PSSI
ALUMNI BRIEF — 1
February 2021

OPEN SOURCE INTELLIGENCE AND TERRORISM

Adéla Klečková

Prague Security Studies Institute

OPEN SOURCE INTELLIGENCE: BOTH THREAT AND OPPORTUNITY TO FUTURE COUNTER-TERRORISM EFFORTS

"Intelligently employed, information technology can dramatically increase the fighting power of military force, but it is no substitute for good judgement."

David Betz

1. INTRODUCTION

The revolution of information technology and its effects everywhere from commerce to politics is increasingly making open sources more accessible, ubiquitous, and valuable. It is estimated that open source data may account for as much as 80-90% (Gibson, 2007) of the overall intelligence that decision-making is based on. In the case of counter-terrorism, the contribution of open source intelligence (OSINT) may even be as high as 95% (Hobbs, Moran and Salisbury, 2014; 9).

The premise of this essay is that OSINT is a useful tool supporting counter-terrorism efforts, however it is no panacea. Its importance has grown since the beginning of the 21st century, as a result of both the technological revolution and the democratization of technologies. This has enabled a significant amount of data and information generated by human activities to be transferred into digital forms. Indeed, this trend is mirrored when investigating or gathering background data on contemporary terrorists, or terrorist groups, for whom the internet and social media have also become increasingly crucial tools. This has enabled activities such as radicalization, the recruitment of new members, and provided a platform for the promotion of propaganda.

Yet, in order to better serve its purposes effectively and efficiently, OSINT needs to be seen for what it is. It is neither a silver bullet for countering terrorism nor an obsolete novelty. Ultimately, one can never accurately distinguish the decisive factor in countering terrorism, and therefore counter-terrorism tools, such as OSINT, are better understood as part of a wider toolkit. Indeed, when combined with stolen secrets, diplomatic reports, and technical collections, for instance, OSINT constitutes an "intricate mosaic" of intelligence practices (Mercado, 2007).

Thus, combining academic literature with practical case studies, the structure of the present essay is as follows. First, the key conceptual terms "counter-terrorism" and "open source intelligence" will be defined. Information technologies of the 21st century have opened new unlimited possibilities to those who wish to fight against terrorism. In the second section, OSINT will be presented as a tool enabling exploration of these possibilities which can potentially be both challenges and opportunities, depending on the context and perception of each user. This essay concludes with a number of practical case studies demonstrating the diverse role which OSINT plays in countering terrorism, supporting the ultimate argument of this essay that OSINT serves the purposes of countering terrorism best when combined with other sources of intelligence.

2. DEFINING OSINT AND COUNTER-TERRORISM

OSINT does not have one universal definition, with some authors even calling it an 'oxymoron' (Carol, 2001). Nevertheless, for the purpose of this essay, a definition which emphases the 'supportive' role of OSINT will be utilised: "OSINT is the exploitation of open source information for intelligence purposes as a part of a broader, all-source intelligence process" (Hobbs, Moran and Salisbury, 2014; 1).

Similarly, there is no universal definition of counter-terrorism. The premise found in literature that counterterrorism is an effort at countering terrorism (Amble, 2014; 168) does not suffice without a definition of terrorism as well. In this essay, a general definition will be used: "Terrorism is a politically motivated tactic involving the threat or use of force or violence in which the pursuit of publicity always plays a significant role" (Weinberg, Pedahzur and Hirsch-Hoefer, 2004).

3. CHALLENGES AND OPPORTUNITIES OF OSINT

OSINT is a relatively new tool in terms of counter-terrorism, and brings with it a number of challenges and opportunities. Scholars such as Gibson (2007) and Sands (2005) list a variety of features of OSINT in cluster-form, whereas Mercado (2007) approaches it by listing explicit challenges and opportunities.

Three OSINT phenomena will now be presented as potentially constituting both challenges and opportunities. Here, it will be demonstrated that the emergence or existence of technology does not necessarily have 'positive' or 'negative' consequences, but that both of these outcomes are in fact subjective, depending on both the perception of the technology and the purpose for which it is being used. In practice, this concerns i) the quantity of data, ii) the democratization of intelligence, and iii) the picture of reality.

3.1. Quantity of data

Terrorist groups/individuals use the internet for various purposes, such as the spread of propaganda, recruitment, and tactical operations through the dark-web, in particular (Akhgar, Bayerl, Sampson, 2017; 5). One of the most valuable contributions of OSINT is therefore the systematic collection and analysis of terrorist group media which, among other opportunities, offers a valuable means of identifying the key players in terrorist operations. This is fundamental for forecasting the nature of the threat each group poses (Hobbs, Moran and Salisbury, 2014; 18), an aspect of counterterrorism which would indeed be made much harder without open source access to the online activities of terrorist groups.

