Communications of the Association for Information Systems

Volume 41 Article 5

8-2017

Social Media Exploitation by Covert Networks: A Case Study of ISIS

Lee Freeman
College of Business, University of Michigan-Dearborn, lefreema@umich.edu

Robert Schroeder
Naval Postgraduate School

Sean F. Everton
Naval Postgraduate School

Follow this and additional works at: https://aisel.aisnet.org/cais

Recommended Citation
Freeman, Lee; Schroeder, Robert; and Everton, Sean F. (2017) "Social Media Exploitation by Covert Networks: A Case Study of ISIS," *Communications of the Association for Information Systems*: Vol. 41 , Article 5.
DOI: 10.17705/1CAIS.04105
Available at: https://aisel.aisnet.org/cais/vol41/iss1/5

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

www.manaraa.com

Communications of the
Association for Information Systems

Research Paper ISSN: 1529-3181

Social Media Exploitation by Covert Networks: A Case Study of ISIS

Lee A. Freeman
Department of Management Studies
University of Michigan-Dearborn
lefreema@umich.edu

Robert Schroeder[1]
Department of Defense Analysis
Naval Postgraduate School

Sean F. Everton
Department of Defense Analysis
Naval Postgraduate School

Abstract:

Social media has quickly become a dominant mode of professional and personal communication. Unfortunately, groups who intend to perform illegal and/or harmful activities (such as gangs, criminal groups, and terrorist groups) also use it. These covert networks use social media to foster membership, communicate among followers and non-followers, and obtain ideological and financial support. This exploitation of social media has serious political, cultural, and societal repercussions that go beyond stolen identities, hacked systems, or loss of productivity. There are literal life-and-death consequences of the actions of the groups behind these covert networks. However, through tracking and analyzing social media content, government agencies (in particular those in the intelligence community) can mitigate this threat by uncovering these covert networks, their communication, and their plans. This paper introduces common social media analysis techniques and the current approaches of analyzing covert networks. A case study of the Syrian conflict, with particular attention on ISIS, highlights this exploitation and the process of using social media analysis for intelligence gathering. The results of the case study show that covert networks are resilient and continually adapt their social media use and presence to stay ahead of the intelligence community.

Keywords: Social Media, Covert Networks, ISIS, Social Media Analysis, Social Media Exploitation, Intelligence Gathering, Case Study.

This manuscript underwent peer review. It was received 01/29/2016 and was with the authors for 12 months for 3 revisions. Jackie Rees Ulmer served as Associate Editor.

[1] The views expressed in this document are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

www.manaraa.com

1 Introduction

Information technology (IT) permeates society and impacts all aspects of personal and professional interactions and communications with other individuals and organizations. Social media has quickly become a dominant mode of professional and personal communication (Fan & Gordon, 2014; Morrison 2014). Services such as Facebook, Twitter, YouTube, Instagram, Snapchat, and Tumblr each have hundreds of millions of users worldwide. Facebook's 1.2+ billion users (Ajmera, 2014) generate more video views than all of YouTube: 12.3 billion versus 11.3 billion in June 2014 (Brynley-Jones, 2014). Twitter sees 500 million tweets per day (Smith, 2015). Instagram has grown to over 300 million active accounts to surpass Twitter's 284 million active accounts (Brynley-Jones, 2014). Most impacts of IT are seen as positive, but individuals and groups can exploit, misuse, or abuse IT. Social networks enhance many forms of socially beneficial activities (Jackson, 2008; McBride & Hewitt, 2013), but they can also encourage harmful and dangerous behaviors. These covert and illegal networks, also referred to as dark networks in the related literature, are in contrast to light networks or bright networks, which are overt and legal (Raab & Milward, 2003; Milward & Raab, 2006). Identifying these threats is not sufficient; we need to mitigate the threats in order to preserve IT's benefits.

Covert networks use social media to foster membership, communicate among followers and non-followers, and obtain ideological and financial support (Freeman, 2011; Everton, 2012a; Topol, 2012; Freeman & Ruehsen, 2013; Freeman & Schroeder, 2014; Sanchez, 2015). This exploitation of social media has serious political, cultural, and societal repercussions that go beyond stolen identities, hacked systems, or loss of productivity. There are literal life-and-death consequences of the actions of the groups behind these covert networks.

The existence of these covert networks is not new. However, their relatively recent integration of social media into their operations and communications represents an exploitation of the Internet and of social media networks in particular. Communication via social media is (usually) instantaneous; reaches hundreds, thousands, or millions of other users; and is easily sharable by anyone even if not an original recipient. Social media benefits covert networks by providing an efficient and effective means of communication, which enables them to spread their messages to a larger audience. The ever-changing nature of these networks and the sheer amount of social media data that exist make it difficult for researchers and analysts to collect data and conduct real-time analyses. In addition, one can quickly and easily create new user accounts when existing accounts are shut down, which enables these networks to stay ahead of the intelligence community (Freeman & Schroeder, 2014).

However, through tracking and analyzing social media content, government agencies and, in particular, those in the intelligence community can mitigate this threat by uncovering these covert networks, their communication, and their plans (Everton, 2012a). When used by those in the intelligence community, social media data can provide an extra-intelligence source of information to supplement other sources. Used carefully, social media can indicate trends and information that inform operational decisions for those in the field: police, military forces, and other law-enforcement agencies.

This paper highlights social media analysis techniques and some of the current approaches to analyze covert networks. We present a framework for analyzing social media along with several analysis methodologies. The framework provides a guide for analysts: begin with a research question, collect baseline data, combine or fuse multiple datasets, and, finally, analyze social media data through a variety of techniques. Such analysis can take many forms, each with its own advantages and disadvantages, including geospatial, relational, temporal, and sentiment analysis.

We present a case study of the Syrian conflict with particular attention on ISIS (the Islamic State of Iraq and Syria) to highlight this exploitation of social media by covert networks, the process of using social media analysis for intelligence gathering, and the inability of the intelligence community to fully mitigate this threat. Opposition groups in Syria, including ISIS, use social media to recruit new members, raise funds, share information, and garner support from the outside world. The case study shows how one can apply the social media analysis techniques to a real-time situation in order to gain additional intelligence information. We conclude the paper by discussing the limitations of such methods and the possibilities for future research.

www.manaraa.com

2 Background

2.1 Social Media

Social media refers to "a group of internet-based applications that build on the ideological and technological foundations of Web 2.0 and that allow the creation and exchange of user-generated content" (Kaplan & Haenlein, 2010, p. 61). With Web 2.0 technologies, users can interact with and collaborate on content rather than simply viewing or reading it (Web 1.0). While Facebook, Twitter, YouTube, Instagram, Snapchat, and Tumblr garner much of the media attention, others such as Google+, LinkedIn, Pinterest, Vine, WhatsApp, Foursquare, and Reddit are but just a small selection of the hundreds of current social media services. There are also regional and country-specific platforms, such as VK in Russia and Eastern Europe (similar to Facebook) and Sina Weibo (a mix of Facebook and Twitter), Tencent Weibo (similar to Twitter), and WeChat (multiple messaging services) in mainland China. Moreover, the social media landscape is constantly changing as new services and networks enter and existing services depart or merge.

Social media concerns interactions and the exchange of content not unlike traditional media. However, social media differs from traditional media in several key ways. The quality of the content has a relatively narrow range in traditional media, while the quality of the content in social media can vary considerably. Traditional media often has centralized structures for organization, production, and delivery, while social media is more decentralized and less structured. Similarly, traditional media outlets are often accessible to a small subset of the population (usually government or privately owned businesses), while social media is available to the public (or at least anyone with Internet access). The time between production and delivery in traditional media can be long (consider a magazine article or even a book), while there is virtually no lag at all in most social media production and delivery.

Although content quality may have greater variation in social media, social media's decentralized structure, widely accessible platforms, and (nearly) instantaneous content delivery provide opportunities for anyone with Internet access on their computer, smartphone, or tablet to easily create content, interact with others, collaborate on projects, and coordinate efforts. Users do not require a degree, specialized software, or expensive equipment. Social media users can, often with little effort and no cost, post, create, share, exchange, and comment as they desire. The ability to participate in social media with mobile devices, especially smartphones, enables individuals around the world to stay in constant contact with their social media networks and actively participate wherever and whenever they wish. As an example, nearly 80 percent of Twitter's users access Twitter via their smartphone (Ajmera, 2014).

Each of the individual social media networks and the collective and interconnected networks that make up the contemporary Web 2.0 landscape provide the means for individuals, groups, and organizations of all types to communicate with their friends, members, and constituents. Set apart from traditional push-based communication of traditional websites, these networks are filled with user-generated content including text, pictures, videos, links, and the interconnections with other users and their content through tags, keywords, and sharing.

As social media usage permeates society, the quantity and value of the data and information communicated on these networks grow. The opinions and thoughts of previously inaccessible populations are now public. For example, social media can provide a strong indication of crowd thinking regarding the stock market (Bollen, Mao, & Zeng, 2011) and disease outbreaks (Schmidt, 2012) and an enhanced understanding of the human domain from a grassroots level (Di Leonardo et al., 2014). Social media communication aggregators can provide analysts and researchers with vast data sets of content pulled from multiple social media services at once. When these data are appropriately filtered and analyzed, researchers can find answers to previously unanswered questions and analysts can fill in gaps of missing information with greater efficacy than using a single social media service.

2.2 Covert Networks

Typically, covert networks refer to terrorist groups, drug traffickers, extreme political movements, gangs, and other criminal enterprises (Bright, Hughes, & Chalmers, 2012; McBride & Hewitt, 2013). The reference point and context are important because the Nazis in Germany would have considered the networks created during WWII to hide and safeguard European Jews as covert (and criminal), while most of the rest of the world would not have. The same definition holds true in networks that exist in social media, and many of these same covert networks have a presence in social media.

www.manaraa.com

Researchers and analysts face increased difficulties analyzing covert networks. Access to data (Sparrow, 1991; Krebs, 2002; Bright, Hughes, & Chalmers, 2012), especially data that clearly show relationships between members of the network, is more challenging with covert networks. Estimates of the size of these networks or the amount of data they produce do not exist (Roberts, 2011). These networks face constant attempts by governments, the intelligence community, and military groups to disrupt their activities (Milward & Raab, 2006), so their members naturally try to evade detection and intervention (McBride & Hewitt, 2013), sometimes with deceptive or misleading data (Roberts, 2011). The criminal (covert) nature of the organizations behind the networks necessitates quick, nearly immediate real-time analysis and reaction for authorities to successfully counter their activities (Everton, 2012a; Dudas, 2013). Covert networks can be resilient (Milward & Raab, 2006; Everton, 2012b; Senekal, 2014), often overlap with other covert networks (Senekal 2014), and act more like traditional organizations (Raab & Milward, 2003) in their attempts to organize and exhibit structure to their activities.

