Keeping an open mindset

Why military intelligence continues to be behind open-source information

by Michael Winberg

Resumé

Sociala medier och det som i folkmun kallas för ”open source intelligence” (OSINT) har exploderat under det senaste årtiondet. I skuggan av kriget i Ukraina har styrkorna såväl som svagheterna med OSINT visat sig, samtidigt som tillgången till sociala medier har blivit ett sätt för medborgaren att hålla sig uppdaterad på en detaljnivå som motsvarar ett lands regering. Men trots en ”oändlig” tillgång på information och trots att det visats vid flertal tillfällen att OSINT hittar svar som underrättelsetjänster missar fortsätter OSINT vara en underrättelsedisciplin som blir underutnyttjad. Denna artikel kommer att argumentera för att den traditionella underrättelsetjänsten behöver bryta sig loss från sina invanda mönster och våga anamma ett mer öppet sinne vad beträffar öppen information på internet.

> *Every collaboration helps you grow.*
>
> – Brian Eno

AS SOCIAL MEDIA and the internet have grown exponentially, so has the community of Open-Source Intelligence (OSINT). Although there seems to be plenty of room for private actors and corporate interests alike, state actors have yet to come to grips with the mindset that brings forth the power of OSINT. One could argue that governmental agencies never really will be able to harness that tenacity individual OSINT researchers seem to be able to raise when gathering data from the seemingly unlimited pool of information that is the internet.

The success of Bellingcat to gather and publish a comprehensive report on the downing of the Malaysian aircraft MH-17 is perhaps the clearest example of when a group of stubborn citizens managed to do what no state seemed to manage – collecting and presenting unquestionable evidence of a Russian anti-aircraft vehicle being the cause of the catastrophe, as well as which Russian unit that specific launcher belonged to. The “failure” by nation-states to fully implement OSINT into their intelligence toolbox can be explained by governmental institutions being narrow-minded and conservative. Where the national intelligence agency is influenced to be efficient with taxpayer money, the OSINT researcher is only limited by her priorities in life. In short, an OSINT researcher can allow herself to pour unlimited hours of work into a small project while the government employee is limited to the time the agency can afford to pay for.

While I am not arguing for the government to pay excess money for limited reach reports, I will in this article argue that adopting an open-source mindset combined with allowing more hours spent on more loosely defined projects will be beneficiary for the overall outcome of the intelligence organisation in long-term.

However, it is not just about granting more hours (and by that more money) to analysts. We also need to address the continuous underuse of OSINT as an intelligence discipline and with that, the culture within the intelligence community where all collection disciplines are equal, but some disciplines are more so than others. Meaning, that while it is common to use classified intelligence to validate OSINT, the intelligence world seems more reluctant to use OSINT to validate classified sources. There is reason to believe that there is a deeply rooted bias towards favouring classified information and distrusting information that is available for everyone to access. This is interesting when considering that a fair amount of basic intelligence from various wars and conflicts is based on publicly available sources like tourist maps and guidebooks. And it is no secret that some intelligence is gathered during exhibits and academic conferences, which is OSINT in its original form.

It seems however that we have forgotten this traditional tradecraft and almost instinctively link open-source with the internet and social media, and as such that nothing really can be trusted without being vetted by some other source. Keep in mind how all intelligence disciplines have their fallacies and that even trustworthy human sources can be wrong, even though they think that they are right, or that a technical sensor may show faulty data. As such, there is a need for a cultural change within the intelligence community to elevate OSINT to the same level as other disciplines.

Why does OSINT prevail when all others seem to fail?

Although a dramatic heading, there exist several cases where established governmental intelligence agencies seem to have been incapable of finding and disseminating information about certain events, whereas individuals using open-source information have been successful. The downing of the civilian airliner MH17 and the following tracking of the air defence system used by Russian forces is perhaps the most famous example. Why is that and how can we approach that problem?

When recruiting intelligence personnel, the common characteristics sought after tend to be integrity, meticulousness, and proneness to initiative. Some branches even look for personnel that are prone to change and who are independent. However, it seems that the institution acts counter-intuitive to all these traits and compels the individual to conform to a certain already established standard where the main task is to uphold the production cycle as set by previous analysts. There is simply no room for changes or initiative when the annual products need to be produced and briefings held per the predetermined template. As such it may be nearly impossible for a single analyst to take the time that is needed to delve deep into the abyss that is the open-source information arena and find the breadcrumbs that eventually will lead to essential information. As with all intelligence work, it takes time to hone the craft. Sources need to be developed and an understanding of the information environment needs to be established.

