Exploiting VKontakte to better understand the Caucasus Emirate's tactics, techniques, and procedures

Milan Villarreal
National Security Studies Institute
University of Texas at El Paso
April 2, 2015

Executive Summary

- Social media intelligence (SOCMINT) is the collection, processing, analysis and reporting of social media information for the benefit of law enforcement and security agencies.
- Foreign terrorist organizations such as the Caucasus Emirate use foreign social media platforms such as VKontakte (VK) for the purpose of spreading propaganda and recruiting new members.
- The Caucasus Emirate has had an online presence since established by a group of the mujahedeen of the Northern Caucasus in 2007, and has had a history of successful attacks, claiming responsibility for the Moscow metro bombings in 2010 and the Domodedovo airport bombings in 2011.
- Successful SOCMINT can be better performed with a dedicated team of experts consisting of intelligence analysts, legal experts, social media content experts, and regional, cultural and language experts.
- Public and private groups/communities on VK that are dedicated to terrorist related themes are an ample source for discovering profiles of interest.
- Sharing music is a technique used by jihadists to further enhance propaganda and attract young supporters online. Art and self-expression is a constant theme among youth on VK, and this is no exception for Islamic youth. Cultural experts can gain further insight into the lives of terrorist groups by understanding such music, its lyrics, and origins.

1. INTRODUCTION

Social media is an ever-changing industry and a growing means of communication for criminals. Terrorist groups like the Islamic State of Iraq and Syria (ISIS) use online social networks such as Facebook to disseminate their propaganda and recruit new members around the globe. Statistically ISIS uses Twitter more than any other social networking site to promote its cause and communicate with followers.[1] Malevolent individuals and organizations are not limited to only one social networking platform and terrorist groups from Russian speaking nations, specifically in the northern Caucasus, are likely to use social media platforms that are unknown to the average American. The top five social media sites used by Russians in order of popularity are: VKontakte (VK), Odnoklassniki, Mail.Ru - My World, Facebook, and Twitter.[2] Examining foreign social media platforms like VKontakte can provide a window into the functioning of terrorist groups and the networks using them.

Criminals are not the only ones using social-media, as investigators and analysts are also developing strategies to harness the power of social media. Social Media Intelligence (SOCMINT) is the collection, processing, analysis and reporting of social media information for the benefit of law enforcement and security agencies.[3] There are numerous SOCMINT gathering methods with various analytical applications. This paper will present some of the essential SOCMINT methodologies available to security professionals, and select a specific methodology to research the Russian terrorist group known as the Caucasus Emirate.

The central research question that this project answer is: How can counter-terror investigators and analysts use the social networking site VKontakte (VK) to better understand the Caucasus Emirate's tactics, techniques, and procedures?

---

[1] Ajbaili, Mustapha. "How ISIS conquered social media", *Al Arabiya News*, 24 June 2014, accessed on 2/3/2015, http://english.alarabiya.net/en/media/digital/2014/06/24/How-has-ISIS-conquered-social-media-.html

[2] "Top 5 social networks in Russia: Traffic and time spent" *Digital Strategy Consulting Limited*, 11/09/2013, accessed on 02/03/2015, http://www.digitalstrategyconsulting.com/intelligence/2013/09/top_5_social_networks_in_russia_traffic_and_time_spent.php 1/2

[3] Antonius, Nicky, and Rich, L. "Discovering collection and analysis techniques for social media to improve public safety." *The International Technology Management Review* 3, no. 1 (2013): 45.

The study intends to reflect an intelligence report, with the aim of being a usable reference for working investigators and intelligence analysts. The research implements an open source SOCMINT gathering method by using the VKontakte (VK) social networking platform. VK was chosen among all other social networking sites because of its popularity among native Russian speakers. The type of data gathered lends the research toward qualitative content analysis. The purpose of the study is to gather enough data to form a set of hypotheses on the tactics, techniques, and procedures targets implement in their support of terrorist goals.

Key Terms

For the purpose of this research tactic, technique and procedure will be defined as follow:

- *Tactic* – a method used for the implementation of an operational strategy. For example, the spread of propaganda on social media for the recruitment of new terrorist members abroad.
- *Technique* – a specific action or path taken to reach a goal, applicable within grand, operational, and tactical strategies. For example, the display of shocking images online to gain media attention and popularity.
- *Procedure* – a set of actions that managers within an organization want its members to implement. For example, the steps terrorists are taught in order to remain anonymous online.[4]

2. SOCIAL MEDIA INTELLIGENCE (SOCMINT)

Criminal investigators and analysts are ever increasing their use of social media as a tool to thwart crime and gather evidence for prosecutions. There are numerous SOCMINT gathering methods with various analytical applications.

