Piotr Karasek

Social Media Intelligence as a tool for immigration and national security purposes[1]

Introduction

Detecting and interdicting terrorist attacks as well as maintaining proper border security are among the key issues in current public security debate, and the role of social media in achieving these goals could still be increased. While countering terrorism is a responsibility of relevant national law enforcement agencies, all possible fronts of threat detection should be used. This is especially important after recognizing that contemporary extremists often act on their own and are not a part of any terrorist organization, therefore the threat may be very difficult to detect using traditional means of protection. From this perspective, public servants who process visa applications may play an important role in a multi-agency approach to maintaining security. With access to verifiable personal data provided by visa applicants and open source information they may be able to use Social Media Intelligence techniques to detect threats and deny individuals entry whenever it is appropriate. Moreover, using such techniques may allow revealing other information relevant to immigration procedures. Such tools are known to have already been employed in the US immigration procedures.[2] While the actual effects of such policies are difficult if not impossible to determine at current point, there are some clear shortcomings of SOCMINT tools one needs to remember about. This paper based on literature review, available case studies, and research interviews with immigration security practitioners aims to explore the possibilities associated with the use of Social Media Intelligence in the field of national security and immigration, and to describe the risks behind it.

Law enforcement, terrorism, and the Internet

The vast possibilities offered by rapid development of the Internet are often perceived as enabling criminal activity, including terrorism, which is not necessarily the whole truth. Limited anonymity, decentralised black markets, dark web forums, and access to all sorts of dangerous content – all this and more come along with the Internet access and indeed help the criminals achieve their goals. On the other hand, the Internet may

[1] The article was prepared within the FP7 PRIME Project that has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608354.

[2] B. O'Brien, *U.S. visa applicants to be asked for social media history: State Department*, Reuters 30 March 2018, online: https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P, [access: 15 IV 2018].

also be very useful for the purposes of regular crime and terrorism prevention as it increases law enforcement intelligence gathering possibilities, potentially benefiting the governments and counterterrorists more than terrorists.[3]

Intelligence practitioners and academics are often referring to social Media Intelligence (SOCMINT) as a new type of intelligence falling into the general Open Source Intelligence category (OSINT)[4], yet specific uses of SOCMINT still remain mostly an unexplored topic. Social media themselves, regardless of their specific definition[5], have become a global phenomenon and contain a tremendous amount of freely uploaded, often easily accessible information about individuals. SOCMINT efficiency is partially based on the fact that while users express themselves, they often give up information they would not want to share when asked directly[6] (especially if asked by the law enforcement). In contrast to subject-specific online forums, social media are designed to allow free expression of lifestyle. Such design actively encourages users to share their thoughts, plans, opinions, photographs, and facts from their lives online. There is an~~d~~ observable tendency among the social media users to 'over-share' private information, which may have dangerous consequences as it makes them vulnerable to various types of crime.[7] On the other hand, it is exactly the 'over-sharing' phenomenon that makes SOCMINT techniques truly effective.

Social media are therefore already one of the obvious sources of intelligence in policing. In criminal investigations, 81% of (American) law enforcement professionals use social media as a tool for information gathering although in almost half the cases (48%)[8] such practice is not encouraged by their superiors. It is important to notice that some information from social media may be accessed freely, without court order or subpoena, even for unregistered users with the use of open source intelligence techniques. Other methods of using social media by law enforcement agencies may include employing powerful SOCMINT tools, e.g. using

[3] D.C. Benson, *Why the Internet is not increasing terrorism,* Security Studies, 23/2(2014), p. 308, 311, 328.

[4] A.N. Liaropoulos, *The challenge of social media for the Intelligence community*, Journal of Mediterranean and Balkan Intelligence, vol. 1 no. 1 (2013), p. 6.

[5] Popularly social media are defined as 'a group of Internet based applications that build on the ideological and technological foundations of Web 2.0 and allow the creation and exchange of user generated content', where the Internet sites are used 'only' as infrastructure allowing their users to upload their own content. See: A. Kaplan, M. Haenlein, *Users of the world, Unite!*, Business Horizons, 53/1(2010), p. 61.

[6] C. Arslan, M. Yanuk, *A New Discipline of Intelligence: Social Media,* ICMSS Istambul 2015, pp. 69–70.

[7] K. Paullet, J. Pinchot, *Cybercrime: the unintentional effects of oversharing information on Facebook*, 2012 Proceedings of the Conference on Information Systems Applied Research, New Orleans 2012, pp. 1–7.

