Open-Source Intelligence in the 82nd Airborne Division G-2

Sergeant Christian Torres

Creating an OSINT Cell at the Division Level

In February 2021, the 82nd Airborne Division's G-2 began operating its first open-source intelligence (OSINT) cell. In establishing the cell, the 82nd G-2 fulfilled all the crucial requirements of the Army OSINT Office and U.S. Army Forces Command (FORSCOM). Specifically, it—

- Staffed positions with analysts who had completed the basic OSINT courses (OS 301 and 302).
- Obtained authority to conduct OSINT research.
- Established risk assessments.
- Created collection plans.

Instead of using all-source analysts, the 82nd Airborne Division chose a signals intelligence (SIGINT) analyst and a geospatial intelligence (GEOINT) imagery analyst as the first members of the team. Having Soldiers with diverse technical backgrounds enables the analysis of different types of publicly available information (PAI) and allows for better-informed tipping of other intelligence capabilities. As a GEOINT analyst, I have analyzed publicly available geospatial data, tipped our GEOINT cell, and structured a request for information to best capitalize on this type of PAI. The OSINT cell also receives weekly assistance from a contracted FORSCOM OSINT analyst whose subject matter expertise provides the G-2 staff with the ability to identify information about OSINT best practices, understand the legal space of OSINT, and help ensure proper legal procedure.

Over the past 11 months, the 82nd Airborne Division G-2 OSINT cell has expanded by adding two Soldiers. In addition to certifying the training our new OSINT analysts received in OS 301 and 302, we also began providing additional training that reflects some of our lessons learned. OS 301 and 302 provide a solid basis for Soldiers and teach that creativity is one of the best tools an OSINT analyst can have because they broaden the type of information analysts think about collecting. What we learned over time is that creativity in OSINT is critically dependent on the quantity and quality of knowledge that analysts possess. The OSINT cell can easily facilitate an increase in knowledge by providing experience and reading material. Unlike any other intelligence discipline, OSINT has many learning resources. The real challenge is teaching analysts how to differentiate between what is important and what is not.

Lessons from *Lawrence of Arabia*

For junior military intelligence Soldiers, too much focus is often on surface-level matters. A GEOINT analyst may fixate on the arrival or departure of a specific piece of equipment, a SIGINT analyst may look at an individual frequency or selector, and an all-source analyst may try to find and accumulate reports to support a single theory. These may lack a deeper analysis—asking the "so what?" For OSINT, this can be an even greater pitfall because of the vast amount of publicly available data. Reading hundreds of news articles in a week may cause information overload that makes finding what is important impossible because PAI is, by itself, often unremarkable. It is only through the aggregation, contextualization, and interpretation of PAI that our minds can process it into information of value. The OSINT analyst must go a step further and take a wide breadth of historical knowledge to fuse the rendered PAI and make it into information of intelligence value.

The movie *Lawrence of Arabia*, a historical drama based on the life of T. E. Lawrence, demonstrates relating PAI with context. Lawrence was a British archaeological scholar, military strategist, and author best known for his legendary war activities in the Middle East during World War I. Early in the movie, he receives an Egyptian newspaper to read the local headlines. As he expected, he reads that Arab tribes were attacking Turkish strongholds, to which he remarks, "I bet that no one in this headquarters even knows it happened. Or would care if it did."[1] Lawrence, using his background as a Middle East scholar and having a desire to find information, was able to identify key PAI that was important for decision makers. In the case of Lawrence, he went deeper in his analysis by identifying the Arab tribes' attacks as an indicator of escalation. This inherently made Arabia a crucial factor in the battlespace, which others had not fully realized. He did not just look at what had happened (in this case, an Arab tribe attacked Turkish forces), but he also looked at what the event meant. He saw there was an additional element, a new player, in the fight against the Ottoman Empire. It was in his later missions that he was able to find a way to capitalize on those indicators because he personally understood the motivations of the Arab tribes. Lawrence was able to do this because he applied strategic thinking—the act of taking background knowledge and weighing it against desired outcomes for an overarching purpose—to the knowledge he already had.

National Library of Norway, Public domain, via Wikimedia Commons

T.E. Lawrence in traditional Arab robes during the World War I and the period of the Arab Revolt.

Applying Game Theory Concepts to OSINT

For our OSINT cell, the way we teach strategic thinking is by teaching and discussing game theory. Simply put, game theory is a theoretical framework of decision making that divides people into "players" as part of a "game." The games can range from economics and evolutionary biology to warfare. Regardless of the player, game theory considers all players as "rational agents." Being rational means players will always seek to make a decision to optimize the yields of their actions. In other words, people will do whatever they think is in their best interest. Examples of this are the prisoner's dilemma and the dictator game.

Game Theory

Game theory is a branch of applied mathematics that provides tools for analyzing situations in which parties, called players, make decisions that are interdependent. This interdependence causes each player to consider the other player's possible decisions, or strategies, in formulating strategy. A solution to a game describes the optimal decisions of the players, who may have similar, opposed, or mixed interests, and the outcomes that may result from these decisions.[2]

Prisoner's Dilemma

American mathematician Albert W. Tucker originally formulated the prisoner's dilemma. Two prisoners, A and B, suspected of committing a robbery together, are isolated and urged to confess. Each is concerned only with getting the shortest possible prison sentence for himself; each must decide whether to confess without knowing his partner's decision. Both prisoners, however, know the consequences of their decisions: (1) if both confess, both go to jail for five years; (2) if neither confesses, both go to jail for one year (for carrying concealed weapons); and (3) if one confesses while the other does not, the confessor goes free (for turning state's evidence) and the silent one goes to jail for 20 years.[3]

The Dictator Game

In the dictator game, the first player, "the proposer," determines an allocation (split) of some endowment (such as a cash prize). The second player, the "responder," simply receives the remainder of the endowment not allocated by the proposer to himself. The responder's role is entirely passive (he has no strategic input into the outcome of the game). As a result, the dictator game is not formally a game at all (as the term is used in game theory). To be a game, every player's outcome must depend on the actions of at least some others. Since the proposer's outcome depends only on his own actions, this situation is one of decision theory and not game theory. Despite this formal point, the name persists in the game theory literature because of the result's usefulness to game theory at large.[4]

Game theory provides the OSINT analyst a structuralized analytical tool to enable finding the "so-what." In our OSINT section, we do this by making a key part of research to investigate the motivations of the actors, identifying factors the "rational agents" will consider. OSINT is particularly well suited for this. With military intelligence naturally focusing through a military lens, an OSINT analyst can step away from this to investigate PAI and examine what an adversary might

be doing in the information environment. Instead of trying to see what kind of capabilities or maneuvers adversaries are concerned with, which is the subject matter other intelligence disciplines focus on, the OSINT analyst is more easily able to see what the adversary's grand strategy might be.

For example, if Country Y begins to withdraw from Country X, this may signal to other intelligence disciplines the end of further escalations, but the OSINT analyst might be able to find economic or political factors indicating inevitable further escalation from Country Y. The OSINT analyst may be able to provide critical awareness that, while immediate concerns have diminished, the threat picture from Country Y has only slightly changed. In another scenario, the amassing of Country Y's forces onto Country X's border may indicate imminent war, but the OSINT analyst might find that Country Y's current dictator is amassing forces to bolster votes in an upcoming election, and that while still possible, Country X is not truly seeking all-out war. In both cases, a grasp of game theory coupled with an OSINT analyst's knowledge facilitates deeper analysis. It is by teaching game theory that we can reliably achieve deeper analysis.

In the G-2 OSINT cell, when looking at a piece of information, we routinely ask our Soldiers, "What does game theory say?" We do this to ensure we are consistently applying analysis to our collection. It forces us to apply a structuralized method of reasoning that makes us collect as much information as possible, analyze the likely courses of action, and assess the data we have. By identifying what an adversary thinks is in their best interest, i.e., how they would best win their "game," we can identify likely courses of action. Since the 82nd Airborne Division serves as America's immediate response force, it is crucial that our research drive our intelligence assessments. Game theory helps our OSINT team digest the data we collect, determine its importance, and make quality OSINT products while we monitor for emergent threats.

> **When you strip away the genre differences and the technological complexities, all games share four defining traits: a goal, rules, a feedback system, and voluntary participation.[5]**
>
> **—Jane McGonigal, American game designer and author**

OSINT Products

In the year since our OSINT cell's inception, we have been able to provide a wide range of OSINT products. Typically, we provide a biweekly summary of major events in the world that could have an impact on the immediate response force. The OSINT cell disseminates this to leadership throughout the 82nd Airborne Division. When major events occur with the potential to trigger an immediate response force deployment, we often provide sentiment analysis to give decision makers an understanding of not only the events but also foreign nationals' reactions.

The OSINT cell also created a coronavirus disease 2019 (COVID-19) hotspot tracker to monitor the impacts of COVID-19 and its subsequent variants. We were able to set up a system to identify how serious an increase of infection was for a specific country. By researching different business statics formulas, we have found ways to see how COVID-19 affects a given country in ways that more accurately captures the growth of cases than merely looking at the daily infection increase. We then used other forms of PAI to assess what response we might see from that country. My own background as a GEOINT analyst helped with this because I was able to take publicly available graphic information system data, also known as GIS data, and combine it with our findings to turn it into a map visually depicting what we found. Prevalence of COVID-19 in any given country is a critical limiting factor to decision making strategies, and PAI is well suited for this kind of collection.

OSINT during Operation Allies Refuge

When the immediate response force was activated to support Operation Allies Refuge, the recent noncombatant evacuation operation in Afghanistan, we had the opportunity to fully test our OSINT capabilities in a real-world scenario. The operation proved to be atypical from most stories one hears about OSINT. The most well-known stories involve an OSINT team that, through creativity and perseverance, found where the "bad guys" were, resulting in clear and decisive action. The reality of Operation Allies Refuge was that our primary mission was to provide the safe evacuation of personnel. The Taliban were providing security around the perimeter of Afghanistan's Hamid Karzai International Airport and throughout Kabul. OSINT collection on the Islamic State–Khorasan Province, also known as ISIS–K, was limited because of the rapid and asymmetric way the group operates. However, the OSINT cell was able to determine how members of the group had attacked in the past and provided situational awareness after major ISIS–K events. The one thing we could do was monitor the information space in Kabul—a wide net to cast. Our primary focus in supporting elements on the ground was monitoring sentiment for potential civil unrest leading to breaches of the perimeter around the airport. Although

we looked for indicators and warnings of future attacks, the biggest threat was from an unruly crowd. This consisted of monitoring an array of public feeds from social media and the news.

OSINT was useful in helping limit the effects of selection bias during Operation Allies Refuge. In numerous instances, we had to dispel or qualify sensationalist PAI. The prevalence of people using sensational PAI likely had to do with our reliance on intelligence products. When other intelligence disciplines create reports, a trained analyst vets the reports. When the intelligence community makes an assessment, one generally has confidence in the corresponding report. This in turn creates an odd effect by which some people may treat raw PAI reporting (i.e., news reports and social media posts) with the same confidence as an intelligence report. Compounding this effect is the nature of the internet, which often gives users information comparable to what they have recently seen. A person looking at PAI, whether it is the news or their own social media feed, can easily get a warped perception of people's sentiments, especially in a rapidly developing, emotionally charged event like Operation Allies Refuge. Our OSINT team helped serve as a preventive and corrective measure against biases and echo chambers.

U.S. Air Force photo by A1C Jade Dubiel

U.S. Army Soldiers assigned to the 82nd Airborne Division, Pope Army Airfield, NC, receive a brief before heading to board a C-17 Globemaster III at Joint Base Charleston, SC, August 14, 2021. The 82nd Soldiers deployed to the Middle East as part of the immediate response force activation to help provide for the safe and secure movement of United States citizens, Special Immigration Visa recipients, and vulnerable Afghan populations from Afghanistan.

Casting a Wide Net for Collection

While there are instances of finding "that one specific message" indicating a possible threat requiring a decision maker's action, the reality is most OSINT activities will likely concentrate on monitoring general sentiments to provide general situational awareness. This is in part due to two things: everyone has access to PAI, and large-scale combat operations demand a general approach.

With everyone having access to PAI, people are inclined to do their own "OSINT." In fact, most people apply OSINT techniques when they use the internet to learn about a type of product they plan to buy, so it is normal for people to want to go online to find information about current operations. However, as these "non-OSINTers" get information, they naturally want to use it, which can sometimes require an OSINT analyst to do damage control. It is like when a judge tells jurors in a high-profile case not to seek out information about the case while the trial is ongoing, expecting them to avoid the internet and the news, which these days is virtually impossible. Therefore, the OSINT analyst needs to accept that others will unintentionally be doing "OSINT." OSINT analysts should therefore situate themselves as the vetters of questionable information. Not only does it reduce redundancy, but it also allows the OSINT analyst to become aware of what others within the team are concerned about.

