Critical Success Factors for OSINT-Driven Situational Awareness

Babak Akhgar
Douglas Wells
CENTRIC, Sheffield Hallam University, United Kingdom[1]

Abstract:
A critical element of successful intelligence-led law enforcement operations is the ability of the police and other security services to obtain timely, reliable and actionable intelligence concerning the problem, incident or investigation under focus. As well as traditional investigative techniques and information sources, open-source intelligence (OSINT) can provide additional capabilities for Law Enforcement Agencies (LEAs) to manage an investigation or address the intelligence requirements of a given incident. This position paper introduces the concept of OSINT, identifies and discusses existing effective practices and critical success factors for the fusion of OSINT with traditional intelligence sources. This paper is written as a position piece based upon CENTRIC operational involvement in 14 UK based LEA open source investigations over the years 2015 to 2017.

Keywords: OSINT, Situational Awareness, Law Enforcement.

Introduction

The private sector has, over recent years, increasingly began to use information from open online source, including social media, to measure customer loyalty, track public opinion and assess product perception (Neri et al., 2012). Coinciding with this trend, Law Enforcement Agencies (LEAs) are applying techniques to enhance their investigative capability towards improving their response to against criminal threats (Gibson 2004; Bell & Congram, 2012). As a result, Open Source Intelligence (OSINT) tools and techniques are increasingly used to be a part of law enforcement's investigative repertoire in the identification of criminals and their activities; including activities targeting recruitment, transfer of money, information and the coordination of illicit activity (Omand et al., 2012).

This paper examines the criteria used by law enforcement to utilise, deploy and maintain effective OSINT investigative tools and tactics, based on experiences gleaned from collaboration, cooperation, training and bespoke investigative work undertaken alongside regional UK police forces. Moreover, the paper highlights critical areas of consideration for modern OSINT practitioners. However, defining the specific characteristics of OSINT is not a straightforward task, the context and definition for the use of OSINT often changes dependent on the country and organisation of origin. The ambiguity of the term is explored in detail later in the 'Current Challenges and Dilemmas' section. Despite this contextual ambiguity, for the purposes of this pa-

[1] Corresponding author's email: d.wells@shu.ac.uk

per a working definition of OSINT is used, following the three following defining principles; *1) OSINT consists of data collected from 'publicly available sources', 2) it is data to be used in an 'intelligence context', and 3) the data collection can be performed in an overt manner.* Furthermore, from an ontological perspective the paper considers OSINT to be part of a LEAs situational awareness capabilities. Situational awareness, in the context of our discussion is defined as; 'the capability to identify, contextualise, visualise, process, and, comprehend the critical elements of intelligence about particular areas of concern. These areas of concern may be anything from an investigation to the management of a major crisis.

The authors acknowledge - and later explore in detail - the strengths and limitations of these terms and how they also allow for flexibility through their interpretation. These three defining statements are rough outlines rather than literal definitions and are explored in the section "Emerging Challenges to OSINT Interpretation". Indeed, it is worth noting that RIPA (Regulation of Investigatory Powers Act 2000) may be interpreted to have been written for the capacity for flexible and dynamic interpretations, and not to be an inconvenience or destructive restriction upon law enforcement.

Importance of Social Media

OSINT is increasingly focused on internet based and social media analysis (SOCMINT). To this extent the UK NPCC (National Police Chiefs Commission) have debated over whether to continue calling it OSINT, or internet investigations (NPCC National Open Source Intelligence and Investigations Conference, 2017). Whilst this may seem like a trivial point, it shows the prevalence and dominance of online and social media aspects of contemporary OSINT investigations over traditional 'offline' approaches. Currently, it appears that the use of internet based OSINT, especially regarding big data analytics are primarily used for intelligence gathering and investigations, and not for general community-policing. As of 2015, it was noted that in general, the majority of police forces and OSINT practitioners used; "social media… to inform strategies such as pre-emptive arrests, interceptions of activities, approaching particular individuals and groups, or change of tactics during events… (the lack of identifying community needs) is not yet part of police practice and raises concerns within police about the level of overlap between intelligence and engagement" (Carey, 2015). As with many aspects of law enforcement and other relevant security practitioners, levels of engagement towards social media largely differ between forces, with most mainly using it to engage with community regarding ad-hoc notifications, such as public information announcements, and petty crime announcements. This in itself may concerns members of the public whom may feel that OSINT monitoring may be a 'two-way mirror'[2], with intelligence practitioners able to observe and investigate, with minimum community engagement and interaction.