[8] LexisNexis, *Social media use in law enforcement: crime prevention and investigative activities continua to driver usage*, November 2014, online: https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf, [access: 15 IV 2018].

'geofencing' technology[9] (such as 'Geofeedia') allowing to locate and manage near real-time threats.[10]

All the methods used to fight 'regular' crime are also very useful in countering terrorism, with particular emphasis on so-called 'Internet monitoring', a category that SOCMINT fall into. As the European Commission FP7 PRIME[11] research project findings show, methods applied by law enforcement to counter solo terrorism do not really disperse from those used to fight group terrorism or even 'regular' and organized crime.[12] As a result of the interviews and questionnaires collected from European, American and Indian practitioners, a hierarchy chart of the most effective and least costly methods of countering terrorism has been compiled.[13] 'Internet monitoring' has been identified as the most effective and least expensive method (94% of responses).

In the context of Internet and social media monitoring, it is important to understand the nature of modern lone actor (or 'lone wolf') terrorists and how they express themselves through social media. While presenting a strict definition of a 'lone actor' terrorist is still problematic in the field of criminology, they are described as individuals who have no formal ties to any terrorist organisation, but who commit an act of violence inspired by an extremist ideology. An archetypical 'lone wolf' follows a path of radicalisation, attack preparation, and attack phases, without any external help. However, lone actor terrorists may (not necessarily consciously) somehow communicate their intent weeks, days or even hours before the attack. A previous research claim that as many as 76% of the post 9/11 lone wolf terrorists in the US have broadcasted their intent (often more than once) using e-mails, text messages, and more importantly – Facebook postings and Twitter feeds.[14] Even when not communicating their intent to attack directly, future perpetrators often reveal signs of radicalization. Much too often it remains undetected prior to the attack.[15]

Social media and the immigration procedures

Taking into account the abovementioned possibilities arising from the use of open source intelligence in regular crime and terrorism prevention, it is worth considering how it may be employed for the purposes of immigration procedures. Or conversely:

[9] M.D. Dabhi, *Geofencing: a generic approach to Real time location based tracking system*, International Journal of Computer Networks and Wireless Communications, vol. 6 no. 6/2016, pp. 35–37.

[10] K. Cooke, *US Police used Facebook, Twitter data to track protesters*, Reuters, Oct 11 2016, online: http://www.reuters.com/article/social-media-data-idUSL4N1CH4J1, [access: 15 IV 2018].

[11] http://www.fp7-prime.eu/home_page.

[12] FP7 PRIME WP7 Deliverable D7.1, *Counter-measures review report,* Restricted access confidential document.

[13] Ibid.

[14] M. Hamm, R. Spaaij, *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies,* February 2015, p. 9.

[15] For example: George Sodini (aka 'the Gym Killer') explained his entire attack plan on his personal blog over many months between 2008 and 2009. See: *Full text of Gym Killer's blog,* online: http://nypost.com/2009/08/05/full-text-of-gym-killers-blog/, [access: 15 IV 2018].

how OSINT and SOCMINT may enhance the role of immigration procedures in safeguarding national security.

The possible role of visa applicant's social media background check is well illustrated by the case of San Bernardino shooting in December 2015. Shortly after the attack some have reported that Tashfeen Malik, the female shooter who has been in the United States on a fiancée visa, posted jihadist propaganda on her Facebook page prior to obtaining the visa.[16] It has to be fully acknowledged that this information turned out not to be entirely true[17], however, it illustrates how such hypothetical situation would be perceived by the general public and what problems may emerge in the future if visa applicants are not vetted correctly.[18]

Contrary to what one may think, performing social media background checks of visa applicants does not necessarily overlap with the tasks of national security agencies. Although intelligence on visa applicants may be delivered to the immigration services by other national agencies (through databases and dedicated sub-agencies such as the Terrorist Screening Center in the U.S.[19] or Schengen Information System in Europe[20]), because of the decentralised nature of modern terrorism it may be not safe enough to rely only on one source of information. Security agencies are good at finding links to terrorist groups or organized crime, but lone radicals may slip through. Moreover, there are numerous of factors that are taken into account when assessing one's visa application, but are not in security or law enforcement agencies field of interest. Applicant's past criminal sentences or serious health problems are good examples, as they usually may be grounds for visa denial, but are not necessarily the type of information gathered by security and law enforcement agencies.

