

Information Management

Lessons learned from III MEF, the MCISRE, and beyond

by Maj Jonathan M. George

Imagine you are an intelligence officer checking in to III MEF G-2 in the summer of 2013, and you're excited to get your hands dirty working an important intelligence function such as targeting, collections, or fusion in the "pivot to the Pacific." You walk into the G-2's office, and he sits you down, and with a straight face, he tells you that he decided that the first officer to check in this summer was going to be the Information Management Officer (IMO) for the G-2.

When this happened to me, the wind left my sails, and, feeling somewhat dejected, I was given the task of fixing data management issues in the G-2 and the greater III MEF intelligence enterprise (IE). What I quickly learned was that the III MEF IE had disparate processes for data management and requests for information (RFIs) and standards for intelligence products. What the IE needed was a focused effort to fix these issues, and III MEF was not alone; the entire Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE) was having similar issues. What I did not know at the time was that our efforts within III MEF would later become the basis for a much larger cooperative MCISRE effort—the creation of the MCISRE knowledge gateway (MKG).

After spending a few weeks looking at the issue, it became apparent just how large this task actually was and just how resistant to change Marines were. Under the III MEF IE, the intelligence and radio battalions and each unit with an S-2 (intelligence section) managed data in different ways, storing intelligence products locally, developing their own product templates and standards, and

>Maj George is currently the S-2, 4th Marine Regiment.

managing RFIs internally. Perhaps the biggest issue facing the IE was the development of disparate and oftentimes duplicative intelligence products, and then the storage of those products on local share drives at each unit—the epitome of one of the post-9/11 criticisms of the intelligence community—the "stovepiping" of intelligence. At the MEF level, the G-2 had the same issues, with a share drive full of incoherent data and a broken RFI process. Marines were stuck in the "this is how we have always done things" mentality.

The largest hurdle to change was the MEF's desire to maintain data on a closed *intranet* SharePoint site, so the first step was to create an external portal on a secure Internet Protocol network intelink site—an interagency-accessible, web-based service with two-factor authentication. Moving outside the purview of the MEF IMO allowed the G-2 free reign to develop a collaboration portal for the MEF IE and move the data to a more stable and secure storage location. Using collaborative tools such as SharePoint, a consolidated RFI portal was created to track all intelligence production within the MEF IE. Once these products were completed, they were embedded in the RFI, and then through a process of tagging and filtering, these products could be displayed on individual unit pages, country pages, or specialized pages created for crisis or contingency operations. These

efforts ensured that relevant and up-to-date operational intelligence was organized, stored, discoverable, and lasting. Through these initiatives in the first year alone, more than 3,000 older and current products were hosted and easily searched and retrieved within III MEF as well as by anyone with access to the secure Internet Protocol router (SIPR), a tremendous resource and capability not available beforehand.

Intelligence analysts within III MEF quickly realized the power of this collaboration. Analysts were now able to see what other RFIs each unit was working with, deconflict any duplication, and start collaborating on products of mutual interest. Because of the utility and impact of these efforts, collaboration sites were quickly built on the non-secure Internet Protocol network (NIPR), Joint Worldwide Intelligence Communications System (JWICS), and even Combined Enterprise Regional Information Exchange Korea (CENTRIX-K). As III MEF is frequently tasked with humanitarian assistance/disaster relief (HA/DR) operations, a Joint Task Force 505 (JTF 505) J-2 website was also established, and it quickly proved its worth. Initially, the ability to disseminate all tactical intelligence at an unclassified level was a difficult task, but it was absolutely necessary to support HA/DR operations. The NIPR website was established during Operation DAMAYAN in 2013, where it eventually hosted more than 2,000 tailored products and images and was critical in aiding relief operations and improving the JTF commander's decision-making ability. This site also enabled the III MEF IE to immediately begin operations and easily transition back into the JTF 505



We have the ability to search for information, submit RFIs, and collaborate with others. (Photo by Cpl Adam Dublinske.)

J-2 following the Nepal earthquake in April 2015 by allowing rapid access to previous work and formats. Because of this repository, the JTF 505 J-2 was able to begin immediate intelligence support to HA/DR operations, even prior to the crisis action team. In total, it took two years to fully develop and establish all four domains, and over the course of the second year, the NIPR, SIPR, and CENTRIX-K sites were fine-tuned based on after-action reports (AARs) and lessons learned.

During this same time frame, the MCISRE was developing an understanding of and solutions to the same issues noted above but on a much larger scale. If we were truly to become an enterprise, we needed do a better job of collaboration and data sharing. Using the III MEF construct as a baseline, and with access to greater resources, the MEFs, Marine Forces, Marine Corps Intelligence Activity, and HQMC Intelligence Department embarked on a plan to professionalize and mature how we collaborate and manage the vast amount of intelligence production requirements created on a daily basis within the MCISRE. Starting once again on the main warfighting domain of SIPR, the MKG was born.

According to MCIA's Knowledge Management Office,

The MKG is the result of extensive collaboration by representatives from MCISRE Fixed Site, MEF G2 staff, MAGTF Intelligence Centers (MICs), MSCs, and forward deployed MAGTF units. The MKG incorporated shared methods, best practices, and agreed upon solutions to provide a centralized library for submission, management, exposure, and discovery of RFIs and products in order to improve enterprise knowledge management and information sharing efficiencies. The MKG is based on unprecedented agreement across the enterprise regarding standard MCISRE processes & metadata.

The MKG is leaps and bounds above where the MCISRE was several years ago in terms of professionalizing the Marine Corps' IE. An analyst, or anyone with SIPR access for that matter, can go to the MKG and search for products, submit an RFI, and collaborate. Since its inception in 2016 with 567 users across the three MEFs, the MKG has grown exponentially, with 15,893 users spread across the entire MCISRE and intelligence community as of June 2018. However, there is still progress to be made. Even with metadata, searching for products can be cumbersome, and naming conventions are not enforced, making the MKG a better-organized share drive. In addition, the MKG is

only as good as the products being uploaded, so to be a true MKG, every unit producing intelligence products must upload those products for the benefit of the entire enterprise—and while this cannot be tasked, it must become institutionalized within the Marine Corps. All of the accomplishments achieved to date with the MKG have been done without a policy, directive, or tasking; the MKG does not solve the local unit data management issues, so this requires IMOs at each unit to force data management policies and best practices.

In addition to the current capabilities outlined above, there are ongoing discussions with MKG stakeholders about how this platform and online community can be leveraged to promote the sharing of professional knowledge, training materials, best practices, and AARs for the MCISRE. Imagine being a new billet holder within an intelligence section and being able to easily access not only products and RFIs that have been previously shared but also examples from doctrinal references, related AARs, and best practices from previous billet holders. This type of persistent learning environment is within reach now and will bring us closer to becoming the type of “learning organization” envisioned by our leadership.

All of the above revolves around making the MCISRE a better enterprise, truly collaborating and sharing data, and making the community more efficient. Now imagine: What if there were a Marine Corps aviation enterprise where the community collaborated and shared products and best practices? Or perhaps a Marine Corps infantry enterprise gateway where units shared tactics, techniques, and procedures, AARs, mission briefs, and lessons learned? What if there were a Marine Corps logistics gateway that shared the above and included convoy briefs and counter-remote-controlled IED electronic warfare system loads for the same area of operations you were about to take over? Best practices learned from III MEF and the MKG can be applied across the Marine Corps to enhance collaboration, reduce redundancy, increase knowledge, and make us all better warfighters.