[4] Drew, Dennis, and Snow, Donald. "Making Twenty-First-Century Strategy: an introduction to modern national security processes and problems", *Air University Press*, Maxwell Air Force Base, Alabama, (2006): 24-26.

2.1 *Open Source Collection*

Intelligence experts tend to consider social media as a subset tool of open source intelligence (OSINT). Social network platforms often openly provide a wealth of data and statistics on their websites, giving investigators access to the same tools usable by marketing groups. These tools are called social media analytics, and range from advertisers monitoring track attitudes on brand names to companies that monitor their social media reputation. Gephi is one example of a popular analytic software package. It provides visualizations for better comprehension of large data sets. Through the use of such software packages, SOCMINT can "illuminate the behavior of certain groups of interest, such as emerging topics within group-specific conversations and how the group reacts to a specific, perhaps volatile, event."[5] Social media data sets are often very large, which makes computational approaches to extract meaningful information helpful.

In addition to a computational approach, human analysts can view user content for themselves. Social media conversations and images are often posted online for the viewing public. Criminals and terrorists regularly post self-criminalizing evidence, most often to boast about their ideology or achievements. When such evidence is posted online it becomes valuable to prosecutors, and can also be used to build behavioral profiles on individuals and groups. According to scholar Daniel Trottier, "social media amplify policing not because of their technological sophistication, but rather because of their social saturation."[6] Through public display, the social lives of various criminals and terrorists can be analyzed, possibly leading to clues regarding their techniques, intents, and future actions.

Many social networks give users the ability to "tag" or link other users, in posts and images. Thus incriminating evidence can be posted unintentionally through "friends". This connection of information is called social creeping. Trottier describes how social creeping branches out, implicating suspects unknowingly, in effect aiding media policing efforts. This can happen when an individual on a social network posts a picture or comments about a friend, providing useful information that the individual of interest

[5] Ibid. 46.
[6] Trottier, Daniel. "Policing social media." *Canadian Review of Sociology,* 49, no. 4 (2012): 412.

would not have otherwise divulged. As social creep develops, the online community becomes aware of suspicious individuals, possibly alerting law enforcement officials or media outlets. Thus the policing of social networks, that is to say the monitoring of criminal activity by investigators and the general public, becomes a natural regulatory process that stems from the network itself.

The growth of SOCMINT techniques also poses a series of important ethical questions. One former senior British intelligence official recommends that SOCMINT "should be based wherever possible on the clearest possible mandate of informed consent. The most preferred route is to access explicitly 'consenting' information from the online community."[7] Social media sites make their policies available online, explaining how investigators can acquire subpoenas and gain access to restricted files. However, there is no law against investigators using covert social profiles, unless a legal counsel represents an individual of interest. Even then, covert SOCMINT gathering should only take place as a last resort, when essential information cannot be reasonably obtained through other methods.

2.2 *Covert Collection*

The purpose of covert SOCMINT is to gain access to restricted and private social media profiles and information. A large amount of information displayed online is only privileged to "friends" that are accepted within a user's network. There are multiple methods to get around this restriction, and one in particular involves the use of false social media profiles, otherwise known as sock puppets. Sock puppets involve the creation of elaborate false identities that can observe and engage with targets online. However, before creating a sock puppet account an investigator must first develop a safe online intelligence gathering protocol.

When online, no matter the activity, investigators should always implement safe and secure protocols. Not using one's own personal or work email address and regularly deleting cookies and browser history are just a few of the basic principles investigators

[7] Omand, David, Jamie Bartlett, and Carl Miller. "Introducing social media intelligence (SOCMINT)." *Intelligence and National Security* 27, no. 6 (2012): 822.

should utilize. Remaining anonymous online is the best method of protecting one's self and organization. Anonymity also helps keep an investigation safe from compromise. To remain anonymous online, investigators should use a separate and secure computer, dedicated to covert SOCMINT activity. Investigators should only use public IP addresses, and for further security use proxy servers to scramble location data. Programs such as "Tor" give users anonymity online by directing internet traffic through more than six thousand relays, thus allowing the user to conceal their location.