Despite its importance in this regard, the sheer quantity of potentially insightful sources and data pumped out daily across the internet, not to mention its differing quality, makes it a very costly and time consuming endeavour. Additionally, it is also difficult to follow and keep track of, which itself creates further problems of sorting information and identifying what is relevant and what is just 'background noise' (Freedman, 2008; 17). Indeed, even with a more targeted approach – such as focusing on specific groups or channels – it is still a rather difficult task overall, given the variety of dissemination methods terrorists employ (Amble, 2014; 171). Take the social media platform 'Twitter' for instance: one must sift through many thousands of statements in order to determine the value of each, and to identify the relevant profiles. This is a supremely difficult task, wherein rather sophisticated methodologies must be employed (Berger and Morgan, 2015).

3.2. Democratization of intelligence

Simply put, a computer and a stable internet connection – technologies readily available to the average citizen – are the only equipment necessary for OSINT practitioners. Most online search tools and databases are publicly available, free to use, and require no expert training. Thus, one key opportunity feature of OSINT is its 'communicability' (Sands, 2005) which, unlike when dealing with sensitive information, means that such data is often shared with the public. As a result, the entry threshold into this field when compared to other intelligence disciplines is low and even though the overall quality of the practitioners does not inherently increase, this allows practitioners

from all spheres of society to participate in this discipline. Besides sinking the costs of both training new analysts, as well as gathering the intelligence itself, OSINT enables security forces to engage and share information with the public. This can help to prevent spread of rumours, hoaxes, or disinformation (Barlett and Miller, 2013). It also allows citizens and security forces to work together on ongoing investigations through volunteer-based, crowd-sourced intelligence (Barlett, Miller, Crump and Middleton, 2013).

Nevertheless, the sharing of such information so publicly also gives terrorists and other criminal groups greater insight into ongoing investigations, which they can, in turn, use to their own benefit. Security forces therefore need to select the publicly available data carefully, in order not to risk either the success of the investigation, nor the safety of the intelligence community. Indeed, lower barriers of entry have in fact opened the door to OSINT practices for both terrorists and criminals. One of the most useful tools for terrorist groups when preparing terrorist attacks (Harding, 2007) has proven to be Google Street View, or Google Maps (The Daily Mail, 2018). And even though there have been attempts to prevent these tools being used and abused by terrorists, thus far, these have proven to be rather ineffectual (Metz, 2009). Indeed, despite the easy accessibility of OSINT, lower barriers to entry and the practice's ubiquity in the modern world also inherently become challenges for counter-terrorism efforts.

3.3. Picture of Reality

OSINT is mainly utilised to provide background analysis and to put pieces of information gathered by other intelligence methods into place. This comes as little surprise, given that it is one of the quickest, cheapest, and most productive methods for gathering intelligence (Sand, 2005). Thus, in terms of providing a more accurate 'picture of reality', OSINT is invaluable. However, when gathering intelligence, analysts must also bear in mind that data needs to be timely, accurate, relevant, and verifiable (Gibson, 2007). Nevertheless, accurately verifying and evaluating data freely drawn from the internet remains rather problematic. This is especially true when one's adversary is aware of their communication being monitored, and they design and disseminate their own information, in part, with this context in mind (Amble, 2014; 172).

Furthermore, disinformation, propaganda, and even simple cognitive biases resulting from the lack of background information are the biggest adversaries of OSINT practitioners. For example, some fake Facebook accounts which have been used for intelligence collection have ended up misleading even highly specialised experts, as in the case of the so-called "Syrian-American lesbian" (Barlett, Miller, Crump and Middleton, 2013). Intelligence personnel have collected and studied books in order to better understand adversaries for decades, helping them to garner sufficient cultural contexts in order to better help them distinguish between the truth and their own biases (Amble, 2014; 170). OSINT, however, poses an additional challenge in terms of a lack of knowledge of foreign languages and local media expertise (Mercado, 2007) and therefore the data gathered might be too biased, or the analysis might be too shallow to provide the decision makers with an accurate picture of reality.

Unfortunately, analysts do often deal with investigations where they have very little reliable data beyond OSINT upon which to base their judgements (Mercado, 2007). This can especially be the case for unknown or newly emerging terrorist groups, or in impenetrable or underdeveloped regions. This can be partially mitigated by coding the sources based on credibility, or simply admitting its un-verifiability. Nevertheless, the best way to decrease the level of cognitive biases and provide an accurate picture of reality to decision makers is to combine OSINT with intelligence gathered through different methods.

