Running head: TOO MUCH INFORMATION

Too Much Information:

Conquering Open Source Intelligence Would Help Drive the CNO's Strategy

Word count: 2,178

By 2020, there will be 50 billion connected devices globally and 44 trillion GB of data (Reuser's Information Services, 2019). That’s a ton of useful open-source information the U.S. Navy is poised to miss out on. And if the Navy’s intelligence apparatus is going to meet the intent in the Chief of Naval Operations’ *Design for Maintaining Maritime Superiority 2.0*, it better prioritize how to exploit the relevant portion of that information, and fast.

The type of machine-learning technology that can assist with such voluminous data is emerging, and the demand signal for private contractors to identify and process this information has never been louder. But as the entire United States Intelligence Community grapples with the big bang that is the current generation of Open Source Information, the U.S. Navy should exploit the opportunity amid the chaos and become the first military branch to make the art of analyzing such information a specialty. That is – it should create a Navy Enlisted Classification Code (NEC) designating certified Intelligence Specialists as OSINT (Open Source Intelligence) Analysts. This would not only increase overall intelligence depth, it would clearly support the CNO’s vision.

Why an Enlisted Classification Code?

Navy Enlisted Classification Codes (NECs) identify a skill set that is not prevalent throughout the entire rating, and then teaches and documents that skill so qualified sailors may then be assigned to those billets requiring that specific skill. For example, the NEC of a Navy Imagery Intelligence (IMINT) analyst is K10A (U. S. Navy, 2019). Any command requiring imagery analysis draws from sailors carrying that specific K10A NEC. An OSINT NEC would enable the identification, training, and designation of qualified OSINT analysts for assignment throughout the force. These billets would reside at watch floors, Carrier Strike Groups, Amphibious Ready Groups, Navy Information Operations Commands, Navy Expeditionary

Intelligence Command, and applicable Naval Special Warfare Groups, Explosive Ordnance Disposal Groups, and Seabee Battalions.

Although OSINT analytic capability currently exists at many locations where U.S. Navy intelligence is present, support in a Joint environment only skims the surface of the useful information available to the Navy war fighter. The Joint Air Force analyst sitting the OSINT desk knows as much about the undersea environment as the Army analyst knows about piracy in the Gulf of Guinea. Adding Navy OSINT specialists to this mix would not add a redundant layer, because the Navy operates in every war fighting domain. There is simply so much information of interest to the U.S. Navy that there isn't enough time for a Navy analyst to spend any resources on the intelligence requirements of other branches.

It's Time to Prioritize OSINT

According to Public Law 109-163, OSINT is "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (Department of the Army, 2018). OSINT overlaps with every other major intelligence discipline, including HUMINT, SIGINT, IMINT, and MASINT – three of which already have NECs in the Navy – and it also supports Counterintelligence (Williams & Blum, 2018). A Navy NEC holder could not be confused with other analysts who occasionally research open sources – that is simply research. An OSINT analyst uses specific techniques to exploit open sources to answer requirements (Department of the Army, 2018).

An OSINT NEC would establish another layer of credibility to the craft. Whereas historical criticism of OSINT has dismissed it because of its lack of a classified status, modern OSINT also suffers from an identity crisis. Critics either don't understand social media, or carry a bias against it because of trends like “fake news” and state misinformation campaigns. The mission of the OSINT analyst is not to propagate uncorroborated items off the bathroom wall that is Twitter – it is instead to discover items that answer requirements and validate them against other information, thus turning information into an intelligence assessment. An established OSINT analyst understands the strategic, operational, and tactical levels of intelligence, and how effects in each have implications on the others. Because world news and events are uninterrupted – unlike source meets, overhead collection passes, and weather effects – the OSINT analyst is constantly feeding the intelligence cycle.

