# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 26-04-2016 | Master's of Military Studies | SEP 2015 - APR 2016 |

**4. TITLE AND SUBTITLE**

A Commander's Guide to Social Radars

**5a. CONTRACT NUMBER**
N/A

**5b. GRANT NUMBER**
N/A

**5c. PROGRAM ELEMENT NUMBER**
N/A

**6. AUTHOR(S)**

Thorpe, Robert, M, Major, Royal Marines

**5d. PROJECT NUMBER**
N/A

**5e. TASK NUMBER**
N/A

**5f. WORK UNIT NUMBER**
N/A

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

USMC Command and Staff College
Marine Corps University
2076 South Street

**8. PERFORMING ORGANIZATION REPORT NUMBER**
N/A

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**
Dr P.D.Gelpi

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
N/A

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

Approved for public release, distribution unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

A social radar is a global and persistent indications and warnings capability, consisting of integrated technologies for detecting, localizing, and monitoring operationally relevant socio-cultural behavior signatures. In the simplest terms, it is the ability to know what people are thinking, where they are thinking it, and how, when, and where they might react. This presents the capacity to better understand and interact with human terrain. It also makes surreptitious social manipulation a realistic possibility. Although concept demonstrators are already in service, this paper argues that the military will not

**15. SUBJECT TERMS**

Social radar; military; predictive analysis; analytics; big data; intelligence; fusion; human terrain; information operations.

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | 43 | 19b. TELEPHONE NUMBER *(Include area code)* |

*United States Marine Corps*
*Command and Staff College*
*Marine Corps University*
*2076 South Street*
*Marine Corps Combat Development Command*
*Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

---

**A COMMANDER'S GUIDE TO SOCIAL RADARS**

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

**AUTHOR: Major Rob Thorpe, Royal Marines**

AY 15-16

---

Mentor and Oral Defense Committee Member: Dr Paul D. Gelpi
Approved: _____
Date: 21 April 2016

Oral Defense Committee Member: Dr Francis H. Marlo
Approved: _____
Date: 21 April 2016

**Executive Summary**

**Title: A Commander's Guide to Social Radars**

**Author:** Major Rob Thorpe, Royal Marines

**Thesis:** Integrated as part of a holistic "Big Data" strategy, "social radars" will unlock the potential of predictive analytics to generate foresight over insight and will potentially enable the manipulation of social outcomes. Consequently, commanders at all levels must have at least a working knowledge of this emerging technology as well as an awareness of the associated ethical, legal, and cultural challenges.

**Discussion:** A social radar is a global and persistent indications and warnings capability, consisting of integrated technologies for detecting, localizing, and monitoring operationally relevant socio-cultural behavior signatures. In the simplest terms, it is the ability to know what people are thinking, where they are thinking it, and how, when, and where they might react. This presents the capacity to better understand and interact with human terrain. However, social radars also multiply the effectiveness of Information Operations, potentially making it possible to alter perceptions surreptitiously. This raises ethical and legal challenges. Social radars are not the realm of science fiction. Research models have predicted civil unrest events in Latin America with 80 percent accuracy, and similar systems are now leading to the notion of predictive policing in the United States and elsewhere. Concept demonstrators and in-service capabilities exist in both the US and UK militaries. However, these systems use only Open Source data and this limits both their accuracy and their military utility. Social radar developers always intended that such systems would eventually integrate all data, classified and open source, and that this was key to their success. However, although the technical solutions to achieve this fusion already exist, the Intelligence Community appears reluctant to embrace a fused intelligence system that would unlock the full potential of social radars.

**Conclusion:** Social radars will not provide a panacea to intelligence collection but do represent the most effective means of persistent Wide Area Surveillance from which to focus increasingly scarce classified collection assets. Their development heralds a new era in predictive analytics for the intelligence community. However, the military will not capitalize on the full potential of social radars until it incorporates them into a holistic Big Data strategy that fuses both open source and classified data sources.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

***Table of Contents***

Page

DISCLAIMER....i

LIST OF ILLUSTRATIONS .... iii

PREFACE ....iv

INTRODUCTION....1

CHAPTER 1 – Warfare in the Information Age ....2

CHAPTER 2 – Social Radars....6

The case for full integration....15

CHAPTER 3 – Technical Limitations and Ethical, Legal, and Cultural Considerations ....19

CONCLUSIONS....26

APPENDIX A: Military Applications of Social Radar Technology ....32

APPENDIX B: Global Digital, Mobile, and Social Media Penetration ....33

BIBLIOGRAPHY ....34

***Illustrations***

Page

Figure 1. ISIL geotagged Tweets in Iraq and Syria, leading to the targeting of Mark Taylor. ..... 5

Figure 2. The Social Radar Concept. ..... 7

Figure 3. The "Analysis" layer of "dashboard" of a social radar. ..... 8

Figure 4. Snapshots from Social Radar analytic tools. ..... 10

Figure 5. The application of "spiral analysis" to understand network linkages. ..... 11

Figure 6. Automated network analysis of 66 prominent Jihadists to identify key influencers ..... 12

Figure 7. Retrospective Twitter trend analysis of key words and phrases immediately preceding the Bardo Museum attack in Tunis, 2015. ..... 15

Figure 8. Social radar heatmapping predicts violent behavior patterns across Africa. ..... 18

## *Preface*

Accurate and predictive social radars are an important step towards the more efficient and effective application of force. It will accelerate decision-making and enable commanders to sustain a greater tempo of operations over protracted periods. In a time of scarce resources and continued reticence to "put boots on the ground," an ability to forecast social activity will enable proactive and targeted allocation of surveillance assets, followed by nuanced, kinetic and non-kinetic operations, actions, or activities. Furthermore, social radars exponentially multiply the power of Information Operations, making it increasingly feasible to purposefully and clandestinely alter a target population's attitude and behavior to meet a desired social outcome. This cognitive engineering on a mass scale unleashes a potentially corrupting power to incite violence or suppress opposition and dissent. Pandora's Box has been opened, and the advent of social radars will call for a steady hand in command.

Personal interest in this topic was sparked by previous experience within the UK's Information Exploitation community, notably as Officer Commanding at Y Squadron, the Royal Marines' dedicated Electronic Warfare and Signals Intelligence unit. I am grateful first and foremost to the great people I had the privilege of working with at that unit for educating me on the centrality of intelligence within the art of warfighting and for unbridling my inner geek. I must also acknowledge those organizations in the United States and back in the United Kingdom that took time to engage with me on this project. My particular thanks must go to Dr Paul Gelpi for guiding me through the writing process, to Jonathan Miles at the British Embassy, and to Colonel Randy Pugh, USMC in the Pentagon. Finally, whole-hearted thanks go to my wife, Dana, for suffering my waves of enthusiasm, despondency, and writers block as I cobbled this together.

# A Commander's Guide to Social Radars

## Introduction

> *Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars. You must get into the hearts and minds of humans. That's where battles are won.*
>
> - Colonel John Boyd, United States Air Force, 1981[1]

War is an inherently social activity, and yet militaries have perennially struggled to comprehend the human aspects of warfare, measure their impact on affected populations, or predict when and where violence may occur. Recent counterinsurgency operations have increased awareness of human terrain analysis, but such activity remains secondary to the identification and targeting of an adversary's military hardware and personnel. Such targeting is supported by an advanced array of surveillance systems that operate for the most part in the physical environments of air, land, sea, and space, or, increasingly, in cyberspace. Meanwhile, the cognitive aspects of warfare, which concern perceptions, sentiments, allegiances, and motivations, are more challenging to understand and more difficult to measurably influence. The advent of the Information Age is changing this. Underpinned by the potential transformative power of "Big Data" analytics, the Information Age is characterized by an explosion of data, the exponential growth in both processing power and data storage capacities, and the combined effects of powerful visualization and collection tools.[2] One emerging application of Big Data analytics that directly affects the cognitive domain is "social radar."

A social radar is a "global and persistent indications and warnings capability, consisting of integrated technologies for detecting, localizing, and monitoring operationally relevant socio-cultural behavior signatures."[3] In the simplest terms, it is the ability to know what people are thinking about and predict how, when, and where they might react to certain stimuli. As a form of Intelligence, Surveillance, and Reconnaissance (ISR), social radars use predictive analytics "to see into the hearts and minds of the people."[4] This capability is no longer the realm of science fiction. Concept demonstrators and even in-service capabilities exist in both the United States and the United Kingdom, albeit not necessarily integrated or deployed at a scale that enables realization of their full potential.[5] Critically, however, such a capability can also be "weaponized", through *prescriptive* analytics, by actively manipulating perceptions within a target population to shape behavior outcomes. Both the predictive and prescriptive elements have utility across the range of military operations and from the strategic to the tactical level.

While the underpinning technology in this area is fueled primarily by the availability of open source data, particularly the global proliferation of social media, the military may not capitalize on the full potential of social radars until it incorporates them into holistic Big Data strategies that fuse both open source and classified data sources. Integrated as part of a multi-source intelligence framework and operating seamlessly across classification levels, social radars will generate foresight over insight and will eventually enable the manipulation of human behavior patterns.

Intelligence, as a tactical function, is a command responsibility. It is critical, therefore, that commanders at the strategic, operational, and tactical levels develop at least a working understanding of emerging social radar technology and can demand more in this area from their intelligence professionals. Designed as a 'Commander's Guide', this paper details the utility and essential features of social radars within the context of the Information Age, outlines why holistic intelligence fusion is necessary to optimize predictive analytics, and discusses some of the ongoing technical hurdles and cultural, ethical, and legal challenges surrounding the use of social radars in the military. It does not detail specific UK and US capabilities for three reasons: first, despite drawing primarily on open source data, the output of these systems remains classified; secondly, direct access to these emerging capabilities for research purposes has been limited; finally, and, more importantly, technology is changing so quickly in this area that in-service versions quickly become obsolete.

## Chapter 1 – Warfare in the Information Age

> *To understand the world and our part in it we will need to advance from an intelligence capability that is built around the fusion of largely secret intelligence augmented loosely by some open sources, to a capability that is built around Open Source, managed by Big Data analytics, and augmented by secret intelligence.*
>
> - General Sir Richard Barrons KCB CBE ADC, Commander Joint Forces Command, 2014.[6]

Before expanding on the social radar concept, this opening chapter considers the impact of the Information Age on intelligence activities and sets out the requirement for social radars that support predictive analysis of Human Social Cultural Behavior (HSCB) modeling. It analyzes the changing relationship between open source and classified data, argues that global Internet connectivity is fueling a democratization of violence, and assesses the rise of social media and its exploitation by the Islamic State in Iraq and the Levant (ISIL).

First, Open Source Intelligence is becoming the backbone of military intelligence activity. In this "wired world" of the "Internet of things," data has become a tradable commodity, accessible at lightning speeds across a globally-connected marketplace, frequently at low or no cost to the end user. This is leading to a democratization of intelligence, in which anyone with Internet connectivity is empowered to harvest data, analyze it using online tools, and exploit it to serve their needs. Using smart phone applications for geospatial and temporal analysis, individuals can exploit unclassified phone metadata as a form of Signals Intelligence (SIGINT), social media data as Human Intelligence (HUMINT), and cheap, on-demand, and commercial satellite imagery and micro-drones as Imagery Intelligence (IMINT).[7]

In one sense, this is eroding the value of classified surveillance. The volume of public data at low or no cost, the legality of collecting it, and the speed of processing it is driving a renascent interest in Open Source Intelligence (OSINT), and this has gained particular governmental appeal in a post-Snowden era of renewed privacy concerns.[8] *Joint Doctrine Publication 2.00 - Understanding and Intelligence Support to Joint Operations* defines OSINT as "intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access."[9] In 2006, with social media still in its infancy, Robert D. Steele, a former Central Intelligence Agency (CIA) case officer, predicted that Open Source Intelligence would provide 80 percent of future intelligence requirements and that the classified world was antithetical to the concept of Multi-national, Multi-agency, Multi-disciplinary, Multi-domain Information Sharing (M4IS).[10]

In another sense, however, the relative value of Steele's 20 percent of intelligence requirements coming from high cost, high fidelity, classified sensors actually *increases* because this may be what gives the military the intelligence advantage, particularly over non-state actors that cannot afford these capabilities. Consequently, militaries must ensure that they not only extract maximum value from OSINT feeds but also that they use this to target increasingly sophisticated but scarce classified collection capabilities more efficiently. Militaries must still invest in clandestine and exotic collections methods, but these become the tip of an intelligence spear that holds OSINT at its core.

Another trend of the Information Age is that individuals can find and connect with a potentially global network of kindred spirits to form "identity clusters" in a way that challenges the role and power of the nation state. The decentralization of instant communication, collaboration, coordination, and action (C3A) amounts to an "associational revolution" and changes the way governments must think about emerging national and

transnational threats.[11] The battle for hearts and minds is now agnostic of state boundaries and instantaneous. In this battle, the public assumes the role of both audience and participant in a global theater of operations in which competing actors use an explosion of images and words to create a mobilizing narrative.[12] The same technology that sustains the democratization of intelligence is also empowering individuals with sympathetic support networks and the downloadable know-how to conduct sophisticated, violent attacks. This marks the democratization of violence.

The meteoric rise of social media can account for much of the way these identity clusters now form and mobilize. Social media played a central role in generating popular support for the Arab Spring in 2010, and yet Western governments failed to anticipate these violent upheavals that had serious consequences for national security interests in the region.[13] The UK strategic trends paper, Future Operating Environment 2035, acknowledges the nefarious use of social media as a growing threat, in particular its exploitation by potential adversaries for the purposes of control, recruitment, manipulation, and targeting.[14] At a 2015 conference on *Warfare in the Information Age*, Commander Joint Forces Command claimed, "open source social media is the most important thing a commander needs to know, allowing us to be first with the truth and to shape the counter-narrative."[15] This has spawned a new intelligence category, Social Media Intelligence or "SOCMINT."

The Islamic State of Iraq and the Levant (ISIL) most pressingly possesses the will and the capability to assert itself through social media in ways inimical to national security interests.[16] It is worth considering, therefore, how ISIL has been so effective in social media and how predictive analytics may have prevented some of the recent terror attacks. More than any other terrorist organization before it, ISIL has achieved a high level of sophistication in manipulating social media to proselytize disenfranchised young Muslims and support its ideological expansion.

The Islamic State maintains 46,000 active Twitter accounts with 500 to 2000 described as "hyper-users" that control messaging. Awareness of operational security is high: most users turn off location services and attempt to conceal their location by changing device time-zones, profile names, or place descriptors.[17] However, a good number still neglect even these basic security measures, most notably, Mark Taylor, a New Zealander, who gave away his location forty-five times with geotagged Tweets.[18] Figure 1 highlights how Open Source Intelligence contributed to targeting operations.


**Figure 1: ISIL geotagged Tweets in Iraq and Syria, leading to the targeting of Mark Taylor [Image Source: IBRABO]**

The use of obfuscated and automated retweet services (known as bots) that can generate up to a million retweets in multiple languages per day is common practice. ISIL-associated Twitter accounts had an average of 1,004 followers. Suspending accounts does disrupt the networks, but accounts quickly reappear and there is a danger that suspensions may accelerate radicalization and impede naturally occurring counter messaging.[19] The Islamic State has a polished strategic communications machine. It has adapted different strands to its messaging campaign to appeal to five distinguishable target audiences, using multiple means including Facebook, Tumblr, justpaste.it, and YouTube. In a video, *ISIL says the end of Sykes-Picot*, the narrator appears relaxed, rational, well-equipped, in control, and able to switch fluently between English and Arabic.[20]

Efforts to provide an alternative narrative have had mixed success. The US State Department's Center for Strategic Counter-Terrorist Communication, despite spending $5.5 million on 300 videos, has failed to have any noticeable impact.[21] Meanwhile, 1.2 million people viewed leaked helmet camera footage of a US Special Forces raid on an ISIL prison, which provoked an outpouring of condemnation of ISIL.[22] Consequently, senior US intelligence officials visited Silicon Valley in January 2016 to elicit the support of Big Data giants such as Google, Facebook, and Twitter. Specifically, they aimed to understand how to identify and disrupt patterns of recruitment, radicalization, and mobilization; create and amplify alternate social media content; establish measures of effectiveness for counter-radicalization; and better anticipate and prevent attacks.[23]

In summary, future war concepts stress the importance of the human domain to conflict, particularly with the rise of megacities, a demographic youth bulge, and the proliferation of globally-connected,

instantaneous communications.[24] Western governments failed to preempt the Arab Spring in 2010 and have struggled to counter ISIL's social media campaign.[25] Coupled with fifteen years of population-centric warfare in Afghanistan and Iraq, and now enabled by Big Data analytics, there is renewed interest in developing cultural understanding and using Human Social Cultural Behavior (HSCB) modeling to predict social outcomes such as civil unrest or radicalization. Development of predictive social radar technology in the United States emerged around 2010 but accelerated when the government dramatically increased funding to HSCB research programs in the wake of the Arab Spring.[26]

## Chapter 2 – Social Radars

> *When the situation was manageable it was neglected, and now that it is thoroughly out of hand we apply too late the remedies which then might have effected a cure…Want of foresight, unwillingness to act when action would be simple and effective, lack of clear thinking, confusion of counsel until the emergency comes, until self-preservation strikes its jarring gong - these are the features which constitute the endless repetition of history.*
>
> - Winston S. Churchill, House of Commons, 2 May 1935.[27]

This chapter breaks down the social radar concept, outlines the essential features of an effective capability, and explains how they will add value to military operations. The 2011 London riots and the recent ISIL attacks in France and Tunisia provide concrete examples of the utility of social radars in preempting social unrest or combating global terrorism. The chapter then argues for the removal of intelligence stovepipes to integrate open source and classified intelligence into a single analysis capability that would greatly improve the speed and accuracy of the social radars. Two hypothetical case studies demonstrate how fully integrated social radar technologies would support a range of UK military operations.

