. Barrows is the lead OSINT Policy Analyst, Deputy Commandant for Information–Intelligence, HQMC. She has been instrumental in Marine Corps OSINT lines of effort: operationalization, institutionalization, professionalization, and partnerships. A Reserve Army officer, she has deployed to Kuwait as a part of the Army Reserve Cyber Operations Group (ARCOG) and established OSINT capabilities at the Regional Cyber Center-Southwest Asia (RCC-SWA) in support of Operation INHERENT RESOLVE.

What happens when your relative, friend, or colleague shares state-sponsored propaganda? What if it seems to align with deeply held personal values? Can the content elicit multiple emotional responses from people with disparate beliefs? Is there a call to action no matter how seemingly innocuous? The intent of state-sponsored propaganda is to create instability with psychological and potential kinetic effects. Our adversaries are adept at exploiting publicly available information (PAI) to oppose United States Government (USG) interests. When citizens look at state-sponsored propaganda and disseminate it through "shares," posts, blogs, gifs, and retweets, they provide unfettered access to the American sentiment.[1] The effective range of weaponized information is the collective response of individuals and subsequent environmental effects. Our adversaries use these tactics against USG and civilian populations world-wide. A Marine Corps Service professionalized open source intelligence (OSINT) workforce is critical to parse, collect, and vet PAI to address the demands of the current and future operating environments.[2]

The keyboard is quickly becoming the modern warfighter's rifle. We have all heard the refrain, "Every Marine a rifleman." This refrain is an affirmation that Marines are proficient in warfighting. The truth still stands that Marines must understand how to shoot, move, and communicate; however, both what it means to be proficient and the weapons being used have changed. It is imperative that Marines are proficient in utilizing information technology and systems to disrupt, degrade, and deny the adversary in the information environment. Marines must understand that weaponized information can penetrate our homes and disrupt us in uniform. The definition of enemy has changed as the means to conduct an attack is ever increasing. Disinformation can be used to influence and control local sentiment in deployed environments with kinetic outcomes against USG interests. The volume of information available creates noise that intensifies the "fog of war." Whether at home or work, the individual Marine is vulnerable to attack from adversaries. It is imperative to train and equip every Marine to maximize lethality in the information environment to ensure that every Marine remains a rifleman—a modern warfighter. Weapons platforms may change, but the resolve of the warfighter to dominate the multi-domain battlespace must not.

OSINT should not be construed as simple based on the availability of PAI. OSINT collectors methodically parse PAI to answer intelligence requirements and produce serialized OSINT reporting. For instance, commercial satellite imagery can be collected and disseminated to a geospatial intelligence cell to answer a request for information. The OSINT cell knows how to minimize their digital signature, use tools that are specific to OSINT, and optimize collection.[3] Without training to collect PAI, intelligence professionals use home computing habits to answer

A keyboard is often the weapon of choice. ***(Photo by LCpl Kyle Bunyi.)***

information requirements. Applying sophisticated Boolean or "Google Dorking" alone is a failure to utilize three-quarters of the measures required to collect PAI securely. All keystrokes, mouse movements, clicks, action, and even inaction contribute to a user's presence in a session. Each action or inaction influences the content that is delivered during a session. Successful employment of OSINT tradecraft facilitates secure collection.

What can be done with OSINT does not reflect where Marine Corps OSINT is today. Every Marine is individually and collectively part of the common operating picture. Marines can be targeted individually and collectively by diverse adversaries with attacks such as phishing or information campaigns meant to degrade confidence in the mission, USG capabilities, and interests. A Marines' ability to ingest, assess, and exploit PAI improves our agility in the information environment. PAI exploitation improves situational awareness and leaves us less vulnerable. However, prior to enabling all Marines to exploit PAI, we must establish a robust OSINT capability. The fundamentals of OSINT collection must translate across domains in any operating environment.

The Marine Corps must establish professionalized OSINT before developing force-wide PAI capabilities to maintain unity of effort. There are several requirements that are necessary to conduct the full-spectrum of OSINT operations. First, provide relevant OSINT support through standardized processes that are captured in policies, doctrine, and disseminated through the Marine Corps. Second, launch a professional occupation field with career growth through a formalized training pipeline. Third, expand OSINT relationships between the Marine Corps, joint force, intelligence community, and coalition partners. Standardized, professionalized, and operationalized OSINT is an intelligence discipline capable of supporting realtime intelligence requirements in dynamic environments.

HQMC Deputy Commandant for Information has initiated movement on professionalization through release of an OSINT strategy, applying outcomes from the May 2019 OSINT Professionalization Working Group, and synchronizing efforts with the Defense Intelligence Agency and the Services. The vision is to establish a Marine OSINT program of record that facilitates resourcing to include commercial–Internet service provider, managed attribution, tools, and training. There are several lines of effort required to execute this vision:

- Operationalization: Enable timely, precise, relevant, and predictive OSINT support to MAGTF, joint force, coalition, and intelligence community decision makers, planners, and operators at all echelons.
- Institutionalization: Provide relevant OSINT support through standardized processes that are captured in policies, articulated in doctrine, and shared throughout the Marine Corps.
- Professionalization: Launch a professional occupation field that encourages career growth through a training pipeline to provide capable Marine Corps OSINT professionals who better understand how OSINT can support the needs of the MAGTF.
- Partnerships: Renew, create, and expand OSINT's relationships between Marine Corps elements, the joint force, intelligence community, and coalition partners to leverage resources, ensure interoperability, and increase mission effectiveness across the intelligence community.