In truth, the Navy has the opportunity to use an OSINT NEC to build a legitimate “all-source” analyst. The OSINT curriculum could allow for not only the teaching of the skill set, but collaboration with other disciplines. The OSINT students should learn the context of how their craft supports other collection, but also observe other students during their capstone evolutions as they become certified in their respective areas of HUMINT and IMINT, to name a few. If OSINT candidates were restricted to sailors with at least two tours and one NEC under their belts, the Navy would be able to invest in a relatively seasoned analyst during the prime of their career, and build them into an all-source expert they could billet to a minimum of two immediate follow-on tours overseas and on shore. This would not only satisfy the demand for OSINT capability, it would increase valuable expertise in the senior enlisted intelligence ranks while satisfying today’s generation of hungry, educated, self-starting intelligence specialists looking for added value to their work. In reviewing the Chief of Naval Operations’ *Design for Maintaining Maritime Superiority 2.0*, the requirements are steep, and the analyst just described is the exactly the high level Navy Intelligence needs to operate at if it is to answer the CNO’s challenge.

OSINT Enhances the CNO's Four Lines of Effort

The establishment of a new OSINT NEC would standardize the means by which the Navy collects information from the public domain, and it would enhance Navy analysts' contribution to the CNO's four Lines of Effort (LOE). A robust, reliable OSINT engine would, "strengthen Naval Power at and from the Sea" by bolstering baseline knowledge of every area of operations and refining the complementary manner in which other intelligence assets are employed (Richardson, 2016). Because the OSINT cycle is continuous and independent of collection requests and limitations such as sensor placement and overhead availability, this analysis would occur on shore or on deployment. An OSINT specialist would constantly update living knowledge bases used to develop port assessments, foreign cultures, strategic implications of Navy operations, and handle daily requests for information on emerging events such as natural disasters, indications and warnings, and trends. An OSINT analyst never sees the same watch twice. Today's North Korean missile launch amidst an Allied exercise becomes tomorrow's Hong Kong protest during a port call. There is no Powerpoint template for the value the OSINT analyst brings to the fight. Their timely, relevant analysis would make the Navy smarter daily – not just in response to events or briefings – and that is how collective "strengthening" occurs.

Given the bottomless trove of publically available data and activity, an OSINT analyst never suffers the inconvenience of a classified system outage or a shortage of sources. With so much information available, an analyst would only be limited by time and the speed of their fingers. An NEC-granting course that taught analysts how to process vast amounts of data in a time-sensitive situation would provide the type of "high velocity outcome" listed as the CNO's second LOE. Major events and crises unfold faster than most intelligence collection assets can collect and process, but indications and warnings can be collected by an OSINT analyst as the scene unfolds. Getting the five Ws of the event and even an assessment to a Skipper can be accomplished in minutes. One famous example of such a sequence was presented by former DIA Director Lt. Gen Vincent Stewart, who told an audience at an intelligence dinner that agency analysts once learned of a missile launch in Yemen from Twitter instead of its acclaimed Space-Based Infrared System. Following the Tweet, national assets were re-tasked to search for more information (Clark, 2015). The same can be said for merchant ships hijacked on the high seas. Anomalies in their movements are often discovered and publicized long before the captain initiates a distress call. This information should not be relegated to the discretion of analysts from other service branches.

The CNO's third LOE is a call to "Strengthen our Navy Team for the Future" by means of modernizing ratings and taking advantage of emerging technologies and commercially available platforms. This is the foundation of an OSINT analyst's capability. While OSINT, as a discipline, has been around since World War II, it has already matured from a system of reading newspapers and recording TV and radio news casts to a high-speed digital landscape of social media, networks, and blogging. While commercial software platforms exist to assist analysts in processing volumes of data, an OSINT NEC would mitigate the unpredictable ups and downs of those platforms by teaching actual OSINT skills applicable across the entire spectrum – not whichever application was contracted (Williams & Blum, 2018). Because OSINT analysts would be built during the primes of their careers, the return on investment would be immediate and enduring well into the future. Additionally, the amount of intelligence expertise the OSINT NEC would build into the senior enlisted ranks would help decision makers think outside the box when it comes to the future of the intelligence corps.