It is essential to understand and respect that many elements of OSINT investigations benefit from refraining full disclosure policies towards the specific tactics and solutions used. It should be made increasingly clear to the public, the tight rules and regulations that warrant and authorise deployment, as well as that public security and safety may benefit from the indiscretion and minimized disclosure of engagement which may help to track down community threats, protect vulnerabilities and to maximise order. It may also be beneficial to reassure public opinions that the police and other OSINT certified practitioners have to adhere to far stricter standards, than the majority of private corporations and enterprises that utilise big data analytics and collect, store and correlate personal data. To the computer-literate generations, the loss of control and ownership over personal data to organisations and corporations is not a revolutionary, or particularly terrifying revelation, however it may prove beneficial to reassure the collective, that OSINT has to adhere to far stricter protocols than agencies such as; Google, Facebook, Microsoft, and Amazon.

LEA Requirements in the Age of Austerity

Contemporary use of internet-based OSINT has helped increase the capacity and efficiency of police forces, this holds a direct knock-on effect for situational awareness capabilities. One of the leading benefits of OSINT is through the reallocation and reduction upon traditional resources. OSINT allows for relatively low-resource operations, these have the potential to save great amounts of physical and financial cost compared to traditional policing as they may carried out

[2] A two way mirror has connotations of surveillance, spying and monitoring without their knowledge: https://dictionary.cambridge.org/dictionary/english/two-way-mirror.

remotely, securely with surveillance and investigative practices often requiring far less manpower than the physical presence of officers 'on the scene'.

Additionally, OSINT training is seen to require relatively low cost and time investments when compared to other police force specialisations. The majority of UK based OSINT courses offer on average 2-7 day training packages, whereas undercover officer, firearms, covert surveillance, traffic, financial and corruption officer training courses often require intensive engagement courses of up to 18 months or longer (Nottinghamshire Police, 2008). Indeed, as of 2014, open source e-learning modules are available from the College of Policing consisting of condensed 35 minute long assignments (College of Policing, 2014) and requires little training for investigators compared to other policing specializations. Furthermore, if procedure, regulation and legislation are properly adhered to, OSINT operations are usually low risk due to the non-physical involvement, with mainly reputational and organisational damages on the line. Indeed, whilst reputational and organisational concerns surrounding online privacy and free speech are increasing, leading to increased force scrutiny from both public, judicial and NGO agencies, OSINT situational awareness also is increasingly utilised, perhaps paradoxically (Barnes, 2006), for public relations monitoring and post-event feedback as a necessary tool in improving community policing approaches.

Noticeably as IoT (Internet of Things) devices increasingly permeate all aspects of modern civilisation, all investigations now have a cyber element, this is especially true of considerations for police contamination of crime scenes through device connections to routers, local WiFi's, etc. potentially compromising evidential material. This concern also encompasses the branches of OSINT situational awareness, one example being officers trained in basic social media search queries alongside traditional note-taking to assist in community roles such as identification of alleged perpetrators. Furthermore, OSINT can be used to parallel intelligence, this capability allows LEAs to protect undercover and embedded agents as well as evidence and intelligence derived from. Closed sources may be passed onto OSINT teams to recreate the same information and leads from publicly available information.

Overall, OSINT is one of the few areas that LEAs and other security practitioners may 'bring the outside in', allowing for (vetted) external expertise and advice. Indeed, conveniently the motto of the UK Army's SGMI (Specialist Group Military Intelligence, whom routinely utilise open source analysis, is; 'bringing the outside in'. Due to the nature of the open source material OSINT situational awareness may be expanded in more convenient manners to the protocols surrounding covert and classified data. For example, the outsourcing of security work to researchers and analysts may allow for taskings that anonymise or mitigate data and intelligence concerns, instead focusing on specific lines of enquiry. For example, when investigating a particular individual, social media pictures may be doctored to hide the subject of enquiry but keep in the background imagery, allowing for external actors to seek intelligence on the desired location without compromising the information of the individual.

