Social Media and Intelligence

Gregory F. Treverton
Renanah Miles

NATIONAL DEFENCE COLLEGE

Social Media and Intelligence

NATIONAL DEFENCE COLLEGE

Social Media and Intelligence

Gregory F. Treverton and Renanah Miles

NATIONAL DEFENCE COLLEGE

Title: Social Media and Intelligence

Authors: Gregory F. Treverton and Renanah Miles
Center for Asymmetric Threat Studies (CATS), Swedish National Defence College

ISBN 978-91-86137-37-3

Printed by: Elanders Sverige AB, 2014

The report can be downloaded from www.fhs.se

Preface

The study “Social Media and Intelligence” by Dr. Greg Treverton and PhD-candidate Renanah Miles is very timely and highlights the social media challenges for most of the Intelligence Communities around the world. It deals with social media from several perspectives: As an internal sharing tool, a tool for strategic influence like we saw during the Ukraine crisis during the spring and summer of 2014, and as a giant well of intelligence to be collected and analyzed. With this paper Greg Treverton concludes his six years productive assignment as a senior fellow with CATS as he now is assigned the position as Chair of the US National Intelligence Council (NIC).

Lars Nicander
Director, Center for Asymmetric Threat Studies (CATS)

Social Media and Intelligence

This paper is part of CATS' project on intelligence for terrorism and homeland security, sponsored by the Swedish Civil Contingencies Agency (MSB). It addresses the use and potential use of social media in intelligence – looking across the range of possible uses both externally and as collaborative tools within and across agencies. The first half of the paper lays out four categories of intelligence interactions using social media, and then discusses them briefly, drawing primarily on U.S. experiences. The second part of the paper turns more specifically to the mix of new media and old at play in conflicts around the world, especially in the Middle East and Russia/Crimea/Ukraine.

Intelligence Uses of Social Media

For starters, it is worth being careful over language. "Social media" has become the umbrella term, but it is not very helpful as a label because it lumps together a range of applications with overlapping and discrete functions. Of familiar media, for instance, Twitter is highly social – anyone can join. By contrast, Facebook is primarily a means of letting people keep in touch with their network of "friends", and various instant messaging (IM) applications tend to be most used in place of email, for peer-to-peer communications. The general term "social media" obscures the discrete functions of individual applications. Moreover, "social" in the label tends to connote non-work purposes.

Social media are important in and of themselves, but they are also at the cutting edge of broader changes that are enveloping intelligence. In many respects, social media are the antithesis of intelligence. Social media are active and transparent, while traditional intelligence is passive and opaque. They blur the distinctions that have been used to organize intelligence – between collector, analyst and operator, or between producer and consumer. They completely upset existing notions about what intelligence's "products" are. Coupled with smart phones, they can turn any human into a geo-located collector and real-time analyst. They offer enormous promise, but also carry large risks and obstacles.

The figure below lays out four kinds of intelligence interactions using social media:

Figure 1: Four Kinds of Intelligence Interactions through Social Media[1]

Familiarity of sharing

	Known	Unknown
External	Examples: Targeting for various purposes using social media	Examples: Twitter, Facebook
Internal	Examples: IM, intraoffice blog	Examples: Intellipedia, A-Space

Familiarity with participants

The functions are based on whether the participants are known or unknown to the official engaging in the interaction, and whether the purpose is communication internal to the agency or Intelligence Community (IC), or external. Plainly, though, the distinctions are not discrete but rather continuums, matters of more or less. U.S. intelligence's Intellipedia (an internal wiki) or A-Space (now iSpace and open to most officers with appropriate clearances, but originally designed for analysts to meet and work together), for instance, might be put in the lower right quadrant because most of the participants may be unknown to each other, at least initially. However, if their names are unknown, salient characteristics are not – they work in or with the Intelligence

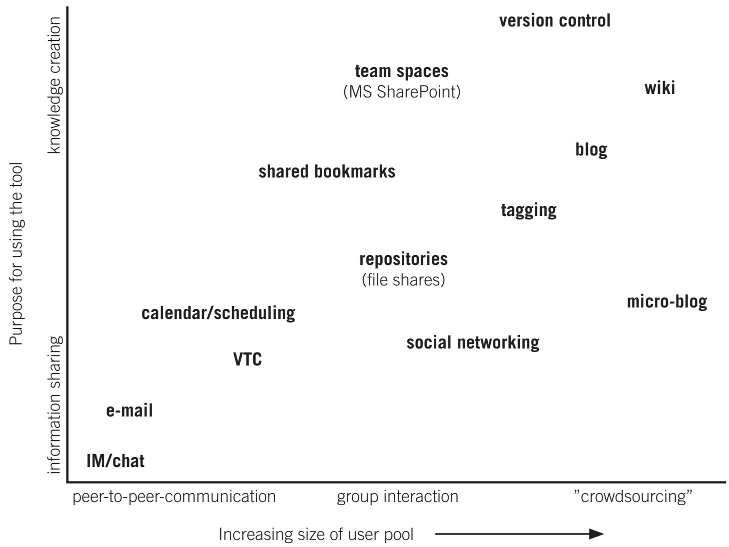
[1] This table is drawn from Drapeau & Wells II (2009), p. 6.

Community, and they have security clearances at a known level. These might be called "enterprise" uses of social media. By the same token, a person targeted for recruitment as an informant, for instance, may be known in advance, but may also be unknown initially; rather the target may be identified through analysis of networks on Facebook or other external social media.

Internal Interactions[2]

Figure 2 makes plain that known/unknown distinction is in fact a continuum, from peer-to-peer communication with a known interlocutor to, in principle, crowdsourcing a question to users unknown (though inside intelligence, all of this happens behind to security fence). The U.S. Intelligence Community has developed an impressive array of collaborative tools, some but not all of which might be labeled social media. However, the most used tools, like instant messaging, are employed primarily *within* agencies for peer-to-peer communication, hence are neither widely collaborative nor especially novel – they are new way of accomplishing familiar functions. SameTime, the IM system at CIA and DIA, has some advantages over email, just as email had some advantages over the telephone, which in turn was much faster than a typed memo.