These difficulties and challenges have not stopped researchers and analysts from analyzing covert networks (Roberts & Everton, 2011; Everton, 2012b). Indeed, the practice dates back to countries' analyzing their enemies' communication patterns in WWII (van Meter, 2001). To overcome the lack of complete data, researchers have applied probabilistic modeling (Miffen, Boner, Godfrey, & Skokan 2004) and Markov processes (Kaplan, 2010), used overlapping network assumptions (Atkinson & Wein, 2010), and approached the problem from a network topology perspective (Xu & Chen, 2008) to model terrorist networks. They have successfully applied social network analysis (SNA) to covert networks such as corporate price fixing, organized crime, drug trafficking, and terrorist groups (e.g., Krebs, 2002; Sageman, 2004; Xu, Marshall, Kaza, & Chen, 2004; Rodriguez, 2005; Keefe, 2006; Natarajan, 2006; Reid, Chen, & Xu, 2007; Bright et al., 2012; Senekal, 2014). Critical to this success has been the more recent use of social media networks and the analysis of these networks and data using existing social network analysis techniques (Everton, 2012a; Schroeder, Everton, & Shepherd, 2012; Freeman & Schroeder, 2014) and new techniques such as real-time Twitter data analysis and visualization (Cheong & Lee, 2011; Dudas, 2013).

3 Social Media Analysis

Social media content ranges from simple text (a tweet on Twitter or a short post on Facebook) to multimedia maps, videos, and pictures. Determining patterns, trends, and connections between and among the content is difficult given the sheer quantity of data. Some social media sites provide built-in, yet somewhat basic, tools so users can better understand how the community is using the platform. Twitter temporally tracks phrases, words, and hashtags in its tweets and then uses these data to provide a list of trending topics. Much of the content of trending topics on Twitter is news related (over 85%), and over half of the re-tweeted content is news related (Kwak, Lee, Park, & Moon, 2010). Twitter content also contains personal biases and perspectives, especially as the content is re-tweeted and filtered via audience gatekeeping (Kwon, Oh, Agrawal, & Rao, 2012). One can combine such content with traditional media to better understand the news, its impact, and the immediate grassroots opinions of those involved (Meraz & Papacharissi, 2013). This type of analysis and research has become common with the aftermaths of both man-made (Lee, Agrawal, & Rao, 2015) and natural (Sutton et al., 2015) disasters and other major political or socio-political events (Starbird, Muzny, & Palen, 2012; Starbird & Palen, 2012). These studies differ from the current study, however, in that they focus on the public reaction and dissemination of news and opinions via social media following a particular event. In contrast, we focus on a particular group's use of social media that does not necessarily relate to a particular event.

One can use data from social media to research a variety of questions and situations. With the vast amount of social media data, researchers and analysts need an organized approach. The process begins with a research question. Second, one needs to collect and organize data. Finally, one can analyze the data.

Figure 1 presents the social media analysis framework that Freeman and Schroeder (2014) outline. The framework begins on the left with a research question. In order to answer this research question, the researcher cycles through the baseline, data-fusion, and data-discovery phases. These data-collection phases often loop back on each other and lead the researcher through the analyses.

www.manaraa.com

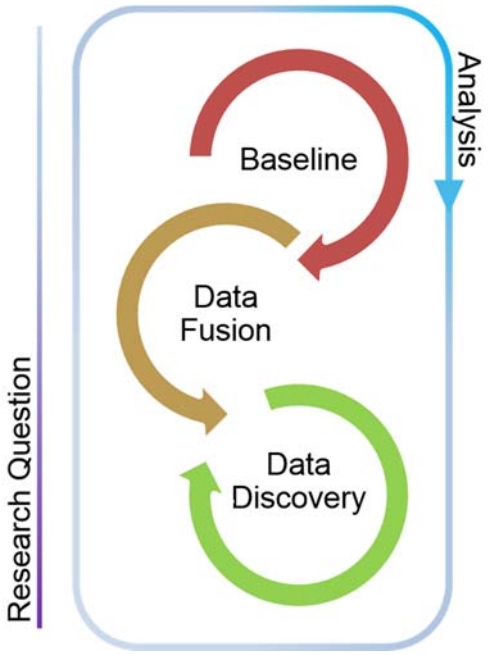

Figure 1. Social Media Analysis Framework

3.1 The Research Question

The research question drives the data collection and data analysis. One must consider the demographics of social media users when developing a research question to ensure social media analysis is an appropriate methodology. One should create research questions with an eye towards the intended level of analysis regarding location, geographic area, user groupings, or quantity of data (Yurdusev, 1993) because the intended level of analysis will influence and drive the collected data. Freeman and Schroeder (2014) provide the following examples:

- What topics are trending in a geographical area?
- Which user accounts potentially have the most influence?
- What content are targeted user accounts posting?
- Where are targeted user accounts posting from for pattern of analysis?

3.2 Data Collection

With a research question in mind, one collects data in three phases: baseline, fusion, and discovery. One needs to structure all data during data collection in a similar way in order to aggregate, filter, and organize the data; researchers often do so using software packages and analytical tools. This point is especially critical when one analyzes large quantities of social media data instead of individual pieces of social media content.

The first phase of data collection involves conducting baseline research, which provides a contextual understanding of the research question. One needs to perform this step because it is unlikely that social media will provide all the information needed to conduct a proper analysis. Instead, the researcher needs information to help guide a structured collection of social media data. For example, reports might provide names of insurgent organizations of interest, which allows the researcher to search for that name when discovering new data via social media. These data often come from unstructured reports; for example, news articles or other textual documents (Freeman & Schroeder, 2014). Additionally, baseline data may provide information that does not exist on social media. For example, while two people might have a relationship by being coworkers, they may not communicate via social media. Having baseline data that are structured and can be merged with social media data can fill in gaps from data gained through social media collection.

www.manaraa.com

After obtaining baseline data, one should fuse or merge these data with other existing datasets. Merging the baseline data with additional datasets provides structure to the baseline data, potential structure to the yet-to-be-collected data from social media, or data that one can use to fill in existing data gaps. For example, providing a basemap where one can plot both baseline data and newly discovered data helps one to fuse the data together geospatially.

Once the baseline phase provides context to the research question and the fusion phase provides structure, the analyst can gather additional data via social media platforms. Information gathered from baseline research will help provide relevant search criteria. The researcher collects data from the social media platforms by creating search parameters to limit the amount of data collected, creating a method to retrieve and store the data, setting a schedule for how to collect the data or information, and constructing a plan for how to fuse newly discovered data with already collected data.

3.3 Data Analysis

The research question will determine which level of analysis to focus on. Social media analysis can take place on a micro-level (individuals), macro-level (society or groups of individuals), or anywhere in between.

Micro-level analysis focuses on specific users, events, organizations, links, or other entities. One typically knows these entities through prior research and breaking events. Macro-level analysis focuses on large-scale data collection typically analyzed for trending content, hotspot analysis, and overall network structure. This requires data from a large number of user accounts and is similar to listening to the wisdom of crowds (Surowiecki, 2005) as opposed to individual opinions.

One can use different levels of analysis to inform additional discovery. An example of macro-level analysis is searching for trending topics related to the Charlie Hebdo attack by querying social media topics such as “Charlie Hebdo”, “Paris terrorism”, and “Islam”. Examples of micro-level analysis related to the Charlie Hebdo example include analyzing the messages and relations between the users in order to identify key or potentially influential user accounts. Additionally, when analyzing a small number of users, one may discover a particular hashtag, topic, or link that can lead to a larger-scale search.

Social media analysis, when guided by a research question, can provide useful information to many different problems. The research question, the availability of existing data, and the social media platforms under analysis will help determine the appropriate methodology.

3.3.1 Geospatial Analysis

Geospatial analysis refers to techniques that one can apply to spatially driven research questions by applying location-based (i.e., mapable) tags to the data. The locations can be as specific as a single point on a map (latitude and longitude) or as broad as an entire country or continent (de Smith, Goodchild, & Longley, 2007). One can reference these locations by coordinates or by name (Goodchild, 2007). Any data that can be mapped can be incorporated into geospatial analysis.

There are three types of location data in social media data: activity locations (based on the actual GPS signal), profile locations (based on user-generated information in users’ account profile), and mentioned locations (based on locations mentioned in posts). Using geospatial data from the content allows social media to be useful in monitoring real-time events. During the Egyptian Revolution in 2011, the term “#Tahrirsquare”—a specific location in Cairo and the center of activity during the protests—spiked in activity (Stefanidis, Crooks, & Radzikowski, 2013). This mentioned location approach can be prone to inflation, however. For example, Katy Perry, the American singer, was one of the most heavily retweeted user accounts that commented on the Egyptian Revolution even though she was not there (Schroeder, Everton, & Shepherd, 2014).

3.3.2 Relational Analysis

Relational analysis refers to techniques that one can apply to relationship-driven research questions by assessing how users interact with each other. Relational data are the foundation of most social media platforms. When looking at a user’s social media account, social media sites typically present basic information on the user account’s relations. Examples of this information include friends, followers, family, likes, retweets, and comments.

www.manaraa.com

Link analysis and social network analysis are the most common relational analysis techniques for visualizing networks. Researchers often use these techniques to determine the popularity of user accounts, the centrality of user accounts, and the roles user accounts play in spreading information across the social media platform (Wasserman & Faust, 1994). Link analysis focuses on the connections between social media entities—user accounts, hashtags, links, or shared posts—using software such as Analyst Notebook, Palantir, or Semantica to visualize the collected data. One can form these connections in many ways, such as: (Freeman & Schroeder, 2014):

- Between user accounts based on following or being friends
- Between user accounts and posts by creating, liking, retweeting, or commenting on a post
- Between users and hashtags by using a hashtag in a post, and
- Between hashtag and hashtag by appearing in the same post.

