OSINT

It's not a dirty word

by Capt Benjamin Siegel

>Capt Siegel is a Company Commander, 1st Intelligence Battalion Camp, Camp Pendleton, CA.

Leaning forward across the table, looking frankly at the reporter of Rossiya-1 news, Russian President Vladimir Putin asserted, "I can tell you outright and unequivocally that there are no Russian troops in Ukraine."[1] Of course, he was lying. But as a former KGB agent and master propagandist, he cast enough doubt to the international community, and more importantly, the European Union, that going to war with Russia was not worth the possibility that Putin was telling the truth. He made this statement on 16 April 2015 on "Direct Line," an annual broadcast with the Russian Prime Minister, live on Channel One, Rossiya-1, and Rossiya-24 TV channels as well as Mayak, Vesti FM, and Radio Rossii radio stations. Meanwhile, Vice News reporter Simon Ostrovsky was not only convinced otherwise, he proved Russia had invaded using social media, terrain analysis, and talking with the locals. Ostrovsky confronted Alexander Hug, Deputy Chief Monitor, Organization for Security and Co-operation in Europe, on the spot in Ukraine, asking him if Russian soldiers had invaded. He replied with, "To draw a conclusion that these uniformed carriers are actually servicemen from another country is not for me to conclude." Ostrovsky and the Atlantic Council used open-source information and social media to prove something the European Union's overt Office for Security and Co-operation in Europe could not, that Russian forces had invaded Ukraine. This ingenuity and powerful display of open-source information gathering is evidence that the Marine Corps must leverage this powerful information just as we expect every Marine to gather information to answer intelligence requirements.

Unfortunately, as soon as open-source intelligence was coined as one of the "five intelligence disciplines," the U.S. Congress, intelligence community, and Department of Defense immediately began regulating it. Figure 1 illustrates the *9/11 Commission Report*'s recommendation to create a "new" open-source agency under the direction and authority of the Director, Central Intelligence Agency (DCIA).[3] Since then, the Government started instituting executive orders, policies, directives, and even a Marine Corps reference publication to figure out how to draw lanes in the road of open-source "authorities." This article will present reasons why open-source intelligence (OSINT) should remain as deregulated as possible in order to maximize information available to non-intelligence Marines. The intent and purpose of OSINT is to exploit information using the least intrusive means possible, thereby empowering small unit leaders to conduct their own intelligence gathering.

Even before I finish laying out my proposals, two camps of readers will likely emerge. The first is the smug intelligence professional with some familiarity in OSINT, and the second is everyone else who has a hopeful optimism that they can do something about battlefield uncertainty. I believe the reason for this divergence is in the functional management design of Executive Order 12333, the National Security Act of 1947, and Title 50 United States Code. The presidential document, last amended by President Barack Obama in 2008, effectively breaks intelligence into five disciplines or stovepipes under functional managers. In the order of management in the document, the intelligence disciplines are: signals intelligence (SIGINT), managed by the National Security Agency Director; human intelligence

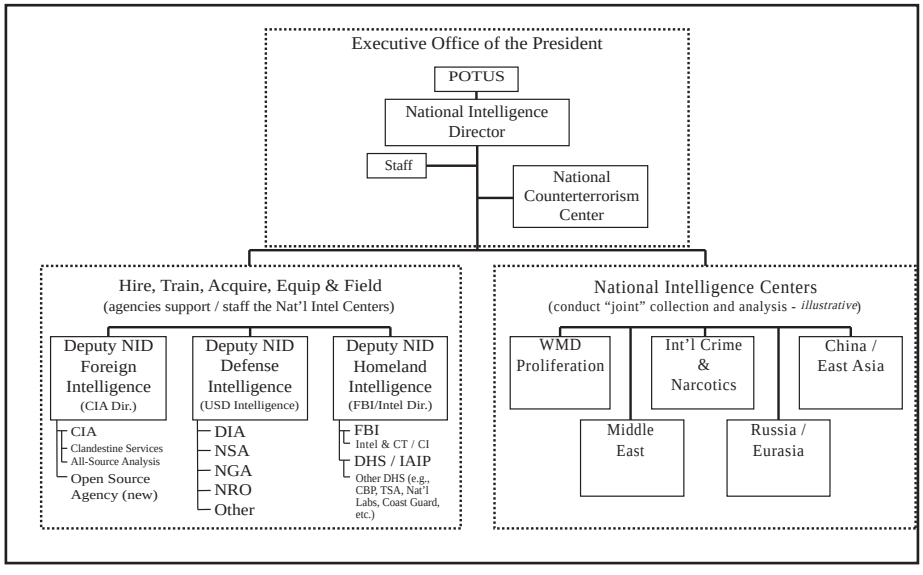

Figure 1. Unity of effort in managing intelligence.