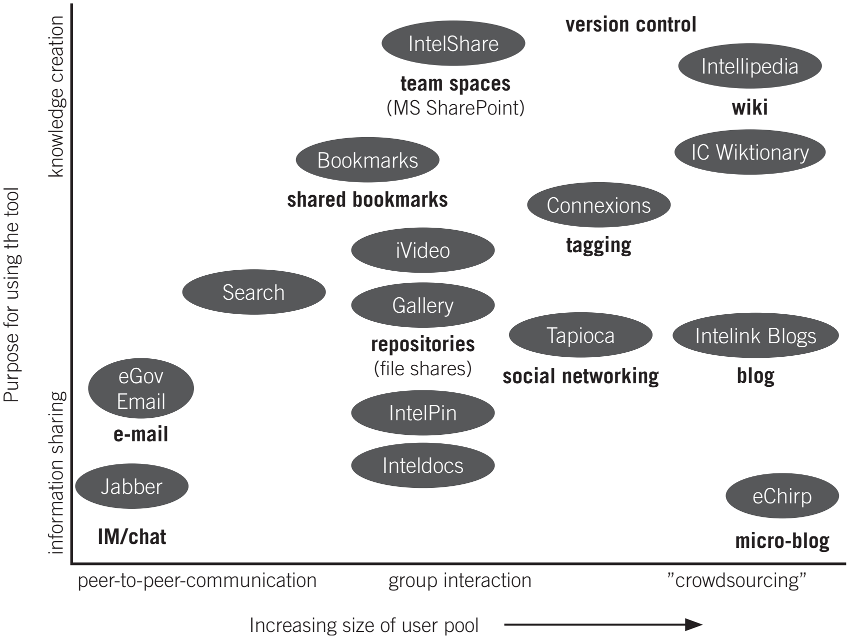
Figure 2: Collaborative Tools



[2] The following discussion draws on two RAND Corporation projects done for the U.S. Intelligence Community, one looking and primarily external uses of social media, the other examining the use of social media and other collaborative tools within and across the U.S. agencies.

The array of collaborative tools *across* agencies – ranging from IM to blogs to Intellipedia, and hosted on a platform called Intelink – is impressive but used mostly by enthusiasts. That array is depicted in Figure 3. Those enthusiasts feel there is little external incentive to use the tools to collaborate, indeed, many feel they pay a price for doing so, that using the tools is regarded as wasting time, as one said: "I'm practically unpromote-able." More fundamentally, on the analytic side of intelligence, collaboration will remain limited *so long as finished intelligence retains its dominant current form – stovepiped, branded words on paper or bytes on a screen*. That relationship between social media-enabled collaboration and the production of finished intelligence comes up again and again in conversations with analysts. Established workflows for producing finished intelligence are *not* collaborative, and so collaboration is mostly limited to what might be called "discourse collaboration" – in communities of interest and not intended to result in a specific product – as distinguished from "structured collaboration" intended to result in a product.

Figure 3: Intelink Tools



That discourse collaboration includes locating other experts in the Community; improving situation awareness (as one Korea specialist put it, "I look at eChirp first thing in the morning because my colleagues in Korea and Japan have been working while I was sleeping"); circulating interim "publications" between more formal ones; "warehousing" and seeking comment on blog items not yet ready for publication; and in the case of CIA's WIRe (for World Intelligence Review, a daily "publication" now available only on classified networks), "outreach", alerting relevant analytic communities about items of interest. Officials often said that there are "too many" tools, but one enthusiast had a simple answer – he registered for every new tool but only with the minimum information required to take a reader to his "home page", for him on Intellipedia.

Crowd-sourcing through social media plainly crosses the internal-external divide. Internally, the U.S. Intelligence Community has developed a "prediction market". The idea stems from observations that financial market traders bet their own money before they offer advice to their clients.[3] In this case, participants make bets by buying or selling contracts that some future event will or will not happen. They buy (go long) if they think the event is likely, sell (go short) if they think it unlikely. If the settlement value of the contract is $1 if the event occurs and 0 if it does not, the current price of a contract might be thought of as the probability that the event will occur. While studies have not conclusively shown prediction markets to be better than simpler techniques – like polling experts separately for their probability estimates, then averaging the results – some eighty Community officials participate, being asked about three new questions a week. Not surprisingly, those most enthusiastic about the Prediction Market tended to be those with "hot" accounts involving lots of interesting "will it or will it not questions?" like "will North Korea conduct another nuclear test by date y?"

The most impressive cross-agency collaboration in the U.S. Community was CollabZones, a virtual collaboration across military watchers and intelligence analysts around events of intelligence interest, like foreign weapons tests. The Zones use a number of tools, but the center is chat rooms, perhaps a dozen at a time across different levels of classification, and the key is "brokers" who move information to and fro across organizational boundaries, and facilitators who specialize in welcoming newcomers and encouraging engagement. The core participants regard themselves as "agency agnostic".

For the non-users or those who tried a tool once or twice and then stopped, the reasons are weak incentives, risk and practical difficulties in some combination, leading officers to conclude that it is not worth the effort. There is no external incentive to collaborate. Moreover, despite the security firewall, officers perceive some risk in collaborating, especially across agencies. For some agencies, the circle of trust does not extend beyond the agency, if that far. *There is no risk in not collaborating*. In addition, the practicalities of using the tools can be daunting for newcomers, as one put it: "When I do need or want something,

[3] The idea was championed in Surowiecki (2004).

my password or access has expired, and/or I can't remember the separate passwords I'm required to have for those applications… I have an Intellipedia page that I have let lapse because I can never remember the command/syntax for changing things and don't have the time to experiment." Intelink is NOFORN (no dissemination to non-Americans), but since NSA tries to share as much as possible with its "five eyes" partners (the U.S., Canada, Britain, Australia and New Zealand), NSA officers have little interest in Intelink and often no easy access to JWICS, the top secret system where Intelink resides.

Looks at various private sector organizations made clear that they are not, in general, far ahead of the U.S. Intelligence Community. They, too, have been through one cycle of tool-building and are looking for ways to drive collaboration deeper into their organizations. One natural point of comparison is journalism. What is different there is that even the highest quality outlets face existential competition from new, mostly web-based sources. By contrast, inside the U.S. Community, recognition of that competition is discernible only at the National Geospatial Intelligence Agency (NGA). The *New York Times* is not a cutting edge social media practitioner. No wikis, no micro-blogs, no fancy or modern in-house tool development is apparent. It encourages collaboration but relies on email. Yet all our interlocutors at the *New York Times*, the journalists, editors, and managers, all stressed how fundamentally journalism has changed in the past decade or so:

Collaboration is the name of the game today. Most bylines are multiple authors, often from different locations.

Speed has forced the *New York Times* and its competitors to push to the edge of their comfort zone with regard to accuracy. The *New York Times*, stressed that, perhaps more than its smaller and less established competitors, it often had to give more weight to being right than being quick, as a result often lost out to other media organizations in the race to publish first. Nevertheless, it, too, has seen an increase in its resort to the "correction" page.

Editing on the fly is imperative in these circumstances.

Evaluation, career development, and incentives have kept pace with the changing nature of the business. The paper takes pains to measure contribution, not just solo bylines, and it values a blog posting that attracts readership as much as a print article on the front page.

Changing impact measures are changing value propositions. Appearing above the fold in the print version of the paper is still regarded the place of honor among journalists, but another enviable distinction is making the *New York Times* "10 most emailed" list.