In addition to safe and anonymous web use, investigators must develop strong documentation and storage policies. Screen-capture and screen-recording programs such as "Screenr" are free to use and are important for keeping detailed records of all activity. During an investigation information needs to be continuously saved, as users online will often delete important conversations, images, and whole profiles. Once a secure online protocol and a record keeping method are developed, investigators can begin in the creation of false identities for sock puppet accounts.

There are generally three steps in creating a sock puppet. First, the false profile must be designed in detail, with specifics such as date of birth, location of birth, religious background, hobbies, and more. Programs such as "Facenamegenerator.com" and "Identitygenerator.com" can create 100 profiles at a time and export them in Excel format. Spreadsheet programs can then be used to keep track of multiple identities. The second step is to open a user account on the social platform of interest. It is important to understand the social network program thoroughly and this may require consultation with internet content experts. The third step is the validation of the false identity. This is most often done through the creation of an email account, a phone number, and the purchase of a prepaid credit card. In some cases this third step may be necessary before a user account can be created.

Once a sock puppet account is developed investigators can begin using various techniques to befriend users and groups of interests. Investigators can also become "befriended" through a deceptive method that utilizes a target's own friend against them. This technique involves copying the profile picture of the target's friend, and using the image to create a mimicking account of that friend. Then using the mimicking account, an investigator may request friendship to the target. The target will accept the friend

request believing it is the same individual friend from before, but with an updated account. Befriending a target's profile gives access to a multitude of conversations, images, and videos, which can lead to information regarding the behavior, personality, and location of an individual. Much of this information can seem overwhelming, but it is important for the investigator or analyst to remain focused on the gold nuggets of vital information. Important information will most likely stem from communications with the target's inner circle, the three to five main individuals with which the target regularly converses.

2.3 *SOCMINT Analysis*

Social media intelligence gathering often provides a vast amount of information. Once organized the data can be better used to formulate hypotheses. Data analysis seeks to join "information from different sources in planning for the formulation of inferences."[8] Below is a summary of various techniques that can be used to make sense of information gathered through SOCMINT.

- *Link Charting* – shows the association between entities highlighting in the investigation.
- *Event Charting* – shows the chronological associations between entities or sequences of events.
- *Commodity Flow Charting* – explores the movement of money, stolen goods, narcotics, or other commodities.
- *Activity Charting* – identifies activities involved in a criminal operation.
- *Financial Profiling* – identifies hidden income of business entities or individuals and to identify indicators of economic crime.
- *Frequency Charting* – organize, summarize and interpret quantitative information.
- *Data Correlation* – illustrates the associations between different variables.[9]

[8] *Social Media Intelligence Analyst Manual*, Version V.1. 2014. McAfee Institute Inc., Saint Louis, MO, USA, 21.
[9] Ibid. 21.

Social media intelligence can be considered a subset of communications intelligence, and a non-literal intelligence discipline. A useful way to analyze SOCMINT is content analysis, that is to say, the "systematic counting, assessing, and interpreting of the form and substance of communication, with three levels of analysis: first word analysis, theme analysis, and item analysis."[10] Foreign themes and languages can make analysis challenging and require the use of search dictionaries, data libraries, and cultural, regional, and language experts.

As information is gathered and organized it can often display a pattern. Patterns can be used to make assumptions and develop hypotheses for testing. Social patterns, for example, provide information on the social profiles of individuals or whole groups of interest. Analyzing the social patterns of terrorists and terror organizations can help predict their future behaviors. SOCMINT's ability to aid in the prediction of a target's behavior makes SOCMINT a useful tool for intelligence operations.

2.4 *Operational SOCMINT*

Social media can provide investigators with near real time and actionable intelligence. SOCMINT can benefit investigators by providing insight into a target's behavior and habits, possibly making apparent the target's future actions. Ultimately actionable intelligence can be used to thwart terrorist and other criminal activities.

Targeted analysis can generate social graphs, highlighting most active users and generating insights that can assist in operational activities such as the targeting of key nodes within a network for the development of agents and sources.[11] As methods further develop in the analysis of social media, SOCMINT becomes a supplement to HUMINT. For example, mobile devices allow social media users to regularly update their status and location. SOCMINT can then be used to help confirm the activities and locations of

[10] Richey, Melonie K., and Binz, Mathias. "Open Source Collection Methods for Identifying Radical Extremists Using Social Media." *International Journal of Intelligence and Counter Intelligence* 28, no. 2 (2015): 354.
[11] Antonius and Rich. "Discovering collection and analysis techniques for social media to improve public safety." 50.

targets, assisting investigators in the field by allowing them to monitor target activities. Platforms such as Twitter are creating near real-time situational awareness.