As the Army transitions from counterinsurgency operations to large-scale combat operations, FORSCOM OSINT will do the same. As mentioned earlier, OSINT success stories often involve applying detective work to find specific adversaries. In reality, this sort of occurrence will be rare. We like to think that in large-scale combat operations, enemy troops will commit a vast number of operations security violations that OSINT analysts will find, or that civilians will readily post on social media about those "noisy tank drivers" who just arrived. This is a misguided expectation that comes from applying our experience in counterinsurgency operations to large-scale combat operations.

While instances of a chance post may reveal enemy positions, the reality is that most civilians will be more preoccupied with surviving conflict than using social media to post comments about the arrival of the enemy, and adversaries will not frequently post revealing information. We saw this during Operation Allies Refuge. Initially, there were a substantial number of posts on social media as people amassed to flee the country. The most informative were daytime videos typically posted on social media at night while people rested to prepare for the next day. As the evacuation progressed, social media posts became less frequent. This was presumably because most people tweeting and posting about the operation early on had either evacuated or begun to accept their new conditions in Afghanistan. Additionally, people were reportedly afraid of retaliation if their posts associated them with trying to leave the country.[6]

In large-scale combat operations, we are likely to see a similar pattern. We can mitigate this situation by casting a wide net for collection rather than focusing on finding information about specific individuals. The OSINT analyst can effectively capture new information by monitoring sentiment, reading articles about strategic efforts, and perusing local news to get a picture of what is happening. Elements within an OSINT cell can investigate specifics, but this may not always be fruitful

because information flow can mask relevant PAI. During the 2020 conflict between Armenia and Azerbaijan, government agencies from the two nations restricted internet access. The presence of disinformation campaigns, misinformation, and growing groupthink created an information environment where it was hard for anyone to get an accurate read of the situation.[7] The reliability of any given post on the conflict would thus be suspect.

The reality of large-scale combat operations is that aggregated information from the news and social media will be the most reliable way of driving OSINT collection. Looking at the greater context of streaming information will provide more effective understanding. Much as it was for T.E. Lawrence, OSINT analysts in large-scale combat operations will be doing most of their work analyzing the nature of the reporting rather than the reporting itself.

Conclusion

As the Army shifts from counterinsurgency operations to large-scale combat operations, establishing an OSINT cell at the division level has provided us an opportunity to form an environment that promotes creative research on globally significant matters. Although our team can exploit clear tactical uses of OSINT, we have found that focusing on the big picture first—the strategic-level issues—helps to illuminate what we find in PAI. Coupled with analytic techniques derived from game theory, we have been able to set up a framework for understanding how to conduct OSINT for the immediate response force mission.

Endnotes

1. *Lawrence of Arabia*, directed by David Lean (1962; London, UK: Horizon Pictures).

2. *Encyclopaedia Britannica Online*, s.v. "game theory," accessed November 1, 2021, https://www.britannica.com/science/game-theory.

3. *Encyclopaedia Britannica Online*, s.v. "The prisoner's dilemma," accessed November 1, 2021, https://www.britannica.com/science/game-theory/The-prisoners-dilemma.

4. Psychology Wiki, s.v. "Dictator game," accessed November 3, 2021, https://psychology.wikia.org/wiki/Dictator_game.

5. Jane McGonigal, *Reality is Broken: Why Games Make Us Better and How They Can Change the World* (London: Penguin Books, January 20, 2011).

6. Katie Collins, "The Taliban are spinning social media to their advantage, despite sites' bans," CNET, August 18, 2021, https://www.cnet.com/news/the-taliban-thrive-on-social-media-despite-sites-bans/.

7. Katy Pearce, "While Armenia and Azerbaijan fought over Nagorno-Karabakh, their citizens battled on social media," *Washington Post*, December 4, 2020, https://www.washingtonpost.com/politics/2020/12/04/while-armenia-azerbaijan-fought-over-nagorno-karabakh-their-citizens-battled-social-media/.

SGT Christian Torres joined the Army in 2017 as a geospatial imagery intelligence (GEOINT) analyst. The following year, he was assigned to the 82nd Airborne Division G-2 GEOINT cell. In 2021, he moved to the newly formed G-2 open-source intelligence team as part of the indications and warnings cell. He holds a bachelor of arts in philosophy.