In the intelligence community, nothing builds a partnership faster than sharing good information. An OSINT NEC would help the Navy “Expand and Strengthen Our Network of Partners” in agreement with the CNO’s fourth LOE. This is proven by the success of the Navy’s long-running International Maritime Intelligence Course, an entirely unclassified course that brings in foreign intelligence officers from around the world to be trained by U.S. Navy Intelligence personnel (Rumsey, 2018). The U.S. Navy trains more forces in more counties than any other entity, and it pays to have those personnel smart on a region’s culture, norms, and political climate prior to these events. A well-trained OSINT analyst could provide real-time social media monitoring to these and other operations to detect unrest, popular or unpopular sentiment, and indications and warnings to include threats – and in extreme cases – possible compromise of sensitive missions. They are also value added to intelligence exchange programs and key leader engagements in Foreign Internal Defense missions. In other cases, OSINT analysts have supported major information operations campaigns, simply by acting as conduits between forward-deployed expeditionary units and Allied partners.

Making a Navy OSINT Analyst

Accomplished OSINT analysts attack their priority intelligence requirements using the context of previous military operations and a deep understanding of the area. OSINT analysts convert information to intelligence, but they also convert knowledge to understanding. For this reason, an OSINT NEC should only be available to analysts on their third tour and beyond. Because their work directly benefits from their accumulated knowledge of the area, each tour should come with the option to extend for one year. There are dozens of jobs available online for OSINT analysts, but these jobs should be filled by hungry Navy analysts who have the appropriate experience and don’t mind standing a 12-plus-hour watch. Because OSINT relies on publically available information and can be conducted virtually anywhere if the right security precautions are observed, the NEC-granting course does not have to be relegated to sensitive spaces. Additionally, because of the nature of the course, the capstone would not need to be a "canned" scenario; rather, it could take place in real time because students have access to the exact same platforms and applications they would have on the job at any unit. This would also enable the course to "keep current" without the need to make painstaking administrative updates to course documentation any time the technology changes.

There are other challenges associated with OSINT collection, but they can be rectified by using the NEC process. For example, sensitivities exist when an OSINT analyst coincidentally comes across a U.S. person in their work. While governed by EO 12333, there are still concerns for possible fraudulent use of any programs (Williams & Blum, 2018). Additionally, protection for the analyst and their unit is also paramount, as some analysts may be tempted to use their capabilities in an environment where they are compromising signals or putting themselves at risk. One benefit, though, of an NEC is the ability to track all NEC holders, and the authorization to remove that NEC in the case of misuse. Any OSINT NEC holder would agree to several caveats, including the removal of the NEC if they misuse permissions, or the removal of the systems access if the analyst does not perform the job over a determined timeframe.

Conclusion

The job of the U.S. Navy Intelligence Specialist is to "own" enemy (red) forces – top to bottom, front to back, port to starboard. If the intelligence rating is to truly "own red," and to truly modernize in support of the CNO's Lines of Effort, OSINT is the way to do it. And because this generation of OSINT is still so immature throughout the greater intelligence community, the Navy could blaze a trail on its own terms, and meet the Skipper's intent in the process.

References

Clark, C. (2015, July 31). *New Intel Era: Tweet Alerts DIA To SCUD Launch, Not Spy Sats*. Retrieved July 21, 2019, from Breaking Defense: https://breakingdefense.com/2015/07/new-intel-era-tweet-alerts-dia-to-scud-launch-not-spy-sats/

Department of the Army. (2018, September). *ADP-20.* Retrieved from U.S. Army Official Web Site: https://armypubs.army.mil

Reuser's Information Services. (2019, April 16). *Open Source Intelligence*. Retrieved July 20, 2019, from Reuser's Information Services: http://arnoreuser.com/

Richardson, A. J. (2016, August). *A Design for Maintaining Maritime Superiority.* Retrieved from U.S. Department of Defense: https://www.navy.mil/navydata/people/cno/Richardson/Resource/Design_2.0.pdf

Rumsey, P. (2018, October 1). *IWTC San Diego Holds International Maritime Intelligence Course Graduation, Strengthens Relationships.* Retrieved July 10, 2019, from U.S. Navy Official Web Site: https://www.navy.mil/submit/display.asp?story_id=107265

U. S. Navy. (2019, July). *NAVPERS 18068F Navy enlisted Classifications.* Retrieved from Naval Personnel Command: https://www.public.navy.mil/BUPERS-NPC/REFERENCE/NEC/NECOSVOLII/Pages/default.aspx

Williams, H. J., & Blum, L. (2018). *Defining Second Generation Open Source Intelligence for the Defense Enterprise.* Retrieved July 8, 2019, from RAND Corporation: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf