THE RISK OF NOT KNOWING: Enabling Intelligence Professionals to Leverage Publicly Available Information

by
Lieutenant
General Laura Potter
and Colonel
Christina Bembenek

War is evolving in form toward informationized warfare, and intelligent warfare is on the horizon.

—2019 Chinese Defense White Paper

We start with a fictional story…

The first indicator was the surge in false tweets about unsafe and discriminatory work conditions for Chinese workers at the Port of Seattle. Then, a human intelligence (HUMINT) analyst building a profile on a prominent Chinese officer in the People's Liberation Army sustainment force noticed a new photo album on the Chinese officer's WeChat profile that featured barren tundra with few roads and structures. She passed the images to a geospatial intelligence (GEOINT) analyst who examined the shadows and angles of the sun, which indicated a point in the Arctic. A signals intelligence (SIGINT) analyst copied phone numbers listed in the officer's WeChat profile and noticed the list included several numbers with the area code for Banks Island, Canada. Tipped by this uncommon activity in social media, all-source analysts dug further into both publicly available information (PAI) and classified databases, leading to a startling discovery—the Chinese were preparing to seize land on Banks Island in order to control a portion of the Northwest Passage. By fomenting unrest at the Port of Seattle, the Chinese were ensuring that any American effort to reinforce troops in Alaska, as well as any support to the United States from its Canadian ally, would be bogged down. The U.S. Army team collaborated with their Canadian partners by quickly sharing the unclassified PAI while they worked through classification guidance on the more sensitive details, and a combined operation began to take shape.

Introduction

Vignettes like this are possible when all intelligence professionals understand how to routinely use PAI to enrich their particular intelligence discipline and to identify indications and warnings of hostile activities. Leveraging PAI as a source of information allows insight into our adversaries' actions almost at the speed of thought, which is critical to obtaining systemic advantage. Soldiers in S-2 sections at every echelon need to analyze the threat in the information dimension of the operational environment. As the intelligence community works toward more clearly defined regulations and governance for open-source intelligence (OSINT), the U.S. Army Intelligence Center of Excellence (USAICoE), supported by the Army OSINT Office, is training our Soldiers on safe and effective ways to use PAI to fulfill commanders' intelligence requirements, which include understanding and articulating the risks.

Distinguishing between PAI and OSINT is a key concern among intelligence professionals, and admittedly, the multiple regulations and directives have left some gray areas, as outlined in Ms. Corrine Geiger's article "The Reawakening of Open-Source Intelligence."[1] Department of Defense (DoD) Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)*, allows for the use of PAI to "plan, inform, enable, execute, and support the full spectrum of DoD missions."[2] As with any intelligence activity, analysts must adhere to proper intelligence oversight procedures, as specified in DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, which ensures any collection occurs "in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons."[3] Both the intelligence community and the DoD are working on updating policies to more clearly outline authorities for working in the information dimension of today's dynamic and technologically evolving operational environment.

> "Understanding the evolving policy and regulations is important, but at the end of the day, intelligence is for commanders"

Understanding the evolving policy and regulations is important, but at the end of the day, intelligence is for commanders, and intelligence professionals must properly advise commanders on the risks inherent to using PAI for intelligence purposes. To clarify the guidance for maneuver commanders, analysts can reference ATP 2-22.9, *Open-Source Intelligence*, which outlines specific risk levels for OSINT collection. These risk levels clarify what levels of operational security risk the OSINT activity could pose to military operations. By coordinating closely with the operations teams, S-2s and G-2s can ensure their teams are prudently leveraging PAI without putting planned or ongoing operations at risk—the same assessment they would make when planning unmanned aircraft system or SIGINT collection.

Publicly Available Information Training

To assist in understanding how to leverage PAI effectively, USAICoE has developed six training modules for all intelligence series analysts on open-source research methodologies, basic workings of the internet (to understand the "tracks" analysts leave when they conduct research online), and ways to create OSINT requests for information. This training will enable analysts to understand how to think through operational security considerations and take measures to mask or safeguard their searches. They will also learn how to distinguish between general research that increases commanders' overall understanding of the operational environment and intelligence preparation for an upcoming mission. Three of the training modules are available on LandWarNet as of March 2022 via interactive multimedia instruction to all intelligence professionals, ensuring we can train the entire military intelligence force now.[4] USAICoE also began integrating the six modules into all courses at Fort Huachuca, starting with the 35F, Intelligence Analyst, and 35M, Human Intelligence Collector, Advanced Individual Training courses in February 2022.

The USAICoE instruction will emphasize that PAI is a source of information that, like any other, must be corroborated by other sources and methods. All-source analysts can validate the authenticity and credibility of a particular source of PAI through coordination with other intelligence disciplines. For example, they can leverage GEOINT or SIGINT to verify if a particular source on social media is physically located in the area the reporting is from or whether other people or journalists in the area reported on the events. Organizations like Bellingcat have developed several techniques to verify the authenticity of PAI and build detailed analytical products. Bellingcat's most famous success was the report they provided to the United Nations that definitively linked Russian forces to the shooting down of Malaysian Airlines Flight 17 over Ukraine. "In the frenzy to determine who—and what—shot down Malaysian Airlines Flight 17, a group of citizen journalists armed with simple intuition and an internet connection has been collecting information more nimbly than American spies."[5]

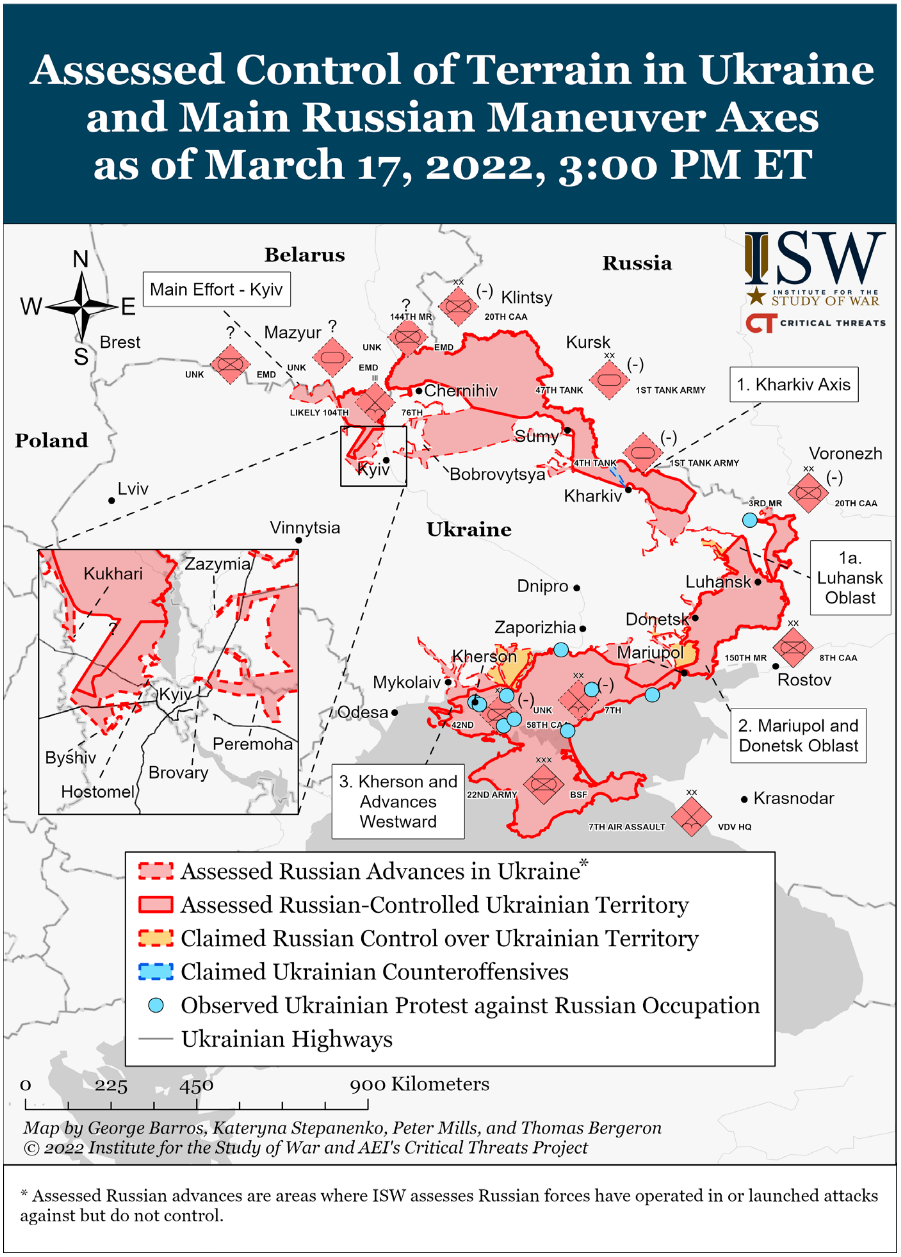
National capabilities are a finite resource. Intelligence professionals must train on how to use every source available and to use traditional analytical tradecraft to assess validity and turn information into actual intelligence. GEOINT analysts have multiple tools to analyze images and videos on the web and in social media to verify location, time of day, and image authenticity. This includes analyzing an image's digital fingerprint, using web map services to map track, or an open-source investigative tool, like the kind developed by Bellingcat, to associate a particular geographic location using Python scripts and Application Programming Interfaces.[6] HUMINT is another area that can benefit greatly from the vast quantities of data available in digital media. During World War II, Allied analysts with the Office of Strategic Services estimated Nazi casualties by reading the obituary sections of German newspapers available in Switzerland.[7] Today, HUMINT analysts can conduct similar research through digital means and then cross-reference with classified information.

In addition, PAI opens an avenue to share unclassified information with our foreign partners and collaborate on adversary assessments. Many intelligence-sharing agreements, particularly in the U.S. Indo-Pacific Command, allow only limited sharing of classified information between intelligence entities. PAI offers a means to share information quickly without compromising sources or methods. Foreign partners will also be more adept at analyzing social media and cultural nuances within their own countries as compared to most U.S. military analysts. An excellent example of this is the work done by European analysts who provide open-source information on pro-Kremlin disinformation trends, trending disinformation topics, and analytical reports on the top sources of Russian disinformation within the EU vs DISINFORMATION database.[8] Establishing routine information exchanges using PAI will help ensure U.S. intelligence professionals receive the high-quality products our foreign partners create and enable a more comprehensive and accurate understanding of the operational environment.

Assessing and Managing Risk

Accessing PAI on the internet opens up an infinite amount of information and data for analysis but also exposes individuals and units to varying levels of risk. This includes the risk that once our adversaries identify the websites where analysts are conducting research, they will begin to add false information to those sites or create a redirect to false sites. This is a valid concern because deception figures largely in both Russian and Chinese doctrine, and our adversaries are actively working to deceive many of our sensors. Like any information, analysts must use other sources and methods to determine the veracity of information.

Another potential risk is that website owners and foreign governments will identify that a U.S. military person or specific unit has accessed their information. Proper use of virtual private networks or managed attribution can lower this risk. However, even if the search is traced, foreign entities still have to analyze the information, determine their own risk calculation, and then take action. For example, if a Russian army officer is communicating on VKontakte and discovers that a United States person is accessing his information, the Russian army officer could stop using that platform—which inhibits his ability to communicate with family, friends, and fellow soldiers—or he could accept the risk.



Assessed Control of Terrain in Ukraine and Main Russian Maneuver Axes as of March 17, 2022, 3:00 PM ET

Map by George Barros, Kateryna Stepanenko, Peter Mills, and Thomas Bergeron
© 2022 Institute for the Study of War and AEI's Critical Threats Project

* Assessed Russian advances are areas where ISW assesses Russian forces have operated in or launched attacks against but do not control.