SOCMINT can support HUMINT in the virtual realm. Investigators can use social media to directly communicate with sources. Chatting involves direct interaction between individuals online, via messaging platforms and chat-rooms. Many social media platforms provide chat and video conferencing capabilities. Chatting with targets requires planning and skill. Content, language, and cultural experts may be necessary to develop believable and useful conversations. Chatting with individuals of interest merges the field of OSINT and HUMINT, which may require collaboration with various experts.

Image analysis can further develop insight on a target. Through the use of geo-locating, images and other online posts can provide the time and location of a user's activity. Geo-locating involves the analysis of metadata, often embedded within images and videos, consisting of longitude and latitude coordinates. This technique can be used by giving investigators to determine the patterns of a target's travel, which can also be used in the formulation of event charting and behavior profiles.

Social media can be used to support cyber operations. As sock puppet accounts become trusted within groups and by targets, an individual of interest may be more inclined to accept an email or link that contains malware specifically designed by the investigating organization. Using various cyber tools, experts can design backdoors and other sustained collection methods to gather intelligence on the target's computer system. Cyber experts can greatly benefit from the use of SOCMINT, both as an intelligence source and platform for operations.

2.5 *SOCMINT challenges*

Like many intelligence disciplines, SOCMINT presents the problem of discerning between noise and signals, that is non-useful and useful information. The amount of information obtained through SOCMINT is often immense, but computer programs can be designed to troll through such large datasets. Search software can be programed for key words and even images. Facial recognition software can be used to locate individuals of interest. Many social media platforms such as Facebook use their own facial

recognition tools, which can be used creatively by investigators to search for and identify suspects.

Denial and deception (D&D) is another challenge that can hinder the effectiveness of reliable SOCMINT. Online criminals and terrorists are often aware that the information they post will be used against them. Thus it is reasonable to consider that some of the information posted by these targets is intended to be deceptive. Most often deception is presented for a wider audience, as terrorist groups consistently use social media to post propaganda commentaries, videos, and images. It can be challenging for officials and social media companies to decide when to delete propaganda and offensive content. This possibility is another reason for investigators to regularly download, save, and record while they carry out research online.

As terrorist groups use social media and gain popularity, social networks or governments may decide to shut down trendy profiles. The Russian government in particular has been able to successfully maintain strict public media enforcement for many years, reinforced by amendments made in 2012 that allow the banning of blacklisted websites without a court order or challenge from site administrators.[12] Terrorist groups are now accustomed to being shut down, and have developed strategies to survive online. The volatility of these groups' online presence poses specific problems to investigators who may find it difficult to keep track of terrorists after their profiles have been deleted. Monitoring activity within popular social groups and websites for terrorists remains a key way to re-discover lost targets.

Social media platforms are very diverse, ranging from open group pages on Facebook to closed chat rooms in games like World of Warcraft. Investigators must have an appropriate level of understanding to navigate the platform of interest as well as cultural expertise to discern conversations. As conversations between individuals develop, the upkeep of sock puppets and the maintenance of online relationships becomes time consuming. Having multiple analysts working as a team is recommended for high priority investigations. Multiple human experts will be able to discern the patterns and contexts of conversations more extensively than a single analyst alone.

[12] "Stifled voices - Restricting the press and freedom of information", *Jane's Intelligence Review,* HIS Inc. 2015, accessed on 2/2/2015, http://janes.ihs.com

2.6 *Managing challenges*

In addition to the complexity of content management, online information posted by terrorist groups is often rooted in an array of complex societal and cultural circumstances, unfamiliar to most westerners. Various experts including language and cultural specialists are crucial in overcoming such challenges. Below is a recommended list of roles that can be used to format a SOCMINT investigative team. A systematic yet organic intelligence gathering strategy can be developed through the use of a SOCMINT team including:

- *SOCMINT Manager* – drafts the research and understands the intelligence requirements, concludes the analysis, organizes, classifies, and disseminates final intelligence product.
- *Legal Expert* – approves the research, ensures compliance with ethical standards, and defines the terms and conditions of the investigation.
- *Content Expert* – an individual with enhanced knowledge regarding the navigation of a social network (Facebook, Twitter, Google+, VKontakte).
- *Domain Expert* – an individual with enhanced subject matter knowledge (Criminologist, Psychologist, Sociologist).
- *Statistics Expert* – uses crawling software, gathers samples, and analyzes large amounts of data.
- *Linguistics Expert* – translates information, provides cultural context, and begins data processing.[13]

Such a team can provide the necessary skills and techniques to harness social media as an effective intelligence tool. Teams can be tasked to focus on a variety of SOCMINT objectives such as gathering and exploitation, analysis, disruption, and prevention.