OSINT and SOCMINT techniques may therefore be viewed as a part of a broad identity and security management system embedded into the immigration process framework to achieve at least two goals: (a) to detect individuals who are prone to violent extremism, and (b) to identify other unique circumstances that may be grounds for visa denial. There are, however, some limitations and risks, which must be considered before implementing such tools. OSINT should be used by the immigration

[16] M. Apuzzo, M.S. Schmidt, J. Preston, *U.S. Visa Process Missed San Bernardino Wife's Online Zealotry*, The New York Times, December 12 2015, online: http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html?_r=0, [access: 15 IV 2018].

[17] R.A. Serrano, *FBI chief: San Bernardino shooters did not publicly promote jihad on social media*, Los Angeles Times, December 16, 2015, online: http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html, [access: 15 IV 2018].

[18] See also: B. Ross, R. Schwartz, J.G. Meek, J. Margolin, *Secret US Policy blocks agents from looping at social media of visa applicants, former official says*, ABC News, December 14 2015, online: http://abcnews.go.com/US/secret-us-policy-blocks-agents-social-media-visa/story?id=35749325, [access: 15 IV 2018].

[19] See: *Terrorist Screening Center*, online: https://www.fbi.gov/about-us/nsb/tsc/tsc, [access: 15 IV 2018].

[20] See. *Schengen Information System*, online: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm, [access: 15 IV 2018].

services in an organized manner, which is not always happening in practice.[21] In the next sections of this article some key areas of this concept are explored. Firstly, it is necessary to specify how a social media background check could be performed in the course of immigration procedure. Secondly, it is equally important to take a hard look at the potential risks and limitations of such method.

Entry data

Searching for potential terrorists on the Internet is like searching for a needle in a haystack. A common problem with SOCMINT techniques is the deluge of information that needs to be processed in order to receive actionable intelligence.[22] Immigration services, however, have an advantage in this regard – they are in possession of reliable and relatively complete set of personal data submitted by applicants themselves on immigration forms. The data may be used as entry data to create a 'data filter' effectively reversing the search process – instead of trying to find worrying content and then trying to identify its author, the search may focus on finding worrying content posted on the Internet by a specific person. It is therefore possible to shift from searching for 'unknown unknown' to a search for 'known unknown', which is relatively more effective and easier to deal with.[23]

Entry data available to the immigration services in each case will vary depending on specific legal regulations. For example: western-European tourists visiting Australia on an e-visitor visa are required to provide their personal data (including full legal name, sex, date of birth, passport number, country of residence), and a working e-mail address. A different example may include an Egyptian applying for a Polish visa, who would have to additionally submit his photograph and other documents or information (such as e.g. official certificate of no criminal record), if requested by the consulate.[24] In case of long-term visas the requirements are usually higher. Typically the initial dataset available for the immigration services and usable for open source research contains at least: applicant's full legal name and date of birth, e-mail address, home address, workplace address, photograph. It is often enough information to identify the person online, provided he or she is not actively trying to hide personal details.

[21] Some Australian immigration service's practitioners, during confidential research interviews, have admitted that although there is no official SOCMINT policy in place, they sometimes use such techniques to check visa applicants out of their own initiative.

[22] D. Omand, J. Bartlett, C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, Intelligence and National Security, n. 1–23(2012), pp. 6–7.

[23] See. N.N. Taleb, *Black Swan. The impact of the highly improbable*, New York 2007, p. 127, 272.

[24] Ministerstwo Spraw Zagranicznych RP, system eKonsulat, online: https://secure.ekonsulat.gov.pl/Uslugi/RejestracjaTerminu.aspx?IDUSLUGI=1&IDPlacowki=157, [access: 15 IV 2018].

Access

After a 'data filter' is compiled, access to relevant online sources must be established. One option is to openly ask the social media service providers for help, but they often do not willingly cooperate with state agencies (especially foreign state agencies). To gain access to user's data directly from social media companies often at least a subpoena or even a proper court order is required.[25] Some companies actively fight for their users privacy[26] or publish 'transparency reports' on law enforcement access demands[27], which, however exemplary it may be from civil rights perspective, has to be seen as an obstacle in the context of national security. It is too early to predict the impact of recent events involving Facebook's data leak[28] on users and companies behaviour, but this issue has definitely raised public concern about data privacy.

Open source background checks, however, do not rely on gaining official access to user's restricted data. The very idea of open source intelligence is based on the fact that a lot of meaningful information is publicly available. This is also true for social media profiles. Of course, users who are conscious of their privacy either do not use social media at all, do not post private information online, or at least set their privacy settings so no third party may access it freely. This, of course, is another obstacle in the context of the proposed method. However, surprisingly high number of social media users has their profiles fully or at least partially visible even for unregistered users.