Even with less popular entities and a smaller dataset, the number of entities and the connections between and among them on a link analysis visualization of social media data can be vast. Social network analysis (SNA), another relational analysis technique, allows researchers to apply metrics to the data to help them make sense of visually complicated networks. They can examine the network's topology, identify central nodes or entities, detect subgroups, and locate the roles that individual nodes may play as brokers or bridges in the network (Bright et al., 2012; Everton, 2012b). Hansen, Shneiderman, and Smith (2010), Shneiderman, Preece, and Pirolli (2011), and Everton (2012b) provide additional details of social network analysis with social media.

3.3.3 Temporal Analysis

Temporal analysis refers to techniques that one can apply to time-driven research questions by assessing temporal tags on the social media data. Most content from social media includes a temporal tag that describes when the content was uploaded. In fact, many social media sites have built-in temporal analysis tools: trending posts on Twitter, most recent posts on Facebook, and views over time on LinkedIn.

Three common techniques for temporal analysis include the panel technique, event-count technique, and event-history technique (Finkel, 1995; Hannan & Tuma, 1979; Long, 1997). With the panel technique, one collects variables over time and then compares them with each other to answer the research question. The event-count technique measures (counts) the number of times an event (the variable of interest) occurs in a period of time and then compares these counts with other variables. The event-history technique measures the time that elapses between two occurrences of an event. One can also combine these three techniques in various ways to analyze data in additional ways.

A common application of temporal analysis techniques involves comparing social media temporal analysis with real-world (on-the-ground) temporal analysis. Using the event-count technique, researchers could compare counts of the hashtag #Homs, a Syrian city, over time to counts of violence in the same location over the same period of time to see if the two have a relationship. From an event-history perspective, a researcher could compare the time difference between posts by an insurgent group and events carried out by the same group to measure whether there is a relationship between their posting about and carrying out these events and what that relationship may be (Freeman & Schroeder, 2014).

3.3.4 Sentiment Analysis

Sentiment analysis refers to techniques that extract feelings and opinions from textual content (Shellman, Covington, & Zangrilli, 2014). One can generally categorize textual information as either objective statements of fact or subjective statements of opinion (Liu, 2010). One can classify most opinions as positive or negative (some can be neutral); they can also "be an emotion, a behavioral disposition, or a rational judgment" (Shellman, Covington, & Zangrilli, 2014). One assesses each piece of content based on a rubric (positive/negative or emotion), and one can analyze an entire conversation or communication stream.

4 Syrian Conflict/ISIS Case Study

Given the previously identified exploitation of social media by covert networks, the intelligence community can use various social media analysis techniques to identify and track the primary social media accounts in these covert networks. Once analysts know who to track, they can follow these accounts and perform

www.manaraa.com

additional analyses to uncover additional intelligence. Combined, all of the intelligence and analyses provide the necessary data needed to fight back against the covert networks whether via social media or in the real world. The following case study of the Syrian conflict with particular emphasis on ISIS provides real-world examples of how a particular covert network uses (exploits) social media, how one can track and analyze this use, how one can mitigate their exploitation of social media, and the limitations that remain (meaning the threat remains).

The growth of social media provided the organizations and individuals involved in the Syrian conflict with new modes of communication. This case study illustrates the exploitation of social media by providing a description of how the opposition groups in Syria (in particular, the Islamic State of Iraq and Syria (ISIS)), have used social media. The analysis techniques used provide a means of mitigating this threat (namely, the influence and spread of such extremist groups and covert networks).

4.1 Initial Research Questions

The following research questions guided the initial work in 2012 (Freeman & Schroeder, 2014):

- Who were the main political and military opposition groups of the Syrian conflict?
- Who were the military leaders of the political and military opposition groups of the Syrian conflict?
- If the Assad regime crossed the “red line” per President Obama’s August 2012 speech, which groups should U.S. Special Operations Forces partner with to secure chemical, biological, and nuclear sites?
    - Are these military opposition groups aligned with violent extremist organizations?
    - Are they successful on the field?
    - Where are their areas of operations?
    - How many fighters do these groups have?

4.2 Baseline Data and Data Fusion

From the beginning, the Syrian conflict was one of the most well-documented conflicts on social media due to Syria’s literacy rate, broadband and cellular access, and smartphone penetration (Lynch, Freelon, & Aday 2014). Individuals used social media to communicate, update, motivate, recruit, and fundraise for various opposition groups (Topol, 2012). However, the Syrian conflict intensified and garnered greater international attention when President Obama’s “red line” regarding the use of chemical weapons was allegedly crossed (Gordon, 2013). The Free Syria Army (FSA) fractionalized (Mahamood & Black, 2013) into multiple, militarized opposition forces. ISIS emerged as a legitimate and successful opposition party (Reynolds & Caris, 2014). With all of these and the loss of control of large territories in the north and east, the Assad regime maintained power (Hwaida & Cowell, 2014).

The combination of these events and changes in the conflict’s landscape has led to greater regional instability and increased violence. Of particular interest for the intelligence community is the emergence and rise of the Islamic State of Iraq and Syria (ISIS), a violent extremist organization that operates in both Syria and Iraq that claims to be a successor to al-Qaeda (Freeman & Schroeder, 2014). ISIS continues to actively use social media to publish information even after accounts are shut down, which can provide critical information and intelligence to support counter-operations both in social media and on the ground.

The Syrian Revolution Martyr Database (2011), a data aggregator of validated and organized crowdsourced information, has provided the names, gender, military/civilian status, age, location (latitude/longitude), and date/time of conflict-related deaths in Syria since 2011. The resulting geospatial analysis in Figure 2 of over 90,000 records shows the intensity of the conflict around Homs, Syria, based on the analysis. The bottom of the screenshot shows a temporal histogram and a time wheel.

www.manaraa.com

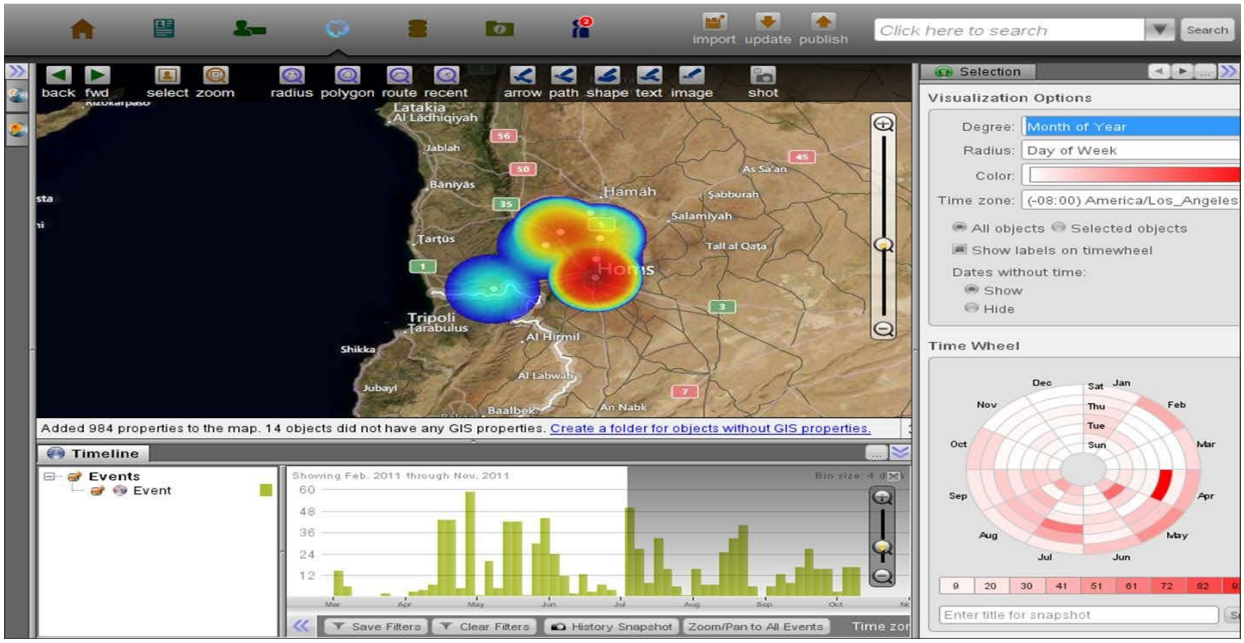

Figure 2. Palantir Screenshot of Shuhada Martyr Data that Visualizes the Intensity of the Syrian Conflict Both Geospatially and Temporally (Freeman & Schroeder, 2014)

The sociogram (a graphical representation of social links and connections in a group via relational analysis) in Figure 3 aided in our effectively analyzing the major opposition group in the early part of the Syrian conflict, the Free Syria Army (FSA). We derived the data for this sociogram from social media sources, the Institute for the Study of War (Holliday, 2011, 2012a, 2012b; O'Bagy 2012a, 2012b, 2012c), and the Syrian National Council (2012) in an attempt to capture the density and centralization of the nodes. The resulting network graph displays the connections between individuals, political organizations, and military units involved with the resistance and opposition to the Assad regime. The hashed oval in the center shows the densest connections between individuals, military opposition groups, and political opposition groups. The solid oval in the upper right indicates a subgroup of the opposition without strong ties to the core of the FSA. This subgroup would eventually split from the FSA to form the National Islamic Front with additional elements breaking away to join ISIS.