(HUMINT), managed by the DCIA; geospatial intelligence (GEOINT), under the Director, National Geospatial Intelligence Agency; measurement and signatures intelligence (MASINT), under the Director, Defense Intelligence Agency; and open-source intelligence (OSINT), under, again, the DCIA.

In an effort to keep OSINT somewhat decentralized, the DCIA, who is also the Executive of the Open Source Committee, allowed for agencies to regulate and create sub-managers. In the DOD, the Defense Intelligence Agency manages OSINT policies, tools, and tradecraft. In the Marine Corps, the joint Marine/Army reference publication outlines restrictive guidelines that further muddy the water and seemingly prohibit the non-intelligence Marines from conducting OSINT collection. According to joint military doctrine, OSINT is intelligence based on open-source information that any member of the public can lawfully obtain by request, purchase, or observation. Although military doctrine notes that OSINT is susceptible to manipulation and deception, all intelligence disciplines are susceptible to deception to varying degrees.[4]

Consider Federal, state, and local laws under the "plain view" doctrine. This rule allows a law enforcement officer to seize evidence of a crime, without obtaining a search warrant, when that evidence is in plain sight. The purpose of both a search warrant and intelligence oversight is to prevent the U.S. Government from violating every citizen's Fourth Amendment right against unreasonable search and seizure. For example, a military police (MP) officer stops a motorist for a minor traffic violation, sees a pistol on the back seat, concludes that the driver is unlawfully in possession of the gun, and may enter the car to seize it.[5] OSINT should be treated similar to the plain-view doctrine. The open-source information the MP collected was the observation and disposition of the pistol. This OSINT tipped the MP to then gather more information in a now-established named area of interest, which is the back seat of the motorist's vehicle. The Fourth Amendment initially protected the motorist from the unreasonable search of his vehicle. However, the OSINT provided the MP with the probable cause necessary to search the vehicle. By its very nature and existence, open-source information is not protected by the Fourth Amendment and should not be treated as such, regardless of its association with a foreign entity or American citizen.

OSINT is not without its vulnerabilities. Compared to the other "INTs," or intelligence disciplines, open-source information is the most vulnerable to manipulation and deception. HUMINT is probably next in line because human sources may or may not understand they are working with the U.S. Government and may have an ulterior motive. The important distinction to make, however, is that some public sources are more susceptible to deception than others, and intelligence sources are also not immune to deception. As we will discuss later, some news outlets and journalists have a weaker reputation than others based on a lack of tradecraft. The OSINT collector must be trained in the basics of research, evaluating reliable sources, and incorporating other intelligence disciplines to increase confidence in assessments. In this context, "source" means the original location of publicly available information, either physical or digital. In *JP 1-02, Department of Defense Dictionary of Military and Associated Terms*, it is a "person, thing, or activity from which information is obtained."[6] The way journalists collect information also puts intelligence analysts at risk because they do not thoroughly evaluate the information and assess the credibility of the source based on a standardized process.

Zvi Reich, an associate professor at Ben-Gurion University of the Negev, explains that reliable sources are validated progressively less, hence the need for tradecraft and the continuous evaluation of sources.[7] In journalism, the journalist-source relationship is complicated but generally favors the source. Bob Franklin and Matt Carlson argue that this paradigm is demonstrated in the crisis of United Kingdom journalism.[8] One suspected cause of the crisis is the media's overreliance on public relations materials because "talking points" are cheap and easy to acquire. Unfortunately, these sources set the agenda for the media, resulting in a clear bias in coverage. The financial crisis of 2008 worsened budgets and working conditions for journalists and exacerbated their dependency on a few easy-to-reach sources. Ultimately, the most reliable source is the reporter or official witnessing events unfold themselves.