OSINT is not just about going online and "googling" information based on the collection plan or to answer a commander's question. First of all, we need to figure out on which platform we may be able to find what information and if that platform affects the type of information available in any way (search engine bias).[1] Then we need to find the sources, hopefully reliable, that produce information that may be of interest to us, both present and future. When those two bases are covered, we can move on to perfecting our use of various OSINT tools to find information that may have been removed or is posted in secluded places where a normal search query may not be enough. Adding to that we now also have to bear in mind that information has moved out to encrypted messenger apps like Telegram and that we in the future may see more blockchain apps being used to post and share information.

Acquiring all this knowledge is not easily done and is not something that you can read in a guide and then become an expert. This brings us back to time being the major factor since we also, as with all intelligence work, need to develop an understanding of the target environment. Thus, not only understanding of the information arena but also language, history, and cultural context within the data exist.[2]

Leaving the ego at the door

Open-source intelligence shares parts of the name with the open-source movement that evolved within the software developer community in the late 1990ies. Although aimed at developers being able to share code and users being able to use software without being billed, the open-source culture has spread across several domains ranging from medicine and research to food production and house construction. As such the mindset built into the open-source world can teach us a great deal about how to become successful in gathering information from the world of "unlimited" data.

The open-source community consists of plenty of individuals that not just enjoy what they do, they are, what could be described as, borderline obsessed with creating, sharing, and learning new things to become even better at their tradecraft. Looking at the OSINT community, the same characteristics are present where individual researchers not only create quality products, they also share how and where they encountered the information which in turn helps others not just to learn, but also to review the data which in turn adds to the value of the end product. Thus, forcing the analysts to move from an inductive methodology into the deductive domain. Meaning that each and every hypothesis on what intent or capabilities an adversary may or may not possess is exposed to a process where others, not limited to the specific section, tries to falsify the hypothesis.[3]

Now, there is a discussion to be had that a governmental intelligence agency cannot operate fully on those terms concerning the need for secrecy. Nonetheless, I would argue that the mindset could be applied on a wider, but still confined, scale within an organization. In reality, connecting analysts both horizontal and vertical within the organization, and inviting each other to scrutinize data within the OSINT realm would help distribute the workload and at the same time reduce the risk of biases and blind spots. In short, adding value and confidence to the conclusion thanks to the addition of other people's conclusions.[4]

Sharing the workload and focusing the effort

As previously stated, the OSINT design shares sources for others to review the data and reduce the risk of sources confirming their data. This also means that the workload can be shared between several nodes depending on specific areas of expertise without actually everyone belonging to a specific group. As such it is also possible to ask specific subject matter experts (SMEs) for their input regarding key intelligence questions that need to be answered. Applied to the military setting this would result in the weight of the workload being distributed throughout the organisation. As of now, intelligence gathering tends to be a top-down process where the strategic level is expected to answer a multitude of questions asked by all levels within the organisation. It stands to reason that a higher echelon will not be able to answer the detailed questions asked by a company. Meaning that there exists an information gap by design where lower levels may not be able to utilize the intelligence they are given.

This gap could be handled with a shared OSINT platform that is widely shared both horizontally and vertically. Which in the long-term would result in an intelligence product that is better suited to answer specific questions for specific units and branches. It would also, as a result of engaging the lower-level intelligence personnel, lead to the person being better skilled in not just compiling and assessing big amounts of data but also becoming more efficient in focusing collection efforts which are of importance for the overall development of the intelligence community.

It could be seen as a variant of crowdsourcing intelligence, defined as a method in which a selected group of individuals collects information on behalf of a national organisation.[5] In this case, the collection is still kept "in-house" but by a group of individuals that is not directly involved in the production of the end product.[6] Thus maintaining an acceptable level of secrecy without hampering the collection capabilities.

Pacing the evolution of technology

It is not just about having access to the internet and a web browser. The evolution continues to add new platforms and new ways of transmitting information. Nowadays much of this can be done by, and sometimes even require, smartphones. This in turn means that OSINT researchers need to have access to both computers and smartphones that can transfer data "seamless" or can use a platform that enables them to use smartphone apps in their computer environment. Also required are the applications needed to translate, review imagery and video as well as be able to create understandable products. At the same time, to maintain a reasonable level of security, there is a need for a virtual private network tunnel (VPN) and virtual machines. This means that lower-level intelligence staff need extra resources to even be able to begin their OSINT journey securely. Much of this work may now either occur on smartphones and private computers or not occur at all which means that a unit may miss information.

