OPEN SOURCE INTELLIGENCE (OSINT)

By CDR Tristan Lovering MBE, Royal Navy
Intelligence Section Head
Joint Warfare Centre

Bloomua/Shutterstock.com

DATA MINING IN **REAL** and **SYNTHETHIC** ENVIRONMENTS

COLLECTING INTELLIGENCE THESE DAYS IS AT TIMES LESS A MATTER OF STEALING THROUGH DARK ALLEYS IN A FOREIGN LAND TO MEET SOME SECRET AGENT THAN ONE OF SURFING THE INTERNET UNDER THE FLUORESCENT LIGHTS OF AN OFFICE CUBICLE TO FIND SOME OPEN SOURCE.[1]

UKRAINIAN pro-Russian rebels use it, as do Boko Haram in Nigeria; Al-Shabaab in Somalia embrace it, as do the terrorist organisation ISIS in Iraq and Syria — in one way or another, all exploit social media for their own recruitment and propaganda purposes. Posts by fighters and their supporters make the news, and no one from across the NATO Alliance could have failed to see the disturbing reports emanating from the Levant in the last year. As an example, while their extremist policy towards the local population is horrific, and actions against their myriad victims utterly deplorable, one area in which the ISIS appears to be particularly effective is in the way they manage and exploit social media for their own ends. Using Twitter, You Tube, Facebook, Google+, Instagram, Pinterest and WhatsApp, both ISIS and Al Qaeda[2] create pages as a means of broadcasting beheadings, public executions, torture and the use of child martyrs. Intelligence commentators have reported that the Web has consequently become the terrorists' "command and control network of choice."[3] Whilst the World Wide Web should be a neutral conduit of data, which sits outside conflict and crime, internet providers not only host material of violent extremism, but also facilitate the flourishing of criminality and terrorism.

"Data Explosion"

The volume of the information flow ("Big Data") is staggering. The growth of Open Source and exponential increase in the use of social media reflects what technology experts call the "data explosion." In every one minute

of internet time 3,000+ photos are uploaded; 277,000 log onto Facebook; there are 330+ new Twitter accounts; 100,000 new tweets; over two million Google search queries and more than 30 hours of video uploaded onto YouTube. Internet users have now passed the 3 billion mark (3 November 2014, 40.4% of the global population), and over 2 billion people now have an active social media account[4] (28% of the global population). The plunging costs of mobile telephone ownership and wider availability have resulted in 1.639 billion (23%) of the global population now having active mobile social media accounts. This trend looks set to continue, as the Apple Corporation sold over 74 million mobile telephones (greater than the entire population of France!) to a burgeoning customer base in China in just one three-month period alone.[5]

"New Media"

Replicating this volume of information and variety of news in JWC's operational level exercises is critical. As the scope which includes individual "citizen reports", photographs and commentaries is also evolving in the real world of journalism, it is how we use this scope in our training and how we export it into a synthetic domain (News Web) which is of key importance.

The evolving media and the "Changing Face of News" was discussed in a recent Chatham House Conference in London. The forum reviewed the new demographics of young people following events in Syria, Ukraine and the terrorist attack in Paris, and concluded that mainstream channels were no longer the preferred means by which many access the latest information.[6] Whilst the stalwarts of the international media (CNN, BBC, Reuters, AFP, Wall Street Journal, etc.) appeal to the older generation, their immediacy, format and style do not attract younger readers.

New sites like the Daily Beast, Vice News and Buzz Feed are changing what is broadcast by whom, and when. No longer the preserve of "long in the tooth" journalists who have practiced their trade for decades, "new media" is less sanitized or edited, and consequently has growing appeal. For the under 35s, as long as the news is vibrant, authentic and live from the front line, many prefer the new type of presentation, most of which also include video clips of varying duration. The report is timely, uncensored and not "interpreted" by an expert — it is simply information uploaded by those whom it affects the most, on the ground, at the epicenter of any given story. The viewer is then left to make their own assessment of the credibility of the source and the reliability of the information. Where the information appears to be actively manipulated or falsely presented, alternative sites, such as stopfake.org, are there to highlight perceived lies, deception, deceit and propaganda.[7]

Simulating this environment in NATO, exercises will require focus and sustained effort. This becomes even more challenging when considering the plethora of new independent sources, and the growing population of citizens "armed" with mobile telephones. As the public upload an array of data onto news and social media sites, it will require flexible, agile and intimate scrutiny by the military. This will impact on all future NATO operations and necessitate full acknowledgement when developing our own Strategic Communications (StratCom) themes. Successful overwatch will be key for maintaining the Information Operations (IO) and Psychological Operations (PsyOps) campaign, and to ensure that whatever information is available is scrutinized appropriately by the Intelligence staff.