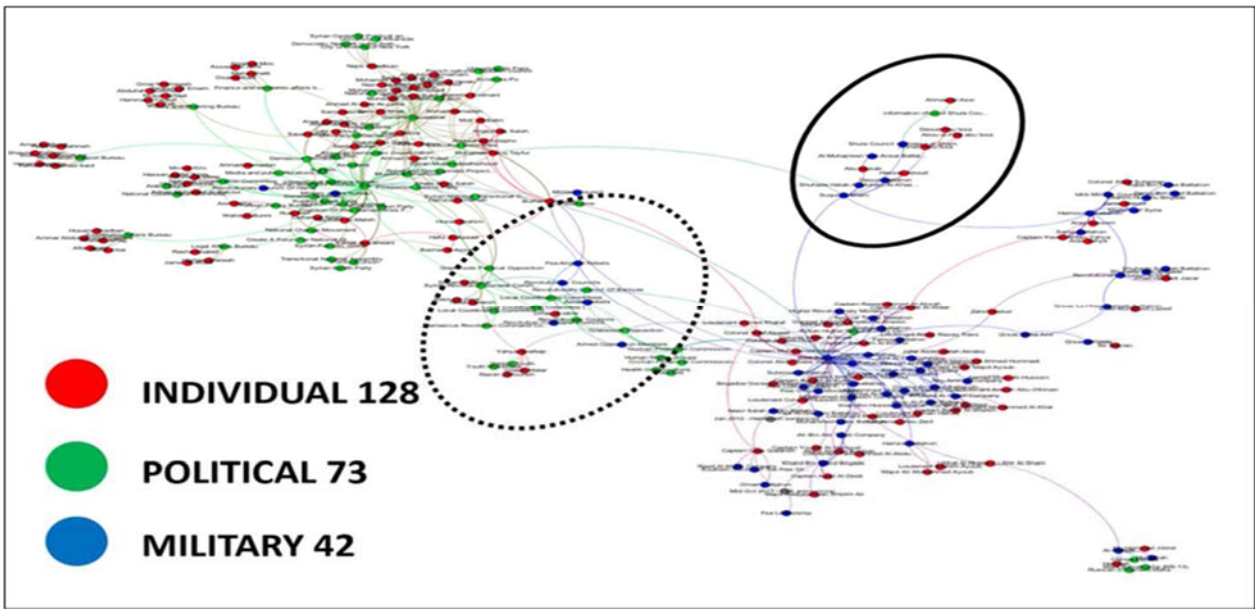

Figure 3. Sociogram of Political and Military Opposition Groups and Affiliated Individuals from Initial Research (Freeman & Schroeder, 2014)

www.manaraa.com

4.3 Data Discovery and Analysis: Development of ISIS and its Use of Social Media

The Islamic State of Iraq and Syria (ISIS) originated primarily in Iraq, but it has a strong presence in Syria. It has undergone several name and leadership changes, and there is every reason to believe that this will continue in the future. In addition to the insurgency operations between ISIS, the Assad Government, and the Iraqi Government, ISIS also conducts operations against other insurgent groups in the region (Freeman & Schroeder, 2014).

ISIS has used social media to frame (contextualize) their arguments and position in the context of the Syrian Conflict and the larger region (Snow, Rochford, Worden, & Benford, 1986). Framing seeks to accomplish three core tasks: 1) identify the problem and its causes ("diagnostic" framing), 2) identify what should be done ("prognostic" framing), and 3) encourage members and potential members to act ("motivational" framing) (Benford & Snow, 2000). Specifically, ISIS has used social media in all three ways. ISIS has blamed the Assad Government, the Free Syrian Army, and many other individuals and groups for the current problems in Syria (diagnostic framing). It has explained what needs to be done and has called for action (prognostic framing). Finally, it has used religious messages and propaganda to encourage such action (motivational framing). Figure 4 presents an example that portrays ISIS in a positive light. It was part of a series of images from Iraq that showed ISIS performing the equivalent of Civil Affairs by providing entertainment for the children followed by candy and a movie night that espoused ISIS propaganda. ISIS propagandist accounts shared the image via Twitter and the website www.justpaste.it.

Figure 4. Image Shared on Twitter and Justpaste.it[2]

ISIS has used textual posts to frame its position and draw attention to its cause. It has incorporated derogatory terms for its opposition that contextualize the conflict into a larger, historical conflict in the entire region. It has conducted this framing to convince others to choose sides—ideally, ISIS's side. ISIS has also often framed its position with images. It has displayed pictures of what happens to its enemies or those who oppose it, of their own forces' providing food and aid, and of their victories in battle.

4.3.1 Geospatial Analysis

ISIS has framed the conflict in Iraq and Syria by calling many of the airstrikes carried out against ISIS, whether carried out by the United States and its coalition partners or by Syria, as attacks by the "Crusader Alliance". Using Sprinklr, a commercial tool for analyzing social media, we collected any tweets from

[2] http://justpaste.it/alkher16a

المنارة للاستشارات
www.manaraa.com

Twitter that mentioned “Crusader Alliance” in Arabic from outside the United States during 3 to 30 August, 2015. We found 23,924 relevant tweets during this time period.

The first analysis looked at from where the tweets originated. For the 1,843 tweets that contained geospatial information (a majority of the tweets did not contain geospatial information), most originated from the Middle East with Saudi Arabia at the top of the list. Figure 5 provides a map of tweets with geospatial information; darker colors indicate more tweets came from that country (countries in grey had no tweets from that location).

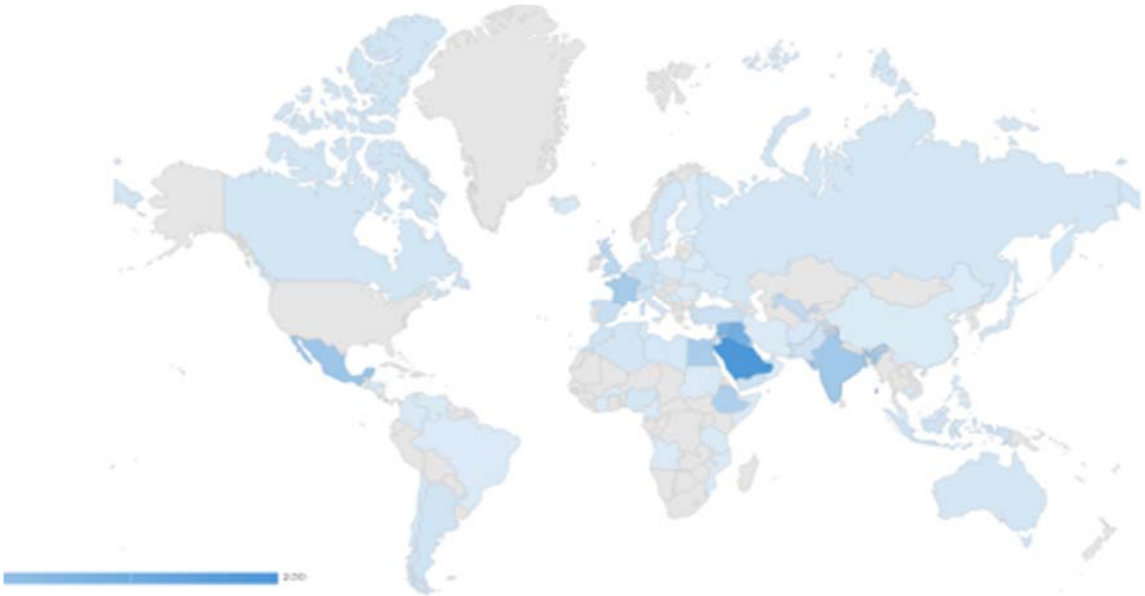

Figure 5. Map of Tweets by Profile Location

While the country information provides some information about where the tweets originated, it is hardly complete. Of the 23,924 tweets, only 230 originated from Saudi Arabia. Another method for conducting geospatial analysis is to analyze the content of the tweets via analyzing the hashtags and the locations that users mention. Table 1 provides a list of the top ten location hashtags.

Table 1. Counts of Location Hashtags

Hashtag	Translation	Mentions
ولايــة الخــير	Wilayat alKhair	2078
ولايــة حلــب	Wilayat Aleppo	1779
ولايــة دمشــق	Wilayat Damascus	1335
ولايــة الرقــة	Wilayat Ar-Raqqa	872
ولايــة الأنبــار	Wilayat Anbar	752
حلــب	Aleppo	643
ولايــة الفلوجــة	Wilayat Fallujah	626
الجــزيرة ولايــة	Wilayat Jazira	562
ولايــة دجلــة	Wilayat Tigris	455
ســوريا	Syria	437

These hashtags had much higher counts than submitted geospatial information, but, instead of explaining where the user accounts tweet from, they explain what they were tweeting. Also, some of these names are not names of established locations but instead new names that ISIS has created for locations. For example, the most prolific hashtag concerned Wilayat al-Khair or the state of Khair. There is no established province of Khair inside Syria, but this is the province that ISIS has created that covers Deir Ezzor and other areas.

المنارة للاستشارات
www.manaraa.com

By knowing from where tweets are being posted and/or the locations they mention, analysts can reach a better understanding of the insurgents' locations and the primary focus of their conversations, respectively. This information enables a more focused analysis than just looking at the messages themselves because it assists analysts in answering the "where" question in real time. Geospatial analysis differs from other analysis techniques of covert networks such as ISIS because so much of data is location based (either from the location of the post or the location mentioned), and understanding the importance of the locations is critical to mitigating the threat of such groups.

4.3.2 Relational Analysis

One can apply relational analysis to the communication patterns of user accounts to analyze the connections between users based on whether a user account mentioned another user account in one of its tweets or replies. The analysis focused only on the largest component of the network, which comprised 1,507 user accounts and 1,850 connections. By analyzing in-degree centrality (see Figure 6), the user accounts that the largest number of other user accounts mentioned the most become evident. The top users (based on their profile information) in terms of in-degree centrality comprised several Islam scholars (largely from Saudi Arabia) and Middle East reporters. Most of these accounts did not have any out degree or messages from them going to other users, which suggests that, while they may have been the target of the conversation, they were not taking part in it.