Although OSINT can be conducted by anyone without the need of any special soft- or hardware, the military setting requires some thought on how to set up a secure yet useable system from which an analyst can work. Such a system needs to either be classified from the beginning or have the ability to transfer data to a classified system with ease. The outcome being while OSINT researchers work within a security mindset of "good enough", the military and other governmental intelligence agencies struggle to combine high-level security with the fast-paced evolution of online applications.

While outside the scope of this article, this author would like to see the development of an OSINT platform being carried out with the same mindset. Meaning, that the workload is shared throughout the available IT staff (both civilian and military) in designing and building such a system. What we don't need is yet another project being delayed, tied to a specific external civilian company with tailored solutions where the cost risks overshadow the outcome of having a capable OSINT platform that is adaptable to the ever-changing environment.

Just because the product is classified doesn't mean it's of greater value

There is reason to believe that there exists a bias where information that has been marked with the label "classified" is viewed as more reliable and correct than information that is labelled open-source.[7] OSINT is usually mentioned as a discipline where information is supported by other, usually covert, sources. This indicates that all intelligence gathering disciplines are not equal and there is a need to monitor for "favorite-INTS" which risk influencing the decision-making.[8] Although seen as an actual security risk where personnel may, unknowingly, spread information that is of value to an adversary, information gathered through publicly accessible sources is still seen as something of lesser value or not reliable.

This points to an ambivalent attitude held within the intelligence community. However, I would argue that open-source data, over time, will give us answers that either would take considerable resources (developing sources, conducting signals intelligence, etc.) to find answers, or not being able to find answers at all. Which is supported by several statements from former intelligence officials stating that 80 to 95 per cent of classified intelligence is built upon information gathered in the realm of open-source information. When open-source information is processed and assessed by intelligence personnel, it becomes an equally valid intelligence product as all other disciplines and as such could, and should, be used in the same manner. Within that process, we assess the reliability of the information. Is it trustworthy at all or could it be false? This does not differ from other disciplines like human intelligence (HUMINT). By enforcing the same standards as other disciplines the outcome of the intelligence process should be equally valid. Thus, OSINT should be used as "supporting", as well as "supported" by, classified information in practice not only in words.

Here is where you probably conclude that even open-source information would become a classified product when processed through the intelligence cycle. You are correct. When the data is completed with the analyst's assessment the OSINT report could (likely would) become classified. Of this, there should be no doubt. However, with the war in Ukraine still ongoing it has been clear that there is a need to quickly reclassify reports to combat disinformation head-on, as well as deliver correct information to the public whom we serve. OSINT reports could be a quick way to push information out in the cognitive arena without having to mask or rewrite it to protect specific sources. The information is already out there for people to find, we just provide an easily accessible package for everyone to read.

It should also be clarified that classification is not the goal, nor should it be seen as a "stamp of approval". Throughout the intelligence community, there seems to exist a culture that over classifies information rather than the opposite. And maybe the fact that OSINT is open to everyone makes it less attractive to work with compared to other disciplines? Where the civilian world sees a challenge to find pieces of gold in a gigantic stream of data, the governmental employee might see a waste of time when the information could be supplied by other means. As such it would be reasonable to conclude that it is about mindset and not whether OSINT could bring forth value or not.

You are likely not alone in asking a specific question

Naturally, the intelligence community has to answer a set of questions, usually from some kind of decisionmaker. Usually, these information requirements are classified as a means to not expose what information gaps a country has about a certain topic. However, it is unlikely that these questions are unique and not asked or even discussed publicly by organisations or even SMEs:s. As such it lies within the interest of an intelligence organisation to find those who seek the same answers and "pick their brain" about certain topics. This could of course be done in various ways, on the spectrum of covertly to overtly, paid or unpaid, even though some argue that crowdsourced intelligence must be collected in an overt manner where the sourced group are aware of what they are taking part of. Either way, there is an ethical discussion to be held that is connected to the overall ethics of OSINT as a discipline. The main takeaway is that you are not alone in wanting to answer certain questions and that the ability to answer those questions should not be hindered by the fear of acknowledging certain information gaps.

The gain from collecting conclusions in this manner is mainly breaking the risk of ending up in an echo chamber. Also, when drawing knowledge from academia, other experts in the field, or even ordinary civilians you benefit from having a range of opinions which may help you refine the question and cover aspects that the organisation may have missed in the first place. The idea of an "intelligence minutemen" seems still to be alive.[9] It may also help in developing further information requirements to cover all aspects of one specific question.