Core Requirements for Situational Awareness

The ability to covertly monitor individuals, suspected of involvement in serious criminal or terrorist activity, has obvious benefits for the LEA and the wider security community. OSINT techniques can be used effectively in response to a range of law enforcement issues, from enhancing community safety, tackling anti-social behaviour, through to fighting serious and organised crime and combating terrorism. Any covert technique, including undercover or publically undisclosed OSINT surveillance and monitoring must be used sparingly, appropriately and where OSINT is deployed, that it is transparent, auditable and in accordance with relevant legislation. CENTRIC OSINT involvement has observed seven priority requirements for emerging situational awareness trends:

1. Counter Terrorism focus of Situational Awareness

As notoriously publicised by the technical and disseminatory skill of the Islamic State in its prime operating years of 2014-2016 (Winter, 2017. p.6.), online open sources play a crucial role in the radicalisation, recruitment, training, financing and incitement of terrorist objectives. Counter terror (CT) situational awareness priority requirements have been observed to revolve around three key vectors:

A) Defensive measures to reduce the vulnerability to attack of populations, territories, infrastructure, *and communication systems of interest.*

B) Offensive measures to locate, prevent, deter and interdict terrorist activities.

C) Measures to limit the consequences of terrorist attacks and to stabilise the situation in the aftermath of such attacks, in support of civilian authorities.

Regarding defensive measures, OSINT situational awareness can greatly assist through measures such as counterintelligence and red-teaming wherein potential target locations and individuals may be examined by researchers to reveal potential data leakage and information freely available that may compromise their security. Offensive situational awareness OSINT measures may predominantly consist of traditional researcher and analyst investigative roles, locating, monitoring and reporting on terrorist sources. Limiting the consequences of terrorist actions are reactive measures including suitable public announcements, open source monitoring from a command and control perspective and may also include the crowdsourcing of intelligence for example when the FBI requested public help unmasking the Boston bombers of 2013 (Bruinius, 2014).

2. Cyber Focus

Cybercrime, cyberwarfare and cyberterrorism have each evolved rapidly and dynamically over the past decade. Although the perception of OSINT may traditionally be considered to be of lower technological finesse than conventional cyberattacks, threats and vulnerabilities, it however has proven to be a valuable tool in identifying emerging cyber trends and promoting greater resilience. One such important area is in the investigation of - and subsequent automated crawling of - forums and dark web markets promoting, encouraging, and selling guides on hacking as well as data and hardware exploitations. Increasingly, there is the demand for LEAs to utilise automated monitoring systems to alert OSINT investigators and analysts to indicators of such behaviours. This may include cross validation of news and public sources reporting discovered data breaches, personal info dumps with cross references to increased activity or keyword appearances on illicit sites such as identified darkweb forums.

3. Threat Financing

A key challenge facing LEAs and the wider security community is in identifying and obstructing the funding of hostile actors. Players participating in terrorism activities are likely to parallel organised crime groups (OCGs) financing tactics which are already proven and known to avoid the scrutiny of the financial and government watch teams. However, despite seeking the same objectives from a financial perspective the two groups may be argued to hold different end objectives: OCGs seek to gain as much profit as possible operating in a stable environment. Usually with a consumer reliant on their activities. It is usual for OCGs in close proximity to operate in some agreed harmony in the best interests of each OCG. On the other hand, terrorist organisations usually harbour a radical and political agenda that requires funding for organisational and operational capacity; as such they are less likely to be limited by considerations to conflict with any partner.

One of the leading and more complex challenges for situational awareness focused OSINT lies in identifying and classifying requirements for the relationship between criminal and terrorist funding, as well as being able to pinpoint when criminal activities may become terrorist financing and escalating to the suitable countermeasures and procedures. Subsequently, the priority approach for OSINT situational awareness of threat financing is:

1. *Establish the identity of funding streams to terrorists*
2. *Identify the bad actors within an OCG who is funding terrorism*
3. *Identify apparently legitimate financial streams that subsequently leads to terrorism.*

4. Analysis of Cryptocurrencies

One increasingly difficult element of threat financing is attached to blockchain cryptocurrencies. Whilst currencies such as bitcoin and Ethereum are publicly available and hold open ledgers, the tracing and monitoring of illicit exchanges requires highly specialised and trained individuals, often operating in the cybersecurity and espionage spheres.