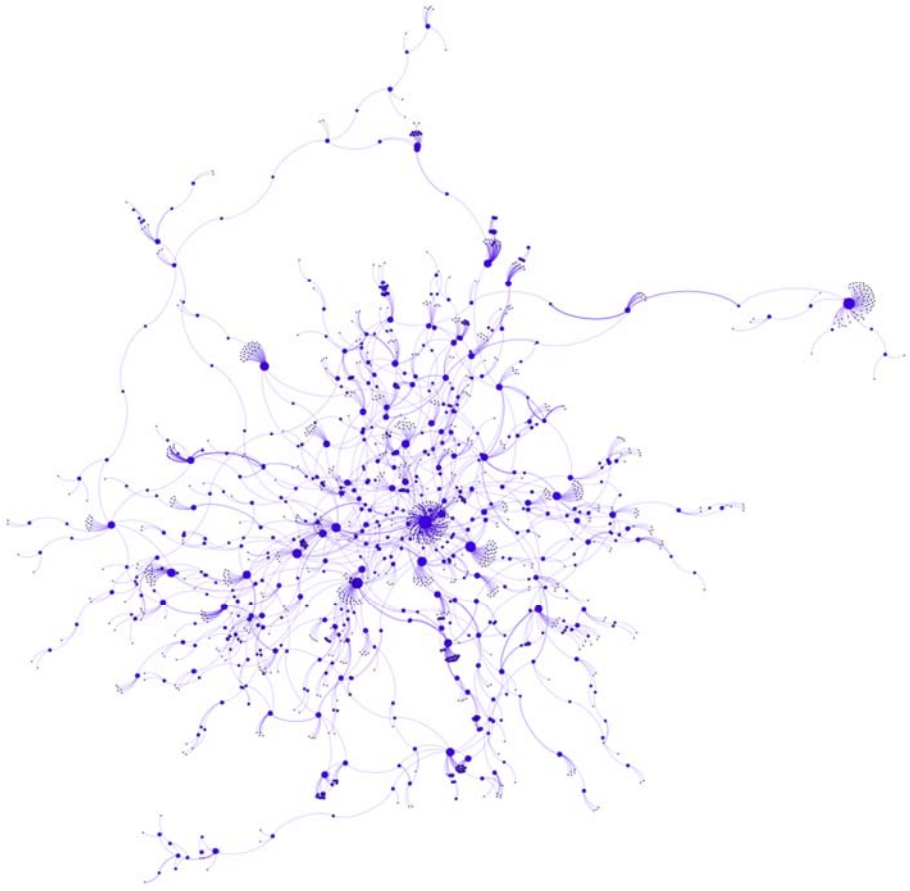

Figure 6. Sociogram Depicting the Largest Component of Conversations about "Crusader Alliance" (Nodes Sized by In-degree Centrality)

One can also use social network analysis to see which accounts might potentially be conduits of information. Analyzing the network as a graph can identify how often a node lies on the shortest path between other nodes by using betweenness centrality (Freeman, 1977). Figure 7 presents the network with nodes sized and colored by betweenness centrality. Many of the nodes that had higher betweenness

www.manaraa.com

centrality have had their accounts suspended. Of those that have not had their accounts suspended, some have already set up backup accounts in case their accounts become suspended. These accounts also had very little profile information, but, based on their tweets, they often engaged in conversations using sectarian language.

Figure 7. Sociogram Depicting the Largest Component of Conversations about "Crusader Alliance" (Nodes Sized and Colored by Betweenness Centrality)

More than perhaps any other analysis technique, relational analysis provides analysts with the connections between the individuals and the groups of individuals being studied. Analysts can focus on the "who" and "how" questions in order to identify leaders, detect subgroups, and uncover the brokers or bridges in the networks. Relationships are the foundation of most social media platforms (friends, followers, likes, retweets, etc.) and, thereby, provide a vast amount of data for analysis. This analysis focuses less on the timing or the location of the messages and more on the connections between users.

4.3.3 Temporal Analysis

One can also analyze this data temporally, and Figure 8 shows mentions of the phrase "Crusader Alliance" peaked on 11 August, 2015, with 2,381 occurrences. On that day, the most common hashtag among these tweets was about Aleppo where the United States reported conducting three airstrikes against ISIS. Table 2 summarizes the top ten hashtags from our collection on 11 August, 2015. Other prominent hashtags were "Atimah" and "Atimah_massacre" where an airstrike reportedly injured civilians inside a refugee camp. This incident prompted many in Turkey to criticize the Turkish Government for allowing the United States to use bases in Turkey as part of the campaign against ISIS; they framed the

www.manaraa.com

issue as Turkey's being complicit in a campaign in which those Twitter accounts may not have particularly agreed.

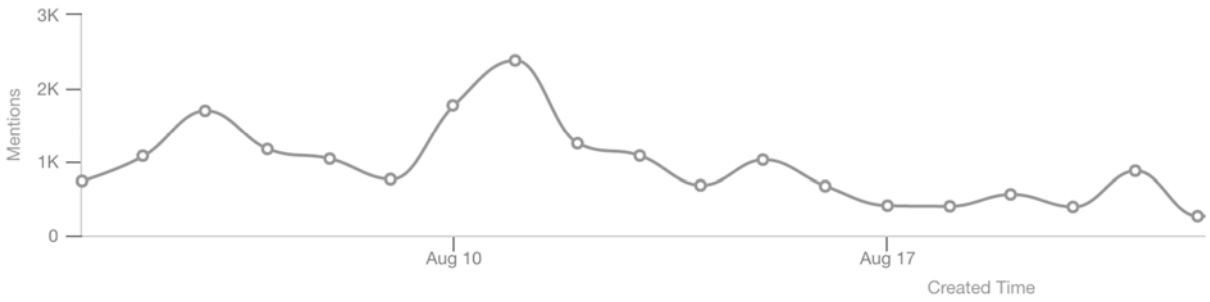

Figure 8. Timeline of Mentions of "Crusader Alliance" in Arabic from Twitter

Table 2. Counts of Hashtags from 11 August, 2015

Hashtag	Translation	Mentions
#حلب_ولايـة	Wilayet_Aleppo	223
#الخلافـــة_دولـة	State_Caliphate	219
#أطمة_مجزرة	Atimah_massacre	179
#عاجل	Urgent	169
#أطمة	Atimah	159
#الســـنة_جيـش	Sunna_Army	156
#إدلـب	Idlib	150
#الفتـــــح_جيـش	Army_conquest	117
#الشـــام_أحرار	Ahrar_alSham	110
#النصـــرة_جبهـة	Alnusra_front	104

Though many tweets might contain a hashtag framing an issue in a particular way, there still might not be many user accounts that use that hashtag. Maher and Carter (2014) are among many who have used Twitter to track and analyze ISIS-related sentiment and other activity. They found that just fewer than 20 percent of the tweets for a single hashtag campaign (#AllEyesOnISIS) originated from a small set of accounts, a participation asymmetry found elsewhere in political-based activism.

Temporal analyses allow analysts to focus on the "when" question by looking at a particular point in time or a particular period of time. Analysts can hone in on events both in social media and in the real world to uncover connections and relationships and, therefore, provide greater insight into the activities on social media relative to significant events in the real world. Temporal analysis focuses less on the relationships between accounts and more on those between the larger subgroups and groups.

4.3.4 Sentiment Analysis

In order to see how prevalent sectarian terms are in an overall conversation, one can use a word cloud to display the content of the conversation by counting how often different words appear (a form of sentiment analysis). Figure 9 presents a word cloud of the most frequent terms (we translated the original Arabic into English using Google Translate). "Crusader" and "Alliance" were the two most prominent terms because they were the search criteria. Also, the tweets often mentioned many place names. Of interest is that "Safavid" and "Alnasiri" are also common terms: they are some of the loaded sectarian terms that have framed the conflict in terms of the Sunni-Shia divide.

www.manaraa.com

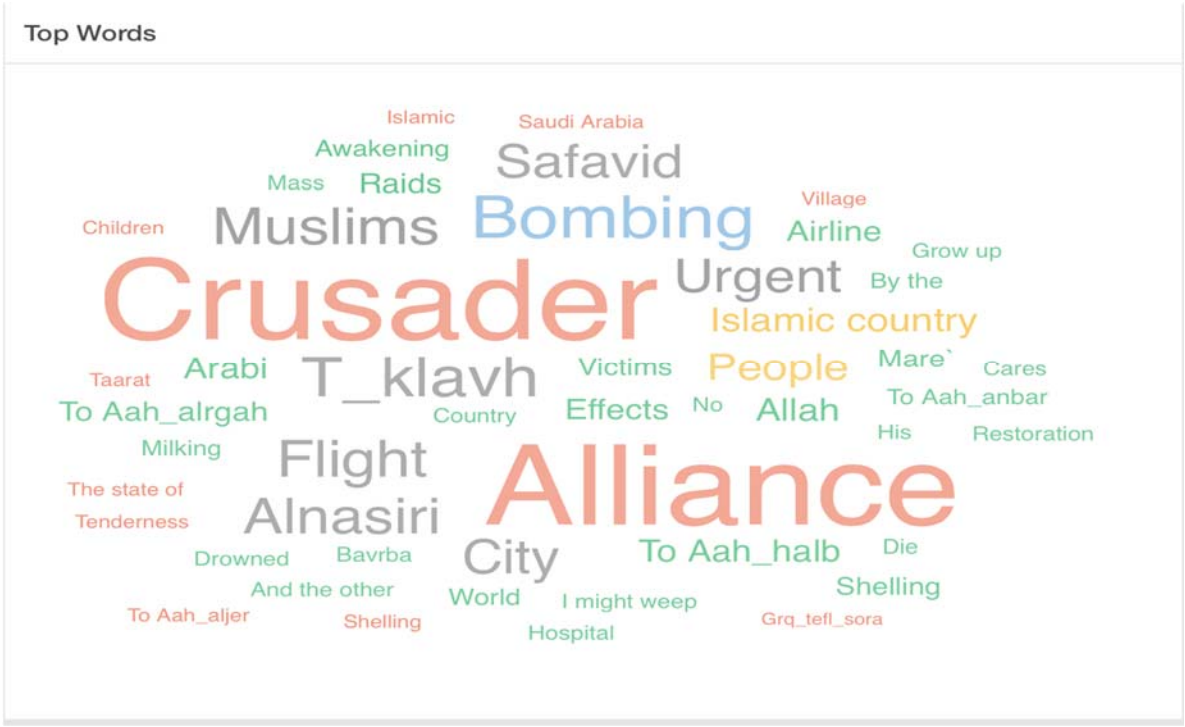

Figure 9. Word Cloud of the "Crusader Alliance" Conversations

Sentiment analysis extracts meaning from data by allowing one to view it in new ways. A word cloud is one method of viewing the social media data through the implied importance of the terms used in the actual posts. This type of analysis does not consider location (geospatial), account connection (relational), or timing (temporal) data. Other forms of sentiment analysis that focus on statements of fact versus statements of opinion provide analysts with insight into the feelings and the potential framing of the propaganda and arguments being made through social media.

4.3.5 Synthesis

This analysis looks at historic data, but one could automate and conduct much of it in real time. Dudas (2013, p. 631) provides examples of more complex visualization and mapping of tweets and data from other online and social media sources from Syria through "dynamic network visualization, a tweet wall post, and [a] map with geotagged tweets". Most importantly, Dudas generated this visualization and mapping in real time. Dudas found that external websites drive much of the Twitter activity, which means the Twitter activity is not original but rather a way of sharing existing content and information.