Content/version control is pervasive and central to the publication process. The ability to track versions, attribute to multiple authors, and control version aimed at print or e-publication is critically important.

Customer knowledge perhaps most distinguishes the *New York Times* from the Community. It knows its readership exquisitely, to an extent the IC can only dream about.

Perhaps most important, the experience of the *New York Times* and, still more, that of GitHub and open access publication, suggest that collaboration becomes real when it drives changes in work flow and product. The process will become collaborative when the product is.

External Interactions

Uses of external social media by intelligence agencies cover the range from open to very secret, from making use of new media as yet another open source to using social media for targeting purposes, not for content. In general, there was more use of social media by American agencies than might have been expected, and more interesting initiatives. The targeting examples are generally classified, but here are examples of the most interesting uses.

Open Source Center (OSC). This organization, the successor to the long-established Foreign Broadcast Information Service, now reports to the Director of National Intelligence. For it, social media are yet the latest in new media it needs to deal with. The challenges are formidable – Twitter, for instance, couples enormous volumes with equally enormous unreliability. For it, the OSC, in effect, tried to convert unknown users into known ones in the sense of reliability. To that end, its methods combined traditional and innovative but almost all have been labor-intensive, it would look at how many times a tweet was re-tweeted, and then look at the reliability of a given popular tweeter over time. Over time, as search processes get better, it will be possible to analyze sentiments. The ultimate challenge for, say, using Twitter and its kin to provide if not early warning, then at least tips for where analysts might look, will be processes that break away from key words. For now, Twitter seems most useful in two circumstances: when, as with the Mumbai bombings in 2008, information on the situation is in short supply and much of it is on social media; and when, as in the aftermath, of the 2009 Iranian presidential elections, social media can provide information about the state of the opposition when polling and other on-the-ground techniques are not available.

Open Source Works (OSW). This small organization was a niche provider since OSC did the main open source exploitation. Sadly, it seems to have ceased to exist. Its model was interesting – about a hundred analysts, none with security clearances and half operating in the language they grew up speaking. Perhaps its signature product was a weekly piece on what was hot on the Chinese blogosphere. We know the Chinese government pays attention to the blogosphere, but this was not the kind of piece the commercial world would produce. OSW was careful in selecting blogs and focused on "buzz", what was hot. This exploitation of social media was also labor-intensive, for while machine translation is now good enough to get the gist of a piece, for blogs it is the subtleties and nuances that matter.

Crowd-Sourcing. External crowd-sourcing includes solicitation of feedback from consumers and even the possibility of using participants as information sources or data collectors – for instance, the FBI's use of crowd-sourcing to seek leads to crimes.[4] External crowd-sourcing has also shown some intriguing possibilities for one of the U.S. IC's core missions – geopolitical forecasting. In 2011, the Office of the Director of National Intelligence's (ODNI) Intelligence Advanced Research Projects Activity (IARPA) sponsored what has become an annual forecasting tournament. The first tournament crowd-sourced more than 100 international affairs questions of interest to thousands of online forecasters, via five participating research teams.

One team significantly outperformed the others. It took approximately 2,000 "average" participants from around the world who then submitted probability estimates for geopolitical outcomes (based on the questions of interest) onto the project website. If participants updated their beliefs based on new research or perspectives from other participants, they could update their predictions on the website as long as each question stayed open.[5] The team used a simple mix of training on how to do probability estimates and avoid inferential traps, teaming to get the "right" people to share insights with each other, and tracking the top performers – the "super-forecasters" – to place in special teams that were given more weight in algorithms that assigned collective predictions.[6] In some cases, the "super-forecasters" reportedly made predictions up to 30 percent better than predictions by intelligence analysts.[7]

National Geospatial Intelligence Agency (NGA). Here, a small unit providing reach-back analyses for Iraq and Afghanistan was developing what has come to be called "activity-based intelligence". Their interest in social media was relatively marginal: as they sought to geolocate everything intelligence knew about, say, locations of interest in Afghanistan, they scraped data off media like Google earth and wikimapia. The leader of the group neatly summarized, in the imagery realm, the change imposed by the terrorist target: "In imagery, we used to know what we were looking for and be looking for things. Now, though, we don't know what we're looking for and we're not looking for things. We're looking for activities, or events." In this case, if a video camera on a Predator

[4] "Stolen Art Uncovered – Is it yours?" (2008).

[5] Mellers et al. (2014), p.1109.

[6] Ibid., p. 1107–1108.

[7] Spiegel (2014).

drone captured a truck pulling up in front of a farmhouse in an area of interest in Afghanistan, analysts could quickly search the database to see if there was any reason that activity should be of interest. If yes, then they could dig into the data. If not, the activity would simply be added to the database in case later events made it interesting. In neither case was the film important. It was the activity that mattered.

Other targeting. Virtually all these initiatives were classified. Suffice to say that many were aimed at enabling more traditional forms of collection. In these cases, the target was in the known category, but that target's communications modes were unknown. As one officer put it: If you're interested in the communications of a terrorist, he's going to have very good comsec [communications security]. But he also may have kids, who are active on social media. And somewhere in the trail, there will be an email address.

Beyond the open source work, most of these initiatives in using external social media were started bottom up: to caricature slightly, an officer would have a good idea. He or she would then spend several months persuading superiors that the idea was work, not play. If that was successful, they would spend the next few months persuading the lawyers it was legal! Or as another observed: think about trying to persuade your boss you need six months to become adept at the World of Warcraft game.

The pitfalls of these uses were also apparent. One CIA scientist was an active gamer. She had met a person through the game that she thought was a woman and a Canadian. She wondered whether she needed to report that as a "foreign contact". Adversaries have used social media against the United States, but many of the pitfalls are simply inadvertence. In one instance that has become public, a CIA officer under cover "friended" on Facebook a number of CIA colleagues who were not under cover but did not "friend" anyone at his cover organization. Yet simply "saying no" by abstaining from social media in private life does not seem wise either. A twenty-something who suddenly disappears from social media becomes conspicuous by his or her absence, all but advertising a move into a secretive organization.

Personas in cyber space are easy to create but hard to sustain. Not only do they have to have a credible life story, one that stands up to some fact-checking, but interlocutors in cyber space may ask to switch media quickly – "let's have a conversation on Skype". Deconfliction is also a problem, one that will only grow as not only intelligence services but law enforcement units seek to operate in cyber space. In one instance, one three-letter U.S. agency created a terrorist persona, which another three-letter agency thought was real. It took yet a third three-letter agency to understand what was going on!