The use of "spinners" or "tumblers" can make it frustratingly difficult for LEAs to track and trace online blockchain transactions (Darknetmarkets, 2017). Whilst it is appropriate to ensure that this funding method is not overlooked by OSINT and situational awareness focused departments, the actual proven cases appear limited; additionally, they appear to rely on a lengthy and complex period of comparing online marketplace details against individual blockchain transactions.

5. Weak Indicator Analysis

Weak indicators can be particularly useful in dealing with situations such as human trafficking, illegal migration, arms and explosives manufacture, and in relation to terrorist funding. Weak indicator crawling analyses the 'ingredients' of potential threats or areas of interest, for example weak indicators, or ingredients, may be rise in hawala networks, increased ivory trade or sim card customs seizures, relating to generating money for terrorist groups. Each individual ingredient isn't a useful indicator of the overall potential funding, however when clustered together, these automated captured ingredients may reveal areas of interest that indicate a wider problem.

When utilising big data solutions and weak indicator analysis, it may be encouraged to split OSINT situational awareness teams between human led investigators and analysts and data scientists and researchers dealing with the interpretation of quantitative data. CENTRIC operations allow for the close proximity of the teams to mutually reinforce the direction of the investigation. One example of harmonious working is through the analysis of alleged terrorist recruitment social media profiles - these profiles may consist of thousands of separate individual connections. The human led operation may focus upon individuals whose profile pictures appear to support terrorist badges, emblems or carry firearms during time restrictions, however the data interpreter may assist leading the investigation towards other profiles, for example female accounts (Dearden, 2017) whom whilst not suspicious looking, are priority accounts mapped out in relation to their connection and prevalence throughout the suspect networks. Here, successful OSINT situational awareness utilises the 'human in the loop' alongside the cognitive objectivity of big data and weak signal analysis. Indeed, 'the major difference between basic and excellent OSINT "operations" lies in the analytical process' (Hribar, et al. 2014), fusing both human led knowledge with machine based capabilities.

6. Data Capture

When conducting research, operators should be encouraged to keep all tabs open, this allows a recollection of how the user got from A to Z and assist them in explaining any links if required by a senior officer. Additionally, the use of secure logbook tools such as OSIRT (OSIRT, 2017) are actively encouraged for managing histories, logging details, data capture and encrypted storage as well as for hashing documents with time stamps. Overall, the tasking document for a specific investigation or operation is the single most important article in the process. All providers should make every and all efforts to ensure all information is provided, including historic emails, mobile numbers, landlines, associates etc. Custodial records often hold a wealth of data that can often be overlooked.

One such recommended approach for data collection best practices is modelled upon the; 'The JAPAN Approach'. First developed in 1998 following the introduction of the Human rights Act by Kent Police; it is broken down in the following diagram and plays an essential role in guiding OSINT and situational awareness practice:

Justified	The actions must be justifiable in the current circumstances. For example; can the 'need for' and 'method of acquisition' to view, collect, store, and, share personal or potentially sensitive information be deemed reasonable.
Authorised	Depending on the circumstances, there may be a need for the authorisation of specific actions or focuses of the investigation. Either the individuals involved should have suitable authorisation to carry out such tasks, or it has been cleared/designated by a manager responsible for such actions.
Proportionate	The actions and data collection of the investigation must be proportionate, it must be ensured that they could not be collected reasonably and efficiently from other means, and it is necessary to pursue them altogether.
Auditable	The chain of evidence gathered from the investigation should be auditable and sufficient enough to hold up in a case of law. There must be evidence and clear presentation of how each step of the investigation is linked and developed.
Necessary	The investigator must ensure that the sought after investigation results are of importance and are being pursued in the best practice.

7. Emerging Challenges to OSINT Interpretation

Despite the best efforts to define OSINT at the beginning of this paper, the term itself and its defining characteristics are not absolute. Indeed, regarding the three defining characteristics of situational awareness OSINT there are significant criticisms of their ambiguity and how they are actually interpreted by law enforcement (Hulnick, 2010). Leading criticisms of the interpretation of OSINT are primarily focused on the definition points one and three (Gibson, 2004) (Holland, 2012), they are explored below:

1) OSINT consists of data collected from 'publicly available sources',
2) It is data to be used in an 'intelligence context',
3) The data collection can be performed in an overt manner.