In business terms, social radars use multiple data inputs to sense perceptions, attitudes, beliefs, and behaviors, and geographically localize and track these to enable smarter engagement with target audiences.[28] It is the same for security. They enable strategic to tactical situational awareness of the human terrain and provide indicators of future activity, support automated analysis of courses of action, and enable measures of effectiveness. As a form of ISR, social radars deliver timely, persistent, global, geo-referenced, multi-lingual, multi-source, clandestine, and verifiable intelligence collection that focuses on providing geographical and topical insight and foresight about target populations.[29] This foresight could include mapping disease outbreaks, showing patterns of migration, detailing the effects of catastrophic weather events, or preempting acts of terrorism or political subversion. Social radars also portend the capacity to exert cognitive influence by

giving a clearer understanding of how to drive target populations towards social tipping points. In this regard, they are at least as significant a breakthrough in the twenty-first century as radar, sonar, and infrared were in the twentieth century. Appendix A shows a list of potential social radar applications.


**Figure 2: The Social Radar Concept [Image source: MITRE Corporation]**

The figure above sets out the MITRE Corporation's concept of a social radar. At a systems level, the concept has a number of components; commanders' focus will be on the "Results" and "Decisions" layers, but they may contribute to the "Sources" layer through the management of Intelligence Surveillance and Reconnaissance (ISR). Intelligence analysts, data scientists, and data managers will oversee an intelligence architecture that fuses all the necessary data, refines it, stores it securely, and processes it to provide actionable intelligence. Analysts will interact with the system through an intuitive and customizable "Analysis" layer or "dashboard" that allows them to use various tools or "widgets" to manipulate the data, test hypotheses, and generate visual outputs to support decision-making. The dashboard concept demonstrator in Figure 3 below plots "heatmaps" of global instability, allowing the social radar to plot indicators of civil unrest in near-real time. Critically, this concept exploits multiple intelligence sources and analyzes raw data using a series of algorithms to produce results in visual formats such as information graphics that facilitate decision-making.

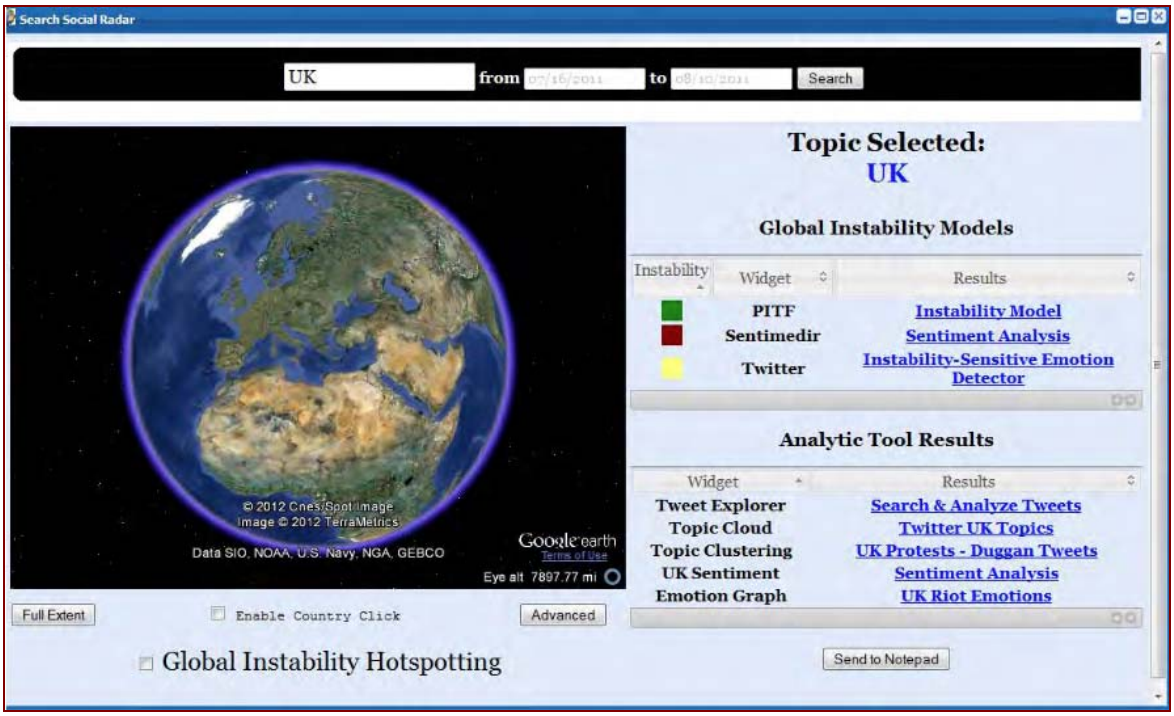


**Figure 3: The "Analysis" layer or "dashboard" of a social radar [Image source: MITRE Corporation].**

There are three system requirements that are critical to social radars. Foremost, evidently, is the continuous flow of raw data, but this is nugatory without predictive analytics that must include topic detection, sentiment analysis, geotagging, and socio- or structural analysis. The third essential requirement is a suitably qualified and experienced workforce. The following chapter deals with the challenge of meeting this last requirement.

The first critical system requirement is the continuous access to global data. Developers in this field always intended social radars to eventually harness all available sources of data, although they recognized social media analytics as the game-changing enabler.[30] Social media analysis uses open source articles and messages from blogs, social networks, news sources, automated video transcripts, imagery metadata, and forums to provide instantaneous insights and measurements of online activity. Social media expresses "a collective wisdom, which, when properly tapped, can yield an extremely powerful and accurate indicator of future outcomes."[31] The success of social radars depends on a target population's Internet access (penetration rate), engagement with social media, and the availability of open data pertaining to that population. In the UK, for example, the Government has made over 9,000 data sets about the British population publicly available and Internet penetration is eighty-nine percent, with seventy percent of users owning at least one social media

profile; 33 million people use Facebook and 22 million use Twitter.[32] A UK-centric social radar would have considerable utility for domestic counter-terrorism or, conversely, for an adversary operating against the UK.

In many developing countries, Internet penetration is lower and the same culture of sharing public information online may not yet exist. This is changing rapidly. Global use of the Internet is growing fastest in Africa and the Middle East, with an average of eight percent year-on-year growth.[33] This equates to over 100 million new users per year, of which ninety-three percent will access the web via smart phones rather than desktop computers. Smart phone ownership in the region will rise to almost 800 million by 2019.[34] In some instances, Facebook monopolizes web-based communications by offering to pay data usage fees.[35] Within the Middle East, Internet penetration is highest in Iran, with thirty-eight percent of the population having regular Internet access.[36] Additionally, Google's Project Loon and Facebook's Aquila Program will eventually accelerate Internet penetration to remote areas while similar Unmanned Aerial Systems could form part of disaster response operations to provide a temporary communications network.[37] While Social Media data may provide valuable insight in areas with high levels of Internet penetration, it has more limited albeit growing utility in remote operating environments. Social radars based purely on open source data will be most effective in areas of high Internet penetration. The table at Appendix B highlights both the opportunities and limitations of using social radars fed only by open source data in areas in which the UK military is likely to operate.[38]

The second critical requirement is the predictive analytics layer, in which there are four essential features: topic detection, sentiment analysis, geotagging, and socio-analytics. First, automated topic detection is now readily accessible through countless commercial applications. Spotter.com provides a useful overview of the capability.[39] Through an intuitive and customizable dashboard, intelligence analysts can scour all intelligence feeds for trending subjects or can set parameters to define the target social group, the geographic area, or the topic itself. Real-time data feeds allow analysts to quickly see the sources of the data to understand the broader context and make a human judgment on the veracity of the sources. The system then uses cascade modeling to make predictions about social behavior based on the dissemination rate of trending topics. When something is said to be "going viral", it is because it has a fast cascade rate. In this regard, the velocity of Big Data is of secondary importance to the acceleration of topic trends.[40]

Second, sentiment analysis is the identification of whether an expression reveals positive, negative, or neutral sentiment. Also known as opinion mining, it provides a view on the attitude or perception of the originator. The commercial sector uses sentiment analysis for marketing purposes but it has obvious utility to

the military.[41] For instance, a commander may wish to understand how people across an area of operations have reacted to a particular trigger event or stimulus and assess the level of emotion this has provoked.

Third, data geotagging enables geotemporal visualization on a digital map. Interactions with social media are by default geotagged with embedded GPS metadata. Despite it being easy to disable this function, most people tend not to, even those with nefarious intent. Just as the jihadist, Mark Taylor, gave away his position in Syria, so too did Russian soldiers operating undercover in Ukraine.[42] However, even if the vast majority of ISIL fighters in Iraq and Syria *have* disabled their location-services, there are other ways to infer location.[43] An online post may include a name of a place, users may allude to a location in the message content, or an attached image may still contain location metadata or visible clues about its location. With ever increasing accuracy, Google's PlaNet application analyzes photographs of landscapes to predict where they were taken. For highly skilled analysts, it is also possible to use open source tools to track individuals' smart phone accelerometer data, which is harder to disable than the GPS function.[44] Figure 4 shows how analysts may combine various social radar tools on a dashboard.

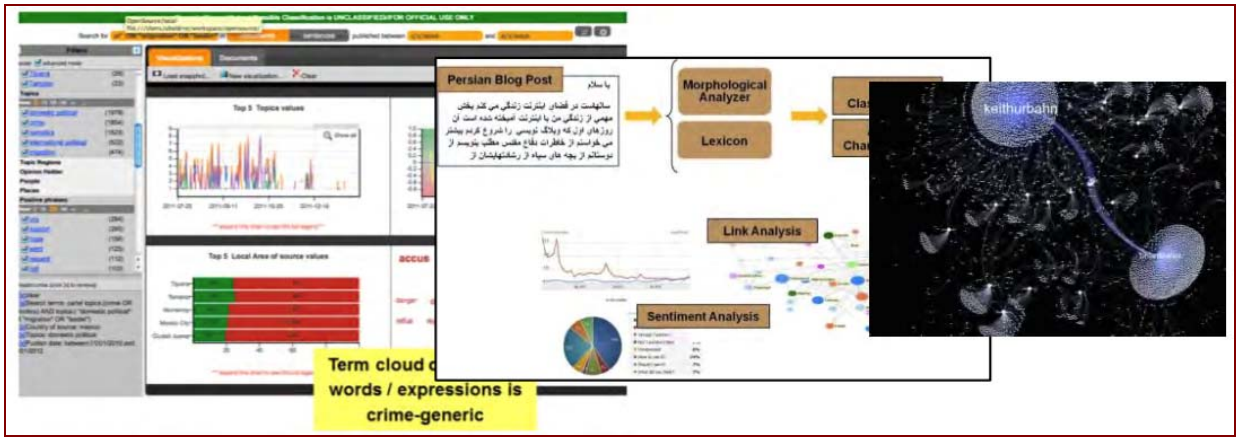


**Figure 4: Snapshots from social radar analytic tools [Image source: MITRE Corporation].**

Finally, understanding the structure of the social network through socio-analytics is critical to the predictive process of social radars. Automated human terrain analysis from social media can map out a social network in seconds in a way that might take Signals or Human Intelligence analysts days to complete. This can identify core and periphery members of an online community and show how one network interacts online with another network.[45] For commanders, this level of analysis identifies the sources of influence messaging, key nodes that spread that influence, and the multiple periphery layers of support. Meso-scale analysis concerns the interactions between individuals in the same network group while macro-scale analysis shows the interactions between different network groups. Transitivity modeling, meanwhile, forecasts the probability of

interconnectedness within a network for if A knows B, and B knows C, there is the possibility that A also knows C. LinkedIn's *People You May Know* (PYKM) application is the most commonly known example of this and would have utility for the intelligence professional.[46] A social radar would list all the possible associates of a enemy fighter; prioritize these according to their levels of activity, assessed threat level, or proximity to friendly forces; and show how they are linked within the network. Automation through social radars accelerates non-linear, or *spiral*, analysis, which identifies network linkages and behavioral trends that would not otherwise be apparent to a human analyst.[47] This is shown in Figure 5 below.

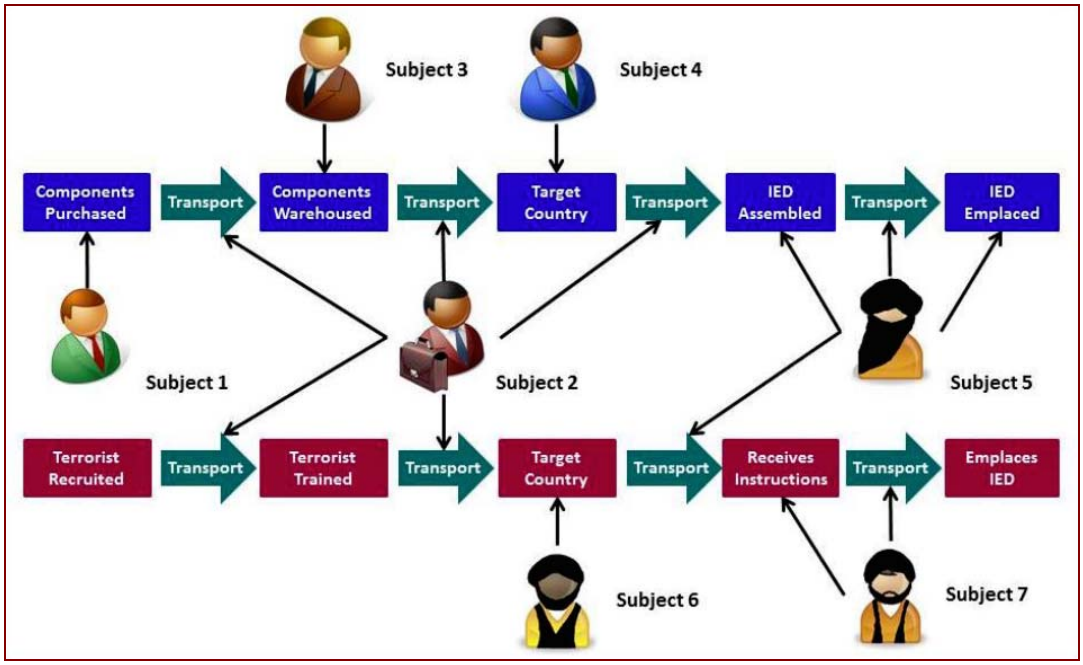


**Figure 5: The application of spiral analysis to understand network linkages**

**[Image source: Concurrent Technologies Corporation].**

Social radars look at trends in these four features over time to formulate predictions about future events. Social radars identify deviations from normal baseline activity. Historic data is essential to understand how previous activity cascades unfolded in reality.[48] Social radars must therefore be calibrated to the cultural sensitivities and baseline of collective emotion within the target audience.[49] Sentiment analysis looks for changes in sentiment over time and can reveal whether the emotions of a given social group are coalescing around a particular issue. At the same time, location data maps the geographic spread of that sentiment, and shows whether the social media users are physically congregating towards a particular geographic location.[50]