Using Social Media and Traditional Media during Conflict

The increasing use of social media in recent conflicts, especially in the Middle East and Russia/Crimea/Ukraine is provocative in thinking about the future. It often mixes new and more traditional media. It offers opportunities for intelligence: as once officer put it, “selfies” (photos people take of themselves with cell phones, then share with others) are our best friend. Not only are about five percent of social media postings geolocated, but even if they are not, the background in the selfie may identify location. In one case, a Russian officer posted a picture of himself with a weapon system in the background that U.S. officials had not seen before.

“Twitter Wars”: The Middle East’s Socially Mediated Conflicts.

The Israeli-Palestinian conflicts are a leading example of the evolving intersection of social media and small wars, using social media to address each other directly and to fight for public opinion on both sides of the conflict.

In November 2012, the Israeli Defense Forces (IDF) launched the eight-day Operational Pillar of Defense in the Gaza Strip, targeting Hamas leadership and infrastructure in response to rocket attacks emanating from Gaza into Israel. Hardly the first escalation of violence between the IDF and Hamas in the Gaza Strip, this conflict was the first to heavily use social media on the propaganda front, leading CNN to query, “Will Twitter War Become the New Norm?”[8] Al-Jazeera noted the same phenomenon, asking “Is social media now an instrument of war?”[9]

For both sides, social media offered unprecedented reach, scope, and speed to get their side of the story out. Sometimes talking to each other, sometimes warning would-be supporters of the other side, they were able to pitch their message directly to the world when they wanted and the way they wanted. When the Israeli Defense Forces launched the air strike operation in Gaza, they announced it on Twitter. In return, Hamas launched operation “ShaleStones”, hurling dozens of tweets in what they called their “first confrontation with Israeli occupation forces on the internet.”[10]

The social media exchanges quickly escalated, with the IDF posting pictures on Twitter of assassinated Hamas leaders with “Eliminated” stamped across the pictures and footage of the assassination on YouTube. Al-Qassam Brigades, the armed wing of Hamas and savvy media users themselves, quickly responded

[8] Sutter (2012).

[9] “Battleground Twitter” (2012).

[10] “Twitter suspends account of Al-Qassam Brigades” (2014).

with counter-barbs and threats. Each threatened the other on Twitter, with Twitter and YouTube suspending the IDF's account but quickly restoring it.[11] Eventually, Twitter suspended Al-Qassam Brigade's official Twitter account in January 2014. The brigade angrily protested, contending that they had never violated the terms of service and that the reason for the suspension was likely "Twitter subordination to US government and 'Israel' as usual."[12]

The latest conflict between Israel and Hamas in Gaza broke out in July 2014 after the June kidnapping and murder of three Israeli teenagers and a reprisal kidnapping and murder of a Palestinian teenager. Hamas militants in Gaza began launching an increasing number of rockets and in turn Israel launched Operation Protective Edge, including a ground incursion into Gaza. Like 2012, each side's campaigns are marked by heavy use of social media; targeting not only their own supporters, but attempting to communicate with each other's supporters. In this context, social media has become the platform over which Israelis and Palestinians duel for public opinion. Yuval Dror, a digital communications expert, told the *Associated Press*, "This is a war over public opinion. It's an inseparable part of battle in the modern age."[13]

As use of smart phones becomes ubiquitous, Twitter, texts, and WhatsApp provide virtually anyone the ability to instantly disseminate unvetted, unvalidated, and often incendiary information. In just one instance of the way these media are used, Israeli families alleged that they learned of the deaths of their relatives in military service via WhatsApp before official notification.[14] In one of the many tit-for-tat uses of social media, the IDF posted a clip on YouTube of four Hamas militants emerging from the sea attempting to infiltrate Israel; they are picked off one by one by Israeli fire. The clip quickly garnered more than one million views. In turn, Hamas aired a video of their navy commandos training, complete with a dramatic musical score.[15]

The Israeli Defense Forces, in addition to dropping leaflets to warn Palestinians to evacuate before air strikes, use SMS text messages sent en masse to Palestinians. In turn, Hamas periodically hacks into Israeli smart phones, sending texts in Hebrew to thousands of users, with threats such as "if you want life, leave this country", and, "We forced you to hide in shelters like mice."[16]

[11] "Israel, Hamas Fight Twitter War" (2012) and MacKey (2012).

[12] "Twitter suspends account of Al-Qassam Brigades" (2014).

[13] Goldenberg (2014).

[14] "Israel detains soldiers after WhatsApp leaks about Gaza casualties" (2014).

[15] Goldenberg (2014). The IDF's video is accessible at: https://www.youtube.com/watch?v=-ff1Vb1ZqSE and the Hamas video is accessible at www.youtube.com/watch?v=4_p6t58YPmI

[16] For two examples see: Cohen & Oren (2014) and/or Rudoren (2014).

While Hamas's official Twitter accounts remain suspended, the group has used a Hebrew Twitter page, @QassamHebrew to claim attacks and post targeted propaganda. In one of the more bizarre exchanges, an Israeli woman tweeted a grammar correction to one of Hamas's Hebrew tweets. In response, she was thanked for the correction by one of the page owners who explained the reason for the original error. As word of the oddly amicable exchange got out, the page's followers leapt from just over 2,000 followers to more than 6,500 – before it too was suspended.[17]

"Social media has put the propaganda war on steroids"[18], for not all of the attempts at psychological operations are crude or darkly humorous. In a deadly serious conflict, each side attempts to incite anger and fear – Israelis reportedly tweet pictures of Palestinians being lead into Israeli interrogation rooms, while Hamas reportedly created a fake Facebook page for an Israeli soldier they claimed to have kidnapped (who was later determined to have been killed in action).[19]

Use of Twitter as primary front for propaganda may be a new dynamic in old conflicts – like the Israeli-Palestinian conflicts – but use of social media is also changing the way *new* conflicts are mediated. In the Syrian civil war, social media has fueled, in the views of many, the very cycles of violence itself. Peter Bouckaert, director of emergencies for the New York-based group Human Rights Watch, told *Time* that the barrage of violent images, uncensored and unfiltered, contributes to escalating cycles of revenge: "When people see these acts of brutality and mutilation, it leaves deep scars, and there will be a temptation to replicate it in revenge."[20]

Dueling narratives are basic features of civil wars, where the contending sides fight for legitimacy. Yet the ability of each side to broadcast their enemies' worst atrocities is new. A report on social media and the Syrian civil war calls it "the most socially mediated civil conflict in history."[21] The worse atrocities in Syria's civil war, including the alleged chemical gassing of civilians by the Syrian government, and rebel groups torturing and murdering their enemies, have played out with images and videos circulating in real-time across the Internet.

The report points out that the flow of graphic material in real-time has dangers, benefits, and unknown implications not yet fully tested or understood, especially in the context of civil war. One of the greatest benefits is the ability to see a ground view of events that is otherwise inaccessible in a closed country

[17] Hod (2014).

[18] Rudoren (2014).

[19] Hod (2014).

[20] Baker (2013).