A map of the situation in Ukraine created from publicly available information by the Institute for the Study of War and AEI's Critical Threats Project. (Reprinted by permission of the Institute for the Study of War and AEI's Critical Threats Project)

Our military leaders increasingly use social media to communicate to the lowest levels, and our adversaries are collecting this information. The risk of not informing our Soldiers generally outweighs the risk of an adversary agency building a source profile. Moreover, we accept as fact that Russia and China are collecting every bit of PAI they can find about United States forces; undoubtedly, they also expect United States intelligence agencies are doing the same. By training intelligence professionals to clearly identify the risks inherent to online research and the ways to mitigate them, they can better assist commanders in deciding whether accessing PAI—or posting unit and individual information—is worth the risk of adversary collection.

Conclusion

In the current operational environment, U.S. forces will rarely be unobserved both at home and overseas. In addition to ubiquitous satellite and unmanned sensors, social media provides near real-time reporting on human activity. Russian and Chinese doctrine is explicit about the importance of gathering information, particularly in cyberspace, to track adversaries. If we are to actively campaign in competition, we must train our intelligence professionals to leverage every source of information available to understand our enemy's activities and intentions. Army intelligence has the benefit of truly exquisite, classified collection capabilities, but PAI is a valuable starting point for all intelligence disciplines, as well as a means to answer commander's information requirements. There will always be a risk to using open-source information, but training all intelligence professionals to safely and effectively leverage PAI provides us an advantage in this exceptionally competitive space that outweighs the risk of not knowing.

Acknowledgment

The map on page 5 titled "Assessed Control of Terrain in Ukraine and Main Russian Maneuver Axes as of March 17, 2022, 3:00 PM ET" is reprinted by permission of the copyright holder, the Institute for the Study of War and AEI's Critical Threats Project, https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-march-17.

Epigraph

The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing, July 2019), 7, http://www.andrewerickson.com/wp-content/uploads/2019/07/China-Defense-White-Paper_2019_English.doc.

Endnotes

1. Corrine Geiger, "The Reawakening of Open-Source Intelligence," *Military Intelligence Professional Bulletin* 48, no. 1, n.d. This article provides a full discussion on the differences between publicly available information and open-source intelligence.

2. Department of Defense Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)* (Washington, DC, June 11, 2019, incorporating Change 1, August 20, 2020), 3.

3. Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC, August 8, 2016), 1.

4. "Publicly Available Information," Learning Innovation Branch, LandWarNet eUniversity, last updated 20 February 2022, https://libicoe.army.mil/products/pai (common access card login required).

5. Lorenzo Franceschi-Bicchierai, "The Group of Bloggers Unearthing MH17 Intel Quicker Than U.S. Spies," Mashable, July 23, 2014, https://mashable.com/archive/citizen-journalists-mh17-spies.

6. "Help Bellingcat Build Tools For Open Source Investigators!" Bellingcat, July 6, 2021, https://www.bellingcat.com/resources/2021/07/06/help-bellingcat-build-tools-for-open-source-investigators/.

7. P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2018).

8. EU vs DISINFORMATION, accessed 16 March 2022, https://euvsdisinfo.eu.

LTG Laura Potter is the Deputy Chief of Staff for Intelligence (G-2) of the U.S. Army. Previously, she was the commanding general of the U.S. Army Intelligence Center of Excellence and Fort Huachuca. LTG Potter has served in multiple intelligence positions at the tactical, operational, and strategic levels. She is a Distinguished Military Graduate of Dickinson College, Carlisle, PA, where she received a bachelor's degree in Russian and Spanish. She holds a master's degree from Georgetown University's School of Foreign Service, Center for Eurasian, Russian, and East European Studies, and a master's degree in national security and strategic studies from the Naval War College.

COL Christina Bembenek is the Commandant for the U.S. Army Intelligence School at Fort Huachuca, AZ. She previously served as the 82nd Airborne Division G-2 and in multiple intelligence positions at the tactical, operational, and strategic levels.