Minutes from Royal Danish Defence College Seminar on Open Source Intelligence, 19. April 2016.

The Seminar on Open Source Intelligence at the Royal Danish Defence College, Tuesday 19th April 2016 has now come to an end. From a hosting perspective, we consider the event as being very successful. We had more than 140 participants with very diverse professional associations and backgrounds, ranging from Defence, Police, Academia, the private sector, and others. There were four key speakers (Mr. Robert David Steele, USA; Maj. Sebastian Hébert, CAN; Capt. Bradley Grimm, USA and Mr. Jonas Alastair Juhlin, DEN) that addressed the subject from four different perspectives adding scope and depth to the general value of the seminar. We also held two fruitful iterations of discussions in smaller groups. It is the findings from these discussions that are summarized into main findings in this text with the purpose of facilitating knowledge sharing among yourselves – the participants:

From the "How to operationalize OSINT". Discussion group with Capt. Bradley Grimm and Maj. Tommy Karstensen:

If we want to use OSINT – we must do it right. The operators must be educated properly and they must be well trained. By that, the OSINT-people should reach the same high level of skills like other single source analysts received. By doing that we will increase the reputation of OSINT and inspire a higher level of confidence towards our costumers/users. It might be that the Danish customers still do not quite know the full potential of OSINT (B. Grimm note: "I would say that the Danes are not alone in this"). We, the participants, should spread the message.

OSINT is a good tool to validate information from other sources. Especially information concerning persons – but not solely limited to that. But on the other hand, OSINT itself should also be validated by other sources and it should never be considered intelligence without validation. An exception from that is pure raw data e.g. aerial photos and similar. The conclusion must be that validation creates and builds confidence in OSINT.

OSINT comes also in handy in the function of giving tip-offs that can be exploited by other collection assets, and another benefit that occurs is that often OSINT has much more rapid turn-around time compared to the tasking, exploitation, and dissemination cycle of events from non-OSINT platforms, which allows us to better get inside the adversary's OODA loop. OSINT can assist in creating new intelligence needs and to deciding on what collection assets to use for further exploitation. By that it is a great tool to use in the preliminary phases of a knowledge development task. It is also a useful tool during buildup of situational awareness and to assist in the IPOE (Intelligence Preparation of the Operational Environment). It is especially useful when building Brown and White overlays to IPOE.

Also in connection to INFO OPS (Information operations) OSINT is very useful. In the passive collection, OSINT is perfect to find general attitudes and meanings among local people in an area of operation. In this role it is most suitable to provide information in support of the targeting process. In the offensive collection role, it is a perfect tool to spread your messages to a target audience. Note that: Using OSINT in other role than the passive, you should consult legal advice.

From the "Avatar discussion group" with Mr. Jonas Alastair Juhlin and Mr. Soeren Tikkanen:

There was a general consensus that OSINT is a valuable source for obtaining information.

The Avatar project was conducted in a controlled environment with good communication infrastructure and easy access to information. This raised the question whether the project should have been/could be carried out under different circumstances, e.g. in a country with poor

communication infrastructure and/or restricted access to the Internet. One delegate had conducted a similar project in such an environment where quote: “aggressive OSINT” and “designed attacks” were used unquote. These terms are better known as phishing and honey pots in the intel community. This lead to a lengthy discussion about ethical and legitimate issues - when is OSINT crossing the thin white line and becomes HUMINT? - but it all boils down to national prerogatives and legislation.

Gaining intelligence from OSINT can be a challenge depending on which topic you are covering. Police officers told about their experiences from pedophile circuits and child pornography in general. The persons involved in this type of crime are very OPSEC-minded so it is a challenge to find these perpetrators and their punters.

"OSINT is an intelligence collection platform that is cost-effective, easy to use, easy to access and a very versatile platform. OSINT is used by private companies to investigate financial fraud, police intelligence to investigate social relations between suspected persons on social media and military units to gain situational awareness in a theater of operation". To sum it all up, OSINT is a source to be reckoned with. We have moved away from OSINF (Information) to OSINT (Intelligence) and the future looks bright.

From the “Doing OSINT right”. Discussion group with Mr. Robert David Steele and Maj. Simon Kempf Danebod:

Robert David Steele is clearly a man with a mission, and trying to cover all the subjects touched upon during the group discussions would go well beyond the scope of this summary. Even though Mr. Steele vividly argues in favor of creating an intelligence community where OSINT would take a leading role, the intelligence communities would still need to maintain their more traditional intelligence disciplines, referred to as the 20/80 rule. According to Mr. Steele, OSINT is currently underutilized and underfunded and by giving pride to OSINT most organizations would find that such a priority would free resources from the traditional disciplines that could then be redistributed to other areas within or outside the intelligence community.

Mr. Steele urged “the Nordics”, not to wait for NATO to come up with a doctrine, but instead go together and start up a Nordic OSINT intelligence center that could serve as an OSINT exchange HUB. The “Nordics” should be responsible for making their own OSINT doctrine, based on the idea that “shared information can create infinite wealth”. The creation of such a center would be the first step in creating a more open and transparent society, where the people would have access to the information used by the politicians as support to the decision making process.

Among the participants in the group discussion there was a general consensus of the many benefits that could be gained from giving priority to OSINT, however, questions concerning the fidelity of the intelligence acquisitioned from the Internet was raised several times. Could open source code be trusted, is the Dark Net and encryption not a danger to OSINT? Can OSINT be used to collect information that can help establish the intent of an adversary, etc? The general answer to many of these questions was that OSINT in most cases could provide the data and information much faster and cheaper than other intelligence disciplines, but, as with all other sources, the data and information would only be as good as the scrutiny gets.