Regarding the first defining point, 'publicly available sources' used in a policing intelligence context also includes financial data (such as credit reports and bank details), vehicle registration data (such as from DVLA databases and insurance providers) as well as additional data supplied to law enforcement from specialists companies that deal in bulk data and communications information. UK based companies such as Connexus GBG (GBG, 2017) and Cosain 9 (Gov.uk, 2017) utilise mobile and social media data, however only sell their specialist services to LEAs, or on occasion to other specialists. The access to such data opportunities is particularly contentious as, despite branding, they are not openly available to members of the public.

Additionally, relating to the third defining factor; the point of challenge relates to the mention that the data collection 'can' be carried out in an overt manner, but rarely does so. Indeed, such online aspects of OSINT require anonymity and discretion, in part due to data protection and policing standards, and, therefore will not be noticeable. For example, the viewing of social media profiles, without direct interaction and communication, will usually never notify the target profile they are being viewed, this is similar for the police use of specialist companies and services as detailed above for big data and communications information.

Sound usage of OSINT situational awareness must therefore include proper situational awareness that reflects on such emerging criticisms as open source investigations and intelligence increasingly become mainstream avenues of enquiry as well as becoming more prominent in the public's general knowledge thanks to modern investigative journalism and media programs. Given the ongoing debate of security and liberty between political groups, members of the public and the current government, the relatively modern integration of internet-based OSINT capabilities for surveillance and investigation, are potentially volatile topics in the post-Snowden era (Rigoglioso, 2014).

Conclusion

Overall, contemporary OSINT situational awareness is largely and increasingly dominated by online research and investigations. Due to the nature of these actions being somewhat ambiguous it is imperative that efforts are made by LEAs to balance a degree of transparency alongside protecting specific methods and tactics. Modern OSINT situational awareness has assisted LEAs with increased capacity and operational effectiveness, additionally its format allows for a degree of outsider support networks through outsourcing tasks to experts and vetted individuals. In particular, this approach has helped through emerging security concerns such as terrorist networking, cybercrime actors and threat financing trends. The inclusion of experts, analysts and security personnel into modern OSINT is an essential factor for success - the importance of the 'human in the loop' is critical for efficient, accountable and proportionate intelligence gathering. Indeed, modern tools supplied to LEAs are often of great value when used to cut away the noise and help focus investigations.

All contemporary OSINT situational awareness should be captured to the highest level of accountability, integrity and proportionality, such as through the 'JAPAN' approach described, by doing so this helps safeguard modern OSINT situational awareness methods against some of the emerging challenges, which include potential negative fallout from increasing public awareness of modern surveillance operations..