The 2011 London riots that followed the shooting by police of Mark Duggan in Tottenham demonstrate the potential value of social radars. Effective social radars could have predicted the ensuing

violence that resulted in sixty-one arrests and injuries to twenty seven police officers. Retrospectively, the MITRE Corporation (commissioned by NATO) showed that the UK was flashing red on a Global Instability Hotspot Dashboard. This model used three indicators to measure public volatility, providing a strategic to tactical focus. Political instability modeling analyzed national factors such as crime statistics, education levels, mortality rates, economic data, and reports of discrimination. The UK Government is the world leader in making 9,000 open data sets publicly available.[51] This provides a baseline understanding of a society. Secondly, sentiment analysis based on national news reporting revealed increased levels of anger aimed at national and community leaders and the police, and heightened concerns about terrorism, human rights, and political dissent. Finally, more detailed assessment of Twitter feeds showed a spike in anger prior to and immediately following Mark Duggan's death. Mapping software illustrated this as a bull's eye over Tottenham, while topic clustering software deduced the root cause of the conflict ("Duggan [...] Mark [...] Police [...] Shot [...] IPCC") and identified both the most prolific social media users within the network and how their influence was spreading within social networks and physically across the UK. The final component of this case study is that an automated detection algorithm could have detected when a particular mobilizing message, in this case, a link to a map showing protest routes, went viral three days before the protests themselves took place.[52]

Similarly, predictive analytics should have anticipated the Islamic State's attacks in Paris and Tunisia in 2015 by spotting the warning signals on social media. Social media analysis has already uncovered ISIL's online social networks, identified key influencers and facilitators, and predicted a number of young British Muslims as being on the brink of radicalization.[53]

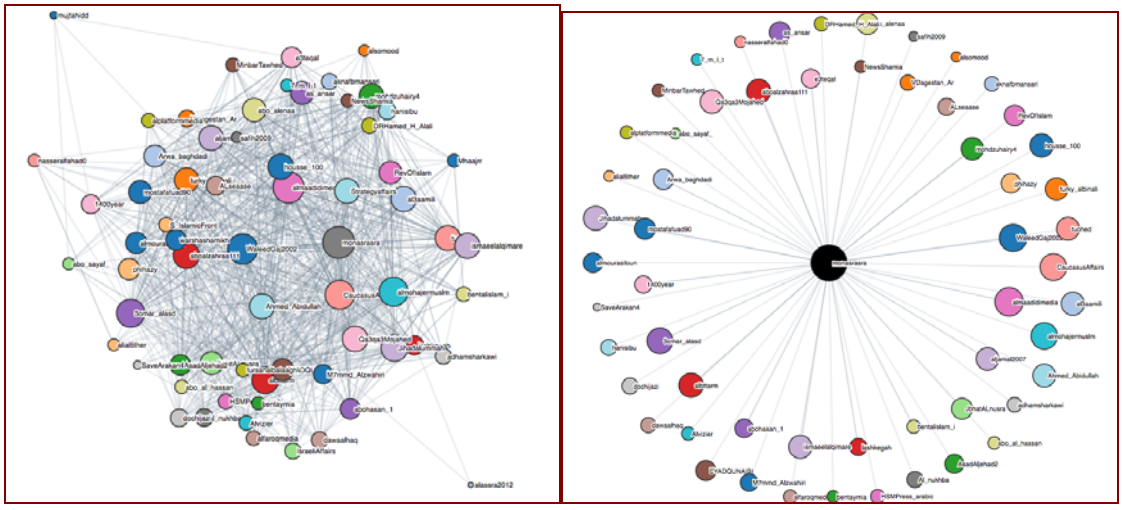

Figure 6: Automated network analysis of 66 prominent Jihadists

to identify key influencers (Image source: Bostok)

ISIL released YouTube videos ahead of each of the three attacks in France (Charlie Hebdo in January, the Lyon train attack in August, and Paris in November).[54] Using only two data sources (the French-language discussion on Wikipedia about ISIL, and Opération Chammal, the French military operation in Syria), a Big Data company in France retrospectively identified spikes in the level of online activity and the sentiment of that activity (sentiment analysis) on these two sites in the days prior to these attacks.[55] Meanwhile, a Tunisian blogger retrospectively identified that terms such as 'the foray of Tunis,' 'tyrants of Tunisia,' and 'good news for Tunisia' trended on Facebook, Twitter, and YouTube for the three days prior to the 19 March attack on the National Bardo Museum.[56] These spikes are shown in the figure below. These descriptive and predictive OSINT applications are all functions of effective social radars. As long as the Islamic State continues to operate on social media, OSINT will play a central role in defeating it.

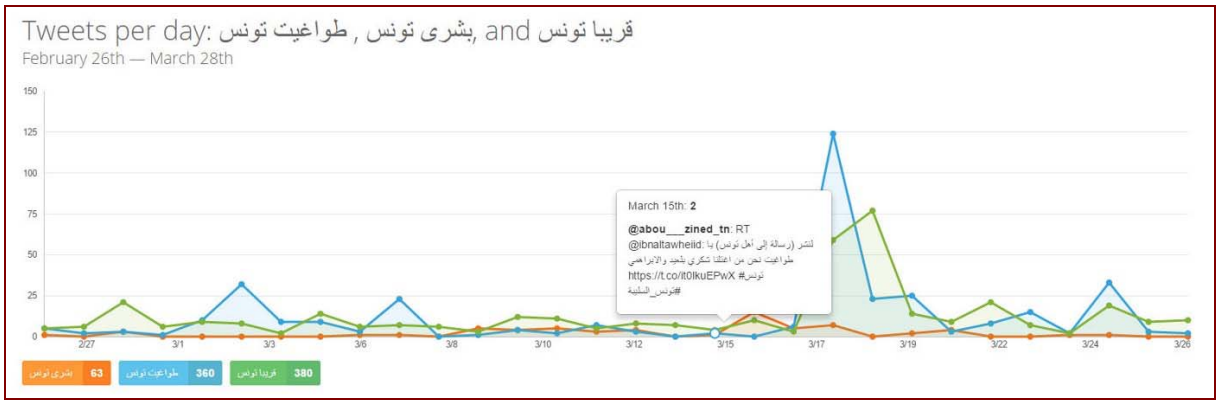


Figure 7: Retrospective Twitter trend analysis of key words and phrases immediately preceding the Bardo Museum attack in Tunis, 2015 [Image source: Zoghlami]

The predictive analytics functions of a social radar outlined above build sociocultural understanding and provide commanders early warning of events. However, by extension, the same tools support Information Operations and decision-making.

Understanding the human terrain is the central component of successful Information Operations. If the warfighter is to dominate the narrative, it is essential to understand the structure in which an adversary operates and how to exploit that structure. The Pew Research Center and Social Media Research Foundation identified six distinct communications structures within Twitter. These were listed as "divided" (polarized networks with little to no cross-pollination); "unified" (tight crowds with lots of cross-pollination); "fragmented" (mass followership but little connectivity between followers); "clustered" (ad hoc community

formed around a particular story); "in-hub and spoke" (broadcast network in which followers of a central instigator amplify the message); and "out-hub and spoke" (support networks where a central node responds to requests for information).[57] Similar studies reveal temporal patterns to social diffusion, which typically accelerates in the late evening and peaks on Fridays in Western societies. Linking this back to activity cascades, targeting particular network nodes or disrupting the entire network at particular times may cause a loss of momentum in the diffusion patterns, shaping the trajectory of the message propagation away from violence.[58] Physically removing a key node from the battlefield may achieve the same effect. Social radars map the communications nodes and allow commanders to more effectively shift perceptions in their favor. Geotagging and sentiment analysis allow a commander to map reactions to a stimulus or IO message and see how that influence activity is resonating with that population.

Most importantly, by improving situational awareness and predicting events, social radars provide commanders "decision space", critical to the maneuvrist approach. Social radars can provide permanent Wide Area Surveillance (WAS) of the human domain and reveal correlations and trends about issues that analysts did not even know to look for - the "unknown unknowns". Thus, Big Data does not so much find the proverbial needle in a haystack as find the right haystack in a field of haystacks.[59] This will initiate the generation of a more nuanced and responsive Decision Support Overlay (DSO) that more accurately reflects the dynamic nature of the human terrain and will cue ISR to corroborate hypotheses or plug intelligence gaps. Intelligence Preparation of the Environment (IPOE) becomes automated. With machine learning technology, automated ISR tasking, collection, processing, and dissemination (PED) may become a background, supporting activity. Insight discovery will accelerate, condensing the Observe and Orient stages of John Boyd's Decision Cycle with more time available for Course of Action development.[60] As tempo increases and confidence in the accuracy of the predictions improves, decision-making must respond to the availability of actionable intelligence. More decisions will be entrusted to lower levels, battle rhythms will become more flexible and dynamic targeting procedures will become the norm for all activities, kinetic and non-kinetic.

These are bold statements and the vision will likely not be fully realized until social radars are integrated as part of a multi-source intelligence framework, operating seamlessly across classification levels. Big Data analytics already has the technical capacity to simultaneously and securely manage classified and open source data streams, fuse these to generate greater fidelity, and filter the results as appropriate to the end user's classification or security environment.

**The case for the full data integration**

In 2014, a consultant at SAS Federal gave a damning indictment of military intelligence fusion procedures,

> Surprisingly, this experience [manual collation of data in a stovepiped system intelligence center] has not changed. In fact, now we integrate data by filling entire rooms with analysts responsible for one or two data feeds, who then consolidate their information with one another through a chain of command to create an integrated picture. In other words, you are doing all the integration in your head, and then you are sharing your data with other warfighters who are integrating data in their heads, which your bosses then integrate in their heads. It's all done to build situational awareness. Analytics integrates this data for you and improves the data quality at its source. Despite an environment of force shaping and budget cuts, analytics can enable you to remain swift and agile in today's rapidly changing operational space.[61]

Intelligence fusion is improving however. The US example of Activity-Based Intelligence (ABI) provides a useful template and it is encouraging that the UK is already leaning in the same direction. Conceived around 2012, ABI breaks down the intelligence silos into a single repository. The identification of trends and predictions of future outcomes relies on all data sources being spatially and temporally indexed, integrated before exploitation, and the sensor and sequencing of events being treated with neutrality. In ABI, Open Source Intelligence would have no greater value attached to it than Geospatial Intelligence, Human Intelligence, or Signals Intelligence, for instance.[62] Technology now allows this smart fusion to occur without compromising the intelligence source or risking the release of intelligence products to the wrong user at the wrong terminal. A user would only see a product at a classification appropriate to his or her clearance level and security environment.

Social radar developers at MITRE Corporation already intended social radars to integrate all intelligence sources because they recognized the efficiencies and predictive accuracies to be gained from doing so. The positive effects of integrating all intelligence sources into a single automated intelligence fusion system outweigh the very slim risk of intelligence contamination. In the case of Syria's use of chemical weapons in 2013, for instance, there is evidence to suggest that the U.S intelligence community failed to join the dots quickly enough despite numerous indicators existing in separate intelligence stovepipes.[63] A fused system would correlate top secret human intelligence against names highlighted through social media analysis, link geotagged Twitter activity to covertly-collected cell phone data, and compare the 1,600 hours of Full Motion Video taken by the US Air Force everyday against open source imagery on Google Earth.[64] It is only

the seamless fusion with classified data that will give commanders the intelligence advantage, optimizing the value of open source data, automatically allocating classified collection assets against known intelligence gaps more efficiently, and generating greater foresight of future events.[65] So long as the data processing power and algorithms can handle it, it stands that the more data in the system, the better the results.

To illustrate the utility of fully integrated social radars, the paper now presents two case studies that demonstrate their benefits at the strategic, operational and tactical levels. The first scenario considers a Humanitarian Assistance mission, the second a Small Scale Focused Intervention using the Joint Expeditionary Force (Maritime).

In the first scenario, a Royal Navy Type 26 Frigate is diverted to South East Asia to respond to a catastrophic weather system due to make landfall in the coming days. A full international assistance mission follows as the death toll rises into the thousands. The UK Government is keen to play a lead role in order to generate goodwill within the region ahead of a planned ministerial trade visit. At the strategic level, the UK Government uses a social radar to monitor the British public's reaction to its initial response. Sentiment analysis on a heat map reveals early positive indicators of empathy and support in the South of the country but indifference in the North caused by having suffered a winter of persistent flooding. However, this trends sharply towards negative sentiment (resentment and anger) when the Government announces a £50 million reconstruction and aid package some weeks into the disaster. The Government is able to take mitigating action to quell indicators of social unrest and possible violent protest in one particular town. Likewise, it reassures and supports South East Asian diasporas in major UK cities, and maps out the positive sentiment this generates within certain Muslim communities.

Over the course of the HADR deployment the Government monitors open source indicators within the affected region. Discussions of the British assistance soon die down on traditional sources (government official websites, news feeds, local blogs). However, a '1-Second Everyday' video showing a Royal Navy medic saving lives goes viral on social media, generating goodwill towards the UK Government that the Foreign Office seizes upon to announce an investment project that also trends positively and paves the way for a successful trade visit.

At the operational level, the National Met Office uses sentiment analysis and crowd-sourced imagery to map the geographic extent and level of the damage in near-real time.[66] Collected intelligence is shared with deployed units, regional authorities and non-governmental response teams. A combination of social media

analysis, commercial satellite imagery, and open-source data on critical national infrastructure enables preemption of the risk to essential services and the tailoring of bespoke technical response teams ahead of international requests for support. As the population evacuates the affected area, the radar predicts the outbreak of an epidemic by analyzing indicators of overcrowding, access to drinking waters, status of solid waste disposal systems, numbers of deployed health workers, and population at risk demographics.[67]

The same radar extrapolates key words from Tweets and correlates these with top secret signals intelligence translated in near-real time using open source translation software. Coupled with the geospatial data, this reveals potential sources of looting and smuggling emanating from an area where historic Human Intelligence reports suggest a dissident faction is known to operate. This correlation focuses classified sensors and, once corroborated, all the open source data is passed to the local authorities.[68] A social analytics boundary box is generated over the top of all deployed UK military units, enabling an Indicators and Warnings "bubble", which can be drilled into and used to prioritize ISR allocation and set local force protection levels. Mapping aid distribution, demographics, and online sentiment gives foresight of potential civil strife and ensures a more efficient, equitable, and peaceful distribution of aid.

Social radars also contributed to tactical level effects. Arriving first on the scene, the Type 26's Commanding Officer already has a nuanced understanding of the situation. Crowd-sourced imagery, overlaid with historic satellite imagery, enables intelligence preparation of the environment and sentiment analysis indicates which areas are most affected and what the locals need most in each area.[69] Isolated locals can use a "Speak-to-Twitter" service, recording a request for assistance that is turned into a Tweet and monitored by aid agencies.[70] This allows aid to move quickly beyond the less affected urban areas to the critical outlying communities. Rumors online of potential armed looters in the port area enable the Commanding Officer to increase ship's security and ensure personal protective measures as the sailors and marines conduct operations ashore.

In the second scenario, the UK and France mount a joint small-scale focused intervention against an ISIL-affiliate conducting cross-border raids, posing a threat to international shipping and threatening local tourist revenues. At the strategic level, a social radar application, similar to that shown in Figure 8 below, had revealed the gradual deterioration of stability in this country over a period of six months, enabling a more efficient allocation of strategic ISR.[71] For the first time, the Joint Expeditionary Force (Maritime) was tasked in accordance with social radar threat analysis and the UK deployed Short-Term Training Teams as part of a

regional approach to stem the tide of violence. Temporal and geo-based analysis of social media following the arrest of an individual on terror charges revealed indicators of violent social unrest emanating from one particular town.[72] Corroborating open sources were shared with the local government, which increased its security presence in this popular tourist hotspot.