From the “Doctrine discussion group” with Maj. Sebastian Hébert and Maj. Erik Gjerstad:

The first issue of discussion was: “How should NATO structure itself to create a robust OSINT Program?” Two options were initially presented to the discussion group:

A virtual NATO “Federated Bureau” with staff operating in their respective Nations (based on the principle “pull from Nations”), or a “Central NATO Bureau” fully staffed by member and partner Nations (based on the principle: “NATO push to the Nations”).

Regarding the first option, the “Federated Bureau”, the advantages appear to be that the option might entail fewer legal restrictions, as the Nations would provide OSINT in accordance with national policies; it might be more economical as less personnel would be needed, and it would thus be cheaper to fund; and OSINT collection and sharing could be coordinated at the strategic level. However, the disadvantages identified by the discussion group included the possible lack – or even loss – of NATO OSINT expertise as well as the usual releasability issues regarding the sharing of nationally produced intelligence.

Regarding the second option, the “Central Bureau”, the group identified the following advantages: Under NATO control (either under the auspices of a sponsor nation or as an integral part of the NATO command structure), NATO would be able to task its own capability and thus be less dependent on the Nations for OSINT products. It would also provide “economy of effort”, as it would reduce the need for the Nations to develop and maintain their own national OSINT capabilities. And it would promote the development and improvement of NATO OSINT policy, doctrine and TTPs. The disadvantages of a centralized approach include the necessity of allocating considerable resources (specialist personnel, facilities, funding, etc.). Furthermore, if no Nation is willing to sponsor a NATO OSINT capability, political turf battles regarding staffing and funding which could prevent its establishment. Finally the establishment of a “Central Bureau” may be a disincentive to the development of national OSINT capabilities, primarily at tactical and operational levels.

A third proposal, which was not included in Maj Hébert’s presentation, was put forward: embedding a NATO OSINT capability within the NIFC (NATO Intelligence Fusion Center).

All three proposals raise legal issues regarding the application of NATO regulations, international and EU law as well as national laws regarding social media exploitation and data privacy. There is also a need for a NATO – and nationally – agreed OSINT policy.

There was also a brief discussion on whether NATO should establish an OSINT COE (Centre of Excellence). The consensus was that a NATO OSINT COE would be needed if the “Central Bureau” option were to be chosen.

Another discussion issue was the content of the emerging NATO OSINT doctrine. The discussion group suggested that policy and doctrine used by law enforcement agencies could provide inspiration for the development of NATO OSINT policy and doctrine. In any case, the legal implications of OSINT collection need to be addressed by NATO legal advisors. Data protection laws may impact on social media exploitation. (The general opinion was that in principle all freely accessible social media and websites (non-encrypted, without passwords) should be “fair game”. However, mission-specific MOUs may need to drafted, which could be a task for a future NATO OSINT COE. The requirement for NATO OSINT capabilities and their support to NATO operations should also be addressed, including the OSINT contribution to the NATO Indication and Warning System (NIWS), OSINT in support of Planning, OSINT in support of strategic assessment, OSINT as a means of cueing other intelligence collection disciplines and OSINT support to targeting.

Social media monitoring should also be included in the future NATO OSINT doctrine publication. However, there is some disagreement as to whether social media exploitation is an integral part of OSINT. This issue will need to be resolved as part of the development of NATO OSINT policy.

From the "Free OSINT discussion groups" with Mr. Lars Baerentzen, Capt. Lars Andreasen and Dr. William L. Mitchell:

Important questions concerning validation – is one -INT more valid than another? Can OSINT validate OSINT? Are the classified INTs more valid? These questions led to a discussion that pointed to the concept of risk management. Every situation is different and therefore the validity 'bar' required for action is not fixed. Validation occur in many forms to manage uncertainty, but validating is still a process to manage uncertainty. In short - in some situations - it could be possible to validate OSINT with more OSINT. OSINT is not a single platform type like many of the other INTs. OSINT differs in that it has many different facets that can be exploited both in the collection and analysis phase.

Fusion and cross-over processes and organizations inherently support the generation and full exploitation of OSINT. This is mainly because different situations may require different areas of expertise or knowledge, and fusion organizations naturally have wider spectrum of expertise for exploitation to begin with.

Organization of OSINT capabilities is the key in using OSINT effectively. This requires a serious and focused approach to informing decision-makers of the role that OSINT plays and the effects it provides, in order to ensure the proper level of organization and resources are provided. E.g. it should not be seen just as an auxiliary skill set to be taught to existing analysts.

On the Danish national OSINT scene there is a need for someone to coordinate and fuse initiatives and training. It was suggested that the Royal Danish Defence College is a good candidate because they have less competing operational interests. Some participants knew of examples where different branches all had trials of different software without coordination. Similar cleavages were noted in OSINT training and education programs as different authorities and sub-departments had developed their own education and training regime. Why not let the Royal Danish Defence College do the coordination and be the anchor for basic OSINT education and training promoting national interagency networking to ensure a national standard? This would, however, require the establishment of an interagency OSINT course program e.g. integrated into the regime of current Master level intelligence courses.

Closing remarks. Please note that these minutes constitutes the general reflection from my staff and me. We might have missed a point or two but we have tried to capture as much as we could to the best of our abilities.

Thank you all for your engagement in this seminar. I hope that you will consider participating in future seminars at the Royal Danish Defence College. Please stay informed by checking news at our homepage.

Also visit YouTube for a review of the 60 mins lecture from Mr. Robert David Steele. Or to view the 13 mins. Interview that Mr. Steele gave before the Lecture.

Niels Ellehoej Pedersen

Royal Danish Defence College