Data access capabilities may also be enhanced by other means, including simple 'tricks' and elaborate OSINT-gathering systems. Among the most basic methods is the creation of 'false' accounts, so the social media platform recognizes the intelligence gatherer as a 'registered user' and allows more access. Although it is usually against the social media policies[29], this method is often used by law enforcement professionals (even though they are discouraged to do so).[30] Of course, accessing and gathering

[25] See e.g.: Facebook, *Information for law Enforcement Authorities*, online: https://scontentfra31.xx.fbcdn.net/hphotosxfp1/t39.23656/12532957_530107840495531_2074830868_n.pdf, [access: 15 IV 2018]; Twitter *Guidelines for law enforcement*, online: https://support.twitter.com/articles/41949#, [access: 15 IV 2018].

[26] A. Fine, *Twitter appeals ruling in bat tle over occupy Wall Street protester's information*, online: https://www.aclu.org/blog/twitter-appeals-ruling-battle-over-occupy-wall-street-protesters-information?redirect=blog/technology-and-liberty-national-security-free-speech/twitter-appeals-ruling-battle-over-occupy, [access: 15 IV 2018].

[27] See. *Google Transparency Report*, online: https://www.google.com/transparencyreport/userdatarequests/#!, [access: 15 IV 2018].

[28] D. Ingram, *Facebook says data leak hits 87 million sers, widening privacy skandal,* Reuters April 4 2018, online: https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM, [access: 15 IV 2018].

[29] All Facebook users should, in theory, use their authentic names, see: *Facebook community standards*, online: https://www.facebook.com/communitystandards, [access: 15 IV 2018].

[30] In an initially confidential guidelines for law enforcement Facebook also discouraged the use of false accounts by law enforcement, see: *Facebook law enforcement guidelines*, 2010, online: https://info.publicintelligence.net/Facebook2010-2.pdf, [access: 15 IV 2018].

information does not have to be performed manually, because of the existence of specialised commercial software designed to collect open source information from the Internet. Such systems are already available to state agencies and may be tailored to their needs and allow a very cost-effective information gathering.[31]

Assessing the information

After defining the initial dataset and establishing access to information, the key phase of any background check is the assessment of the data gathered. The approach to data assessment should depend on what information has been found online about the individual on one hand, and the specific visa and security requirements on the other.

There is a number of common visa requirements (such as 'good health' or 'good character') which may be at least partially verified through open source intelligence, but it is important to know where to look for relevant information. First of all, one should review all the available original content posted by the person checked. Due to the aforementioned 'over-sharing' of private information, online postings might reveal information, which may be grounds for visa denial. For example, visa applicants are usually expected to state that they have no criminal record and are not subject to any current criminal investigation, which may sometimes be proven untrue after a careful search of their Internet postings indicating past or present legal problems. There have been also many cases in which a photograph posted online was found by the law enforcement, which has led to a criminal investigation.[32] There is no reason not to use the same information gathering technique in the immigration process.

Apart from the original content posted online, it is also important to review one's 'shared' posts, 'liked' pages, 'followed' users, and joined 'groups' (on Facebook, Twitter and other micro-blogging platforms and social media – the specific terminology about 'sharing', 'liking', 'following' etc. may vary) which may indicate personal views, interests, and life situations which may lead to a visa denial. This may be important especially when looking for signs of radicalisation; someone 'following' accounts known to be posting terrorist propaganda[33] is an obvious cause to concern.

When making the assessment of the information gathered one should also know how to judge less 'obviously worrying' content. This has been already explored in previous research and a set of 'warning behaviour' signs has been already described.[34]

[31] A couple of major software manufacturers such as Symantec, Oracle, or Wynyard offer such 'intelligence gathering solutions' (terminology and specifications vary, but all these are commercially available for law enforcement agencies).

[32] There are many examples of such behaviour. See. A. Shontell, *7 People who were arrested because of something they wrote on Facebook*, Business Insider 9 Jul 2013, online: http://www.businessinsider.com/people-arrested-for-facebook-posts-2013-7?IR=T, [access: 15 IV 2018].

[33] See. J. Klausen, *Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq*, Studies in Conflict and Terrorism, 38(2015), pp. 1–22.

[34] In particular, it is possible to detect some types warning behaviours online, using social media analysis (by detecting linguistic markers for 'leakage', 'fixation', and 'identification' warning

Whether the occurrence of a specific 'warning behaviour' should result in visa denial (or, in some instances, even further action against the individual such as informing the relevant authorities about the threat) should depend on the adopted internal policy.