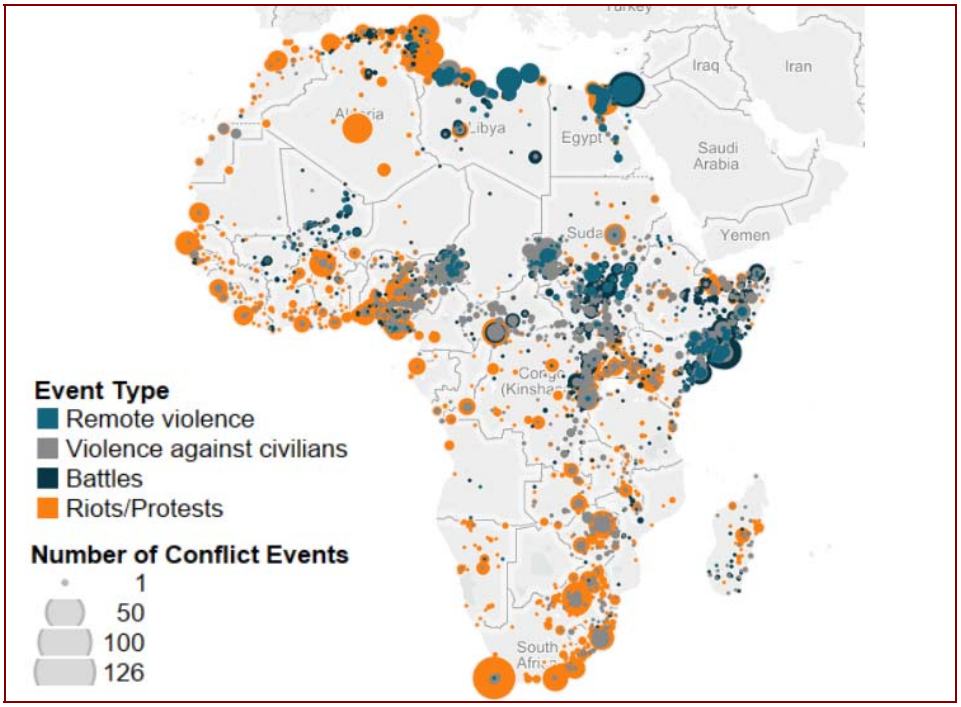


**Figure 8: Social radar heatmapping predicts violent behavior patterns across Africa [Image source: ACLED]**

The Foreign and Commonwealth Office (FCO) used social media to post a travel advice alert and mapped the spread of this message across the UK. Open Source Intelligence over the next forty eight hours revealed that flight bookings to the country had declined by seventy percent. Social media analysis revealed that holidaymakers in the country were largely ignorant of or unfazed by the local news but the FCO prepared social media messages targeted at this population just in case it needed to instigate a Non-combatant Evacuation Operation.

Moving to the operational level, US, French and British analysts worked collaboratively to share intelligence on this mission. The social radar automatically filtered out the 5-Eyes only data or assessments before sharing with the French authorities. The instability hotspots provided the Joint Force Commander with a nuanced understanding of the human terrain from social media activity, including identification of key sources of instability, which were corroborated through Signals and Human Intelligence. Sentiment mapping revealed areas of intelligence interest, which became Named Areas of Interest for supporting ISR. The social

radar also mapped areas of pro- and anti-government sentiment. The analysis included automated credibility assessments to rule out any deception efforts. The pre-emptive deployment of an Operational Liaison and Reconnaissance Team meant that the Joint Force Commander had sufficient situational awareness to respond to Ministry of Defence enquiries when the unrest hit the public media outlets. The social radar predicted unrest near a tourist resort; the Task Force deployed units closer in-shore as a visible deterrent. Temporal patterns in the dissemination of tweets by nefarious actors enabled the coordination of an offensive cyber operation to disrupt messaging at a selected time.[73]

Finally, at the tactical level, when the social radar indicated an attack was highly likely, open source data was automatically fused with classified sources to corroborate likely target locations and plotted the militants' likely base locations. Data fusion through a single system enabled the rapid production of a target pack. The ISR tasking process and Course of Action (COA) modeling ahead of a joint UK/French raid was automatic. Advanced reconnaissance forces used a secure PDA application to receive social radar intelligence of the human terrain in the target vicinity. This alerted them to the presence of potential instigators of violence, provided profile data (photos, previous intelligence reports, known and likely associates). Social media monitoring contributed to Battle Damage Assessment and predicted a retaliatory, small boat attack against the Task Force, which was successfully repelled.

These two case studies demonstrate some of the potential applications of social radars within the military. However, there are a number of technical, legal, and cultural hurdles that the Intelligence Community must overcome before social radars are able to contribute as described. It is these challenges, along with some ethical considerations, that form the subject of the following Chapter.

## Chapter 3: Technical Challenges and Ethical, Legal, and Cultural Considerations

> *Using Big Data is like mining for gold. You've got to go through a whole lot of dirt to get to the nuggets.*
>
> - Colonel Bobby Saxon, US Army.[74]

The potential transformative value of social radars in forecasting population-level changes is beyond doubt. Through its Open Source Indicators (OSI) program, the US Intelligence Advanced Research Projects Activity (IARPA) was able to forecast civil unrest events in Latin America using open source data feeds only. This project, the Early Model-Based Event Recognition using Surrogates (EMBERS), successfully forecast the date and location of the 'Brazilian Spring' in 2013 and the student-led protests in Venezuela in 2014. By

March 2014, EMBERS was successfully forecasting events with 80 to 90 percent accuracy, typically seven days ahead of the news.[75] However, social radars do not provide an all-seeing eye and their predictive capabilities remain limited, not least because in-service and concept demonstrators have not fully overcome the challenges of integrating classified and open source data within a single system. This chapter highlights some of the technical challenges that currently constrain the utility of social radars. More important, however, are the ethical, legal and cultural considerations, which assume greater significance as technological advances improve the predictive power of the system.

Despite IARPA's success rate, developers across the research community continue to refine the data handling processes and invent new algorithms to improve social radar technology. The primary challenges concern the accuracy of sentiment analysis, the assessment of data veracity, the integration of unstructured data, and establishing causation as opposed to correlation.

Accurate sentiment analysis remains a challenging area although natural language processing and the development of semantic filters are rapidly overcoming problems associated with the recognition of sarcasm, intonation, deciphering punctuation or emoticons, and interpreting slang or jargon, emanating from different cultures in multiple languages. Data scientists use scoring systems to grade levels of sentiment, essentially creating an emotional barometer based on the strength of the vocabulary.[76] Ultimately, the output of any inquiry will only be as good as the algorithm beneath it. A further challenge is in understanding the link between sentiment analysis, motivation, and behavior. Data and social scientists are collaborating to improve accuracy in this regard. Historic data can be used to take a society's "resting pulse" so that alert levels within each predictive model are calibrated to the target society. This reduces the signal to noise ratio.[77]

Assessing data veracity (the 4th "V" of Big Data) remains one of the greatest challenges affecting the employment of social radars in the military. Analytics software may be prone to interference, spoofing, and cyber-attack, a simple tactic being to use bots to create "noise" in the system and skew analysis. However, in this regard, the bigger the baseline data set, the harder it would be to deceive the system as there would be more sources to confirm or refute any anomalous activity. It would likely require a focused effort by a sophisticated and nefarious user and the simple use of bots and sock puppets to automatically amplify noise would be detectable. However, it is a credible threat: in 2013, hackers sent a Tweet from the official Associated Press account claiming that the White House had been attacked and that Barack Obama had been injured. The momentary shockwaves of this Tweet, though corrected within minutes, nonetheless caused a

143-point fall in the Dow Jones.[78] Researchers are mitigating this risk by using Big Data analytics to assess the likely veracity of a piece of information based on the prior truthfulness of the source and the presence of corroborating evidence.

The success of social radar technology depends on an ability to analyze unstructured data. This is defined as data that does not conform to pre-defined data formats and can be textual (emails, news feeds, Tweets) or non-textual (voice recordings, still or moving imagery).[79] Analysis of unstructured data is a significant problem challenge and far from unique to social radars. However, given the nature of the types of outcomes social radars will be looking for, unstructured data is the lifeblood of the system. Incorporating classified, unstructured data from multiple intelligence feeds is an added complication. Consider again that the US Air Force collects 1600 hours of motion imagery everyday. This is over seven terabytes of unstructured data, only five percent of which is currently analyzed in detail.[80] The continued proliferation of unmanned systems only increases the requirement for greater automation in intelligence analysis and for all data to be cross-referenced with other sources. The private sector recommends storing data in its original format but ensuring the metadata is "cleansed" at the point of data storage to ensure it is appropriately tagged and easily retrievable. This massive undertaking, particularly for historic data, could be outsourced to data-entry contractors. Data stewardship becomes a command responsibility to ensure all information actually has utility to the intelligence enterprise.[81]

Finally, the number of potential variables assessed within a single algorithm can reveal patterns of correlation without necessarily identifying causation. In other words, social radars may tell the analyst what is likely to happen without clarifying why it will happen. Conducting the system diagnostics to dissect the algorithm may be so time-consuming as to prove counterproductive. Big Data applications, therefore, including social radars, may result in an overall loss of accountability and traceability in the decision-making process.[82] Data-to-decision analysis, however, challenges the traditional role of intuition. Therefore, until social radar technology is commonplace, user interface should provide for simple interrogation of the results such that analysts can understand and explain to the commander the types of data that the model considered and how the relative values of those data sets affected the outcome. Indeed, Value is frequently listed as another "V" within the list of Big Data characteristics. This links to a means of system validation to allow for automated machine learning without the system generating its own biases by placing particular values on certain data sets that may actually be less relevant in the next situation.

Of greater consequence to commanders are not the technical challenges, which the research and commercial sectors will naturally seek to overcome, but rather the ethical, legal, and cultural considerations surrounding the collection and processing of open source data and the exploitation of the resulting predictive intelligence. Public concern regarding the pervasiveness of government access to the "Internet of things", coupled with questions of privacy and civil liberty, heightened by the Snowden leaks, and the sluggishness of the law to adapt to Big Data technologies, threaten to stifle the legitimate use of predictive analysis within the intelligence community.[83]

In the commercial sector, data activities that do not even stir public consciousness can suddenly assume a more ominous hue when applied to governments. The warfighter must be wary of public perceptions regarding how Big Data is used. What may appear legal and ethical for the purposes of marketing, customer service, or product functionality may appear illegal and unethical for the purposes of security. In the "quantified society", individuals willingly release personal transactional data to one entity without realizing that this may entitle other entities to access that data for other purposes.[84] Data has become transactional, that is, individuals exchange it in return for some perceived benefit, perhaps social recognition, a more efficient online shopping experience, or the ease of hailing a taxi. Wittingly or unwittingly, individuals are liberally giving up their privacy and providing information to companies, sales representatives, or social media platforms.[85] However, when a government accesses that data, even if entirely legally and through exactly the same processes as a commercial enterprise, it may be perceived to cross an ethical threshold. This may be because it is harder for individuals to accept the use of *their* data by the government because they cannot appreciate any immediate personal benefit.

To combat this, the intelligence community should be as transparent as possible about how it uses aggregated social data to serve national security interests. The preeminent role of open source data within social radars facilitates openness with the public. Clearly, it will be easier to discuss how social radars could support the military's contribution to flood relief than how social media intelligence is used to predict radicalization. Publishing regular privacy impact studies would be one way of educating the public and policy-makers and desensitizing what could otherwise remain an inflammatory issue.

While the collection and processing of Big Data raises some concern, of greater concern is the application of predictive analytics to anticipate or shape social outcomes. In the wrong hands, the ability to monitor a population's sentiment and accurately predict social unrest is a dangerous power. Social radars

provide considerable scope to suppress fundamental, democratic rights, such as freedom of religion, speech, and peaceful protest. That authorities, even in liberal democratic societies, could abuse or be tempted to abuse this power is not beyond imagination. In 2014, the US Department of Defense was linked to a Facebook experiment to manipulate the news feeds of 700,000 Americans in order to research the ability to sway a target population towards a desired social outcome.[86] Similarly, IARPA's EMBERS project has now switched focus from Latin America to the Middle East and over a dozen US government agencies receive regular progress reports.[87] The increasing accuracy of this project raises questions for how and when the United States might choose to take preemptive action and with whom it might decide to share the information. Providing the government of Saudi Arabia with the date and location of a potential mass protest in Riyadh may benefit the stability of global oil markets but may come at the cost of a brutal government crackdown on political opposition. As Karen Greenberg, Director of the Center for National Security at Fordham University, New York, remarks, "nations must agree that we are so unsafe that we need [social radars] to reduce our risk to zero at the expense of our privacy."[88]

Turning to the legal considerations, it currently is unclear what impact security technologies may have on human rights. This is because the gravity of the impact is a factor of both the nature of the right and the intended use of the data.[89] The legality of "mass surveillance" through social media remains a grey area because Big Data analytics blurs the distinction between "mass" and "individual" surveillance. In the UK, this has implications for the Regulation of Investigatory Power Act 2000 (RIPA).[90] According to the UK Chief Surveillance Commissioner, "just because the material is out there in the open, does not render it fair game […] Certain activities will require authorization, [including] repetitive viewing of what are deemed to be 'open source' sites for the purpose of intelligence gathering and data collation."[91] However, this appears to apply to targeted collection against individuals. By contrast, a Linklaters report suggests that the collection of general trends from Big Data is unlikely to be legally objectionable.[92] In all cases, data collection must comply with the Data Protection Act 1998.[93] Associational profiling, which is the primary method of a social radar, risks at best discrimination, at worst, wrongful targeting. Intelligence analysts must be particularly careful about casting judgment or making predictions that could be perceived as discriminatory on the grounds of religious belief, political affiliation, trade union membership, health, sexuality, or criminal record. Corroboration through other sources and the maintenance of a human-in-the-loop remain critical features of an effective data strategy.

A further area of legal concern is the sharing of open source data between allies. Even within the 5-Eyes community, privacy and civil liberty laws vary widely; what may be legal in the UK, for instance, might infringe the First Amendment in the United States. Just as with cyber activity, early engagement with legal advisors is critical and the intelligence community will have an increasing role for dedicated legal advisors, specializing in media and privacy law. Frequent and open legal forums on the use of social radar technology will promote transparency and develop technical understanding and appreciation for the military objectives.[94]

In considering the cultural challenges, the development of social radar technology represents only a single strand in the evolution of Big Data analytics within the military. Consequently, cultural challenges pertain on the whole to Big Data in general and to the rise of Open Source Intelligence. Cultural challenges are identified in the willingness to engage with intelligence fusion, manpower, data management, systems procurement, and the role of the commander.

The intelligence community is prone to interdisciplinary snobbery and shrouds itself unnecessarily in mystery and protocol, which can occasionally cause it to forget that the purpose of all intelligence is to allow commanders to make informed decisions.[95] Cultural resistance to a multi-intelligence fusion center is counterproductive and undermines the warfighter's ability to receive the right intelligence at the right place at the right time to make the right decision. The UK Defence Geospatial Intelligence Fusion Centre [sic.] at Wyton is now established as a central intelligence hub despite certain departments continuing to resist the concept of data fusion. Technology is overcoming any excuses for slow-rolling the integration process, allowing analysts to work collaboratively from multiple locations around the UK or globally. The 5-Eyes Signals Intelligence community was already established as a "hub and spoke" model, providing constant coverage to deployed units. Continued careful appointment of Commander, Joint Forces Intelligence Group, is essential to ensure that nascent social radar technologies continue to support the entire military in the most pragmatic and streamlined manner, free of any regimental or institutional bias.

The recruitment and retention of a suitably qualified workforce is a critical requirement of an effective social radar capability. The military faces cultural challenges in how it will attract IT professionals, data managers, and data analysts, either through outsourcing or direct employment. Interestingly, the commercial sector notes a general reduction in the value of subject matter experts (SME) and the rise of the generalist, all-source analyst.[96] This does not fully apply to the military. Instead, analysts will become SMEs in their own right, highly skilled at sourcing and manipulating large data sets and identifying and visualizing trends to

satisfy commanders' information requirements. The role of the traditional intelligence operators does not disappear but refocuses on collection and data cleansing before it hits the data warehouse. Assuming the increased emphasis on open sources, intelligence analysts must be highly inquisitive, mathematically minded, and experimental.[97] Increasingly, they must ask "what if?" rather than "so what?", trust the algorithms to generate insights, and be given the time and latitude to innovate, particularly with the manipulation of data sets from potentially unusual sources.

The increasing complexity of intelligence analysis demands greater openness with the commercial and academia sectors. The military will not be able to permanently retain the data scientists to design the base algorithms but analysts must be able to employ all the open source tools at their disposal, including those on the Internet. Outsourcing intelligence requests will become the norm and JFIG's use of the US Multi-Agency Collaboration Environment (MACE), which is a US Public Private Initiative for all-source intelligence fusion, provides precedent of where this has worked well.[98] Likewise, "hackathons" and specific analytical competitions have their place and can be useful for generating solutions to specific problems quickly.[99] Moreover, such activities enable the MOD to leverage sectors of society that might not otherwise be drawn to full-time employment with the military but may still be motivated by a sense of patriotic duty or financial reward.

Complexity also places a new burden on the intelligence community to understand the analytics layer of any predictive modeling and to ensure that it is adapted to the particular mission and the specific decision.[100] This is the role of a Chief Analytics Officer or Data Advisor ("DATAD.")[101] The DATAD should be included in the planning process from the outset in exactly the same way as Legal, Policy, and Cultural Advisors. Indeed, these advisors are likely to become natural bedfellows in the exploitation of social radars. The DATAD should also lead User Experience Teams to constantly review and adapt the data modeling and visualization tools to ensure they meet commanders' requirements.