ISIS propaganda accounts often link to other websites that can anonymously host longer postings such as www.dump.to, an anonymous posting website similar to pastebin.com and Justpaste.it, a website that used to have much more ISIS-related postings until they started being deleted. ISIS also uses websites that can host videos as alternatives to YouTube, such as the Internet Archive.

ISIS has proven to be resilient in their use of social media. Many Twitter accounts have been suspended or shut down many times (frequently due to gruesome content). Still, when old accounts are shut down, new accounts continue to emerge. Some of these accounts will post information about their backup accounts to maintain communication in the event of a shutdown.

Overall, ISIS has successfully used social media to spread their influence. It has an organized mechanism and uses a variety of social media networks. It effectively uses social media to attack other groups and individuals, to report its on-ground battles and attacks, to provide evidence of its effective leadership and aid to the areas it controls, and to justify its actions. It does all of these things, of course, with the larger goal of gaining ideological and financial support from members and non-members.

www.manaraa.com

4.4 Adaptation of ISIS and its Use of Social Media

The social media activities of the insurgency have changed and adapted over the course of the Syrian conflict. Early in the conflict, new members of the insurgency would typically post YouTube videos in which they announced their defection from the Syrian military or government and often showed their government identification as further insult. While these groups did not necessarily join ISIS, they did create their own covert network in Syria. Lately, video postings show group events such as attacks, humanitarian efforts, and ideological speeches.

Additionally, over time, ISIS has used Twitter and Facebook less, but daily tweets about ISIS still number around 90,000 (Sanchez, 2015). The number has likely decreased due to the Assad Government's increased listening efforts on these public networks (Freeman & Schroeder, 2014). ISIS has turned to products such as Skype for video sharing and communication. No longer public, these messages are much harder to track and analyze, but not impossible (Faris, 2012).

As social media sites suspend ISIS and affiliated accounts, the effect is only temporary. New accounts are created, and they quickly regain their followers. The use of dump.to, as we describe above, allows individuals to anonymously post and disseminate content. Users post pictures of textual content, rather than the actual text, to avoid automated social media content analysis, translation, and queries. Still, this case study demonstrates some of the intelligence-gathering techniques in use that take advantage of the wealth of data available on social media. New analysis techniques will only improve the accuracy and effectiveness of the analysis going forward.

5 Discussion

Keeping track of social media accounts, especially new accounts, that are affiliated with a covert network is a difficult task; however, the network's interactions with other users may provide the ability to quickly identify these new accounts. As user accounts affiliated with a covert network are repeatedly shut down, the covert network needs a way to communicate to their members which accounts are the new accounts. One way in which these new accounts attract their audience is for affiliated accounts that have not been shut down to mention, or link to, the new account, which lets their followers know that the newly mentioned account is one that they should follow. This method makes it harder for researchers or analysts who simply read the tweets of popular accounts to quickly find out what account they should watch. However, a social network analysis of the mentioning of the new account creates a unique and very distinguishable pattern. In particular, it creates an area with a very high density of mentions when looking at a sociogram of the conversation (see Figure 10), which may make it easier for researchers or analysts to identify the new accounts. Nodes are user accounts, and the sociogram connects accounts if they send a message or re-post a message to another user account. Nodes are colored by a subgroup-detection algorithm. The green subgroup (in the center) largely includes ISIS-affiliated propaganda accounts.

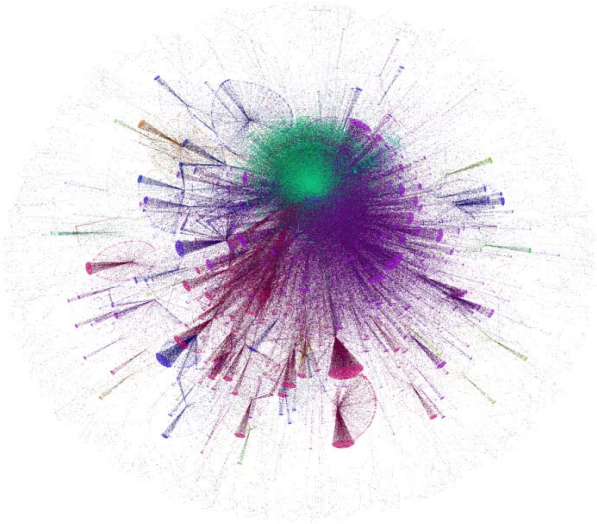

Figure 10. Sociogram of Twitter Conversation about ISIS

www.manaraa.com

While social media analysis provides an additional means of information gathering about covert networks, it only does so because those covert networks choose to post that information in a public setting. Additionally, depending on the country of interest, different social media platforms may contain more or less information. For example, to analyze actions carried out by the insurgency in Ukraine, more relevant information may be found on VK, a Russian social media platform, than other social media platforms. In order to conduct effective analysis using social media, one needs to understand whether the covert network uses social media platforms and, if so which ones.

The Syrian conflict and ISIS case study demonstrates covert networks' exploiting social media. Unfortunately, the nature of social media and the nature of covert networks' use of social media make this threat difficult to mitigate. In addition, social network analysis researchers often have limited control over their access to data sources and the quality of these data sources. Bright et al. (2012) argue that this inherent challenge, especially regarding research into covert networks, has a tendency to "foster opportunistic rather than theory driven research" (p. 153), a sentiment that Morselli (2009) also acknowledges. Theory does exist regarding the disruption of covert networks (McBride & Hewitt, 2013; Everton, 2012b; Roberts & Everton, 2011, 2016), but this case study concerns how covert networks (ISIS in particular) use social media and how one can use social media analyses to track and learn about them. The case study stops short of the strategies and tactics used to disrupt ISIS. Therefore, this descriptive case study (Yin, 1984) follows an opportunistic approach that would hopefully lead to better strategies and tactics for disruption based on identifying the network, its participants, and their connections. This research also has the potential to provide a more robust understanding about how covert networks frame their arguments and position as Snow et al. (1986) and Benford and Snow (2000) describe.

The social media analysis techniques we use here all have characteristics that limit their effectiveness. Of all the different methodologies that one can apply to social media data, geospatial analysis is currently the most limited. Activity location data are rarely available because most users do not enable the GPS feature on their mobile devices (Backstrom, Sun, & Marlow, 2010), and social media platforms would not collect these data from content created on devices without this feature. Because users can easily falsify profile information and have out-of-date profile information, profile locations are often inaccurate. However, a user can mention any location without actually being in that location at the time. Considering that most of the social media data are either missing geospatial information or may have inaccurate geospatial information, researchers must be skeptical about the data's validity.

Social media sites are built on the basis that interaction takes place, and social network analysis is an effective way to analyze interactions between entities (Freeman, 2004). However, one needs to understand the differences that exist between how people interact in the real world and how user accounts interact via social media (Kane, Alavi, Labianca, & Borgatti 2014). First, social media networks, due to the way in which they create nodes and connections, do not necessarily share the same characteristics of social networks found in society. Second, not all user accounts are individuals. Third, not everyone who follows an account actually knows the account holder. Still, relational analysis is a common methodology for analyzing social media data. In addition, social media users can intentionally create noise and false connections by interacting with random, unconnected accounts, and they can create false and misleading posts to thwart effective observation.

There are serious limitations to effective sentiment analysis as a result of idioms, sarcasm, double negatives, innuendos, foreign words/phrases, cultural references/idiosyncrasies, and homonyms/homographs. As a result, researchers have begun using machine learning and powerful language parsing tools to increase the efficacy of sentiment analysis techniques (Paltaglou, 2014).

Additionally, individuals often use social media for real-time communication, planning, and coordination. If the analysis is not available in real time, appropriate and effective countermeasures and reactions are not possible (Everton, 2012a). Covert networks and their supporters and followers will attempt to fool the intelligence community and evade detection by using multiple social media accounts, fake accounts, and misleading information (Roberts, 2011; McBride & Hewitt, 2013). New analysis techniques will only improve the accuracy and effectiveness of the analysis going forward.

Based on recent history, we can reasonably assume that social media platforms and functionality will continue to evolve. They will become faster and easier to use and provide new functionality, which will them more attractive to these covert networks (Everton 2012a). So long as the leadership and members of these covert networks perceive that their posts are not being analyzed, they will have no reason to change their operations. However, once they feel threatened, the covert networks will move on to other

www.manaraa.com

social media networks and, thus, stay one step ahead of those who attempt to track them. As such, to mitigate this threat, the intelligence community needs to continue to stay abreast of the technological revolution that is social media (Freeman & Schroeder, 2014).

Dudas (2013) addresses three areas for future research. The first uses a sentiment lexicon to rate keywords on a positive/negative scale and then maps these keywords against the target keyword over time. Figure 11 provides an example of this sentiment analysis.

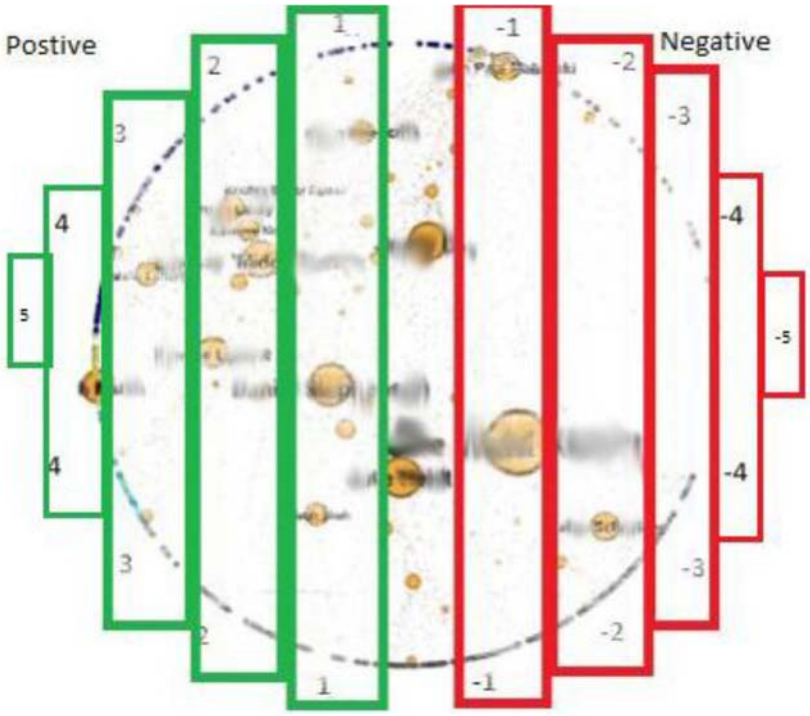

Figure 11. A Markup of the Sentiment Visualization (Dudas, 2013)

Another area attempts to extend the analysis of social networks beyond username → username connections. Using username → hashtag and hashtag → hashtag connections will hopefully lead to new insights into the structure of covert networks. A third area looks to further enhance existing temporal data visualization functionality to allow for prediction and forecasting through machine learning. It is not sufficient to only look at historical or even real-time data; staying ahead of the covert networks and their potential activity is critical to successful counter-efforts.