Open Source

Advocates such as Major General Michael T. Flynn and Robert David Steele (a former Marine and a former CIA officer) frequently stress

Jordanians gather in Amman to light candles in memory of the Jordanian fighter pilot Moaz al-Kasasbeh who was burnt alive by the ISIS militants in Syria, 6 February 2015. Photograph by Zaid Saadallah/Shutterstock.com.

the need for new methods to transform the craft of Open Source Intelligence (OSINT).[8] They and others recognize that OSINT often equals or surpasses classified material and is frequently faster to arrive, easier to access and significantly cheaper than alternative sources.[9] That being said, some military observers still view OSINT as a less reliable source than other types of Intelligence (Imagery, Signals, Human, Electronic, Technical, etc.) — an assumption which is flawed, as OSINT deserves greater focus and attention. Just as with all Intelligence, the key is to get the analysis right, both in terms of confidence in the source and an accurate assessment of the reliability of that information.

At the operational level, no single source of Intelligence is of greater value than the other. However, the emphasis on one particular type may weigh more heavily depending upon the target, and on whether the Joint Force Command (JFC) has the most appropriate collection capability for that objective.[10] Despite reliance possibly switching from one type to another, *all* Intelligence has value. Confidence in that reporting increases exponentially if cross-checked with other sources and corroborated. The aim is to build an all-source, integrated Intelligence picture in which the JFC has an articulated level of confidence. Regardless of source or agencies, promoting a particular type (primacy) undermines the value of the whole Intelligence enterprise. Timely fusion of all Intelligence types, and objective reports with sound analysis is what distinguishes a great Intelligence section from an adequate one.

However, it is not just those from the Intelligence community who need to be cognizant of this plethora of useful information online — the ability to scrutinize and assess is dependent upon the whole staff monitoring, evaluating and recognizing salient information when "surfing". The old adage that soldiers, sailors and airmen are the best sensors is not only true on the battlefield, but is equally critical for today's personnel while navigating the Web. They need to remain alert when accessing social media in order not only to safeguard personal and unit security, but should remain cognizant of information available in Open Source to identify potential leads for NATO exploitation.

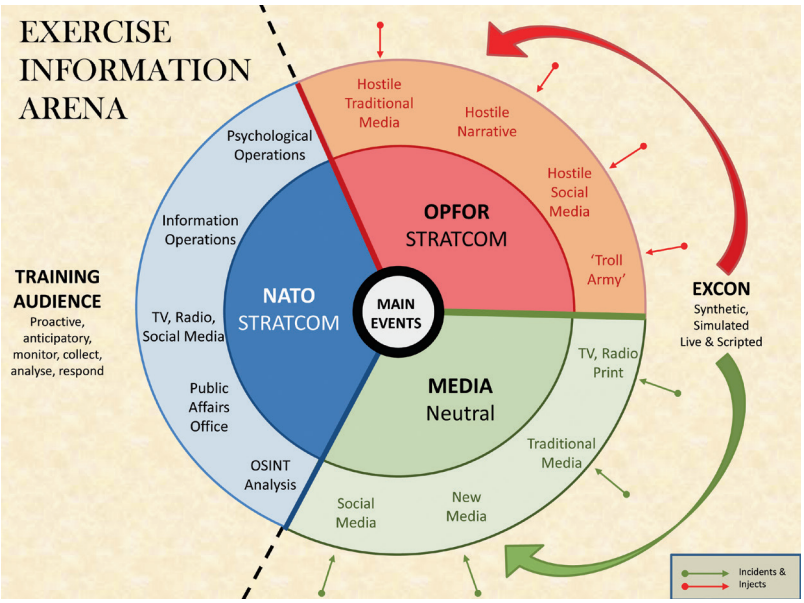
Whether Web based aerial imagery, or information gleaned from social media, if it enhances military understanding, it should be fused with data retrieved from other sources and agencies. A photograph of a terrorist outside a building (posted on Facebook), a ground-based SAM engagement of a helicopter (video uploaded to YouTube), or of rebels executing prisoners (Instagram), it is not just news; it is unprocessed "raw" intelligence.

Precedent

Tracking the activities of potential enemies via Open Source is nothing new; precedent of this source confirms its value in building early Situational Awareness (SA). The U.S. Government, for example, relied upon information gleaned from Japanese newspapers in the 1930s in order to build a better understanding of the Imperial Japanese Navy, the number and type of warships and their home port. Whilst time consuming, the American military attaché oversaw the translation, then read and analyzed newspapers from Tokyo, before forwarding his findings to the Office of Naval Intelligence (ONI) in Washington.

A decade later in 1943, the Allies called upon the British public for holiday brochures and postcards from the coastal areas of Norway, Denmark, the Netherlands and France prior to D-Day. Intelligence staff trawled thousands of documents, listed and "fused" information about potential landing beaches and then made recommendations for further Intelligence, surveillance, and reconnaissance collection (e.g. aerial imagery, submarine surveillance, close target reconnaissance by French Resistance, etc.) of the most suitable landing sites.

The European Union Naval Force monitored Twitter for indicators and warnings that Pirate Action Groups were about to strike from



Left: A powerpoint slide showing the Information Arena for JWC exercises at the operational level. **Right:** A press conference during exercise TRIDENT JAGUAR 14, Menorca, Spain. Photograph by JWC PAO.

the Somali coast, and Israeli organisations (e.g. Meir Amit) tracked Facebook accounts used by Hamas Youth Camps operating across the Gaza strip as they trained new activists.

The Russians are seeking to exploit all multilingual data in Open Source, and their Defence Ministry is developing new computer programmes designed to monitor and analyse social media.[11] Reports refer to a proactive and highly competent "Troll Army", refining propaganda skills and taking the initiative online. A Kremlin "Troll Factory" has been established in Savushkina street in St. Petersburg, with the aim of spreading disinformation, creating parallel "reputable" media websites and producing fake reporting.[12] They re-write breaking news, undertake crude spamming, post aggressive comments on forums and present Putin's alternative view on the conflict in Ukraine. A number of the NATO members are determined to exploit the new opportunities presented by the plethora of media websites and commentary on Facebook and Twitter. The UK military are establishing a "new Brigade for the Information Age", a team of "Facebook warriors",[13] whose role will be to monitor and track 24-hour news, smartphones and social media, with the objective of "controlling the narrative".

A spokesperson for the intended 1,500 personnel in the new 77 "Chindit" Brigade said: "77 Brigade is being created to draw together a host of existing and developing capabilities essential to meet the challenges of modern conflict and warfare. It recognizes that the actions of others in a modern battlefield can be affected in ways that are not necessarily violent and it draws heavily on important lessons from our commitments to operations in Afghanistan, amongst others."[14]

The advent of the new "citizen journalist" is a good example of how much can be drawn from social media. From a bland office in Leicester, Eliot Higgins successfully tracked the removal of the Russian missile launcher linked to the downing of Malaysian airliner MH17 in 2014.[15] In three years, the investigative blogger has tracked weapon sales to ISIS, plotted locations of executions in the Syrian Desert, and identified specific chemicals used by the Assad regime.

Sleuths from the website bellingcat.com have demonstrated just how effective fusion of online information can be. Investigators are exposing how much key material is available, and how, if assessed and scrutinized appropriately, it can lead to real, tangible and actionable intelligence. Vladimir Putin's propaganda chiefs as well as ISIS now have an unlikely nemesis, as people like Higgins scroll through posts made by unwitting fighters in different conflicts around the world.[16]

Challenges

Within the military, the most salient problems remain attitudinal, cultural and human. There is a misperception that because information has been classified "SECRET", it automatically becomes Intelligence, and conversely, because information might have been collected from Open Source, it is consequently *not* Intelligence. Other challenges are that the Intelligence community's standard mode of

TRADITIONAL MEDIA

Observer: Trained journalist
Assessment: Informed analysis
Information: Filtered/compressed
Type: TV or print
Credibility: Good +
Reliability: Good +

NEW MEDIA

Observer: Citizen journalist
Assessment: Basic or specialist
Information: Immediate/agile
Type: TV and print
Credibility: Good —
Reliability: Fair

Twin Design/Shutterstock.com

SOCIAL MEDIA

Observer: Public/witness
Assessment: Limited/none
Information: Raw/uncensored
Type: All formats
Credibility: Unknown
Reliability: Fair +/—

operation is generally passive about aggregating information that is not enemy related, and some individuals remain transfixed by one type of collection capability and ignore feeds from other sources. Maintaining Operational Security (OPSEC) in this evolving, dynamic environment also remains a challenge — specifically in terms of identifying that information, which is suitable for release and that which, if shared, would undermine NATO's operational effectiveness. Protecting personnel whilst online is imperative, and therefore the widest promulgation of NATO security policy for social networking remains critical.[17]

JWC's synthetic environment

Simulating Open Source information is a challenge because of the volume of data, differing levels of reliability and confidence in that information as well as the frequency of information posted or uploaded online. A former director of U.S. Defense Intelligence, Lieutenant General Samuel V. Wilson, said that "90% of Intelligence comes from open sources,"[18] so it is important to get the synthetic domain right. It is an area, which will impact on the JFC, not only in terms of the requirement for suitably trained OSINT analysts, but on cyber and CIS capabilities as well. The challenge rests not only with the Intelligence section, but with the Media/Public Affairs, StratCom, Information Operations and Psychological Operations teams, in translating and interpreting a plethora of information and identifying "the wood from the trees." It is not good enough simply to cut and paste; the skill lies in analysis, building understanding, assessing reliability and confidence in the sources, and presenting it in a timely and digestible format.

The successful delivery of JWC exercises depends upon the provision of a realistic environment replicating the real world. The Scenario Section in JWC's Joint Exercise Division (JED) constructs this from early concept through to execution. In Phase III (force activation, deployment and operations) it is supported by relevant Subject Matter Experts (SMEs) in the Exercise Control (EXCON) who undertake live (dynamic) scripting, enhancing both context and content. The Training Audience (TA) builds a comprehensive picture around this information, and the Intelligence staff provides a holistic assessment of the complex, inter-locking and overlapping factors which shape that scenario.

The "Information Arena"

The "Information Arena" requires careful coordination in order to ensure that the synthetic picture is realistic, relevant to operational dilemmas and designed to ensure opportunity to satisfy all TA Training Objectives. Appropriate injects via the media, close collaboration with the Opposing Forces (OPFOR), and a scenario that is flexible enough to shape — in line with the direction taken by the TA's Operational Plan (OPLAN) — is the foundation to success. Replicating this on exercises is crucial, particularly with SACT's focus on the Joint Intelligence, Surveillance and Reconnaissance (JISR) objectives and its prominent endorsement in the latest keystone Intelligence Doctrine.[19] This aim is to ensure Intelligence understands the complexity of modern operations and facilitates a single Intelligence environment to support decision makers at all levels. The task is to make the Intelligence community not only stronger, but relevant, and JWC exercises

A close-up of the simulation media equipment, Joint Warfare Centre.

provide the perfect forum for achieving that objective. The Media cell established an active social media environment in 2012 and it continued to build on replicating Facebook with "Face Page", and Twitter with "Chatter", in each exercise since then. They provide comments on the unfolding story of the conflict, create posts by fictional characters which add further depth, and ensure an alternative source of information for the JFC to assess.

Information exploitation

Publicly available data is so voluminous, detailed, explicit, and broader than ever before that replicating it will remain a challenge. Much is rudimentary "background noise", or repetition, some is useful or provides context, and occasionally some material is like a gold seam from which the most revealing data can be mined. Intelligence-led operations are about exploiting all available information. A "call to arms" is required so that commanders recognize that Open Source information is a crucial strand of evidence, which assists in building understanding. It underpins the "Joint Intelligence Preparation of the Environment" and shapes subsequent operations in conflict.[20]

The replication of Open Source will continue to be delivered and enhanced in JWC-facilitated scenarios in 2015 and beyond. Exercise TRIDENT JUNCTURE 15 (TRJE 15) will provide an opportunity to practice Open Source analysis, and getting the appropriate training methodology and suitably qualified personnel in place will be key. Of course, the perennial military dilemma remains: does the JFC then decide to exploit that source of information for strategic/operational Intelligence purposes, or does the commander seek tactical advantage by targeting or neutralizing in order to deny the enemy their ability to communicate? Whether social media is used as a source for enhancing Situational Awareness or to cue JISR activity, publicly available information is invaluable. Analysis of Open Source is now a "must do" not a "nice to have." Consequently, the requirement to monitor all aspects of online activity remains mission critical not only for Intelligence specialists, but for the JFC as a whole. We need to look through our target's eyes, uncover their digital footprints, understand their deception and reveal their identity. It requires imaginative and agile solutions, to be embraced and resourced in reality, and fully replicated and practiced on exercise. After all, the secrets are out there, it is just a matter of knowing where to find them.

END NOTES:

(1) Studies in Intelligence (CIA Journal, Declassified or Unclassified Articles), Vol. 48, No. 3, pp. 45–55, "Sailing the Sea of OSINT in the Information Age", by Stephen C. Mercado, (2004).

(2) Inspire is Al Qaeda in the Arabian Peninsula's (AQAP) magazine, and is one of many English language extremist publications now available online.

(3) Financial Times, 3 November, 2014: "The web is a terrorist's command-and-control network of choice", by Robert Hannigan.

(4) See for example http://www.internetlivestats.com/internet-users/ (Accessed 22 January 2015).

(5) New York Times, 27 January 2015: "Apple's China Strategy Pays Off With Surge in Earnings", by Brian X. Chen. Sales of iPhones shattered analysts' predictions. Apple said it sold 74.5 million iPhones in the quarter, as many as 12 million more than expected.

(6) Chatham House, The Royal Institute of International Affairs, 28 January 2015: "The Changing Face of News' forum: The panelists explored the evolving digital news landscape and considered whether new formats are engaging younger audiences by challenging mainstream news reporting. See: http://www.chathamhouse.org/event/changing-face-news#sthash.mMkhyPNv.dpuf (Accessed 29 January 2015).

(7) See: www.stopfake.org, established to stop fake information about events in Ukraine. The main purpose of this particular community is to "check facts, verify information, and refute distorted information and propaganda about events in Ukraine covered in the media." (Accessed 2 February 2015)

(8) OSINT also referred to as Digital intelligence (DIGINT) by some national intelligence agencies.

(9) Studies in Intelligence (CIA Journal, Declassified or Unclassified Articles), Vol. 49, No. 2, "Re-examining the Distinction Between Open Information and Secrets", by Stephen C. Mercado, (2005).

(10) For some Component Commands this may only require IMINT, for others only SIGINT, HUMINT, TECHINT or GEOINT etc.

(11) Gazeta Russia, "Social Networks Under the Hood of Shoigu", [Russian Defense Minister Sergei Shoigu], 29 January 2015. See: http://www.gazeta.ru/politics/2015/01/28_a_6391297.shtml (Accessed 29 January 2015).

(12) The Interpreter, A Special Project of Institute of Modern Russia, "Russia Update: Defense Ministry Plans New Computer Programs to Monitor & Analyze Social Media", and "Confessions of a Former Kremlin Troll", by Catherine A. Fitzpatrick, both articles available at http://www.interpretermag.com/russia-update-january-29-2015/#6579 (Accessed 29 January 2015).

(13) The Guardian, 31 January 2015: "British Army creates a team of Facebook Warriors", by Ewen MacAskill. See: http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade (Accessed 31 January 2015).

(14) BBC, 31 January 2015: "Army sets up new brigade for information age" http://www.bbc.com/news/uk-31070114 (31 January 2015)

(15) See: "Geolocating the MH17 Buk Convoy in Russia", 29 September 2014, by Veli-Pekka Kivimäki https://www.bellingcat.com/resources/case-studies/2014/09/29/geolocating-the-mh17-buk-convoy-in-russia/

(16) The Independent, Sunday 18 January 2015: "With ISIS, Assad and Putin exposed, who's next on citizen journalist Eliot Higgins' list?", by Ian Burrell.

(17) See: NCIA, Cyber Security Service Line: "Security Recommendations for Social Network usage", [NATO UNCLASSIFIED], (V1.0, January 2015).

(18) The Washington Times, 14 November 1997, Reported "Aspiring to Spying," by David Reed.

(19) See: NATO Doctrine, Intelligence AJP-2, [NATO UNCLASSIFIED], (Edition A, Version 1, 2014).

(20) Kings College London, The Policy Institute at Kings: "A Call to Arms: Open Source Intelligence and Evidence Based Policymaking", by Mick Endsor and Dr Bill Peace, Visiting Senior Research Fellow at the International Centre for Security Analysis (19 Jan, 2015). Available at: http://blogs.kcl.ac.uk/policywonkers/osint-and-evidence-based-policymaking/ (Accessed 20 January 2015).