Social media platforms are diverse in construct and function, and so are the terrorist organizations that use them. A well-structured group like ISIS has a much

[13] Gritzalis, D., M. Kandias, and V. Stavrou. "The NEREUS Platform: An Open Source Intelligence software tool for exploiting national defense capabilities." (2015).

greater and organized online presence than lone wolves. To better understand how a terrorist group uses social media, counter-terror experts must gain a foundational knowledge about the group of interest.

3. CASE STUDY: THE CAUCASUS EMIRATE

In October 2014, U.S. Secretary of State John Kerry announced an intelligence-sharing agreement with Russia, which the Russian foreign minister swiftly denied.[14] Despite current tensions within U.S.-Russian relations "the United States should continue to direct resources toward engaging Russia and other CT partner nations in exchanging 'best practices' on countering violent extremism."[15] SOCMINT is one practice that can be shared with international partners in the fight against global terror. In addition, foreign partnerships can provide U.S. SOCMINT analysts with crucial cultural and language expertise. Such knowledge is extremely beneficial when studying groups such as the Caucasus Emirate and using foreign social media platforms.

3.1 *Overview of the Region*

Complex religious, social and political issues interconnect terrorist groups in the Russian Caucasus, as well as in Eastern Europe and Central Asia. Muslim fighters within these regions have in the past united due to conflicts such as the Soviet war in Afghanistan and the 1995 Chechnya uprising. Today separatist groups in the Caucasus do not only express an official stance against the dominating Russian state, but also against America and all "global infidels." Globalization and technology such as social media have made it possible for historically influential separatists such as the Chechen Republic of Ichkeria to expand their influence on Muslims well beyond the North Caucasus.[16]

[14] "TSG IntelBrief: The Chechen Foreign Fighter Threat", *The Soufan Group*, November 21, 2014, accessed on 03/11/2015, http://soufangroup.com/tsg-intelbrief-the-chechen-foreign-fighter-threat
[15] Sharyl, N. "Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for US-Russia Cooperation Beyond the "Reset"." *Journal of Strategic Security* 6, no. 4 (2013): 1.
[16] Hahn, Gordon. "Anti-Americanism, Anti-Westernism, and Anti-Semitism among Russia's Muslims." *Demokratizatsiya: The Journal of Post-Soviet Democratization* 16, no. 1 (2008): 50.

Currently the official Russian FSB website publicly recognizes 20 groups as terrorist threats.[17] According to the Global Terrorism Database, the most active of these organizations in recent years have been: "Islamic Group" ("Al-Gama'a al-Islamiya"), “Muslim Fundamentalists”, “Ansaru ash-Sharia”, “the Armed Forces of the Chechen Republic of Ichkeria” (“ChRI”) and the “Caucasus Emirate”.[18] Among all these groups, the Caucasus Emirate is particularly worthy of interest, as they are a direct offshoot of the prestigious and influential ChRI, and have developed a strong online and offline terror track record.

3.2 *The Caucasus Emirate*

The Caucasus Emirate has had an online presence since its infancy. Established by a group of the mujahedeen of the Northern Caucasus in 2007, the Caucasus Emirate first announced its existence online, and since then primarily existed in cyberspace.[19] Along with its strong online presence the Caucasus Emirate has had a history of successful attacks, claiming responsibility for the Moscow metro bombings in 2010 and the Domodedovo airport bombings in 2011. Since then the group has lead a sporadic suicide bombing campaign in the Northern Caucasus.[20]

Through their website “kavkazcenter.com,” the Caucasus Emirate has expressed a global support for jihad and Muslim fighters around the world. This support for global extremism makes the Caucuses Emirate a security concern to the United States. Recently the Caucasus Emirate has become divided, as some of its mid-level commanders defected to the Islamic State in early 2015.[21] Russia is concerned that fighters who left to support ISIS will return to rejoin Caucasus fighters. Indeed such fighters can return to Russia or