It has been shown that open source data alone does not provide a panacea. Neither can the automation of data processing avoid the underlying requirement to get smarter at data collection and data entry. The compilation of metadata, potentially entered laboriously by hand, is a necessary evil. This is particularly true of historical records. In a new operating environment, intelligently written and correctly indexed intelligence summaries will be critical. Prior to the existence of social radars, the US Air Force's Joint Improvised Threat Defeat Organization eventually achieved fifty percent accuracy in predicting IED events in Iraq but this relied

on meticulous data-entry following every IED event.[102] The importance of data-entry should be factored into basic military training and become a feature of Continuous Professional Development courses. From the lowest tactical levels to the most strategic, operators and analysts must become better at handling and collating intelligence, feeding it all into a data repository in formats that make retrieval and analysis as easy as possible.

A further cultural challenge concerns the requirements process. The UK MOD currently has access to two social radar technologies as capability demonstrators. These are the UK's Social Media Intelligence (SOCMINT) Predictive Analysis and Exploitation Service (SPAES) and a capability on loan from the US Defense Intelligence Agency (DIA).[103] Anecdotal evidence from the United States suggests that the acquisition of predictive analytical capabilities needs to focus on establishing a secure framework for Big Data analytics rather than worrying about the hardware and software tools, which will likely be obsolete before they even enter service.[104] If the MOD trains analysts only in "buttonology" on a single platform, the social radar experiment will surely fail. Adaptive training that encourages experimental, innovative approaches to data manipulation and the repurposing of open source analysis tools is essential. The MOD should explore opportunities to embed analysts in Big Data academies or allied intelligence fusion centers.

Finally, commanders cannot be bystanders in the Information Age. They must fight to understand and embrace technology. Commanders that struggle with their own computer, do not understand social media, or have never considered their online security risk being incapable of keeping pace with the lance corporal delivering an intelligence briefing. Social radars call for innovative thinkers. Even individuals that are comfortable using smart phone applications may fail to conceive of operationalizing these apps for use on the battlefield. Commanders should immerse themselves in the technology, explore the power of Open Source Intelligence applications available on the Internet, and continue to challenge the Intelligence Community and procurement agencies to deliver against their operational requirements.

In sum, commanders can largely rely on Moore's Law to overcome the technical stumbling blocks that currently limit the accuracy of social radars. However, the real impediments to progress may be as much cultural as they are technical. Consequently, commanders should become familiar with social radar technologies and, cognizant of the ethical and legal considerations, push for continued development and integration in the Intelligence Community.

## Conclusions

Harnessing the power of Big Data predictive analytics, particularly topic detection, sentiment analysis, sociocultural modeling, and geotagging, social radars can provide commanders with the best means yet of understanding and engaging with the human aspects of conflict in complex operating environments. Advanced concept demonstrators have been predicting civil unrest in Latin America for the last four years and could have predicted the Arab Spring, riots in London, or the terror attacks in France and Tunisia. Social radars work, and the technology merits continued development and commanders' attention. With time, they will support a range of military operations, from Humanitarian Assistance and Disaster Relief missions to full spectrum targeting operations.

The notion of accurate and predictive social radars is an important step towards Activity-based Intelligence that take a more holistic approach to data fusion, and leads to the more effective application of force. As a form of persistent Wide Area Surveillance, social radars will identify gaps in knowledge, extract maximum value from open source and classified data feeds, and generate efficiencies in the employment of classified collection capabilities. Social radars will accelerate decision-making and enable commanders to sustain a greater tempo of operations over protracted periods.

Finally, social radars exponentially multiply the power of Information Operations, making it increasingly feasible to purposefully and clandestinely alter a target population's attitude and behavior to meet a desired social outcome. This cognitive engineering on a mass scale unleashes a potentially corrupting power to incite violence or suppress opposition and dissent. Pandora's Box has been opened and the advent of social radars will call for a steady hand in command.

**Notes**

[1] John Boyd, quoted by Henry Eason, "New Theory Shoots Down Old War Ideas," Atlanta Constitution, March 22, 1981, in Lt Col Tamara Schwartz, "The Art of the Now: Decision Making and the Big Data Conundrum," White Paper (Cary, NC: SAS Federal, 2014), http://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/art-of-the-now-107418.pdf.
[2] General Sir Richard Barrons, "Warfare in the Information Age" (UK Joint Forces Command, December 3, 2014).
[3] Barry Costa and John Boiney, "Social Radar," Technical Paper, NATO (McLean, Va.: The MITRE Corporation, March 2012), http://www.mitre.org/publications/technical-papers/social-radar.
[4] Mar Maybury, quoted in Noah Schactman, "Air Force's Top Brain Wants a 'Social Radar' to 'See Into Hearts and Minds,'" *Wired.com*, January 19, 2012, http://www.wired.com/2012/01/social-radar-sees-minds/.
[5] Commander Joint Forces Intelligence Group, "Future and Emerging Capabilities within Defence Intelligence at Wyton" (Joint Forces Intelligence Group, June 2, 2015).
[6] Barrons, "Warfare in the Information Age."
[7] Colonel Robert Dixon, "Bringing Big Data to War in Mega-Cities," *War on the Rocks*, 19 January 16, http://warontherocks.com/2016/01/bringing-big-data-to-operations-in-mega-cities/; Robert Picarillo and Chelsey Gray, Multi-Agency Collaboration Environment (MACE), September 30, 2015.
[8] David Lyon, *Surveillance after Snowden* (Cambridge ; Malden, MA: Polity Press, 2015).

[9] Development, Concepts, and Doctrine Centre, "Joint Doctrine Publication 2.00: Understanding and Intelligence Support to Joint Operations, Third Edition" (UK MOD, August 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.
[10] Steele, Robert D. *Open Source Intelligence* in Loch K. Johnson, ed., *Strategic Intelligence*, vol. 2, Intelligence and the Quest for Security (Westport, Conn: Praeger Security International, 2007), 336, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiW7c_E0p3KAhWKaz4KHdxrCgwQFggiMAE&url=http%3A%2F%2Fwww.oss.net%2Fdynamaster%2Ffile_archive%2F060409%2F00b583e458c7fb78e96ddc3a8444ae30%2FSTEELE%2520Draft%2520Chapter%2520for%2520Strategic%2520Intelligence%2520on%2520OSINT%2C%25202.4.doc&usg=AFQjCNELlXzQTRQ6ZE2Bko8qwCOgFocUHg&sig2=eMo0xR1NIkOdiDQO4FnjGw&bvm=bv.111396085,d.cWw.
[11]Christoper Burnett, 2000, quoted in: Thomas E. Nissen, *#TheWeaponizationOfSocialMedia: @Characteristics_of_Contemporary_Conflicts* (Copenhagen: Royal Danish Defence College, 2015), 75.
[12] Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (London: Penguin, 2006), 17.
[13] "Why Did the World Miss the Arab Spring?," *Exemplifier*, September 24, 2013, http://exemplifier.org/?p=179.
[14] Development, Concepts and Doctrine Centre, "Future Operating Environment 2035," Strategic Trends Programme (Shrivenham: Ministry of Defence UK, November 30, 2014).
[15] Major Michael Macdonald, "JFC Conference: 'Warfare in the Information Age' Brief," in *Horizon Scanning and Awareness* (Warfare in the Information Age, 30 Commando Information Exploitation Group, 2015).
[16] Barrons, "Warfare in the Information Age."
[17] J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," *The Brookings Project on U.S. Relations with the Islamic World*, The Brookings Institute, no. 20 (March 2015), http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.
[18] Yasmin Tagjdeh, "Big Data Helping to Pinpoint Terrorist Activities, Attacks (UPDATED)," *National Defense Magazine*, April 2015, http://www.nationaldefensemagazine.org/archive/2015/April/Pages/BigDataHelpingtoPinpointTerroristActivitiesAttacks.aspx.
[19] Javier Lesaca, "Fight against ISIS Reveals Power of Social Media | Brookings Institution," *Brookings.edu*, November 19, 2015, http://www.brookings.edu/blogs/techtank/posts/2015/11/19-isis-social-media-power-lesaca; J.M. Berger, "How Terrorists Recruit Online (and How to Stop It)," *Brookings Institution*, November 9, 2015, http://www.brookings.edu/blogs/markaz/posts/2015/11/09-countering-violent-extremism-online-berger; Berger and Morgan, "The ISIS Twitter Census."
[20] ISIL, *ISIL Says The End of Sykes Picot - YouTube*, 2014, https://www.youtube.com/watch?v=AzDJgv6sNYI; Nicole Matcjic, "How ISIL Have Weaponized Social Media in Iraq – Info Ops HQ," *InfoOpsHQ.com*, July 6, 2014, http://www.infoopshq.com/2014/07/06/case-study-isil-weaponized-social-media-iraq/.
[21] "Why It's so Difficult to Counter ISIS on Social Media," *CBS News*, accessed September 29, 2015, http://www.cbsnews.com/news/why-so-difficult-counter-isis-social-media/.
[22] Lesaca, "Fight against ISIS Reveals Power of Social Media | Brookings Institution."
[23] Danny Yadron, "Revealed: White House Seeks to Enlist Silicon Valley to 'Disrupt Radicalization' | Technology | The Guardian," *Theguardian.com*, January 7, 2016, sec. Technology, http://www.theguardian.com/technology/2016/jan/07/white-house-social-media-terrorism-meeting-facebook-apple-youtube-.
[24] Development, Concepts and Doctrine Centre, "FOE35"; Development, Concepts and Doctrine Centre, "Global Strategic Trends - Out to 2045," Strategic Trends Programme (Shrivenham: Ministry of Defence UK, August 29, 2014); Dixon, "Bringing Big Data to War in Mega-Cities."
[25] "Why Did the World Miss the Arab Spring?"
[26] Schactman, "Air Force's Top Brain Wants a 'Social Radar' to 'See Into Hearts and Minds.'"
[27] Winston S. Churchill, *Speech to the House of Commons*, 2 May 1935. *Parliamentary Debates*, Commons, vol. 301 (1935), col. 602. http://hansard.millbanksystems.com/commons/1935/may/02/foreign-office.
[28] Mark Maybury, "Social Radar for Smart Power," Technical Paper (Bedford, Ma.: The MITRE Corporation, April 2010), http://www.mitre.org/publications/technical-papers/social-radar-for-smart-power.
[29] Costa and Boiney, "Social Radar."
[30] Maybury, "Social Radar for Smart Power"; Costa and Boiney, "Social Radar."
[31] Sitaram Asur and Bernado A. Huberman, "Predicting the Future with Social Media," *Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2010 IEEE/WIC/ACM International Conference on, 1 (2010): 492–99, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5616710&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5616710.
[32] *Open Data White Paper: Unleashing the Potential.* (London: Stationery Office, 2012); "Internet Penetration in the Middle East," Presentation, *Wearesocialsg*, (July 2014), http://was-sg.wascdn.net/wp-content/uploads/2014/07/Slide007.png; Abigail Edge, "Digital Habits in the UK: Social Media, Mobile Apps, and Online

News," *Themediabriefing.com*, August 12, 2015, http://www.themediabriefing.com/article/digital-habits-in-the-uk-social-media-mobile-apps-and-online-news.
[33] Noyan Ayan, "Double-Digit Growth of Mobile in MENA Continues," *Webrazzi*, September 30, 2014, http://en.webrazzi.com/2014/09/30/double-digit-growth-of-mobile-in-mena-continues/.
[34] Ayan, "Double-Digit Growth of Mobile in MENA Continues"; eMarketer, "Digital Marketing Article Search Results," *eMarketer.com*, September 16, 2015, http://www.emarketer.com/articles/results.aspx?q=Middle%20East.
[35] Newley Purnell, "Facebook's Free Internet Access Program in Developing Countries Provokes Backlash," *Wall Street Journal*, September 24, 2015, Online edition, sec. Tech, http://www.wsj.com/articles/facebooks-free-Internet-access-program-in-developing-countries-provokes-backlash-1443119580.
[36] Internetworldstats.com, "Middle East Internet Statistics, Population, Facebook and Telecommunications Reports," January 2016, http://www.Internetworldstats.com/stats5.htm.
[37] Alex Hern, "Facebook Launches Aquila Solar-Powered Drone for Internet Access," *The Guardian*, July 30, 2015, London edition, sec. Technology, http://www.theguardian.com/technology/2015/jul/31/facebook-finishes-aquila-solar-powered-Internet-drone-with-span-of-a-boeing-737.
[38] We are social Singapore, "Digital, Social & Mobile in 2015," January 20, 2015, http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015/214.
[39] "Spotter: Media and Social Media Analytics," *Spotter.com*, accessed January 23, 2016, http://www.spotter.com/.
[40] Adam Karcher, "The Federal Bureau of Investigation - Big Data Perspectives and Challenges" (Powerpoint Presentation, Big Data for Defense and Intelligence, Arlington, VA, October 9, 2015), http://www.globaleventslist.elsevier.com/events/2015/10/big-data-for-defense-and-intelligence-symposium/.
[41] Interview with Ted Ziemer, operations manager at Pulic Relay, a marketing analysis company based in Virginia, September 9, 2015.
[42] Dimitry Volchek and Claire Bigg, "Ukrainian Bloggers Use Social Media to Track Russian Soldiers Fighting in East," *The Guardian*, June 3, 2015, Online edition, sec. World News, http://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine.
[43] Berger and Morgan, "The ISIS Twitter Census."
[44] Jun Han et al., "ACComplice: Location Inference Using Accelerometers on Smartphones" (IEEE, 2012), 1–9, doi:10.1109/COMSNETS.2012.6151305.
[45] Richard Colbaugh and Kristin Glass, "Early Warning Analysis for Social Diffusion Events," *Security Informatics* 1, no. 1 (2012): 18, doi:10.1186/2190-8532-1-18.
[46] LinkedIn.com, "People You May Know Feature - Overview," *LinkedIn.com*, November 13, 2015, https://help.linkedin.com/app/answers/detail/a_id/29/~/people-you-may-know-feature---overview.
[47] Randy A. Weaver, "The Application of 'Spiral Analysis' to ABI: Lessons Learned in the Interagency Environment - An Examination of Lessons Learned in the Interagency Law Enforcement Environment and the Potential Application of Those Lessons to Activity-Based Intelligence.," Corporate research paper (Arlington, VA: Concurrent Technologies Corporation, August 2014), https://info.publicintelligence.net/CTC-SpiralAnalysis.pdf.
[48] Jose Cadena et al., "Forecasting Social Unrest Using Activity Cascades," ed. Tobias Preis, *PLOS ONE* 10, no. 6 (June 19, 2015): e0128879, doi:10.1371/journal.pone.0128879.
[49] Maybury, "Social Radar for Smart Power"; Costa and Boiney, "Social Radar."
[50] Costa and Boiney, "Social Radar."
[51] *Open Data White Paper*.
[52] Jennifer Mathieu et al., "Social Radar Workflows, Dashboards, and Environments," Technical Paper, NATO (McLean, Va.: The MITRE Corporation, March 2012), http://www.mitre.org/publications/technical-papers/social-radar-workflows-dashboards-and-environments.
[53] Berger, "How Terrorists Recruit Online (and How to Stop It)"; Multi-Agency Collaboration Environment, "Open-Source Analytic Assessment - HQ JFIG JIOC RFI - ISIL Use of Social Media" (Multi-Agency Collaboration Environment, August 11, 2015).
[54] Lesaca, "Fight against ISIS Reveals Power of Social Media | Brookings Institution."
[55] Richard Laurent, "We Built a Model That Could Have Predicted the Paris Attacks. Here's How. — Medium," Company Website, *Predata.com*, (November 20, 2015), https://medium.com/@predata/we-built-a-model-that-predicted-the-paris-attacks-here-s-how-8141934b4abe#.lhxek3hre.
[56] Wassim Zoghlami, "How Data Mining Could've Prevented An ISIS Attack," *Iafrikan.com*, June 22, 2015, http://www.iafrikan.com/2015/06/22/data-mining-isis-tunisia-tunis-bardo-terror-museum-atack/.
[57] Kevan Lee, "10 Surprising and Important Social Media Stats You Need To Know," *Buffer App*, June 23, 2014, https://blog.bufferapp.com/social-media-stats-you-need-to-know.
[58] Cadena et al., "Forecasting Social Unrest Using Activity Cascades."
[59] A.R. Guess, "The Trick to Big Data Analytics Isn't Finding the Needle, It's Defining the Haystack," *Dataversity.com*, accessed January 19, 2016, http://www.dataversity.net/trick-big-data-analytics-isnt-finding-needle-defining-haystack/.
[60] Schwartz, "The Art of Now."
[61] Schwartz, "The Art of Now."
[62] Mark Phillips, "A Brief Overview of ABI and Human Domain Analytics," *Trajectory Magazine*, September 28, 2012, http://trajectorymagazine.com/civil/item/1369-human-domain-analytics.html; Chandler P. Atwood, "Activity-Based

Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Forces Quarterly*, National Defense University Press, 77, no. 2 (April 1, 2015): 24–33, http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/581866/jfq-77-activity-based-intelligence-revolutionizing-military-intelligence-analys.aspx.
[63] Atwood, "Activity-Based Intelligence."
[64] Kenny O'Neal, "U.S. Air Force National Intelligence Coordination Cell" (Powerpoint Presentation, Big Data for Defense and Intelligence, Arlington, VA, October 8, 2015), http://www.globaleventslist.elsevier.com/events/2015/10/big-data-for-defense-and-intelligence-symposium/.
[65] Dixon, "Bringing Big Data to War in Mega-Cities."
[66] Cornelia Caragea et al., "Mapping Moods: Geo-Mapped Sentiment Analysis during Hurricane Sandy," in *ISCRAM*, 2014, https://scholar.google.com/scholar?q=mapping+moods+hurricane+sandy+sentiment+analysis+during+disaster+relief+operations&btnG=&hl=en&as_sdt=0%2C47&as_vis=1.
[67] Dr Jim Goodnight, "Disaster Relief Efforts Show Promise of Analytics and Seemingly Unrelated Data Sources," Company Website, *Sas.com*, (July 8, 2015), http://blogs.sas.com/content/corneroffice/2015/07/08/disaster-relief-efforts-show-promise-of-analytics-and-seemingly-unrelated-data-sources/.
[68] Atwood, "Activity-Based Intelligence."
[69] Gao Huiji, Geoffrey Barbier, and Rebecca Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief," *Intelligent Systems*, IEEE Intelligent Systems, 26, no. 3 (June 16, 2011): 10–14, http://doi.ieeecomputersociety.org/10.1109/MIS.2011.52.
[70] Nissen, *The Weaponization of Social Media*.
[71] Dr. Michael S. Toney, CEO, Social Analysis and Intelligence Group, LLC, September 1, 2015.
[72] Toney, CEO, Social Analysis and Intelligence Group, LLC.
[73] Nissen, *The Weaponization of Social Media*.
[74] Colonel Bobby Saxon, Chief of the U.S. Army Force Management Enterprise Division, quoted in Custom Strategies, "Putting Predictive Analytics to Work for the Army—An Executive Perspective," *Governmentexecutive.com*, April 30, 2015, http://www.govexec.com/govexec-sponsored/2015/04/putting-predictive-analytics-work-army-executive-perspective/111406/.
[75] Leah McGrath Goodman, "The EMBERS Project Can Predict the Future With Twitter," *Newsweek.com*, July 3, 2015, Online edition, sec. Tech and Science, http://www.newsweek.com/2015/03/20/embers-project-can-predict-future-twitter-312063.html.
[76] IBM, "IBM i2 Enterprise Insight Analysis," accessed January 7, 2016, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&appname=SWGE_ZZ_ZZ_USEN&htmlfid=ZZS03203USEN&attachment=ZZS03203USEN.PDF; Toney, CEO, Social Analysis and Intelligence Group, LLC.
[77] Maybury, "Social Radar for Smart Power."
[78] "AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging | Business | The Guardian," accessed January 16, 2016, http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.
[79] Margaret Rouse, "What Is Unstructured Data?," *TechTarget*, April 2010, http://searchbusinessanalytics.techtarget.com/definition/unstructured-data.
[80] O'Neal, "U.S. Air Force National Intelligence Coordination Cell."
[81] Mark Krzysko, "Big Data for Defense and Intelligence" (Powerpoint Presentation, Big Data for Defense and Intelligence, Arlington, VA, October 8, 2015), http://www.globaleventslist.elsevier.com/events/2015/10/big-data-for-defense-and-intelligence-symposium/.
[82] Mayer-Schonberger and Cukier, *Big Data - A Revolution That Will Transform How We Live, Work, and Think*.
[83] Colleen McCue, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*, 2 Edition (Waltham: Elsevier, 2015).
[84] Rafal Rohozinski and Robert Muggah, "Brace for the Quantified Society," opencanada.org, (January 9, 2015), https://www.opencanada.org/features/brace-for-the-quantified-society/; Lyon, *Surveillance after Snowden*, 88.
[85] "CIA Director John Brennan on 60 Minutes - CBS News," Talk Show Interview, *CIA Director John Brennan on 60 Minutes* (CBS, February 14, 2016), http://www.cbsnews.com/news/cia-director-john-brennan-60-minutes-scott-pelley/.
[86] The Week, "Was Facebook's 'Creepy' Study Funded by the US Military?| Facebook News | The Week UK," *The Week UK*, July 3, 2014, http://www.theweek.co.uk/facebook/59210/was-facebooks-creepy-study-funded-by-the-us-military; Reuters, "Facebook Mind Control Experiments Linked to DoD Research on Civil Unrest — RT USA," *RT Question More*, July 2, 2014, https://www.rt.com/usa/169848-pentagon-facebook-study-minerva/.
[87] Goodman, "The EMBERS Project Can Predict the Future With Twitter."
[88] Goodman, "The EMBERS Project Can Predict the Future With Twitter."
[89] Maria Grazia Porcedda, "Surveille Deliverable 2.4: Paper Establishing Classification of Technologies on the Basis of Their Intrusiveness into Fundamental Rights" (Collaboration Project, April 30, 2013), https://cyberwar.nl/d/fromEUFP7/SURVEILLE/D2.4%20Paper%20establishing%20the%20classification%20of%20technologies%20on%20the%20basis%20of%20their%20intrusiveness%20into%20fundamental%20rights.pdf.
[90] HM Government, *Regulation of Investigatory Powers Act 2000: Chapter 23.*, *Chapter 23*, 2000, http://www.fipr.org/rip/ripa2000.htm.

[91] Stationery Office (Great Britain), "Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014" (London: House of Commons, September 4, 2014), https://osc.independent.gov.uk/wp-content/uploads/2014/09/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf; Ibrahim Hasan, "Facebook, Social Networks and the Need for RIPA Authorisations," *Actnowtraining.wordpress.com*, September 10, 2015, https://actnowtraining.wordpress.com/2015/09/10/facebook-social-networks-and-the-need-for-ripa-authorisations/.
[92] Marly Didizian and Richard Cumbley, "Social Media and the Law: A Handbook for UK Companies" (Linklaters LLP, January 16, 2014), http://www.linklaters.com/Insights/Social-media-law-A-handbook-UK-companies/Pages/Index.aspx.
[93] HM Government, *Data Protection Act (1998)*, *Chapter 29*, 1998, http://www.legislation.gov.uk/ukpga/1998/29.
[94] Picarillo and Gray, Multi-Agency Collaboration Environment (MACE).
[95] Robert D. Steele, "Open Source Intelligence," in *Strategic Intelligence*, vol. 2, n.d.
[96] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data - A Revolution That Will Transform How We Live, Work, and Think* (New York: Houghton Mifflin Harcourt Publishing Company, 2013), 142.
[97] Picarillo and Gray, Multi-Agency Collaboration Environment (MACE).
[98] Multi-Agency Collaboration Environment, "Open-Source Analytic Assessment - HQ JFIG JIOC RFI - ISIL Use of Social Media."
[99] Mark Braggins, "Good Stuff, Continued," *Good Stuff, Continued*, October 14, 2015, https://data.gov.uk/blog/good-stuff-continued; Ministry of Defence, Defence Science and Technology Laboratory, "MOD Hackathon to Mine the Deep Web," News Story, (September 14, 2015), https://www.gov.uk/government/news/mod-hackathon-to-mine-the-deep-web.
[100] James Taylor, "Avoiding Generic Dashboards with Decision Modeling — JT on EDM," Blog, *James Taylor on Everything Decision Management*, (January 14, 2016), http://jtonedm.com/2016/01/14/avoiding-generic-dashboards-with-decision-modeling/.
[101] Bill Schmarzo, *Big Data: Understanding How Data Powers Big Business* (Indianapolis, IN: John Wiley & Sons, 2013), 48.
[102] Picarillo and Gray, Multi-Agency Collaboration Environment (MACE); Brigader General Robert Walters, "Remarks by Brigadier General Robert Walters, Deputy Director for Operations and Intelligence" (Speech, Pakistan Counter-IED Symposium, May 20, 2013), https://www.jieddo.mil/content/docs/20130520_BG_Walters_remarks_at_Pakistan_Counter-IED_Symposium_AS_PREPARED.pdf.
[103] Commander Joint Forces Intelligence Group, "Future and Emerging Capabilities within Defence Intelligence at Wyton."
[104] Picarillo and Gray, Multi-Agency Collaboration Environment (MACE).

**Appendix A**

**Example Military Applications of Social Radar Technology**

| Example Military Applications of Social Radar Technology | | |
|---|---|---|
| **Type of Operation** | **Social Radar Application** | **Utility** |
| **Security Cooperation** | Predict Global Instability | Pre-emptive deployment of Training Teams and Defense Engagement. |
| | Geographically understand population's perceptions of indigenous security forces | Recognize and adapt training shortfalls.<br>Support Information Operations.<br>Provide Measures of Effectiveness. |
| | Identify nefarious elements | Counter the Insider Threat. |
| **Stability Operations** | IPB | Map Human Terrain Data. |
| | Support Battle Damage Assessment (BDA) | Track impact of operations. |
| | Predict and track movement of Internally Displaced Persons (IDP) and identify their requirements | Pre-emptively deploy support services or liaise with NGOs. |
| | Understand impact of long deployments on military recruitment and retention | Support to manning strategies. |
| | | Cue support ISR |
| | Track geographic and temporal propagation of Information Operations | Support and improve IO. |
| **COIN** | Human Terrain Modeling | Map Human Terrain Data<br>- Reconcilable/Irreconcilable groups<br>- Plot interest groups<br>- Understand local issues and tensions. |
| | Targeting Operations | Identify key agitators.<br>Understand terror networks. |
| | Predict attacks or civil unrest | Support Force Protection. |
| **Humanitarian Assistance and Disaster Relief** | Human Terrain Modeling | Disseminate and track emergency alert messages.<br>Predict IDP movements.<br>Predict and map disease outbreaks. |
| | Targeting Operations | Identify vulnerable people. |
| | Information Operations | Advertise distribution points. |
| | Force Protection | Predict violence and civil unrest. |

**Appendix B**

**Global Digital, Mobile, and Social Media Penetration**

| Global Digital, Mobile, and Social Media Penetration (March 2015)[cv] | | | | | |
|---|---|---|---|---|---|
| Figures in millions unless indicated | **Population** | **Active Internet Users** | **Active Social Media Users** | **Mobile Connections** | **Active Mobile Social Users** |
| **Global** | 7.219 billion | 3.038 billion | 2.126 billion | 3.679 billion | 1.753 billion |
| | Urbanization: 53% | Penetration: 42% | Penetration: 29% | Vs Population: 51% | Penetration: 24% |
| **Asia-Pacific** | 4,026 | 1,436 | 1,088 | 3,722 | 906 |
| | Urbanization: 45% | Penetration: 36% | Penetration: 27% | Vs Population: 92% | Penetration: 22% |
| **South East Asia** | 623 | 225 | 209 | 744 | 182 |
| | Urbanization: 45% | Penetration: 36% | Penetration: 34% | Vs Population: 119% | Penetration: 29% |
| **South Asia** | 1,691 | 329 | 166 | 1,296 | 144 |
| | Urbanization: 31% | Penetration: 19% | Penetration: 10% | Vs Population: 77% | Penetration: 9% |
| **Middle East** | 239 | 87 | 43 | 294 | 38 |
| | Urbanization: 67% | Penetration: 36% | Penetration: 18% | Vs Population: 123% | Penetration: 16% |
| **Africa** | 1,136 | 298 | 109 | 900 | 93 |
| | Urbanization: 40% | Penetration: 26% | Penetration: 10% | Vs Population: 79% | Penetration: 8% |

Source: **We are social Singapore, "Digital, Social & Mobile in 2015," January 20, 2015, http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015/214.**

## Bibliography


"Army Research Laboratory Technical Implementation Plan 2015 – 2019." Army Research Laboratory, January 2015. http://www.arl.army.mil/www/pages/172/docs/ARL_Technical_Implementation_Plan.pdf.

"AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging | Business | The Guardian." Accessed January 16, 2016. http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

Asur, Sitaram, and Bernado A. Huberman. "Predicting the Future with Social Media." *Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2010 IEEE/WIC/ACM International Conference on, 1 (2010): 492–99. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5616710&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5616710.

Atwood, Chandler P. "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis." *Joint Forces Quarterly*, National Defense University Press, 77, no. 2 (April 1, 2015): 24–33. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/581866/jfq-77-activity-based-intelligence-revolutionizing-military-intelligence-analys.aspx.

Ayan, Noyan. "Double-Digit Growth of Mobile in MENA Continues." *Webrazzi*, September 30, 2014. http://en.webrazzi.com/2014/09/30/double-digit-growth-of-mobile-in-mena-continues/.

Baesens, Bart. *Analytics in a Big Data World: The Essential Guide to Data Science and Its Applications*. Hoboken: John Wiley & Sons, Inc, 2014.

Barrons, General Sir Richard. "Warfare in the Information Age." UK Joint Forces Command, December 3, 2014.

Bensoussan, Babette, and Craig Fleisher. *Analysis without Paralysis - 10 Tools to Make Better Strategic Decisions*. New Jersey: Pearson Education, 2008.

Berger, J.M. "How Terrorists Recruit Online (and How to Stop It)." *Brookings Institution*, November 9, 2015. http://www.brookings.edu/blogs/markaz/posts/2015/11/09-countering-violent-extremism-online-berger.

Berger, J.M., and Jonathon Morgan. "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter." *The Brookings Project on U.S. Relations with the Islamic World*, The Brookings Institute, no. 20 (March 2015). http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

Boiney, John. "Sentiment Analysis and Social Media in HSCB." *HSCB Modeling Program*, http://www.ms.army.mil/news/HSCB%20Summer%202012%20Newsletter.pdf, no. 13 (Summer 2012).

Bostok, Mike. "66 'Important Jihadist' Accounts on Twitter." *Wandrenpd.com*, February 2013. http://wandrenpd.com/Graphs/66jihadi/Graph.html.

Bouchard, Martin, ed. *Social Networks, Terrorism and Counter-Terrorism: Radical and Connected*. Contemporary Terrorism Studies. London ; New York: Routledge, Taylor & Francis Group, 2015.

Braggins, Mark. "Good Stuff, Continued." *Good Stuff, Continued*, October 14, 2015. https://data.gov.uk/blog/good-stuff-continued.

Bright, Jonathan, Great Britain, and Department for Work and Pensions. *The Use of Social Media for Research and Analysis: A Feasibility Study*. Leeds: Corporate Document Services, 2014.

Buxbaum, Peter. "Predictive Analytics for Intel Advantage." *KMImediagroup.com*, February 6, 2014. http://www.kmimediagroup.com/military-logistics-forum/424-articles-gif/predictive-analytics-for-intel-advantage.

Cadena, Jose, Gizem Korkmaz, Chris J. Kuhlman, Achla Marathe, Naren Ramakrishnan, and Anil Vullikanti. "Forecasting Social Unrest Using Activity Cascades." Edited by Tobias Preis. *PLOS ONE* 10, no. 6 (June 19, 2015): e0128879. doi:10.1371/journal.pone.0128879.

Caragea, Cornelia, Anna Squicciarini, Sam Stehle, Kishore Neppalli, and Andrea Tapia. "Mapping Moods: Geo-Mapped Sentiment Analysis during Hurricane Sandy." In *ISCRAM*, 2014. https://scholar.google.com/scholar?q=mapping+moods+hurricane+sandy+sentiment+analysis+during+disaster+relief+operations&btnG=&hl=en&as_sdt=0%2C47&as_vis=1.

Centre for Defence Enterprise. “Competition Summary: Open-Source Big Data Insight.” *Www.gov.uk*, July 10, 2015. https://www.gov.uk/government/publications/cde-themed-competition-open-source-big-data-insight/competition-summary-open-source-big-data-insight.

Churchill, Winston S. *Speech to the House of Commons*. Commons, Vol. 301 (1935), Col. 602, 1935. http://hansard.millbanksystems.com/commons/1935/may/02/foreign-office.

“CIA Director John Brennan on 60 Minutes - CBS News.” Talk Show Interview. *CIA Director John Brennan on 60 Minutes*. CBS, February 14, 2016. http://www.cbsnews.com/news/cia-director-john-brennan-60-minutes-scott-pelley/.