In addition to developing new social media analysis techniques or attempting to guess where covert networks will turn to next in terms of their social media usage, some in the intelligence community believe that one can use social media itself to counter and alienate the covert networks by reframing the covert networks' messages and turning public opinion against them (Kilcullen, 2010; Everton, 2012a). Those outside of the intelligence community have also entered this fight by attempting to disrupt or shut down known ISIS accounts and followers—a form of justified hacking (Freeman & Peace, 2005)—as the recent success of the hacking group Anonymous evidences (Petroff, 2015).

6 Conclusion

Covert networks can exploit social media—especially due to its being available to nearly anyone with Internet access—to foster membership, communicate among followers and non-followers, and obtain ideological and financial support. The intelligence community can track and analyze these covert networks' use of social media via a variety of tools and techniques, but the analysis is imperfect and incomplete. Our case study of the Syrian conflict, the emergence of ISIS, and ISIS's use of social media provide examples of the current state of affairs regarding the use of social media by this particular covert network.

In our analysis, we provide maps of the groups' communication patterns and identify potentially influential user accounts. This new intelligence will hopefully lead to informed operational decisions and greater

www.manaraa.com

success in combatting these covert networks. However, these covert networks also continue to adapt and remain difficult to track. New user accounts are quickly created when existing accounts are shut down, and these new accounts regain the followers of the former accounts. While one can mitigate the threat, one cannot eliminate it.

As long as the leaders and members of covert networks believe the benefits of using social media outweigh the negatives, these opposition groups will continue to use social media to frame their messages and communicate with their followers. These groups will continue to adapt and improve how they use social media in an attempt to remain hidden from governments, the intelligence community, and law enforcement. As such, we need additional advances in social media analysis to continue this ongoing battle.

Acknowledgments

We pulled much of the content for the Syrian Conflict/ISIS case study from a project funded by the Office of the Secretary of Defense Rapid Reaction Technology Office (RRTO) and conducted by the Common Operational Research Environment (CORE) Lab, located in the Defense Analysis Department at the Naval Postgraduate School. Established in 2007, the CORE Lab directly supports students, operational units, field operatives, and analysts by developing their knowledge, skills, and abilities to implement the CORE Lab's primary methodologies. The CORE Lab develops and teaches methods to map out the human domain—primarily focused on covert networks (i.e., illegal or covert networks)—by advancing three primary types of analysis: social network, geospatial, and temporal analysis. The CORE Lab is sponsor funded and always looking for opportunities for collaboration.

www.manaraa.com

References

Ajmera, H. (2014). Social media 2014 statistics—an interactive infographic you've been waiting for! *Digital Insights*. Retrieved from http://blog.digitalinsights.in/social-media-users-2014-stats-numbers/05205287.html

Atkinson, M., & Wein, L. (2010). An overlapping networks approach to resource allocation for domestic counterterrorism. *Studies in Conflict and Terrorism*, *33*, 618-651.

Backstrom, L., Sun, E., & Marlow, C. (2010). Find me if you can: Improving geographical prediction with social and spatial proximity. In *Proceedings of the 19th International conference on World Wide Web* (pp. 61-70).

Benford, R., & Snow, D. (2000). Framing processes and social movements: An overview and assessment. *Annual Reviews of Sociology*, *26*, 611-639.

Bollen, J., Mao, H., & Zeng, X. (2011). Twitter mood predicts the stock market. *Journal of Computational Science*, *2*(1), 1-8.

Bright, D., Hughes, C., & Chalmers, J. (2012). Illuminating dark networks: A social network analysis of an Australian drug trafficking syndicate. *Crime, Law and Social Change*, 57, 151-176.

Brynley-Jones, L. (2014). 8 useful social media statistics for 2015. *Our Social Times*. Retrieved from http://oursocialtimes.com/8-useful-social-media-statistics-for-2015/

Cheong, M., & Lee, V. (2011). A microblogging-based approach to terrorism informatics: Exploration and chronicling civilian sentiment and response to terrorism events via Twitter. *Information Systems Frontiers*, *13*(1), 45-59.

de Smith, M., Goodchild, M., & Longley, P. (2007). *Geospatial analysis: A comprehensive guide to principles, techniques and software tools* (2nd ed.). Leicester, UK: Matador.

Di Leonardo, A., Fairgrieve, S., Gribble, A., Prats, F., Smith, W., Sweat, T., Usher, A., Woodley, D., & Cozzens, J. (2014). Identifying locations of social significance: Aggregating social media content to create a new trust model for exploring crowd sourced data and information. In G. Meiselwitz (Ed.), *Social computing and social media* (pp. 170-177). Switzerland: Springer International Publishing.

Dudas, P. (2013). Cooperative, dynamic Twitter parsing and visualization for dark network analysis. In *Proceedings of iConference* (pp. 623-632).

Everton, S. (2012a). Contemplating the future of social media, dark networks, and counterinsurgency. *Combating Terrorism Exchange, 2*(4), 69-73.

Everton, S. (2012b). *Disrupting dark networks.* New York: Cambridge University Press.

Fan, W., & Gordon, M. (2014). The power of social media analytics. *Communications of the ACM*, *57*(6), 74-81.

Faris, S. (2012). The hackers of Damascus. *Bloomberg Businessweek.* Retrieved from http://www.businessweek.com/articles/2012-11-15/the-hackers-of-damascus

Finkel, S. E. (1995). *Causal analysis with panel data*. Thousand Oaks, CA: Sage.

Freeman, G., & Schroeder, R. (2014). *Social media exploitation: An assessment*. Monterey, CA: CORE Lab.

Freeman, L. (1977). A set of measures of centrality based on betweenness. *Sociometry*, *40*(1), 35-41.

Freeman, L. (2004). *The development of social network analysis: A study in the sociology of science.* Vancouver: Empirical Press.

Freeman, L., & Peace, A. (2005). Revisiting Mason: The last 18 years and onward. In L. Freeman & A. Peace (Eds.), *Information ethics: Privacy and intellectual property* (pp. 1-18). Hershey, PA: Idea Group Publishing.

Freeman, M. (2011). The sources of terrorist financing: Theory and typology. *Studies in Conflict and Terrorism*, *34*(6), 461-475.

www.manaraa.com

Freeman, M., & Ruehsen, M. (2013). Terrorism financing methods: An overview. *Perspectives on Terrorism*, 7(4), 5-26.

Goodchild, M. (2007). Citizens as sensors: The world of volunteered geography. *GeoJournal*, 69, 211-221.

Gordon, M. (2013). Aim of U.S. attack: Restore a "red line" that became blurred. *The New York Times*. Retrieved from http://www.nytimes.com/2013/08/30/world/middleeast/aim-of-a-us-attack-on-syria-sharpening-a-blurred-red-line.html

Hannan, M., & Tuma, N. (1979). Methods for temporal analysis. *Annual Review of Sociology*, *5*, 303-328.

Hansen, D., Shneiderman, B., & Smith, M. (2010). *Analyzing social media networks with NodeXL: Insights from a connected world.* Boston: Morgan Kaufmann.

Holliday, J. (2011). *The struggle for Syria in 2011*. Washington, DC: Institute for the Study of War.

Holliday, J. (2012a). *Syria's armed opposition*. Washington, DC: Institute for the Study of War.

Holliday, J. (2012b). *Syria's maturing insurgency*. Washington, DC: Institute for the Study of War.

Hwaida, S., & Cowell, A. (2014). Assad begins a third term in Syria, vowing to look after its people. *The New York Times*. Retrieved from http://www.nytimes.com/2014/07/17/world/middleeast/assad-sworn-in-for-third-term-as-syrian-president.html

Jackson, M. (2008). *Social and economic networks*. Princeton, NJ: Princeton University Press.

Kane, G., Alavi, M., Labianca, G., & Borgatti, S. (2014). What's different about social media networks? A framework and research agenda. *MIS Quarterly*, *38*(1), 275-304.

Kaplan, A., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59-68.

Kaplan, E. (2010). Terror queues. *Operations Research*, 58, 773-784.

Keefe, P. (2006). Can network theory thwart terrorists? *The New York Times*. Retrieved from http://www.nytimes.com/2006/03/12/magazine/312wwln_essay.html

Kilcullen, D. (2010). *Counterinsurgency*. Oxford: Oxford University Press.

Krebs, V. (2002). Mapping networks of terrorist cells. *Connections*, 24(3), 43-52.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What is Twitter, a social network or a news media? In *Proceedings of the 19th International Conference on World Wide Web* (pp. 591-600).

Kwon, K. H., Oh, O., Agrawal, M., & Rao, H. R. (2012). Audience gatekeeping in the Twitter service: An investigation of tweets about the 2009 Gaza conflict. *AIS Transactions on Human-Computer Interaction, 4*(4), 212-229.

Lee, J., Agrawal, M., & Rao, H. R. (2015). Message diffusion through social network service: The case of rumor and non-rumor related tweets during Boston bombing 2013. *Information Systems Frontiers, 17*, 997-1005.

Liu, B. (2010). Sentiment analysis and subjectivity. In N. Indurkhya & F. Damerau (Eds.), *Handbook of natural language processing* (2nd ed., pp. 627-665). Cambridge: Taylor & Francis Group.

Long, J. S. (1997). *Regression models for categorical and limited dependent variables*. Thousand Oaks, CA: Sage.

Lynch, M., Freelon, D., & Aday, S. (2014). *Blogs and bullets III: Syria's socially mediated civil war.* Washington, DC: United States Institute of Peace.