The OSINT strategy is a roadmap to establish OSINT as a formal intelligence discipline within the Marine Corps.

OSINT enables the gathering and processing intelligence that would have been difficult or impossible to collect a generation ago.[4] 26th MEU and Marine Corps Forces Cyberspace Command (MARFORCYBER) OSINT activities demonstrate OSINT's capacity as a force-multiplier. The 26th MEU deployed from February to August 2018 and used OSINT to answer intelligence requirements. 26th MEU's OSINT requirements were federated among intelligence specialists from each element of the MEU, information operations planners, and communications strategy personnel. These Marines utilized DATAMINR for near-realtime monitoring of force protection/indications and warnings, resulting in contingency triggers supporting European Command, Africa Command, and Central Command. The Conflict Zone Tool Kit proved instrumental in identifying narratives of interest, trend analysis, assessing online personas, and conducting network analysis. OSINT enabled 26th MEU to respond to realtime requirements and provide critical information

The Marine Corps must become an effective employer of publicly available information. *(Photo by LCpl Kyle Bunyi.)*

OSINT enables units to respond to realtime requirements. (Photo by LCpl William Chockey.)

to facilitate successful operational outcomes across domains.

From October 2018 to February 2019, the MARFORCYBER G-2 OSINT Cell began supporting Joint Task Force-Ares. MARFORCYBER G-2 OSINT cell provided violent extremist organization website characterization. The sensitivity of the G-2 OSINT cell's activities cannot be overstated. Through the employment of OSINT tradecraft, the G-2 OSINT cell monitored and collected information from violent extremist organization websites without compromise. The G-2 OSINT cell provided descriptions of website operability and content that enabled Joint Task Force-Ares to adjust operational missions accordingly. As our OSINT capability develops, it will be possible to ingest large data streams, discern patterns, and utilize them to project real-world outcomes with greater frequency than we can today. If the adversary has situational awareness of the OSINT cell's activities, they could target Marine Corps networks, interests, and operations—affecting multiple domains. The challenge of collecting and disseminating critical information to the audience is best left to a professionalized OSINT Marine. OSINT collectors are in strong position to provide vetted information to support other intelligence disciplines across domains. Execution of the OSINT strategy serves as a force-multiplier through the professionalization, standardization, and operationalization of OSINT while providing layers of security for collection activities. Threats in the information environment and cyberspace demand rapid response including the ability to answer realtime requirements. OSINT presents a corridor to synchronize efforts across domains by developing space and time for decision makers to seize initiative and advance objectives.

The sensitivity of the G-2 OSINT cell's activities cannot be overstated.

While out of uniform and at home, Marines may think and even believe they are a long way from the front line of inter-state warfare.[5] However, in today's world, citizens, their devices, their workplace, the company used to purchase office supplies, and its supply-chain are all critical parts of the battlefield that can be exploited to further adversary objectives.[6] No single intelligence discipline, capability, or domain can respond to the sophistication of the adversary threat. Capabilities that can synchronize effects across multiple domains are necessary to ensure the commander's freedom of action today. *To respond to the demands of the modern operating environment, the Marine Corps must execute the four OSINT lines of effort: operationalization, institutionalization, professionalization, and partnerships.*

Notes

[1] Emerson T. Brooking and P.W. Singer, "The Empires Strike Back," *Like War*, (New York, NY: Harcourt Publishing Company, 2018); see also, Keir Giles, *Handbook of Russian Information Warfare*, (Rome, Italy: Research Division North Atlantic Treaty Organization Defense College, November 2016).

[2] Headquarters Marine Corps, *Marine Corps Operating Concept*: *How an Expeditionary Force Operates in the 21st Century*, (Washington, DC: September 2016); see also Marine Corps Intelligence Activity, *2015-2025, Future Operating Environment Implications for Marines*, (Quantico VA: September 2016); Headquarters Marine Corps, *Marine Corps Intelligence Surveillance, and Reconnaissance Enterprise Plan*, (Washington, DC: September 2014); and MAJ Ryan Kenny, USA, "Disruptive by Design: Intelligence Fusion Inoculates Against Cyber Threats," *Signal*, (Fairfax, VA: June 2019).

[3] Headquarters Marine Corps, "Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise Implementation Guidance for Open Source Intelligence," *Marine Corps Intelligence, Surveillance, and Reconnaissance Decision Memorandum 01-2019,* (Washington, DC: February 2019); see also Headquarter Marine Corps, *Marine Corps Reference Publication 2-10A.3*, (Quantico, VA: June 2017).

[4] Ilana Bum and Heather J. Williams, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, (Santa Monica, CA: RAND Corporation, 2018).

[5] Staff Reporter, "Cyber Warfare and the Future of Cyber Security," *Tech Times*, (New York, NY: June 2019).

[6] Edward Wood, "To Win the Cyber War, A Great Defense is the Best Offense," *Forbes*, (Jersey City, NJ: May 2019).