[21] Lynch et al. (2013), p.5.

and violent conflict where journalists have extremely limited access. Yet Lynch et al. find that "social media create a dangerous illusion of unmediated information flows", when in reality social media flows through "key curation hubs" that selectively disseminate information based on the disseminator's desired narrative. This creates the risk of biases and fallacies given the false perception of transparency and creates the need for better structural analysis of social media hubs, trends, and implications.[22]

Much of this remains the work of media and communication doyens, web-savvy observers, and passionate activities; less chartered, as Lynch and his colleagues observe, is the actual causal link between social media movement and developments on the ground or political outcomes. In addition to surveying the current conflict and social media contributions across different levels of analysis, Lynch's study uses big data analysis to examine more than 38-million tweets in English and Arabic over a 28-month period. Their findings show that, related to Syria, divergent discourses have unfolded in English and Arabic. Most importantly, the dominant online discourse, tracked by the actual participants in the conflict, is the Arabic-language one. In contrast, they found that the English-language discourse was limited and inwardly focused, missing much of the relevant information circulating in Arabic. This suggests the intuitive yet profound observation – that information operations within civil wars are primarily undertaken in their native languages. For journalists and defense analysts hoping to leverage the ever-growing power of social media to understand conflict, this means that using English as a common language platform for rapid information sharing may no longer cut it.[23]

Russian Info Ops in the Ukraine-Crimea Conflict

Social media provided the first clues about who was behind the crash of Malaysia Airlines flight MH-17, which went down on July 17, 2014, close to the Ukraine-Russia border. All 298 people aboard died in the crash. Minutes after MH-17 went down, pro-Russian separatists on the social media site VK bragged about shooting down a Ukrainian military cargo plane. A U.S. Defense Intelligence Agency (DIA) analyst noticed immediately.[24] The VK post was made on a page associated with Igor Strelkov, commander of the separatist forces in the self-declared Donetsk People's Republic. In the post – which was hastily deleted – Strelkov boasted that rebels had just downed a Ukrainian military transporter near Torez. There were no reports or images of a Ukrainian

[22] Ibid., p.3.

[23] Ibid., p.6.

[24] Barnes (2014).

transporter shot down that day, but MH-17 went down just north of Torez minutes before his posting. In his post, Strelkov said, "We warned them – don't fly 'in our sky'."[25]

Of course, social media was not the only intelligence source – a U.S. spy satellite detected a missile launch immediately before the plane went down and the Ukrainian government intercepted a phone conversation between two rebel leaders.[26] Yet the role of social media highlights this emerging form of open-source intelligence collection – one akin to social media providing situation awareness during the Mumbai attacks. "The first indication of who shot it, what shot it and when and where it was shot was all social media", former DIA chief Lt. Gen. Michael Flynn told *The Wall Street Journal* – "It was literally within minutes."[27]

In interviews three days after the incident, U.S. Secretary of State John Kerry cited intelligence including a recording of the trajectory of the missile, intercepts of conversations, and monitoring of weapons flows into Donetsk. Yet he too emphasized the role of social media. "The social media showed them with this [SA-11] system moving through the very area where we believe the shoot-down took place hours before it took place. Social media – which is an extraordinary tool, obviously, in all of this – has posted recordings of a separatist bragging about the shoot-down of a plane at the time, right after it took place."[28]

If social media and a smart phone "can turn any human into a geo-located collector", they can also turn any human into an intelligence collection target. *The Wall Street Journal* recently highlighted a DIA intelligence tool that can scan huge amounts of social media looking for individuals using facial recognition techniques. In one instance, the DIA tracked a soldier first seen in a Russian uniform at the Novorossiysk Naval base in September 2013. Using this tool, the agency tracked him in a series of social media postings as he moved across Russian territory into Crimea in March.[29]

As much as the incident highlighted the potential of social media for intelligence exploitation, it also highlighted its limitations. Although social media quickly incriminated rebel forces, definitive proof of who downed the airliner or whether Russian forces were directly involved remained out of reach. In a

[25] Specia (2014).

[26] Chappell (2014).

[27] Barnes (2014).

[28] Gregory (2014).

[29] Barnes (2014). See also BBC program on Russia's "useful idiots": http://www.bbc.co.uk/worldservice/documentaries/2010/07/100624_doc_useful_idiots_lenin.shtm.

briefing with reporters five days after the incident, intelligence officials stressed they had more sources than social media – yet proof remained elusive.[30]

Moreover, social media works both ways and have been, often in synergy with traditional media, employed aggressively in Russia to disseminate a different narrative. Indeed, the Russian Information Security Doctrine, approved by President Vladimir Putin on September 9, 2000, prominently includes "the assurance of a spiritual renewal of Russia, and the preservation and reinforcement of the moral values of society, traditions of patriotism and humanism and the cultural and scientific potential of the country." At that time, the salient issue was Chechnya, so speculation focused on dealing with the information/influence aspect of that conflict.

At that point, the primary point of the effort at narrative-building was internal, but the 2008 conflict over Georgia did involve international targeting as preparation of an actual battlefield. Then there was the cyber campaign against Estonia, which was a political statement as much as a proof of concept. With regard to the Ukraine, the Snake/Ouroboros malware has targeted both the Prime Minister's office and Ukrainian embassies in at least 10 countries.[31] On August 24, Ukraine's Independence Day, a pro-separatist hacker group, Cyber Berkut, temporarily blocked the mobile phones of the Rada deputies as well as over 500 pro-government information resources.[32] While the connections between such operations and operators remain unconfirmed, as Russia uses private companies, research centers, and the like, it appears that cyberops are not designed entirely separately from influence ops, and information gathered through either approach is used to feed into the other. This is a whole-of-government effort and the legislative and social developments in the last decade have created an environment particularly conducive to it.

One of the fundamental issues on social media is trust – as users, as publishers, as analysts – who do we trust for information. From an info-ops perspective one way of tackling this issue is relentlessly producing variations on the main points of the narrative and drowning the discourse in a cacophony of 'alternative explanations' thus creating a haze of uncertainty (this includes the use of trolls) – the MH17 flight narrative is an excellent demonstration of that approach. Sheer volume and continuity of effort might not produce perfect results, but disinformation does not require full acceptance to have observable results.

[30] Harris (2014).

[31] Jones (2014).

[32] Itar-tass (2014).

According to one poll by a Russian research organization, the Levada Center, 82 percent of Russians believe MH-17 was shot down by Ukrainian forces.[33]

Storyful, a news agency that discovers and verifies social media, followed the issue closely, reaching similar conclusions using open source data. By scouring images, videos, tweets, and other social media posts, Storyful published evidence two days after the downed flight pointing both to the rebels' claims of responsibility and to rebel possession of a 'Buk', or SA-11, missile system in the Donetsk region at the time of the attack.[34]

Twitter accounts linked to the Donetsk People's Republic that had earlier claimed possession of Buk systems quickly deleted tweets, but other users had already captured the evidence. One such user retweeted screenshots of the tweets with pictures of the Buk system on July 17 shortly after the flight went down, while another commented that attempts to cover tracks were "like the criminal trying to toss the evidence during a televised police chase."[35]

Moreover, despite historically-founded skepticism among Russians towards all that is being produced by traditional, 'official' media, a July 2014 Levada Center poll revealed that anti-Western and anti-American sentiments in Russia have reached record levels since the break-up of the Soviet Union. Seventy-four percent of respondents expressed negative attitudes towards the USA (compared to 40 percent in January 2014), while 61 percent agreed that Russia is "threatened by numerous external and internal enemies". 27 percent still believe that such assertions are a manipulation by the authorities, but that is a decrease compared to the 30 percent who considered such claims propaganda in a 2007 poll when the same question was posed.

The sustained use of stable troops in Russian info-ops in the past decade (or even past few decades) appears to be paying off (even if it is not entirely by design and possibly reflects genuine beliefs among some in the Russian elites). While the volume and tone of the rhetoric has been ramped up considerably since the beginning of the Ukraine crisis and the Crimea operation, the lack of a powerful enough counter-narrative within the Russian-speaking space has further enabled its effects. Moreover, even spaces with no direct connection to political affairs have been affected by the intensified narrative. While cause and effect can be debates, a clear change in the character of the posted and most voted jokes can be seen. The volume of Ukraine-jokes increased significantly and the tone of the jokes was not merely the usual benevolent Russian supremacy, portraying the former subjects of the USSR as less developed and stupid, but became more militant and targeting the new Kiev authorities. An example

[33] Luhn (2014).

[34] Specia (2014).

[35] Katz (2014).

from August 25th 2014: "From Yatsenyuk's [his name is spelled in an offensive way, making a pun on the phonetic similarity with the word egg] address: The citizens of Kiev will be able to make significant economies this year – saving on gas and hot water bills." The site anekdot.ru has existed since 1995 and ranks second of 469 humor resources on the mail.ru ranking system.

The exact birthdate of state-sponsored and centrally-directed trolling on social media is somewhat unclear but seems to run back to the early 2000s.

In any case, it is not a new phenomenon and got high on the Kremlin's agenda after the winter 2011 protests. The so-called "creative classes", deemed by the regime an internal enemy, live on the interwebz, and the Kremlin appears to have decided on a systematic approach with the ascendance of Vyacheslav Volodin and his colleagues in the presidential administration.[36] Interestingly, the derogative term used for those trolls – "murzilka", a slang word for prostitute and the title of a famous Soviet/Russian children's magazine – has become an insult outside Russian and has spread to Bulgarian online spaces, where users shun/insult almost anyone with a pro-Russia position using the same word.

Moreover, the troll nexus is evolving, and according to Russian-language sources has spread to Germany, with expansion to the United States imminent – which may well be an overstatement. The latter might be an overstatement, but the perceived weakness of European countries is one of the contributing factors emboldening the operation. The dueling narratives extend to hashtags. The Russian spelling of the tag "Crimea is ours", #Крымнаш, produces ironic and propaganda news, comments and stories, while the Ukrainian spelling, #Кримнаш, delivers negative news and comments on the Russian handling of Crimea as well as patriotic messaging.

In sum, the Ukraine conflict has been accompanied by an aggressive Russian propaganda campaign; while the tactics and techniques are themselves fairly traditional, use of social media as a platform has simultaneously enabled rapid, widespread diffusion of content and obscured its source. In just one example, a photo of armed "American mercenaries" on the ground in the Ukraine circulated Russian social media in May 2014, cited as proof of U.S. interference in the conflict. State Department officials in turn accused "Kremlin-sponsored websites" of doctoring what was in fact a photo of law enforcement personnel in New Orleans keeping order after Hurricane Katrina in 2005.[37] The director of the Levada Center, Lev Gudkov, told the BBC that Russian attempts to shape the narrative are "aggressive and deceptive propaganda... worse than anything I witnessed in the Soviet Union."[38]

[36] Elliott (2014).

[37] Richter (2014).

[38] Kendall (2014).

VK, the social media site where separatists first posted about shooting down a plane, is the former VKontakte, Russia's largest social networking site. With around 240 million Russian speakers – and 88 million users in Russia alone – it is a powerful tool for mass mobilization, information dissemination, and, more darkly, crowd surveillance. After a series of publicized feuds with government authorities over refusing to share data on Ukrainian users – and allowing political protesters to post on the site – the youthful founder, Pavel Durov, was fired over an apparent technicality in April. On his way out, Durov alleged that two Russian oligarchs and Putin loyals now control the company.[39]

Writing for *The National Geographic*, David Stern notes how Twitter and other social media platforms are structurally conducive to mis- or disinformation: "Twitter, in particular, with its strict parameters, is a particularly distorting lens: A myriad of tweets providing partial or incomplete information do not ultimately create a full picture – they provide a giant incomplete picture. Especially if they're all tweeting the same thing."[40] Stern reports that the Russian parliament recently passed a law that would restrict blogs and other sites that attract a certain number of viewers.[41] In addition to censoring websites, Russia appears to maintain "web brigades", or as they are known to some, the 30-Ruble Army. These human "bots" are paid to monitor blogs, websites, and chat forums to comment with pro-Russian propaganda and criticism of Russian opponents.[42]

Looking to the Future

Conflicts are increasing played out over social media; a dynamic that has indelibly changed some aspects of the conflicts in ways that are not yet fully understood. Governments and militaries are usually able to harness the state's resources to communicate, whether through radio and TV broadcasts or other mechanisms. For non-state actors, social media serves to level the playing field. We are seeing, in that sense, "fourth generation" warfare, where the line between military and civilian is entirely blurred. A savvy individual user – or even better, a small group of dedicated activists – can use basic social media tools to launch sophisticated information operations. Those media also offer a measure of anonymity, or at least deniability. Recall the famous *New Yorker* cartoon from the 1990s in which one dog says to another, "Remember, on the internet no

[39] "Head of Russia's largest social network VKontakte leaves his post" (2014). And "Russia's VKontakte CEO says he was fired, flees Russia" (2104).

[40] Stern (2014).

[41] Ibid.

[42] Allnutt (2012).

one has to know you are a dog." It is an intriguing question whether, as social media become more sophisticated and ubiquitous – all geolocated, for instance – the process will become more self-policing, as many internet advocates have argued. Will it become more difficult to establish and sustain a narrative that selectively uses facts.

Looking at use of social media for internal collaborative purposes, what is striking that, for all the social media of the 2010s, intelligence-policy relations in the United States is still mostly an oral and paper affair. Most officials prefer the two modes in some combination, either being briefed, with interesting items left behind for later reading, or reading first, then asking questions. That will change. Technology will continue to rush ahead, enabling new forms of interaction between intelligence and policy, and intelligence's clients will come to expect from intelligence what they came to count on from Google. Already, the U.S. president sometimes receives his President's Daily Brief (PDB) on an iPad, though at this point that is more a demonstration than a process. The same president came into office a tweeter. Technology will enable, but the challenge for intelligence will be work processes and organizational culture.

Some of the advances will be relatively straightforward. Over time, despite the oral and paper practices of current senior officials, more and more intelligence will be read online. That opens the possibility of quick feedback. Intelligence agencies know from long, hard experience how difficult it is to get busy policy officials to read intelligence items, much less comment on them. Yet online they could provide useful feedback in a few seconds, not a few minutes, for instance by ranking an item on scales of quality and relevance.

In imagining what a different future for what intelligence analysis and its connection to policy might look like, the prototype produced by the NGA called *Living Intelligence*, is provocative. It aims to merge the virtues of crowd-sourcing with agency vetting, and to reduce duplication in the process.[43] It would use Google Living Story software, software developed for a 2009-2011 experiment involving Google plus the *New York Times* and *Washington Post*. Every topic would have its own URL. At the top of the page for each "story" would be a summary, and below that a timeline, which the user could move back and forth. On the left side of the page would be the filters, letting users drill down to the level of detail they sought. On the right is a time sequence of important events. In the center is the update stream that keeps track of the entire story. Once a user has read a piece, that piece grays out, so the user need not read it again. The scheme keeps repetition to a medium. For intelligence, it would help

[43] For a video explaining the idea, see: http://www.youtube.com/watch?v=9ft3BBBg99s&feature=plcp.

to distinguish between useful tailoring for different audiences and the "stock" story merely repeated.

Finally, the content would be fully vetted by the contributing agencies, thus diminishing the worry that content on collaborative tools is second-rate or less reliable. Using WordPress and MediaWiki (the same software as Wikipedia and Intellipedia), the page would use grayed versus lit agency icons, plus color coding, to make clear which contributions to the topic had been vetted and cleared at which level of the contributing agencies. Both the software programs permit geospatial location, so the topic page would add a spatial dimension as well. The hope behind *Living Intelligence* was that this form of collaboration would encourage agencies to play to their strengths, rather than try to do the entire story themselves. In a more distant future, it is possible to imagine policy officials contributing as well, clearly marked as such; for critical parts of the intelligence mystery – what might drive foreign leaders, for instance – those policy officials often know more than intelligence.

Yet even *Living Intelligence* is just a modern, and more collaborative, way to assemble intelligence analyses and "push" them out in dissemination. It would be interactive with clients only to a limited extent. Yet, future clients of intelligence are going to want to receive intelligence on their iPads, if they do not already. They will want information on demand, "when they have a few minutes", as one of our interviewees put it, *not* when the briefing is scheduled or the intelligence analysis finished. They will want to have, though iPads or similar technology, the conversation that senior officials have with their PDB briefers, asking questions, getting answers on the spot, or getting additional analysis soon thereafter.

Using these new technologies, however, cuts across how most intelligence services do their business. That is most visible in quality control: one of the reasons that intelligence has clung so tenaciously to those products, words on paper or bytes on a screen, is that they can be subjected to a careful process of quality control (leave aside for the moment whether those processes produce better documents or just more vanilla ones). Not so analysts answering questions by iPad more or less on the fly. The officials who brief cabinet officers on the PDB prepare to answer the most probable questions, and come to the briefings with notes in order to do so. A less formal process would require empowering analysts. The quality assurance would rest on the people, not their products. And those people would also be the outputs of intelligence.

Google Glass suggests other possibilities that technology will enable. Especially at the more operational level, the technologies could enhance situation awareness but letting clients not only ask questions but call up images and maps at will – all with hands free. More and more of the content on the open web is images, not words. While intelligence is likely to lag behind that change, especially in more strategic analysis, it will not be immune from it. Preparing to do for policy clients what Glass aims to do for civilian users will require a dramatic change in how intelligence agencies do their work and conceive of their products. It will require being serious about moving toward client service and adjusting its processes according – with implications that range from recruitment and training, to quality control and collaboration.

List of references

Allnutt, Luke (2012). "Russia's 30-Ruble Army Emerges Again". *Radio Free Europe/Radio Liberty,* February 8, 2012.
Accessed at:
http://www.rferl.org/content/russia_30_ruble_army_emerges_again/24477703.html

Baker, Aryn (2013). "Savage Online Videos Fuel Syria's Descent into Madness". *Time*, May 12, 2013.
Accessed at:
http://world.time.com/2013/05/12/atrocities-will-be-televised-they-syrian-war-takes-a-turn-for-the-worse/

Barnes, Julian E. (2014). "U.S. Military Plugs Into Social Media for Intelligence Gathering". *The Wall Street Journal*, August 6, 2014.
Accessed at:
http://online.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557

"Battleground Twitter" (2012). *Al-Jazeera*, November 15, 2012.
Accessed at:
http://stream.aljazeera.com/story/201211151954-0022405

Chappell, Bill (2014). "Flight MH17: U.S. Builds Its Case; Plane Wreckage Reportedly Cut Apart". *NPR*, July 22, 2014.
Accessed at:
http://www.npr.org/blogs/thetwo-way/2014/07/22/334100145/flight-mh17-u-s-builds-its-case-plane-wreckage-reportedly-cut-apart

Cohen, Gili & Oren, Amir (2014). "Hamas sends Israelis threatening text messages". *Haaretz*, March 23, 2014.
Accessed at:
http://www.haaretz.com/news/diplomacy-defense/.premium-1.581403

Drapeau, Mark & Wells II, Linton (2009). *Social Software and National Security*: An Initial Net Assessment. Washington: Center for Technology and National Security Policy, National Defense University.
Accessed at:
http://www.dtic.mil/dtic/tr/fulltext/u2/a497525.pdf

Elliott, Chris (2014). "pro-Russia trolling below the line on Ukraine stories". *The Guardian*, May 4, 2014.
Accessed at:
http://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

Goldenberg, Tia (2014). “Israel, Hamas battle over public opinion online”. *Associated Press*, July 23, 2014.
Accessed at:
http://bigstory.ap.org/article/israel-hamas-battle-over-public-opinion-online

Gregory, David (2014). “Interview [with Secretary of State John Kerry] with David Gregory of NBC’s Meet the Press”. *U.S. Department of State*, July 20, 2014.
Accessed at:
http://www.state.gov/secretary/remarks/2014/07/229507.htm