Operation INFEKTION is another prominent example of the vulnerability

Bato Dambaev, a soldier in the Russian army, posed for a snapshot at a battlefield checkpoint. Simon Ostrovsky, right, located the same spot in Vuhlehirsk, in Ukraine's Donetsk region, and posted the photo on Dambaev's VKontakte profile.[2]

of OSINT and how powerful state intelligence agencies can proliferate bogus information using foreign news media. In 1983, in an obscure Indian newspaper called the *Patriot*, the Soviet KGB planted a conspiracy that the United States created the AIDS pandemic. The article was written anonymously and stated that "AIDS ... is believed to be the result of the Pentagon's experiments to develop new and dangerous biological weapons."[9] The article claimed Fort Detrick, MD, discovered AIDS by analyzing samples of "highly pathogenic viruses" collected by American scientists in Africa and Latin America. Then, on 30 October 1985, the newspaper *Literaturnaya Gazeta*, the KGB's "prime conduit in the Soviet press for propaganda and disinformation," published an article by Valentin Zapevalov, titled "Panic in the West or What Is Hiding behind the Sensation Surrounding AIDS," citing the original *Patriot* article from 1983.[10] Deliberate disinformation ploys and faulty reporting requires particular care when exploiting OSINT information.

Because OSINT collection is a capability best employed by every level of command, a few analytic techniques are necessary to mitigate inaccuracy. According to *JP 2-0*, *Joint Intelligence*, OSINT requires tradecraft in the areas of research expertise and operations security for Internet-based activities. In Marine Corps and joint doctrine, the *commander* is ultimately responsible for directing the intelligence collection effort and the priority intelligence requirements (PIRs). Revealing these collection requirements on the open Internet may reveal sensitive information about our own information gaps; however, commanders must give their staff intelligence officers the authority to break these into elements for specific research questions. This could be designated in writing but should be a unique ability given to every lieutenant colonel-level commander and above.

Second, because of the disaggregated nature of Marine Corps operations and decentralized command and control, platoon and company commanders should have the ability to research their own PIRs at the unclassified level in garrison and at the level of classification required in the theater of operation. *MCWP 3-11.1, Infantry Company Operations*, states,

> In addition to those received from HHQ, company commanders need to designate their own PIRs. Company commanders should not simply restate HHQ PIRs; rather, they should determine what local PIRs best enable them to support their portion of the mission—both horizontally with adjacent units and vertically with senior and subordinate commands.

The MCWP also stresses the need for every patrol member to glean valuable information for processing back at the company combat operations center. Company commanders must also have the inherent authority and duty to collect open-source information on their future area of operation in order to aid the Marine Corps Planning Process.

Deliberate disinformation ploys and faulty reporting requires particular care.

A counterargument to the aforementioned point is that all intelligence requirements should be submitted through their respective S-2s and G-2s. I generally agree with this assertion; however, I disagree if this means waiting for the approval of OSINT collection requirements. Every Marine has the means and ability to collect open-source information at their fingertips and should not be delayed by the battalion, regiment, division, MEF, joint task force, or combatant command higher headquarters. Company operations and patrols exist in time frames of minutes and hours, not days and weeks. Open-source information is already considered "not sensitive" by public officials and should allow for expedient collection and processing. Title 50, United States Code, Section 403–5 states:

> The dissemination and use of validated open-source intelligence inherently enables information sharing since open-source intelligence is produced without the use of sensitive sources and methods. Open-source intelligence products can be shared with the American public and foreign allies because of the unclassified nature of open-source intelligence.

The third and last condition that will allow for the decentralization of OSINT collection is the establishment of standard skill sets in research, source validation, and analysis. The Director of National Intelligence published Intelligence Community Directives 203, *Analytic Standards*, and 206, *Sourcing Requirements for Disseminated Analytic Products*, to set forth rigor and excellence in intelligence analysis. Also, because of OSINT's susceptibility to deception, analysts must be able to articulate their confidence in the information, where they found it, who published it, why they published it, and their political allegiances. The three-day expeditionary OSINT course offered at the Regional Intelligence Training Centers is a step in the right direction, but it needs deeper investigative practical exercises to exploit gray literature, news media, social media, academic journals, and Open Source Enterprise (formerly Open Source Center) transliterated documents.