As was demonstrated in the three examples above, OSINT is merely a tool helping researchers gather and process data in the arena of the modern technologies in the 21st century. Indeed, as with any other newly-emerged technology, it creates a number of possibilities which can be perceived as both challenges as well as opportunities. That is the reality which no one can do much about, and the best preparation for every individual wishing to utilize OSINT in countering terrorism is to be aware that just like any other, this sword also has two edges.

4. OSINT IN PRACTICE

As shown above, OSINT is a valuable analytical tool. To explore its role in countering terrorism in more detail, this chapter presents a variety of case studies where OSINT is being employed to gather a different kind of data serving different purposes. However, just like any other source of information, it is not the be all and end all, suggesting it serves its purposes best when combined with other sources of intelligence and counter-terrorism measures.

In May 2013, a plot to bomb the Embassy of Myanmar in Indonesia was detected and foiled when one of the terrorist perpetrators revealed his plans to execute the attack through a Facebook status update (Younas, 2014). Unfortunately, it is rarely the case that terrorists post their plans on social networks, intentionally or otherwise. The work of an OSINT practitioner is often more subtle and not limited to social networks.

OSINT should prevent the radicalization of new recruits by identifying narratives, influences, and propaganda over the surface web (Akhgar, Bayerl, Sampson, 2017; 5). These narratives could be consequently challenged through counter-narrative or counter-ideology, and their spread on the internet, including social media, are crucial for prevention of radicalization (Younas 2014). This could open the door to cooperation between the OSINT practitioners identifying propaganda, disinformation and radical narratives and communication departments of security forces to engage with the public through social media to reassure and disperse accurate information (Barlett, Miller, Crump and Middleton, 2013).

In case of prevention of actual terrorist attacks, this could be done primarily through gathering intelligence through open sources and collection of evidence for securing convictions (Akhgar, Bayerl, Sampson, 2017; 6). This was the case of Smadi, Martinez, Younus and Ali (Younas, 2014), whose arrests serve as an example of terror plots foiled by counter-terrorism practitioners through effective monitoring of jihadist chat rooms and social media and follow up operations. Effective monitoring of such sources have led to more accurate threat assessment, and therefore jihadist media are considered to be an easy and important source of intelligence.

OSINT is valuable for its real-time analytical capabilities, which can support counter-terrorism efforts by providing greater situational awareness (Akhgar, Bayerl, Sampson, 2017; 26). During the 2013 attack in Westgate, one of the attackers was tweeting on seven different Twitter accounts (Younas, 2014). Not to focus on only lone wolf attackers, OSINT has been a priceless tool in the fight against Daesh. As a high number of foreign fighters are actively using social media, they have become an essential source of information on what happens on the ground (Carter, Maher and Neumann, 2014), including pictures or discussions of battles, reporting on current locations or activities related to battles, and references to incidents both inside and outside Syria. On a reviewed sample of 563 Tweets, up to 40.32 % of them included such content (Klausen, 2014).

The quantity of insights that can be gained from analyzing information that is publicly available online is enormous (Carter, Maher and Neumann, 2014). Even though the contribution of OSINT to counter-terrorism efforts is undeniable, is it actually possible to answer the original essay question and specify what actually is the role that OSINT plays in countering terrorism and how valuable it is for the overall result.

5. CONCLUSION

OSINT is a powerful tool in the fight against terrorism. As argued above, it brings many challenges for practitioners, but at the same time opens doors to immeasurable amounts of information, which can help save lives. And as demonstrated in the third chapter, OSINT contributes to counter-terrorism in many ways, from providing contextual analysis to helping to better understand the adversary to strategic intelligence on how to prevent the attacks, especially when combined with other forms of intelligence.

Just as the jihadist organizations do not form a homogenous body readily counted by a single strategic approach (Amble, 2014; 181), so is intelligence and its effectiveness a slippery concept hard to pin down or measure (Hobbs, Moran and Salisbury, 2014; 12). Measures of success that are touted as useful and accurate so often fail in the real world (Quin, Zhou, Lai, Reid, Sageman and Chen, 2005; 316). As a result, it is impossible to determine how important the role of OSINT is in the fight against terrorism. It indeed differs from case to case. Nevertheless, even when looking at separate investigations or operations against terrorists, it is hard to measure the success of OSINT in isolation. However when taken as a tool with other forms of counter-terrorism, its strengths become clear, and a number of its limitations are mitigated. Indeed, it is the most powerful when augmenting existing closed-source intelligence by providing additional information and direction to where further information may be required (Akhgar, Bayerl, and Sampson, 2017; 8).