Risks and obstacles

Using open source information gathered from the social media to assess visa applicants is associated with a handful of serious risks and may encounter various obstacles. Knowing them and having at least a sound plan how to react when such problems occur is an important step in adopting social media background checks as a policy designed to effectively ensure security. Among the most important problems are verifying one's true online identity, language and cultural barriers, organizational issues, legal and ethical concerns, and the problem of final decision-making.

True identification

Although in theory social media users should use their true personal data, in practice it is obviously untrue[35], which is perhaps the most significant problem associated with targeted social media intelligence gathering. An alias may be used for privacy reasons - a premeditated or instinctive decision not to post true personal data online (which, on the other hand, is a good sign of one's caring for security). Some users create fake profiles on purpose, to steal other's identity or to engage in 'cyber-bullying'. Whatever the reason for using an alias is, it limits the possibility of establishing a reliable access to one's online postings. The intelligence gatherer has to be also wary that even when a social media profile is created with a real name and surname, it does not necessarily belong to the person one is trying to review. Names alone do not allow identifying anyone online, as many users may share the same legal name. For example, searching Twitter for this paper's author's name[36] will result in a couple of records, none of which is his, as he not maintain a Twitter account at all.

Unfortunately, there is no ideal method to doubtlessly verify one's online identity without confronting the person in question. Best course of action is to (a) cross-check the data available from the social media profiles with the dataset created on the basis of the visa application, (b) remain suspicious about the users perceived identity, especially when drawing conclusions.

behaviours), see. K. Cohen, F. Johansson, L. Kaati, J.C. Mork, *Detecting linguistic markers for radical violence in social media*, Terrorism and Political Violence, 26/1(2014), pp. 246-256, and: J. Reid Meloy, *Identifying warning behaviors of the individual terrorist*, FBI Law Enforcement Bulletin, April 2016, online: http://drreidmeloy.com/wp-content/uploads/2016/05/2016_IndividualTerrorist.pdf, [access: 15 IV 2018].

[35] See. K. Raynes-Goldie, *Aliases, creeping and wall clearing: understanding privacy in the age of Facebook*, First Monday, vol. 15 no. 1–4.

[36] The author has decided to use his own name as an example due to ethical concerns about using other people's data. This experiment, however, may be reproduced with other names easily.

Language and cultural barriers

Language and cultural barriers may be problematic when gathering information especially by the immigration services. Obviously, social media users post their content using many national languages, not always known to immigration officers. These issues may be partially addressed by promoting diversity among immigration workers and employing those with higher language skills. Machine translation is another option as more and more advanced automatic translation services are being developed, which may at least reduce the need for the analyst to be fluent in the original language of the text.[37]

Cultural barriers and lack of knowledge may prohibit some immigration workers from understanding the specific context and true meaning of one's postings. Without the proper knowledge about current trends in extremist ideology and propaganda it may be difficult to pinpoint suspicious Internet activity associated with terrorism. For example, in 2014 ISIS successfully used World Cup themed hashtags (e.g. #Brazil2014) to disseminate its propaganda[38], and anyone posting under such hashtag could be either a genuine sports fan or an ISIS supporter. This problem may be addressed with appropriate training programmes within the immigration services.

Legal and ethical issues

Collecting personal information about foreign individuals, other than willingly provided by themselves on visa application forms, may raise questions about legality and ethics of such process. Information from social media profiles very often will fall into the category of 'personal data', and whether its collection by the immigration services is legally acceptable or not will depend on the specific legal system. For example, such methods would be at least questionable under European law which strongly protect personal data and describes who and when is allowed to process it.[39] Therefore in some jurisdictions minor changes in legislation would be necessary to allow it.

Another option to address this issue is to semi-overtly ask visa applicants for their consent to gather additional personal data, which may allow to move the intelligence gathering process away from the legally and ethically gray area. This is unfortunately associated with the risk of alarming those who may try to remove or hide relevant information. A general consent form could be included in the visa application documents,

[37] K. Cohen, F. Johansson, L. Kaati, J.C. Mork, *Detecting*, op. cit., p. 251.

[38] C. Milmo, *Iraq crisis exclusive: Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter*¸ The Independant 22 June 2014, online: http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promote-9555167.html, [access: 15 IV 2018].