Colbaugh, Richard, and Kristin Glass. “Early Warning Analysis for Social Diffusion Events.” *Security Informatics* 1, no. 1 (2012): 18. doi:10.1186/2190-8532-1-18.

Commander Joint Forces Intelligence Group. “Future and Emerging Capabilities within Defence Intelligence at Wyton.” Joint Forces Intelligence Group, June 2, 2015.

Cook, Malcolm, Janet M Noyes, and Yvonne Masakowski. *Decision Making in Complex Environments*. Aldershot, England; Burlington, VT: Ashgate, 2007. http://public.eblib.com/choice/publicfullrecord.aspx?p=429567.

Copeland, B. Jack, ed. *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life, plus the Secrets of Enigma*. Oxford : New York: Clarendon Press ; Oxford University Press, 2004.

Costa, Barry, and John Boiney. “Social Radar.” Technical Paper. NATO. McLean, Va.: The MITRE Corporation, March 2012. http://www.mitre.org/publications/technical-papers/social-radar.

Cross-Government Technology Security Working Group. “20150813_BDSUS_JA/JM_01 Aligning the UK and U.S. on the Use of Open Source Information in Intelligence and Strategic Decision Making.” British Defence Section United States, August 20, 2015.

Custom Strategies. “Putting Predictive Analytics to Work for the Army—An Executive Perspective.” *Governmentexecutive.com*, April 30, 2015. http://www.govexec.com/govexec-sponsored/2015/04/putting-predictive-analytics-work-army-executive-perspective/111406/.

Davenport, Thomas H. *Big Data at Work: Dispelling the Myths, Uncovering the Opportunities*. Boston: Harvard Business School Publishing Corporation, 2014. http://www.amazon.com/Big-Data-Work-Dispelling-Opportunities/dp/1422168166/ref=sr_1_1?ie=UTF8&qid=1443562687&sr=8-1&keywords=big+data+%40+work.

Davis, Kerry. “US Military Looks to Social Nets for Intelligence Strategy.” *PCworld.com*, July 26, 2013. http://www.pcworld.com/article/2013726/us-military-looks-to-social-nets-for-intelligence-strategy.html#comments.

Development, Concepts and Doctrine Centre. “Future Operating Environment 2035.” Strategic Trends Programme. Shrivenham: Ministry of Defence UK, November 30, 2014.

———. “Global Strategic Trends - Out to 2045.” Strategic Trends Programme. Shrivenham: Ministry of Defence UK, August 29, 2014.

Development, Concepts, and Doctrine Centre. “Joint Doctrine Publication 2.00: Understanding and Intelligence Support to Joint Operations, Third Edition.” UK MOD, August 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

Didizian, Marly, and Richard Cumbley. “Social Media and the Law: A Handbook for UK Companies.” Linklaters LLP, January 16, 2014. http://www.linklaters.com/Insights/Social-media-law-A-handbook-UK-companies/Pages/Index.aspx.

Director, National Intelligence. *Intelligence Community Directive: National Open Source Enterprise*. *Intelligence Community Directive Number 301*. Vol. 301, 2006. https://fas.org/irp/dni/icd/icd-301.pdf.

Dixon, Colonel Robert. “Bringing Big Data to War in Mega-Cities.” *War on the Rocks*, 19 January 16. http://warontherocks.com/2016/01/bringing-big-data-to-operations-in-mega-cities/.

Edge, Abigail. "Digital Habits in the UK: Social Media, Mobile Apps, and Online News." *Themediabriefing.com*, August 12, 2015. http://www.themediabriefing.com/article/digital-habits-in-the-uk-social-media-mobile-apps-and-online-news.

Edwards, John. "Military, Intel Turn to Big Data for Better Situational Awareness | Federal Times | Federaltimes.com," June 2, 2014. http://archive.federaltimes.com/article/20140602/FEDIT/306020009/Military-intel-turn-big-data-better-situational-awareness.

eMarketer. "Digital Marketing Article Search Results." *eMarketer.com*, September 16, 2015. http://www.emarketer.com/articles/results.aspx?q=Middle%20East.

Eustice, Owen. "Big Data; Big Words; And the Soldier's Search for the Easy Button." Government Blog. *ISSInc.com*, March 15, 2014. https://www.issinc.com/big-data-big-words-and-the-soldiers-search-for-the-easy-button/.

"Facebook Launches Aquila Solar-Powered Drone for Internet Access | Technology | The Guardian." Accessed January 24, 2016. http://www.theguardian.com/technology/2015/jul/31/facebook-finishes-aquila-solar-powered-Internet-drone-with-span-of-a-boeing-737.

"Facebook Mind Control Experiments Linked to DoD Research on Civil Unrest." *RT Question More*, July 2, 2014. https://www.rt.com/usa/169848-pentagon-facebook-study-minerva/.

"Facebook Mind Control Experiments Linked to DoD Research on Civil Unrest — RT USA." Accessed January 17, 2016. https://www.rt.com/usa/169848-pentagon-facebook-study-minerva/.

"Facebook Mind Control Experiments Linked to DoD Research on Civil Unrest — RT USA." Accessed January 7, 2016. https://www.rt.com/usa/169848-pentagon-facebook-study-minerva/.

"Facebook's Free Internet Access Program in Developing Countries Provokes Backlash - WSJ." Accessed March 18, 2016. http://www.wsj.com/articles/facebooks-free-Internet-access-program-in-developing-countries-provokes-backlash-1443119580.

"Facebook, Social Networks and the Need for RIPA Authorisations | Blog Now." Accessed February 19, 2016. https://actnowtraining.wordpress.com/2015/09/10/facebook-social-networks-and-the-need-for-ripa-authorisations/.

Fahey, Sean. "Big Data and Analytics for National Security." Powerpoint Presentation, Johns Hopkins University Laboratory of Applied Physics, 2012. http://web.stanford.edu/group/mmds/slides2012/s-fahey.pdf.

Fast, Major General Barbara G. "Open Source Intelligence." *Military Intelligence* 31, no. 4 (December 2005): 2 and 4. http://fas.org/irp/agency/army/mipb/2005_04.pdf.

Frank, Christoper J., and Magnone, Paul F. *Drinking from the Fire Hose: Making Smarter Decisions without Drowning in Information*. New York: Penguin Group (USA), 2011.

Friedman, George, Meredith Friedman, Colin Chapman, and John S. Baker Jr. *The Intelligence Edge - How to Profit in the Information Age*. New York: Crown Publishers, Inc, 1997.

Girard, Ted. "Big Data and Virtualization: A Formidable Defense -- Defense Systems." Defense Sector Website. *Defensesystems.com*, March 5, 2015. https://defensesystems.com/Articles/2015/03/05/Comment-Defense-big-data-and-virualization.aspx?m=2&Page=1.

Goodman, Leah McGrath. "The EMBERS Project Can Predict the Future With Twitter." *Newsweek.com*, July 3, 2015, Online edition, sec. Tech and Science. http://www.newsweek.com/2015/03/20/embers-project-can-predict-future-twitter-312063.html.

Goodnight, Dr Jim. "Disaster Relief Efforts Show Promise of Analytics and Seemingly Unrelated Data Sources." Company Website. *Sas.com*, July 8, 2015. http://blogs.sas.com/content/corneroffice/2015/07/08/disaster-relief-efforts-show-promise-of-analytics-and-seemingly-unrelated-data-sources/.

Guess, A.R. "The Trick to Big Data Analytics Isn't Finding the Needle, It's Defining the Haystack." *Dataversity.com*. Accessed January 19, 2016. http://www.dataversity.net/trick-big-data-analytics-isnt-finding-needle-defining-haystack/.

Han, Jiawei, and Micheline Kamber. *Data Mining: Concepts and Techniques*. San Fransisco: Elsevier Inc, 2006.

Hardy, Michael. "Big Data Plays Key Role in Army Technical Plan." *C4ISRnet.com*, February 26, 2015. http://www.c4isrnet.com/story/military-tech/it/2015/02/26/army-technical-implementation-plan/24060299/.

Hasan, Ibrahim. "Facebook, Social Networks and the Need for RIPA Authorisations." *Actnowtraining.wordpress.com*, September 10, 2015. https://actnowtraining.wordpress.com/2015/09/10/facebook-social-networks-and-the-need-for-ripa-authorisations/.

Headquarters, Department of the Army. "FM 3.24/MCWP 3-33.5, C1 - Insurgencies and Countering Insurgencies," May 13, 2014. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_24.pdf.

Hern, Alex. "Facebook Launches Aquila Solar-Powered Drone for Internet Access." *The Guardian*, July 30, 2015, London edition, sec. Technology. http://www.theguardian.com/technology/2015/jul/31/facebook-finishes-aquila-solar-powered-Internet-drone-with-span-of-a-boeing-737.

HM Government. *Data Protection Act (1998). Chapter 29*, 1998. http://www.legislation.gov.uk/ukpga/1998/29.

———. *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom.* London, 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

———. *Regulation of Investigatory Powers Act 2000: Chapter 23. Chapter 23*, 2000. http://www.fipr.org/rip/ripa2000.htm.

House of Commons Defence Committee. "Re-Thinking Defence to Meet New Threats." London: House of Commons Defence Committee, n.d.

Huiji, Gao, Geoffrey Barbier, and Rebecca Goolsby. "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief." *Intelligent Systems*, IEEE Intelligent Systems, 26, no. 3 (June 16, 2011): 10–14. http://doi.ieeecomputersociety.org/10.1109/MIS.2011.52.

IBM. "IBM i2 Enterprise Insight Analysis." Accessed January 7, 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&appname=SWGE_ZZ_ZZ_USEN&htmlfid=ZZS03203USEN&attachment=ZZS03203USEN.PDF.

"Internet Penetration in the Middle East." Presentation. *Wearesocialsg*, July 2014. http://was-sg.wascdn.net/wp-content/uploads/2014/07/Slide007.png.

Internetworldstats.com. "Middle East Internet Statistics, Population, Facebook and Telecommunications Reports," January 2016. http://www.Internetworldstats.com/stats5.htm.

Interview with Ted Ziemer, operations manager at Pulic Relay, a marketing analysis company based in Virginia, September 9, 2015.

ISIL. *ISIL Says The End of Sykes Picot - YouTube*, 2014. https://www.youtube.com/watch?v=AzDJgv6sNYI.

Johnson, Kimberly. "Getting a Handle on Big Data." Defense Sectory Website. *Defensesystems.com*, September 23, 2013. https://defensesystems.com/Articles/2013/09/23/big-data.aspx?m=2&Page=1&p=1.

Johnson, Loch K., ed. *Strategic Intelligence*. Vol. 2. Intelligence and the Quest for Security. Westport, Conn: Praeger Security International, 2007. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiW7c_E0p3KAhWKaz4KHdxrCgwQFggiMAE&url=http%3A%2F%2Fwww.oss.net%2Fdynamaster%2Ffile_archive%2F060409%2F00b583e458c7fb78e96ddc3a8444ae30%2FSTEELE%2520Draft%2520Chapter%2520for%2520Strategic%2520Intelligence%2520on%2520OSINT%2C%25202.4.doc&usg=AFQjCNELlXzQTRQ6ZE2Bko8qwCOgFocUHg&sig2=eMo0xR1NIkOdiDQO4FnjGw&bvm=bv.111396085,d.cWw.

Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, and Joy Zhang. "ACComplice: Location Inference Using Accelerometers on Smartphones," 1–9. IEEE, 2012. doi:10.1109/COMSNETS.2012.6151305.

Karcher, Adam. “The Federal Bureau of Investigation - Big Data Perspectives and Challenges.” Powerpoint Presentation presented at the Big Data for Defense and Intelligence, Arlington, VA, October 9, 2015. http://www.globaleventslist.elsevier.com/events/2015/10/big-data-for-defense-and-intelligence-symposium/.

Kase, Sue E., Elizabeth K. Bowman, Md. Tanvir Al Amin, and Tarek Abdelzaher. “Exploiting Social Media for Army Operations: Syrian Crisis Use Case.” edited by Barbara D. Broome, David L. Hall, and James Llinas, 91220D, 2014. doi:10.1117/12.2049701.

Kirk, Major Christopher J. “The Demise of Decision Making How Information Superiority Degrades Our Ability to Make Decisions.” */Luce.nt/ A Journal of National Security Studies*, U.S Naval War College, 2014, no. Special Edition (2014): 84–93. https://www.usnwc.edu/Publications/-Luce-nt-/Archives/2014/Special-Edition/Kirk_The-Demise-of-Decision-Making-Colbert_Kirk-C-.aspx.

Krzysko, Mark. “Big Data for Defense and Intelligence.” Powerpoint Presentation presented at the Big Data for Defense and Intelligence, Arlington, VA, October 8, 2015. http://www.globaleventslist.elsevier.com/events/2015/10/big-data-for-defense-and-intelligence-symposium/.

Land Warfare Development Group. “ARMY Field Manual Countering Insurgency Volume 1 - Part 10,” January 2010. https://www.defencegateway.mod.uk/linkedfiles/reference_portal/doctrine/army_field_manuals/land/20130204_afmv1p10counteringinsurgencyamdt1_p_u.pdf (requires log in).

Laurent, Richard. “We Built a Model That Could Have Predicted the Paris Attacks. Here’s How. — Medium.” Company Website. *Predata.com*, November 20, 2015. https://medium.com/@predata/we-built-a-model-that-predicted-the-paris-attacks-here-s-how-8141934b4abe#.lhxek3hre.

Lee, Kevan. “10 Surprising and Important Social Media Stats You Need To Know.” *Buffer App*, June 23, 2014. https://blog.bufferapp.com/social-media-stats-you-need-to-know.

Leese, Commander Bryan. “Mining Social Media for Intel.” *U.S. Naval Institute Proceedings* 141, no. 8 (August 2015): 82–84.

Lesaca, Javier. “Fight against ISIS Reveals Power of Social Media | Brookings Institution.” *Brookings.edu*, November 19, 2015. http://www.brookings.edu/blogs/techtank/posts/2015/11/19-isis-social-media-power-lesaca.

LinkedIn.com. “People You May Know Feature - Overview.” *LinkedIn.com*, November 13, 2015. https://help.linkedin.com/app/answers/detail/a_id/29/~/people-you-may-know-feature---overview.

LocationKit. “Free iOS and Android Location Manager SDK for Apps. Mobile Location Services.” Accessed January 14, 2016. https://locationkit.io/.

Lohr, Steve. *Data-Ism: The Revolution Transforming Decision Making, Consumer Behaviour, and Almost Everything Else*. New York: HarperCollins Publishers, 2015.

Lyon, David. *Surveillance after Snowden*. Cambridge ; Malden, MA: Polity Press, 2015.

Macdonald, Major Michael. “JFC Conference: ‘Warfare in the Information Age’ Brief.” In *Horizon Scanning and Awareness*. 30 Commando Information Exploitation Group, 2015.

Marshall, Patrick. “Don’t Look Now, but Everybody (CIA, DHS, Etc.) Is Watching.” *GCN.com*, March 28, 2012. https://gcn.com/articles/2012/04/02/social-media-analytics-hits-privacy-line.aspx.

Matcjic, Nicole. “How ISIL Have Weaponized Social Media in Iraq – Info Ops HQ.” *InfoOpsHQ.com*, July 6, 2014. http://www.infoopshq.com/2014/07/06/case-study-isil-weaponized-social-media-iraq/.

Mathieu, Jennifer, Michael Fulk, Martha Lorber, Gary Klein, Barry Costa, and Dylan Schmorrow. “Social Radar Workflows, Dashboards, and Environments.” Technical Paper. NATO. McLean, Va.: The MITRE Corporation, March 2012. http://www.mitre.org/publications/technical-papers/social-radar-workflows-dashboards-and-environments.

Maybury, Mark. “Social Radar for Smart Power.” Technical Paper. Bedford, Ma.: The MITRE Corporation, April 2010. http://www.mitre.org/publications/technical-papers/social-radar-for-smart-power.

Mayer-Schonberger, Viktor, and Kenneth Cukier. *Big Data - A Revolution That Will Transform How We Live, Work, and Think*. New York: Houghton Mifflin Harcourt Publishing Company, 2013.

Mazzetti, Mark, and Michael R. Gordon. "ISIS Is Winning the Social Media War, U.S. Concludes." *The New York Times*. June 12, 2015, sec. Middle East. http://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-us-concludes.html?_r=0.

McCue, Colleen. *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. 2 Edition. Waltham: Elsevier, 2015.

Microsoft. "SocialRadar – Windows Apps on Microsoft Store." *Microsoft Corporation*. Accessed January 14, 2016. https://www.microsoft.com/en-us/store/apps/socialradar/9wzdncrdn7qw.