Given the nature of terrorism and the requirements of countering it, OSINT offers opportunities to help to craft strategic responses that have yet to be fully exploited (Hobbes, Moran and Salisbury, 2014; 181). **Nevertheless, it is without any doubt that purposeful and legal monitoring analysis of open source data should be considered mandatory for any national counter-terrorism strategy (Akhgar, Bayerl, Sampson, 2017; 9).**

Adéla Klečková *focuses on hybrid warfare and resilience building of national states. Currently, she is researching new forms of civic activism in the virtual space as a non-resident fellow of the German Marshall Fund and pursuing her MA degree at the War Studies Department at the King's College London. She works as the Critical Thinking Program Director at the "Together for Czechia" think tank based in Prague. She was listed among the 35 under 35 young in Global Techno Politics by the Barcelona Center for International Affairs.*

6. BIBLIOGRAPHY

Akhgar, B., Bayerl P. and Sampson F. (2016). *OSINT as an Integral Part of the National Security Apparatus*. Cham: Springer

Barlett, J. and Miller C. (2013). "The State of the Art: a Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism." [PDF]. *The Demos*. http://www.demos.co.uk/files/DEMOS_Canada_paper.pdf

Barlett, J., Miller, C., Crump, J. and Middleton L. (2013). "The Policing in an Information Age." [PDF]. *The Demos*. http://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365

Berger, J. and Morgan, J. (2015). "The ISIS Twitter Census." [PDF]. *The Brookings*. https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

Betz, D. (2006). "The more you know, the less you understand: The problem with information warfare." *Journal of Strategic Studies*, 29(3), 505-533. http://dx.doi.org/10.1080/01402390600765900

Carrol, T. (2001). "The Case Against Intelligence Openness." *International Journal of Intelligence and Counterintelligence*, 14, 559-574. https://doi.org/10.1080/08850600152617164

Carter, J., Maher S. and Neumann, P. (2014). "#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Network." [PDF]. *The International Center for the Studies of Radicalization and Political Violence*. https://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf

Freedman, L. (2006). *Transformation of Strategic Affairs*. London: International Institute for Strategic Studies

Gibson, S. (2007). "OSINF: the lifeblood of decision-making." *The Royal United Services Institute*, Accessed October, 2020. https://rusi.org/publication/osinf-lifeblood-decision-making

Gibson, S. (2007). "Open Source Intelligence (OSINT): A contemporary Intelligence Lifeline," [PhD thesis]. *Cranfield University*. https://dspace.lib.cranfield.ac.uk/handle/1826/6524

Harding, T. (2007). "Terrorists use Google maps to hit UK troops." *The Telegraph*, Accessed October, 2020. https://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html

Hobbs, C., Moran, M. and Salisbury, D. (2014). *Open source intelligence in the twenty-first century: new approaches and opportunities*. Basingstoke: Palgrave Macmillan

Klausen, J. (2015). "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." *Studies in Conflict & Terrorism*, 38(1), 1-22. https://doi.org/10.1080/1057610X.2014.974948

Mercado, S. (2007). "Sailing at the Sea of OSSINT in the Information Age." *Central Intelligence Agency*, Accessed October, 2020. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html

Metz, C. (2009). "Google Earth faces terrorist target airbrush bill." *The Register*, Accessed October 2020. https://www.theregister.com/2009/03/05/google_earth_blur_bill/

Qin, J., Zhou, Y., Lai G., Reid, E., Sageman, M. and Chen, H. (2005). *The Dark Web Portal Project: Collecting and Analyzing the Presence of Terrorist Groups on the Web*. Berlin: Springer

Sands, A. (2005). *Integration Open Sources into Transnational Threat Assessment* in Sims, J. and Gerber B. (eds.), *Transforming US Intelligence*. Washington, DC: Georgetown University Press, 63-78

Amble, J. (2014). *Jihad Online: What Militant Groups Say About Themselves and What It Means for Counterterrorism Strategy* in Hobbs, C., Moran, M. and Salisbury, D. (eds.), *Open source intelligence in the twenty-first century: new approaches and opportunities*. Basingstoke: Palgrave Macmillan, 168-184

The Daily Mail. (2018). "Terrorism 2018: Al Qaeda uses Google Maps to plan a terrorist attack in new propaganda video that features a former Guantanamo prisoner." *The Daily Mail Online*, Accessed October, 2020. https://www.dailymail.co.uk/news/article-5642361/Al-Qaeda-appears-use-Google-Maps-plan-terrorist-attack-new-propaganda-video.html

Weinberg, L., Pedahzur, A. And Hirsch-Hoefler, S. (2004). "The challenges of conceptualizing terrorism." *Terrorism and Political Violence*, 16(4), 777-794. https://doi.org/10.1080/095465590899768

Younas, M. (2014). "'Digital Jihad' and its Significance to Counterterrorism." *International Centre for Political Violence and Terrorism Research*, 6(2), 10-17. http://www.jstor.org/stable/26351231