Harris, Shane (2014). “US intelligence no closer to pinning MH17 downing on Russia”. *Foreign Policy*, July 22, 2014.
Accessed at: http://thecable.foreignpolicy.com/posts/2014/07/22/us_intelligence_no_closer_to_pinning_mh17_downing_on_russia

“Head of Russia’s largest social network VKontakte leaves his post” (2014). *RT*, April 22, 2014.
Accessed at:
http://rt.com/news/durov-resigns-vkontakte-social-904/

Hod, Itay (2014). “Israel, Hamas, WhatsApp and Hacked Phones in the Gaza Psy-War”. *The Daily Beast,* July 26, 2014.
Accessed at:
http://www.thedailybeast.com/articles/2014/07/26/israel-hamas-whatsapp-and-hacked-phones-in-the-gaza-psy-war.html

“Israel detains soldiers after WhatsApp leaks about Gaza casualties” (2014). *Reuters*, July 24, 2014.
Accessed at:
http://in.reuters.com/article/2014/07/23/us-palestinians-israel-whatsapp-idINKBN0FS21920140723

“Israel, Hamas Fight Twitter War” (2012). *The Huffington Post*, November 15, 2012.
Accessed at:
http://www.huffingtonpost.com/2012/11/15/israel-hamas-twitter_n_2138841.html

Itar-tass (2014). “Организация «КиберБеркут» заблокировала телефоны депутатов Верховной рады”. *Itar-tass*, August 24, 2014.
Accessed at:
http://itar-tass.com/mezhdunarodnaya-panorama/1396949

Jones, Sam (2014).”Ukraine PM’s office hit by cyber attack linked to Russia”. *Financial Times*, August 7, 2014.
Accessed at:
http://www.ft.com/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0.html

Katz, Walter (2014). *Twitter @walterkatz*, 06:58, July 17, 2014.
Accessed at:
https://twitter.com/walterwkatz/status/489816362068348928

Kendall, Bridget (2014). “Russian propaganda machine ‘worse than Soviet Union’”. *BBC News*, June 5, 2014.
Accessed at:
http://www.bbc.com/news/magazine-27713847

Luhn, Alec (2014). “MH17: vast majority of Russians believe Ukraine downed plane, poll finds”. *The Guardian*, July 30, 2014.
Accessed at:
http://www.theguardian.com/world/2014/jul/30/mh17-vast-majority-russians-believe-ukraine-downed-plane-poll

Lynch, Marc, Freelon, Deen & Aday, Sean (2013). *Blogs and Bullets III: Syria’s Socially Mediated Civil War*. Washington DC: United States Institute of Peace.

MacKey, Robert (2012). “Israel’s Military Begins Social Media Offensive as Bombs Fall on Gaza”. *The New York Times*, November 14, 2012.
Accessed at:
http://thelede.blogs.nytimes.com/2012/11/14/israels-military-launches-social-media-offensive-as-bombs-fall-on-gaza/

Mellers, Barbara et al. (2014). “Psychological Strategies for Winning a Geopolitical Forecasting Tournament”. *Psychological Science* 25(5):1106-1115.

Richter, Paul (2014). “White House accuses Russia of anti-U.S. propaganda war in Ukraine,” *Los Angeles Times*, May 20, 2014.
Accessed at:
http://www.latimes.com/world/europe/la-fg-ukraine-propaganda-20140521-story.html

Rudoren, Jodi (2014). “In Gaza, Epithets are Fired and Euphemisms Give Shelter”. *The New York Times*, July 20, 2014.
Accessed at:
http://www.nytimes.com/2014/07/21/world/middleeast/in-a-clash-between-israel-and-gaza-both-sides-use-social-media-to-fire-epithets-and-hide-behind-euphemisms.html?emc=eta1

"Russia's VKontakte CEO says he was fired, flees Russia" (2104). *Reuters,* April 22, 2014.
Accessed at:
http://www.reuters.com/article/2014/04/22/russia-vkontakte-ceo-idUSL6N0NE1HS20140422

Specia, Megan (2014). "How Social Sleuthing Uncovered Evidence of Surface-to-Air Missile Systems in Eastern Ukraine". *Storyful Blog*, July 19, 2014.
Accessed at:
http://blog.storyful.com/2014/07/19/how-social-sleuthing-uncovered-evidence-of-anti-aircraft-missile-system-in-eastern-ukraine/#.U-qnC-J3n99M

Spiegel, Alix (2014). "So You Think You're Smarter Than A CIA Agent". *NPR*, April 2, 2014.
Accessed at:
http://www.npr.org/blogs/parallels/2014/04/02/297839429/-so-you-think-youre-smarter-than-a-cia-agent

Stern, David (2014). "The Twitter War: Social Media's Role in Ukraine Unrest". *The National Geographic*, May 10, 2014.
Accessed at:
http://news.nationalgeographic.com/news/2014/05/140510-ukraine-odessa-russia-kiev-twitter-world/

"Stolen Art Uncovered – Is it yours?"(2008). *The Federal Bureau of Investigation*, November 8, 2008.
Accessed at:
http://www.fbi.gov/page2/august08/arttheft_081108.html

Surowiecki, James (2004). *The Wisdom of Crowds: Why the Many Are Smarter than the few and How Collective Wisdom Shapes Business Economies, Societies and Nations.* Boston: Little Brown.

Sutter, John D. (2012). "Will Twitter war become the new norm?". *CNN*, November 19, 2012.
Accessed at:
http://www.cnn.com/2012/11/15/tech/social-media/twitter-war-gaza-israel/

"Twitter suspends account of Al-Qassam Brigades" (2014). *Official statement Al-Qassam Brigades*, January 10, 2014.
Accessed at:
http://www.qassam.ps/news-7910-Twitter_suspends_account_of_al_Qassam_Brigades.html

Social Media and Intelligence

This paper is part of CATS' project on intelligence for terrorism and homeland security, sponsored by the Swedish Civil Contingencies Agency (MSB). It addresses the use and potential use of social media in intelligence – looking across the range of possible uses both externally and as collaborative tools within and across agencies. The first half of the paper lays out four categories of intelligence interactions using social media, and then discusses them briefly, drawing primarily on U.S. experiences. The second part of the paper turns more specifically to the mix of new media and old at play in conflicts around the world, especially in the Middle East and Russia/Crimea/Ukraine.

Gregory Treverton is chairman of the U.S. National Intelligence Council. However, this paper was written when he was a Director of the RAND Corporation's Center for Global Risk and Security, and a visiting fellow at CATS.

Renanah Miles is a Ph.D. candidate in Political Science at Columbia University and a summer associate at the RAND Corporation. She concentrates in international relations with a focus on security studies and the Middle East. Previously she was a program analyst in the Office of the Secretary of Defense.

ISBN 978-91-86137-37-3

National Defence College
Box 27805
SE-115 93 Stockholm