"Middle East Internet Statistics, Population, Facebook and Telecommunications Reports." Accessed January 22, 2016. http://www.Internetworldstats.com/stats5.htm.

Miles, Jonathan. "A Summary of the Notes Taken at Discussions That Occurred during the Recent DOD CIO Industry Liaison Trip to Silicon Valley between the Dates 8th and 13th June 2015." British Defence Section United States, July 2015.

———. "Notes from CIO Symposium 29-30 Jun 15 and JFC 'Warfare in the Information Age' Study Day 1 Jul 15." London: British Defence Section United States, 2015.

———. "Summary of Meeting Regarding Big Data." British Defence Section United States, February 27, 2015.

Ministry of Defence, Defence Science and Technology Laboratory. "MOD Hackathon to Mine the Deep Web." News Story, September 14, 2015. https://www.gov.uk/government/news/mod-hackathon-to-mine-the-deep-web.

Multi-Agency Collaboration Environment. "Open-Source Analytic Assessment - HQ JFIG JIOC RFI - ISIL Use of Social Media." Multi-Agency Collaboration Environment, August 11, 2015.

"National Security Strategy and Strategic Defence and Security Review 2015," n.d.

Nguyen, Ted. "Social Media Revolution Ignites Middle East and North Africa | Ted Nguyen USA | PR, Social Media and Other Moving Solutions." *Tednguyenusa.com*, 2011. http://www.tednguyenusa.com/social-media-ignites-revolutions-in-middle-east-and-north-africa/.

Nissen, Thomas E. "Get Used to Losing Control: Social Media, Strategic Narratives and Stratcom." *The Three Swords Magazine - The Magazine of NATO's Joint Warfare Center*. Accessed January 5, 2015. http://www.jwc.nato.int/images/stories/threeswords/SOCIAL_MEDIA_STRATCOM.pdf.

———. *#TheWeaponizationOfSocialMedia: @Characteristics_of_Contemporary_Conflicts*. Copenhagen: Royal Danish Defence College, 2015.

Office of Corporate Communications, NGA. "Remarks as Prepared for Robert Cardillo, Director, National Geospatial-Intelligence Agency for the 31st Annual Space Symposium, Colorado Springs, CO. April 14, 2015." Colorado Springs, CO.: National Geospatial Intelligence Agency, 2015. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi17s6M8ZjKAhUGShQKHQmhCfcQFggdMAA&url=https%3A%2F%2Fwww.nga.mil%2FMediaRoom%2FSpeechesRemarks%2FDocuments%2F2015%2F2015414_SpaceSymposium_AsPrepared.pdf&usg=AFQjCNHAczXd8H1cyMsG9aNSO9M5nXHU-Q&sig2=pKaj6H5V7yi7mH6qt0ORww.

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. "Report of the Defense Science Board Task Force on Defense Intelligence Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations." Washington D.C.: Defense Science Board, February 2011. http://www.acq.osd.mil/dsb/reports/ADA543575.pdf.

Oluwatola, Tobi. "Nigeria's Election: Who Is Winning the Twitter War?" *Naijatowncrier.com*, March 27, 2015. http://naijatowncrier.com/nigerias-election-who-is-winning-the-twitter-war-by-tobi-oluwatola/.

Omand, David, Jamie Bartlett, and Carl Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security* 27, no. 6 (December 2012): 801–23. doi:10.1080/02684527.2012.716965.

O'Neal, Kenny. "US Air Force National Intelligence Coordination Cell." Powerpoint Presentation presented at the Big Data for Defense and Intelligence, Arlington, VA, October 8, 2015. http://www.globaleventslist.elsevier.com/events/2015/10/big-data-for-defense-and-intelligence-symposium/.

*Open Data White Paper: Unleashing the Potential.* London: Stationery Office, 2012.

"Open-Source Analytic Assessment - HQ JFIG JIOC RFI ISIL Use of Social Media 11 August 2015." Herndon: MACE, August 11, 2015.

Page, Christopher. "Architecture for Intelligence Analytics." Powerpoint Presentation presented at the Big Data for Defense and Intelligence, Arlington, VA, October 8, 2015. http://www.globaleventslist.elsevier.com/events/2015/10/big-data-for-defense-and-intelligence-symposium/.

Payton, Theresa, and Theodore Claypole. *Privacy in the Age of Big Data - Recognizing Threats, Defending Your Rights, and Protecting Your Family*. Lanham: Rowman & Littlefield, 2014.

Phillips, Mark. "A Brief Overview of ABI and Human Domain Analytics." *Trajectory Magazine*, September 28, 2012. http://trajectorymagazine.com/civil/item/1369-human-domain-analytics.html.

Picarillo, Robert, and Chelsey Gray. Multi-Agency Collaboration Environment (MACE), September 30, 2015.

Porcedda, Maria Grazia. "Surveille Deliverable 2.4: Paper Establishing Classification of Technologies on the Basis of Their Intrusiveness into Fundamental Rights." Collaboration Project, April 30, 2013. https://cyberwar.nl/d/fromEUFP7/SURVEILLE/D2.4%20Paper%20establishing%20the%20classification%20of%20technologies%20on%20the%20basis%20of%20their%20intrusiveness%20into%20fundamental%20rights.pdf.

Purnell, Newley. "Facebook's Free Internet Access Program in Developing Countries Provokes Backlash." *Wall Street Journal*, September 24, 2015, Online edition, sec. Tech. http://www.wsj.com/articles/facebooks-free-Internet-access-program-in-developing-countries-provokes-backlash-1443119580.

Ramakrishnan, Naren, Gizem Korkmaz, Chris Kuhlman, Achla Marathe, Liang Zhao, Ting Hua, Feng Chen, et al. "'Beating the News' with EMBERS: Forecasting Civil Unrest Using Open Source Indicators," 1799–1808. New York, 2014. doi:10.1145/2623330.2623373.

Reuters. "Facebook Mind Control Experiments Linked to DoD Research on Civil Unrest — RT USA." *RT Question More*, July 2, 2014. https://www.rt.com/usa/169848-pentagon-facebook-study-minerva/.

"Revealed: White House Seeks to Enlist Silicon Valley to 'Disrupt Radicalization' | Technology | The Guardian." Accessed January 10, 2016. http://www.theguardian.com/technology/2016/jan/07/white-house-social-media-terrorism-meeting-facebook-apple-youtube-.

Rohozinski, Rafal, and Robert Muggah. "Brace for the Quantified Society." Opencanada.org, January 9, 2015. https://www.opencanada.org/features/brace-for-the-quantified-society/.

Rosenburg, Barry, and Amber Corrin. "Command Conversation: Robert Cardillo." *C4ISR and Networks* June 2015 (June 10, 2015). http://www.c4isrnet.com/story/military/interview/command/2015/06/08/services-talent-alignment-top-nga-priority-list/28550813/.

Rouse, Margaret. "What Is Unstructured Data?" *TechTarget*, April 2010. http://searchbusinessanalytics.techtarget.com/definition/unstructured-data.

Sanchez, Ray. "ISIS Exploits Social Media to Make Inroads in US - CNN.com." *CNN.com*, June 5, 2015. http://www.cnn.com/2015/06/04/us/isis-social-media-recruits/.

Savas, Onur, Yalin Sagduyu, Julia Deng, and Jason Li. "Tactical Big Data Analytics: Challenges, Use Cases, and Solutions." *ACM SIGMETRICS Performance Evaluation Review* 41, no. 4 (April 17, 2014): 86–89. doi:10.1145/2627534.2627561.

Schactman, Noah. "Air Force's Top Brain Wants a 'Social Radar' to 'See Into Hearts and Minds.'" *Wired.com*, January 19, 2012. http://www.wired.com/2012/01/social-radar-sees-minds/.

Schmarzo, Bill. *Big Data: Understanding How Data Powers Big Business*. Indianapolis, IN: John Wiley & Sons, 2013.

Schmitt, Eric, and Thom Shanker. *Counterstrike: The Untold Story of America's Secret Campaign against Al Qaeda*. 1st ed. New York: Times Books, 2011.

Schmorrow, Dylan, and Jack Zaientz. "Realizing the Vision of Social Radar: Trends, Opportunities, and Analysis of Sociocultural Behavior S&T for the DoD." Ann Arbor, Missouri, February 4, 2014. http://www.dtic.mil/ndia/2014human/Schmorrow.pdf.

Schwartz, Lt Col Tamara. "The Art of the Now: Decision Making and the Big Data Conundrum." White Paper. Cary, NC: SAS Federal, 2014. http://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/art-of-the-now-107418.pdf.

Siegel, Eric. *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*. Hoboken, NJ: Wiley, 2013.

Silver, Nate. *The Signal and the Noise: Why so Many Predictions Fail - but Some Don't*. New York, NY: Penguin Books, 2015.

"Single Open Source Intelligence Battlespace - Blueprint v1." UK MOD, June 12, 2015.

"SitScape | Smart Visual Analytics with Real-Time Collaboration." Accessed September 30, 2015. https://www.sitscape.com/homepage/products.html.

Slabodkin, Greg. "GEOINT Tradecraft: 'Human Geography.'" *Defensesystems.com*, October 29, 2013. https://defensesystems.com/articles/2013/10/29/geoint-human-geography.aspx.

"Spotter: Media and Social Media Analytics." *Spotter.com*. Accessed January 23, 2016. http://www.spotter.com/.

"SpyMeSat - Know When a Satellite Could Be Imaging You." Commercial App. *SpyMeSat.com*. Accessed November 3, 2015. http://www.spymesat.com/.

Stationery Office (Great Britain). "Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014." London: House of Commons, September 4, 2014. https://osc.independent.gov.uk/wp-content/uploads/2014/09/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf.

Stearns, Josh. "Tools for Verifying and Assessing the Validity of Social Media and User-Generated Content." *JournalistsResource.org*, April 2, 2015. http://journalistsresource.org/tip-sheets/reporting/tools-verify-assess-validity-social-media-user-generated-content.

Tagjdeh, Yasmin. "Big Data Helping to Pinpoint Terrorist Activities, Attacks (UPDATED)." *National Defense Magazine*, April 2015. http://www.nationaldefensemagazine.org/archive/2015/April/Pages/BigDataHelpingtoPinpointTerroristActivitiesAttacks.aspx.

Taylor, James. "Avoiding Generic Dashboards with Decision Modeling — JT on EDM." Blog. *James Taylor on Everything Decision Management*, January 14, 2016. http://jtonedm.com/2016/01/14/avoiding-generic-dashboards-with-decision-modeling/.

Tennant, Major Gareth. "How Will Sea Based Theatre Entry Forces Be 'Information Centric' in the FOE?" 30 Commando Information Exploitation Group, 2015.

"The Art of the Now: Decision Making and the Big Data Conundrum." SAS Institute Inc., n.d.

"The EMBERS Project Can Predict the Future With Twitter." Accessed January 16, 2016. http://www.newsweek.com/2015/03/20/embers-project-can-predict-future-twitter-312063.html.

Theohary, Catherin A. "Information Warfare: The Role of Social Media in Conflict." *CRS Insights*, Federation of American Scientists, March 4, 2015. https://www.fas.org/sgp/crs/misc/IN10240.pdf.

Tim Slater. Joint Forces Intelligence Group Open Source Social Media Exploitation Team Leader, November 9, 2015.

Toney, Dr. Michael S. CEO, Social Analysis and Intelligence Group, LLC, September 1, 2015.

Tucker, Patrick. "Naren Ramakrishnan: How Technology Can Spot a War before It Starts." *Slate.com*, March 5, 2014. http://www.slate.com/articles/technology/future_tense/2014/03/naren_ramakrishnan_how_technology_can_spot_a_war_before_it_starts.html.

Tunnell IV, Col. Harry D. "Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy." *Military Review* May-June 2014 (June 2014): 43–50. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20140630_art011.pdf.

"US Military Looks to Social Nets for Intelligence Strategy | PCWorld." Accessed January 8, 2016. http://www.pcworld.com/article/2013726/us-military-looks-to-social-nets-for-intelligence-strategy.html#comments.

Van Engelen. "Datafloq - Big Data Will Effectively Fight Terrorism In The World." *Datafloq.com*, January 23, 2015. https://datafloq.com/read/big-data-will-effectively-fight-terrorism/785.

Virginia Tech Data Analytics Center. "Forecasting the Future: The EMBERS Predictive Analytics Success Story," 2015. http://www.basistech.com/wp-content/uploads/pdf/EMBERS-Case_Study.pdf.

"Visualization of the Week: Clustering Your Social Graph - O'Reilly Radar." Accessed January 14, 2016. http://radar.oreilly.com/2012/04/facebook-visualization-app-friends-experiences.html.

Volchek, Dimitry, and Claire Bigg. "Ukrainian Bloggers Use Social Media to Track Russian Soldiers Fighting in East." *The Guardian*. June 3, 2015, Online edition, sec. World News. http://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine.

Walters, Brigader General Robert. "Remarks by Brigadier General Robert Walters, Deputy Director for Operations and Intelligence." Speech. Pakistan Counter-IED Symposium, May 20, 2013. https://www.jieddo.mil/content/docs/20130520_BG_Walters_remarks_at_Pakistan_Counter-IED_Symposium_AS_PREPARED.pdf.

"Was Facebook's 'Creepy' Study Funded by the US Military?" *The Week UK*, July 3, 2014. http://www.theweek.co.uk/facebook/59210/was-facebooks-creepy-study-funded-by-the-us-military.

"Was Facebook's 'Creepy' Study Funded by the US Military?| Facebook News | The Week UK." Accessed January 7, 2016. http://www.theweek.co.uk/facebook/59210/was-facebooks-creepy-study-funded-by-the-us-military.

Watters, Audrey. "Visualization of the Week: Clustering Your Social Graph." *O'Reilly Radar*. Accessed January 14, 2016. http://radar.oreilly.com/2012/04/facebook-visualization-app-friends-experiences.html.

We are social Singapore. "Digital, Social & Mobile in 2015." January 20, 2015. http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015/214.

Weaver, Randy A. "The Application of 'Spiral Analysis' to ABI: Lessons Learned in the Interagency Environment - An Examination of Lessons Learned in the Interagency Law Enforcement Environment and the Potential Application of Those Lessons to Activity-Based Intelligence." Corporate research paper. Arlington, VA: Concurrent Technologies Corporation, August 2014. https://info.publicintelligence.net/CTC-SpiralAnalysis.pdf.

Weyers, Jeff R., and Cammie Condon. "New Zealand Jihadist Deletes Tweets after Discovering He Left Geotagging On." *Ibrabo.wordpress.com*, December 30, 2014. https://ibrabo.wordpress.com/2014/12/30/new-zealand-jihadist-deletes-tweets-after-discovering-he-left-geotagging-on/.

*What Is Predictive Analytics?* IBM Online Tutorial, 2013. https://www.youtube.com/watch?v=0KXME_y-3QA.

"Why Did the World Miss the Arab Spring?" *Exemplifier*, September 24, 2013. http://exemplifier.org/?p=179.

"Why It's so Difficult to Counter ISIS on Social Media." *CBS News*. Accessed September 29, 2015. http://www.cbsnews.com/news/why-so-difficult-counter-isis-social-media/.

"Why It's so Difficult to Counter ISIS on Social Media - CBS News." *CBSnews.com*, June 23, 2015. http://www.cbsnews.com/news/why-so-difficult-counter-isis-social-media/.

Wood, Colin. "How Does the Military Use Big Data?" *Emergencymgmt.com*, January 6, 2014. http://www.emergencymgmt.com/safety/Military-Use-Big-Data.html.

Woodie, Alex. “How Analytics Is Driving Military Intelligence.” *Datanami.com*, February 3, 2014. http://www.datanami.com/2014/02/03/how_analytics_is_driving_military_intelligence/.

Yadron, Danny. “Revealed: White House Seeks to Enlist Silicon Valley to ‘Disrupt Radicalization’ | Technology | The Guardian.” *Theguardian.com*, January 7, 2016, sec. Technology. http://www.theguardian.com/technology/2016/jan/07/white-house-social-media-terrorism-meeting-facebook-apple-youtube-.

Young, Chris. “Military Intelligence Redefined: Big Data in the Battlefield.” *Forbes.com*, March 12, 2012. http://www.forbes.com/sites/techonomy/2012/03/12/military-intelligence-redefined-big-data-in-the-battlefield/.

Zoghlami, Wassim. “How Data Mining Could’ve Prevented An ISIS Attack.” *Iafrikan.com*, June 22, 2015. http://www.iafrikan.com/2015/06/22/data-mining-isis-tunisia-tunis-bardo-terror-museum-atack/.