References

- Barnes, S., (2006) A Privacy Paradox: Social networking in the United States.
  Available at: http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523 (Accessed online: 17/12/2017)
- Bell, P. & Congram, M. (2013) Intelligence-Led Policing (ILP) as A Strategic Planning Resource in the Fight against Transnational Organized Crime (TOC). International Journal of Business & Commerce, 2 (12), 15-28.
- Bruinius, H., (2014) FBI asks Americans to help IS masked Islamic State Jihadi. Good idea?
  Available at: https://www.csmonitor.com/USA/Justice/2014/1008/FBI-asks-Americans-to-help-ID-masked-Islamic-State-jihadi.-Good-idea (Accessed online: 17/12/2017)
- Carey, Z., Denick, L., Hina, P. & Hintz, A. (2015) Managing 'Threats': Uses of Social Media for Policing Domestic Extremism and Disorder in the UK.
  Available at: http://www.dcssproject.net/files/2015/12/Managing-Threats-Project-Report.pdf (Accessed online: 17/12/2017)
- College of Policing (2014) e-Learning Release Bulletin.
  Available at: http://www.ncalt.com/file/October%202014%20E-Learning%20Release%20Bulletin.pdf (Accessed online: 16/12/2017)
- Darknetmarkets (2017) Best Bitcoin Mixers 2017.
  Available at: https://darknetmarkets.co/category/btc-mixer-tumber/ (Accessed online: 17/12/2017)
- Dearden, L. (2017) How Isis attracts women and girls from Europe with false offer of 'empowerment'.
  Available at: http://www.independent.co.uk/news/world/europe/isis-jihadi-brides-islamic-state-women-girls-europe-british-radicalisation-recruitment-report-a7878681.html (Accessed online: 17/12/2017)
- Denick, L., Hintz, A., et al., (2015) Managing 'Threats': Uses of Social Media for Policing Domestic Extremism and Disorder in the UK.
  Available at: http://www.dcssproject.net/files/2015/12/Managing-Threats-Project-Report.pdf (Accessed online: 09/04/2018)
- GBG (2017) Introducing GBG Connexus.
  Available at: https://www.gbgplc.com/uk/products/gbg-connexus/ (Accessed online: 18/12/2017)
- Gibson, S. (2004). Open source intelligence: An intelligence lifeline. *The RUSI Journal*, 149(1), pp.16-22.
- Gov.uk (2017) Digital Marketplace: Cosain 9.
  Available at: https://www.digitalmarketplace.service.gov.uk/g-cloud/services/945108024310388 (Accessed online: 18/12/2017)
- Greenberg, J., "Why Facebook and Twitter can't just wipe out ISIS online". Wired Online, November, 2015.
  Available at: https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/ (Accessed online: 01/02/2017)
- Holland, B. (2012) Enabling Open Source Intelligence (OSINT) in private social networks. Graduate Theses and Dissertations, 12347.
  Available at: https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3354&context=etd (Accessed online 09/04/2018)
- Hribar, G., Ivanusa, T. & Podbregar, I., (2014) OSINT: A 'Grey Zone'? International Journal of Intelligence and Counter Intelligence, 27(03), 529-549.
- Hulnick, A. (2010) The Dilemma of Open Sources intelligence: Is OSINT Really Intelligence? In: Johnson, L.K. (ed.): The Oxford Handbook of National Security Intelligence. DOI:10.1093/oxfordhb/9780195375886.003.0014
- Kent Police (1998) The JAPAN Test.
  Available at: http://www.kelsi.org.uk/__data/assets/pdf_file/0003/26706/Japan-Test.pdf (Accessed Online: 13/01/2017).
- Neri, F., Aliprandi, C., Capeci, F., Cuadros, M., & By, T. (2012) Sentiment analysis on social media. Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining, 919-926.
- Nottinghamshire Police (2008) Procedure on Firearms Learning and Development V.20.
  Available at: https://www.nottinghamshire.police.uk/sites/default/files/documents/files/pd%20514%20Firearms%20Learning%20and%20Development%20-%20PROCEDURE%202008%20-%202010.pdf (Accessed Online: 16/12/2017)
- Omand, D., Bartlett, J., & Miller, C. (2012) Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security, 27 (6), 801-823.
- OSIRT, (2017). The Browser Made for Open Source Intelligence.
  Available at: http://osirtbrowser.com/ (Accessed online: 17/12/2017)
- Rigoglioso, M. (2014) Civil Liberties and Law in the Era of Surveillance. Stanford Lawyer, 91.
  Available at: https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance/ (Accessed 09/04/2018)
- SRIEE (2017) Personal Communication, West Yorkshire Police Cybercrime Officer, Tallinn Estonia.

- Strauss, J, S., (2004) Dangerous thoughts? Academic freedom, free speech, and censorship revisited in a post September 11th America. Washington University Journal of Law & Policy, 15(01).
  Available at: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1290&context=law_journal_law_policy (Accessed online: 01/02/2017)
- Stone, G. (2009) Free Speech and National Security. University of Chicago Law School. Chicago Unbound, 84.
  Available at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2975&context=journal_articles (Accessed online: 01/02/2017)
- UNSC (2016) Security Council Presidential Statement Seeks Counter-Terrorism Committee Proposal for 'International Framework' to Curb Incitement, Recruitment.
  Available at: https://www.un.org/press/en/2016/sc12355.doc.htm (Accessed online: 01/01/2017)
- Winter, C. (2017) Media Jihad: The Islamic State's Doctrine for Information Warfare. Institute for Strategic Dialogue.
  Available at: http://icsr.info/wp-content/uploads/2017/02/Media-jihad_web.pdf (Accessed online: 16/12/2017)