Mahamood, M., & Black, I. (2013). Free Syrian Army rebels defect to Islamist group Jabhat al-Nusra. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/may/08/free-syrian-army-rebels-defect-islamist-group

Maher, S., & Carter, J. (2014). Analyzing the ISIS "Twitter storm". *War on the Rocks*. Retrieved from http://warontherocks.com/2014/06/analyzing-the-isis-twitter-storm/

McBride, M., & Hewitt, D. (2013). The enemy you can't see: An investigation of the disruption of dark networks. *Journal of Economic Behavior & Organization*, *93*, 32-50.

www.manaraa.com

Meraz, S., & Papacharissi, Z. (2013). Networked gatekeeping and networked framing on #Egypt. *The International Journal of Press/Politics*, *18*(2), 138-166.

Miffen, T., Boner, C., Godfrey, G., & Skokan, J. (2004). A random graph model for terrorist transactions. In *Proceedings of the IEEE Aerospace Conference* (pp. 3258-3264).

Milward, H., & Raab, J. (2006). Dark networks as organizational problems: Elements of a theory. *International Public Management Journal*, *9*(3), 333-360.

Morrison, K. (2014). The growth of social media: From passing trend to international obsession. *SocialTimes*. Retrieved from http://www.adweek.com/socialtimes/the-growth-of-social-media-from-trend-to-obsession-infographic/142323

Morselli, C. (2009). *Inside criminal networks*. New York: Springer.

Natarajan, M. (2006). Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. *Journal of Quantitative Criminology*, 22(2), 171-192.

O'Bagy, E. (2012a). *Backgrounder: Syria's political struggle*. Washington, DC: Institute for the Study of War.

O'Bagy, E. (2012b). *Jihad in Syria*. Washington, DC: Institute for the Study of War.

O'Bagy, E. (2012c). *Syria's political opposition*. Washington, DC: Institute for the Study of War.

Paltaglou, G. (2014). Sentiment analysis in social media. In N. Agarwal, M. Lim, & R. T. Wigand (Eds.), *Online collective action: Dynamics of the crowd in social media* (pp. 3-17). New York: Springer.

Petroff, A. (2015). Anonymous: We've taken down 800 ISIS Twitter accounts. *CNN Money*. Retrieved from http://money.cnn.com/2015/02/10/technology/anonymous-isis-hack-twitter/

Raab, J., & Milward, H. (2003). Dark networks as problems. *Journal of Public Administration Research and Theory*, *13*(4), 413-439.

Reid, E., Chen, H., & Xu, J. 2007. Social network analysis for terrorism research. In H. Chen, T. S. Raghu, R. Ramesh, A. Vinze, & D. Zeng (Eds.), *Handbook in information systems: National security* (pp. 243-270). Oxford: Elsevier.

Reynolds, S., & Caris, C. (2014). *Middle East security report 22: ISIS governance in Syria.* Washington, DC: Institute for the Study of War.

Roberts, N. (2011). Tracking and disrupting dark networks: Challenges of data collection and analysis. *Information Systems Frontiers*, *13*(1), 5-19.

Roberts, N., & Everton, S. (2011). Strategies for combating dark networks. *Journal of Social Structure*, 12(2), 1-32.

Roberts, N., & Everton, S. (2016). Monitoring and disrupting dark networks: A bias toward the center and what it costs ss. In A. Dawoody (Ed.), *Eradicating terrorism from the Middle East: Policy and administrative approaches* (pp. 29-42). New York: Springer.

Rodriguez, J. (2005). *The March 11th terrorist network: In its weakness lies its strength*. Barcelona, Spain: Departament de Sociologia i Anàlisi de les Organitzacions, Universitat de Barcelona.

Sageman, M. (2004). *Understanding terror networks*. Philadelphia, PA: University of Pennsylvania Press.

Sanchez, R. (2015). Authorities: Three men attempted to join ISIS, had ambitious plans. *CNN*. Retrieved from http://www.cnn.com/2015/02/25/us/new-york-terror-plot/index.html

Schmidt, C. (2012). Using social media to predict and track disease outbreaks. *Environmental Health Perspectives*, 120(1), A30-A34.

Schroeder, R., Everton, S., & Shepherd, R. (2012). Mining Twitter data from the Arab Spring. *Combating Terrorism Exchange*, *2*(4), 56-64.

Schroeder, R., Everton, S., & Shepherd, R. (2014). The strength of Tweet ties. In N. Agarwal, M. Lim, & R.T. Wigand (Eds.), *Online collective action: Dynamics of the crowd in social media* (pp. 179-196). New York: Springer.

www.manaraa.com

Senekal, B. (2014). Mapping a dark network with social network analysis (SNA): The right wing Vaal Dam bomb plot. *Journal for Contemporary History*, *39*(1), 95-114.

Shellman, S., Covington, M., & Zangrilli, M. (2014). Sentiment & discourse analysis: Theory, extraction, and application. In C. Ehlschlaeger (Ed.), *Socio-cultural analysis with the RSI paradigm* (pp. 66-82). Vicksburg, MS: U.S. Army Engineer Research and Development Center.

Shneiderman, B., Preece, J., & Pirolli, P. (2011). Realizing the value of social media requires innovative computing research. *Communications of the ACM*, *54*(9), 34-37.

Smith, C. (2015). By the numbers: 250+ amazing Twitter statistics. *Digital Advertising*. Retrieved from http://expandedramblings.com/index.php/march-2013-by-the-numbers-a-few-amazing-twitter-stats/

Snow, D., Rochford, E., Worden, S., & Benford, R. (1986). Frame alignment processes, micromobilization, and movement participation. *American Sociological Review*, *51*(4), 464-481.

Sparrow, M. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, *13*(3), 251-274.

Starbird, K., & Palen, L. (2012). (How) will the revolution be retweeted? Information diffusion and the 2011 Egyptian uprising. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work.*

Starbird, K., Muzny, G. & Palen, L. (2012). Learning from the crowd: Collaborative filtering techniques for identifying on-the-ground Twitters during mass disruptions. In *Proceedings of the Conference on Information Systems for Crisis Response and Management.*

Stefanidis, A., Crooks, A., & Radzikowski, J. (2013). Harvesting ambient geospatial information from social media feeds. *GeoJournal*, *78*, 319-338.

Surowiecki, J. (2005). *The wisdom of crowds*. New York: Anchor Books.

Sutton, J., Gibson, C. B., Phillips, N. E., Spiro, E. S., League, C., Johnson, B., Fitzhugh, S. M., & Butts, C. T. (2015). A cross-hazard analysis of terse message retransmission on Twitter. *Proceedings of the National Academy of Sciences*, *112*(48), 14793-14798.

Syrian National Council. (2012). *Syrian National Council*. Retrieved from http://www.syriancouncil.org

Syrian Revolution Martyr Database. (2011). *Martyr statistics. Retrieved from* http://syrianshuhada.com

Topol, S. (2012). Syria's rebels raise funds online. *Bloomberg Businessweek*. Retrieved from http://www.businessweek.com/articles/2012-10-18/syrias-rebels-raise-funds-online#p2

van Meter, K. (2001). Terrorists/liberators: Researching and dealing with adversary social networks. *Connections*, *3*, 66-78.

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications.* New York: Cambridge University Press.

Xu, J., & Chen, H. (2008). The topology of dark networks. *Communications of the ACM*, *51*(10), 58-65.

Xu, J., Marshall, B., Kaza, S., & Chen, H. (2004). Analyzing and visualizing criminal network dynamics: A case study. In H. Chen, R. Moore, D. D. Zeng, & J. Leavitt (Eds.), *Intelligence and security informatics* (LNCS, vol. 3073, pp. 359-377). Berlin: Springer.

Yin, R. (1984). *Case study research: Design and methods*. Beverly Hills, CA: Sage.

Yurdusev, A. (1993). “Level of analysis” and “unit of analysis”: A case for distinction. *Millennium Journal of International Studies*, 22(1), 77-88.

www.manaraa.com

About the Authors

Lee A. Freeman is an Associate Professor of Management Information Systems in the College of Business at The University of Michigan–Dearborn. He has a B.A. from The University of Chicago, and he received both his MBA. and PhD in Information Systems from Indiana University. His teaching interests include systems analysis and design, information technology strategy, and information technology policy; his primary research interests include online pedagogy, systems analysis and design, and information technology in sports. He has published over 35 refereed manuscripts in journals and at conferences, including *MIS Quarterly*, the *Communications of the ACM*, the *Journal of Information Systems Education*, and the *Communications of the Association for Information Systems*, among others. He is currently the Editor-in-Chief of the *Journal of Information Systems Education*.

Robert Schroeder is a Research Associate in the CORE Lab within the Defense Analysis Department at the Naval Postgraduate School (NPS) where he focuses on analyzing big data using statistics, social network analysis, geospatial analysis, and temporal analysis. Prior to working at the Naval Postgraduate School, he received a MA in International Policy with a focus on Conflict Resolution at the Monterey Institute of International Studies (2011) and a B.A. in International Relations at Boston University (2008). He is currently researching how to use open source information gathered largely from social media in order to understand and map the Syrian opposition as well as looking at how different types of external support to insurgencies relate to length of conflicts and the ways in which those conflicts end. Besides doing research, he also has helped train members of the Joint Special Operations Task Force – Philippines (JSOTF-P) in collecting relational information using smart phones and tablets and analyzing that information using social network analysis.

Sean F. Everton is an Associate Professor in the Department of Defense Analysis at the Naval Postgraduate School (NPS). Prior to joining NPS in 2007 he was an adjunct professor at both Santa Clara University and Stanford University. He earned his M.A. and PhD in Sociology at Stanford University (2007) and wrote his doctoral thesis on causes and consequences of status on the economic performance of venture capital firms. He has published articles in the areas of social network analysis, sociology of religion, economic sociology, and political sociology, and he currently specializes in the use of social network analysis to track and disrupt covert networks (i.e., criminal and terrorist networks). His monograph, *Disrupting Dark Networks*, was published by Cambridge University Press in 2012. His latest book (written with Daniel Cunningham and Philip Murphy), *Understanding Dark Networks*, was published by Rowman and Littlefield in 2016.

Copyright © 2017 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints or via e-mail from publications@aisnet.org.

www.manaraa.com