[39] See the newest EU personal data protection act, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

and it does not have to disclose exactly what information and how will be gathered by the immigration services. More specifically, visa applicants may consent to 'a search for relevant information from other sources accessible to the immigration services', which should cover all the SOCMINT gathering techniques without sounding too alarming. Similar consent forms are known to exist both in the public and private sector, where employees agree to background searches.[40] Too vague consent form may, however, still be not enough to assure the legality of the discussed methods in some jurisdictions, especially when sensitive information (such as information about one's health and personal views) is to be gathered.

Decision-making

Whenever suspicious social media content is found, it is essential to take into account all the limitations of SOCMINT techniques to exclude any misunderstandings. A questionable social media posting may be misunderstood, falsely attributed to a specific person, simply untrue or even published as a jest. Posts meant to be humorous were known in the past to cause people problems on the international border. Such was the case of Leigh Van Bryan and Emily Bunting - a couple of British tourists who 'tweeted' that they were going to 'destroy America'. Although what they meant by that statement was merely 'heavy partying', the context of the post was not taken into account and the couple was denied entry to the United States.[41] In another example: someone who applied for a one-week tourist visa, but posted online 'farewell message' indicating several months of planned absence may want to overstay his or her visa, but might as well be planning to visit many countries in that time or switch visa classes (e.g. due to a genuinely planned marriage).[42]

It is essentially true that the success of intelligence gathering is not the information itself, but the value it adds to decision-making.[43] Therefore the most important part is the evaluation of the data gathered and the resulting decision-making, which should ensure the legitimacy and integrity of the visa granting process. Creation of a sound internal policy in this respect is highly advised, so no immigration officer is left alone with the decision about how to react in specific cases. It is essential to define internal rules of conduct in SOCMINT gathering, containing specific guidelines on how and when to react, what content should be flagged for further investigation, how to cross-check information, when to ask for additional documents, or personally confront the individual about their social media postings in questionable cases before making a final decision.

[40] See e.g. background check consent form for candidates for public office positions required in Canada, online: http://www.fja-cmf.gc.ca/appointments-nominations/forms-formulaires/bc-va/bc-va.pdf, [access: 15 IV 2018].

[41] R. Hartley-Parkinson, *'I'm going to destroy America and dig up Marilyn Monroe': British pair arrested in the US on terror charges over Twitter jokes*, Daily Mail 31 January 2012, online: http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html, [access: 15 IV 2018].

[42] Such case has been presented to the author during an anonymous research interview with an Australian government agency representative.

[43] D. Omand, J. Bartlett, C. Miller, *Introducing…*, op. cit., p. 7.

Conclusions and recommendations

SOCMINT use opens many possibilities for all types of state and private entities (including those involved in terrorist or criminal activity). Applying SOCMINT techniques in the immigration procedures may serve to gain an additional layer of security against terrorism threats as well as to help check applicant's visa eligibility better than before. Its use in the field of national security is therefore highly recommended. Immigration services are in perfect position to create appropriate 'data filters' using real personal data, which is an essential asset in terms of open source intelligence gathering. However, such use of personal data may require validation through at least vague background check consent form – depending on the specific conditions of the legal system.

Assessing one's social media postings may reveal threats to national security or other grounds for visa denial, but because of the potential problems with online identity verification and context-sensitive content it must be done with extreme care and with an 'innocent until proven guilty' mindset. Taking all the possible benefits and risks associated with SOCMINT use, it is highly advisable to develop an internal agency-wide policy concerning social media background checks. To conserve resources and minimise the risks, appropriate SOCMINT policy should cover such issues as: when to perform background checks (should all visa applicants be checked or just some groups, e.g. first-time visitors?), what tools should be used to gather information (will a SOCMINT gathering software be purchased?), where to look for information, how to cross-check findings and verify perceived online identity (should visa applicants be confronted with the suspicious content found on the social media profiles?), and how to assess various findings when it comes to the point of decision making. Creation of such policy should be followed with appropriate specialist training given to those who are to use it.

Abstract

Internet monitoring and open source intelligence techniques are becoming an important part of terrorism detection and prevention system. The abundance of personal information in the social media is currently used not only to detect terrorist activities but in 'regular' policing as well. The article explores the possibilities of the use of the so-called Social Media Intelligence (SOCMINT) in immigration procedures. Immigration services have unique capability to screen visa applicants in the context of their Internet postings. Such activity may allow to detect serious threats to national security, as well as verify visa eligibility in a more effective manner. However, SOCMINT techniques have their shortcomings which should be addressed in an appropriate internal policy governing their use.

Keywords: terrorism, immigration, OSINT, SOCMINT, social media