Tying It All Together

Identity operations in support of information operations

by CWO3 Justin D. Hays

>CWO3 Hays is a Criminal Investigation Division Officer currently assigned to 2d Law Enforcement Battalion, II MIG, II MEF. He has served as the CID OIC at all three law enforcement battalions. He has completed two deployments to Iraq and multiple deployments in the Pacific Command area of responsibility.

Over the past two decades, the Marine Corps has made itself at home in fighting a hidden enemy. For years now, the Commandant and higher headquarters have emphasized the need to capitalize on lessons learned to create, develop, and employ many new concepts and capabilities to combat our future enemies.[1] One specific concept is information operations within the information environment (IE). Although information operations is not an entirely new concept, the addition of new technologies and networks has created fundamental changes for information operations within the battlespace.[2] This specific concept has resulted in the refinement of the MEF headquarters group (MHG) into the MEF information group (MIG), charged with the task of managing information operations. The big questions are: What, specifically, is information operations, and how can we quantify this abstract concept or that of the information environment? More importantly, how do we fight in this nebulous environment?

The Marine Corps Information Operations Center defines information operations as

> the integration, coordination, and synchronization of all actions taken in the information environment to affect a target audience's behavior in order to create an operational advantage for the commander.[3]

One of the foremost evolving concepts that directly supports information operations is identity operations. Identity operations joins the capabilities of biometrics, forensics, and identity intelligence under a single umbrella in order to lift the fog of anonymity. Identity operations is a "mission enabler for law enforcement, intelligence, counterintelligence, [and] force protection."[4] If we were to overlay identity operations with the intelligence cycle, we could see that it serves the vital role of collecting, exploiting, and analyzing biometric and forensic information to directly feed the shaping actions within the information environment. Once analysis is completed, the MIG commander is able to levy the specialized capabilities under the MIG to then gain and maintain the initiative within the information environment.

Fingerprints are just one part of the expeditionary exploitation capability. *(Photo by LCpl Careaf Henson.)*

Information Environment

As we look deeper at the identity operations construct, the actual material and the personnel identified to conduct biometric and forensic collection operations are organic to the law enforcement battalions under the MIG. The capabilities come in the form of site exploitation, expeditionary forensic exploitation, and the secure electronic enrollment kit (SEEK II) under the Identity Dominance System-Marine Corps (IDS-MC).[5] Site exploitation and expeditionary forensics form a mutually supporting relationship that ties evidence to individuals or threat networks. The expeditionary forensic exploitation capability employs a broad spectrum of forensics techniques, including fingerprint collection, DNA collection, chemical identification, and document and media collection and exploitation.[6] The biometric tool sets under IDS-MC are used to collect vital biometric information to be further preserved and analyzed against biometric databases. After collection and exploitation, law enforcement battalion personnel then use intelligence portals to directly coordinate, integrate, and rapidly feed intelligence fusion. When used collectively, these specific capabilities equip the MIG commander with vital tool sets that serve as a form of intelligence sensor.

The implementation of basic policing techniques is not a new concept in the battlespace; however, the use of more advanced policing techniques struggles to gain widespread application and understanding. In many cases, the thought that law enforcement capabilities are separate from intelligence activities has been the prevailing sentiment, when in fact, these capabilities feed and drive the intelligence/information cycle. *Joint Publication 1-02* states that information operations is not a standalone capability; rather it is

> the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[7]

The material solutions under the identity operations program are part of this greater system of supporting capabilities that are already organic to the Marine Corps under the MIG. When employed appropriately, biometrics and forensics can turn tangible evidence into actionable intelligence that supports targeting throughout the physical, informational, and cognitive dimensions.[8] In short, law enforcement battalions have a robust and dynamic capability that collects information and directly supports intelligence which can be rapidly fed into targeting through information operations warfare. Identity operations is part of the future fight with a hybrid enemy; its integration is crucial to future successes in the information environment.

Imagine a military police detachment taking part in a security patrol through a neighborhood that has been known to have a persistent IED threat. As part of their pre-mission planning, the military police prepare site exploitation kits and SEEK II biometric tool sets and coordinate for an explosive detection dog to accompany the patrol. Shortly after departure, the canine scouting in front of the patrol alerts on a device, and explosive ordnance disposal triages the device and renders it safe. Military police then conduct site exploitation and collect items of evidentiary value. While the site exploitation takes place, military police and intelligence Marines conduct tactical questioning and biometric enrollments of personnel within the immediate vicinity. Once complete, the evidence is delivered to criminal investigators operating the expeditionary forensic exploitation capability. The information gleaned from the device is submitted through the intelligence portals for fusion. Multi-source reports are returned through the portal, identifying similar devices that have been used in the area and a positive match to a local national that was enrolled on the SEEK II.

Using additional local intelligence, the commander directs a raid and the detainment of the person of interest. Site exploitation of the individual's house yields additional evidence, including the cellular extraction of his phone, which reveals additional persons of interest. The MIG commander directs COMMSTRAT to work with local media to release a story on the identification of the detainment of the individual responsible for attacks. Intelligence and radio battalion personnel focus on the positive identification of the additional cell members. Commanders are provided intelligence on the threats and the tactics, techniques, and procedures to defeat similar threats. In total, the MIG commander is able to levy multiple assets to affect the enemy throughout all dimensions in the information environment.

Here is another example regarding the discovery of a mass burial site during later phases of an operation. Military police and criminal investigators can use site exploitation to collect evidence, use the expeditionary forensic exploitation capability to process the evidence collected, and access intelligence portals to ensure rapid and multi-tier intelligence fusion. The outputs from the process can confirm or deny friendly involvement. If determined that the grave was a result of enemy actions, COMMSTRAT can then use the information to develop an accurate news story to inform international and domestic audiences and influence foreign target audiences. The overarching information also adds to the commander's awareness of enemy or criminal tactics within the battlespace.

Notes

[1] 1stLt Monica Witt, "II MHG Redesignates as II MIG," (Online: 21 July 2017), available at http://www.iimef.marines.mil.

[2] Deputy Commandant for Combat Development and Integration, *Marine Corps Operating Concept for Information Operations*, (Quantico, VA: 4 February 2013).

[3] Headquarters Marine Corps, "Definition of Identity Operations," (Online: 10 February 2018), available at http://www.quantico.marines.mil.

[4] Headquarters Marine Corps, *Marine Corps Order 5530.17, Marine Corps Identity Operations*, (Washington, DC: 13 November 2012).

[5] Capabilities Development Directorate, *USMC Identity Operations Concept of Operations*, (Quantico, VA: November 2012).

[6] Capabilities Development Directorate, *MAGTF Expeditionary Forensics Exploitation Capability (EFEC)*, (Quantico, VA: 28 November 2017).

[7] Department of Defense, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, (Washington, DC: 31 October 2009).

[8] Department of Defense, *Joint Publication 3-13, Information Operations*, (Washington, DC: 27 November 2012).