Let the personnel have "side projects"

Training analysts takes time and much of the training is conducted on the job. While important, this training may create less desirable effects when analysts only work with a specific set of sources during their training. Unlike other disciplines that may be limited to their specific sources (human sources as an example), OSINT allows the analyst to gather additional information from a multitude of sources where information gaps occur during the process. The information-gathering process also forces the analyst to become familiar with other "INT:s" depending on the information found, often geographical intelligence (GEOINT). But most important, letting analysts operate within a sphere of trust, allowing them to spend time on projects that are of personal interest could create both a wider and deeper range of knowledge, in turn adding value to formalized projects.

As previously stated, one key to OSINT beating governmental intelligence agencies is the mere fact that people are "emotionally" connected to what they are doing. They have an interest from which energy could be drawn and focused on a particular goal for extended periods of time. This does not mean that the employee can use governmental resources for any type of project. The concept of "side project time" aims to empower the individual to pursue questions and knowledge that she might have in mind and thus advance her skill set which benefits the organisation. The evolution of intelligence throughout the ages has largely been driven by a sense of loyalty and dedication to very specific problems.

A military organisation that wants to stay relevant and ahead needs to curate the will to learn new things about the world, which in the end will lead to an enhanced collective understanding benefiting the decision-makers at various levels. Letting the personnel act for themselves would also likely have a positive effect on their ability to act within the realm of "mission command".[10] Understanding not only the detailed needs of each level of decision-makers but also the needs of the overall organisation will further enhance the capabilities of the armed forces. Thus, closing the information gap that is present today.

Challenges to overcome

There exist some challenges to overcome, challenges that need to be addressed for this to work. The largest might be changing the culture by allowing personnel to work with projects where the future value may be unknown and where the commander or director may not feel in control. Just like physical fitness, not everyone is comfortable with the weight of owning the responsibility for a project. However, that does not stop military organizations from pushing the responsibility down to the individual. The same could be said for conducting weapons or medical training. We, as a collective, expect that the individual take charge of their own skill set and works on it every day. The same approach could and should be applied within the intelligence community. With freedom comes responsibility, the proposal of side projects does not mean that the individual is free to do whatever she feels like whenever, there should still be a degree of control where the commander should be kept in the loop of how the project is developing and should also have the mandate to cancel a project if it starts to affect the daily production negatively or risk wandering outside of the legal framework.

Conclusion

To conclude, intelligence work has for several decades relied on open-source information as a means to create an understanding and answer questions from decision-makers. Although the technology has helped, the technology that exists today cannot yet help us gather, analyse and apply found knowledge. For this, we are still dependent on the individuals who have the willpower to "put in the effort"-- the willpower that intelligence organizations need to be able to harness. Furthermore we must not forget the culture change that may need to be set in motion where we need to "loosen up" the definition of OSINT to fully be able to reap the benefits of open-source. OSINT may not be as distinct from academic or journalistic research as one may think.[11] There are further discussions to be held about the development of OSINT to adapt it for the future information arena.

The author serves as a sergeant first class in the Swedish Armed Forces.

Noter

1. A consequence of user-optimization of the search results by the search engine companies.
2. Yates, Athol and Zvegintzov, Nicholas: "A Siberian reality check on open source information", *The Australian Library Journal*, vol. 48, no. 4, 1999, p. 343-357.
3. Martin, Alex and Wilson, Peter: "The Value of Non-Governmental Intelligence: Widening the Field", *Intelligence and National Security*, vol. 23, no. 6, 2008, p. 767-776.
4. Nolan, Phil: "A Curator Approach to Intelligence Analysis", *International Journal of Intelligence and CounterIntelligence*, vol. 25, no. 4, 2012, p. 786-794.
5. Stottlemyre, Steven A.: "HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence", *International Journal of Intelligence and CounterIntelligence*, vol. 28, no. 3, 2015, p. 578-589.
6. Dover, Robert: "Adding value to the intelligence community: what role for expert external advice?", *Intelligence and National Security*, vol. 35, no. 6, 2020, p. 852-869.
7. Op. cit., Nolan, Phil, see note 4, p. 789.
8. Gentry, John A.: "Favorite INTs: how they develop, why they matter", *Intelligence and National Security*, vol. 33, no. 6, 2018, p. 822-838.
9. Politi, Alessandro: "The Citizen as 'Intelligence Minuteman'", *International Journal of Intelligence and CounterIntelligence*, vol. 16, no. 1, 2003, p. 34-38.
10. Mission command is used in this article as a translation of the swedish word "uppdragstaktik" and refers to the individual being encouraged to act in accordance with a set of goals and guidelines set by higher command.
11. *NATO AJP-2.9 Allied Joint Publication For Open-Source Intelligence*, Edition A Version 1 June 2019, p. 1-2.