Finally, the Marine Corps Director of Intelligence and MEF commanders should re-evaluate their OSINT policies to encourage a climate of "every Marine a collector" rather than the idea that only those with the "authority" can do this. According to LtCol Matthew Reiley and then-LtCol William Wilburn,

> Each MEF's garrison communications infrastructure was not built or resourced to perform these [OSINT] functions. Foremost among the shortfalls are communications pipes sufficient to perform GEOINT, SIGINT, and OSINT production and analysis.[11]

While GEOINT data requires significant storage space, OSINT data collection, analysis, and production could be carried out through humble Internet speeds at the company level and above. Furthermore, each command could contract high-speed commercial Internet yearly at marginal financial cost.

In conclusion, Marine Corps culture and doctrine encourages a bias for action, mission-type orders, and decentralization, yet our OSINT apparatus is centralized at the three-star level. We need to increase innovation, opportunity, access to data and tools, education, and OSINT authorization at the lowest level possible in order to keep up with the demands of the 21st century and support the MCISRE with as many small unit, non-intelligence leaders as possible. A company commander has the inherent responsibility to send his Marines on patrol in hostile and unfamiliar territory, yet they are hesitant to research publicly available information on the open Internet. It is time to change this paradigm.

Notes

1. "Direct Line with Vladimir Putin," *The Kremlin*, (Online: 16 April 2015), available at http://en.kremlin.ru.

2. Vice News, "Selfie Soldiers: Russia Checks in to Ukraine," YouTube video, (Online: 16 June 2015), available at https://www.youtube.com.

3. U.S. Government 9/11 Commission, *The 9/11 Commission Report*, (Washington, DC), available at https://www.9-11commission.gov.

4. U.S. Joint Force Command, *Joint Publication 2-0, Joint Intelligence,* (Washington, DC: 2014).

5. Cornell University, "Plain View Doctrine," available at https://www.law.cornell.edu.

6. Joint Staff, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms,* (Washington, DC: 15 February 2016).

7. Zvi Reich, "Source Credibility as a Journalistic Work Tool," in *Journalists, Sources, and Credibility: New Perspectives,* (New York, NY: Routledge, 2011).

8. Matt Carlson and Bob Franklin, "Whither Anonymity? Journalism and Unnamed Sources in a Changing Media Environment," in *Journalists, Sources, and Credibility: New Perspectives*, (New York, NY: Routledge, 2011).

9. Thomas Boghardt, "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence*, (Washington, DC: December 2009), available at https://www.cia.gov.

10. Oleg Kalugin, *The First Directorate: My 32 Years in Intelligence and Espionage against the West,* (New York: St. Martin's Press, 1994).

11. LtCols Matthew A. Reiley, USMC(Ret), and William T. Wilburn, "Operationalizing the MAGTF Intelligence Center (MIC): A way to support garrison and Operating Forces," *Marine Corps Gazette*, (Quantico, VA: December 2015).

The LtGen Bernard E. "Mick" Trainor
Military Writing Award

The Lieutenant General Bernard E. Trainor writing contest invites papers that propose an innovative solution to one of the warfighting challenges that the Marine Corps will face in the future operating environment where "controlling physical terrain is no longer a sufficient condition for battlefield success" and under "conditions in which 'to be detected is to be targeted is to be killed."

2000 to 2500 words

The *Marine Corps Gazette* Writer's Guidelines may be found at
https://www.mca-marines.org/gazette/writers-guidelines

Deadline | 30 Oct 2018

$1000 and a commemorative plaque shall be presented to the winner of the contest . The winning essay will also be published in the *Marine Corps Gazette.*

Presented by
The 1st Reconnaissance Battalion Association, The Marine Corps Association & Foundation, and the *Marine Corps Gazette* in honor of a lifetime of exceptional military service and journalistic excellence.

MARINE CORPS
ASSOCIATION & FOUNDATION
EST 1913