[17] “Unified federal list of organizations, including foreign and international organizations recognized by the courts of the Russian Federation as terrorist.” *Federal Service of Safety (FSB) of the Russian Federation,* 2015, accessed on 02/02/2015, http://www.fsb.ru/fsb/npd/terror.htm
[18] *Global Terrorism Database*, 2013, accessed on 2/4/2015, http://www.start.umd.edu/gtd/
[19] Knysh, Alexander. "Islam and Arabic as the rhetoric of insurgency: The case of the Caucasus Emirate." *Studies in Conflict & Terrorism* 35, no. 4 (2012): 315.
[20] *Global Terrorism Database*, 2013, accessed on 2/4/2015, http://www.start.umd.edu/gtd/
[21] “Whither Caucus Emirate”, *Center for Security Policy*, Jan 15, 2015, accessed on 03/11/2015, http://www.centerforsecuritypolicy.org/2015/01/15/whither-caucasus-emirate/

move to other locations where they could make a criminal use of their military experience.

3.3 *VKontakte as a SOCMINT platform*

VKontakte (VK) is the most popular social network for Russian speakers today, and a growing platform for terrorist groups around the world. When ISIS beheaded James Foley in 2014 the online community responded in a crackdown on various ISIS websites and Twitter accounts, by deleting official jihadi websites. Militants were thus encouraged to move onto less popular social networking platforms such as VK.[22] In the past VK has been accused of being too lax in its effort to fight against terrorist groups on its platform.[23] The platform now claims that it has shut down all official ISIS profiles.

In light of the 2014 uprising in Ukraine, founder of VK Pavel Durov faced hard times when the Russian FSB began demanding more details on VK's users. Due to FSB pressure, in April 2014 Durov was dismissed as CEO, claiming that the site was now in the control of Putin's allies. Since Durov's dismissal, the site has begun to develop a harder policy toward copyrighted material and malicious activity, including terrorism online. However, VK is becoming more popular every day, and keeping track of all potential terrorist profiles is difficult. VK is the largest European social network with 290 million registered accounts and over 69 million average daily users. Registered users increased by ten million since 2014. The site is most popular with Russian speaking communities, but is still available in a wide variety of languages such as English, Chechen, Ukrainian, Persian, and many more.

The structure of VK is very similar to that of Facebook. VK was originally launched in 2006 to mimic Facebook in style, but tailored to the Russian population for language and customer service. Functionally, VK users can form communities, design news feeds, share multimedia, and sync mobile devices. Over the years VK has not developed as innovatively as Facebook, but it provides a helpful platform for communicating with others and searching out new contacts. In addition, the ability to

[22] Lorenzo Franceshi-Bicchierai, "Russia's Facebook 'VKontakte' Shuts Down All ISIS Accounts," Sept 12, 2014, accessed on 03/11/2015, https://shariaunveiled.wordpress.com
[23] Ibid.

post a wide range of multimedia, including copyrighted material, quickly made VK popular online. Regulation on VK is a wide concern, as the platform still struggles to manage copyrighted material and inappropriate content for children.

When using VK, terror groups are often branching out, seeking like-minded thinkers to share ideas with and coordinate. VK is also used as a propaganda tool and platform for recruitment. As online terror supporters gain popularity on VK, peaceful members of the VK community will often confront them in debate. Debates gather attention, and soon analysts, investigators, and web administrators become aware of these. It is important for investigators to find these trending groups, to locate profiles of interest, before administrators delete them. SOCMINT analysts surfing on VK can use key word searches to locate trending social topics and media, including extremist themes. Analysts can supplement their VK searches through the monitoring of various jihadi websites. Additional websites such as "The Cyber & the Jihad Lab" regularly post online articles concerning terror online.[24] Such tools can give insight into what key words analysts and investigators should be looking for.

SOCMINT analysts can search on VK for profiles and groups that post terror related topics and media, including topics related to the Caucasus Emirate. VK can display a profile's background, interests, and location. Such information can be used to develop a social profile on targets that have a relation with or support terror groups and them. Through the use of sock puppet accounts investigators can attempt to befriend targeted VK profiles. Once investigators have access to a target's VK profile, much information can be collected, including information on the profile's timeline and his/her top five most intimate and regular relationships. The collection of conversations, media displayed, and connections among individuals can then be analyzed to create inferences regarding the tactics, techniques and procedures of an organization they claim to support.

[24] "Analysis and Special Reports" *The Cyber and the Jihad Lab*, December 2014, access on 03/11/2015, http://cjlab.memri.org/analysis-and-special-reports/cyber-jihad/

4. METHODOLOGY

The case study initially intended to use covert SOCMINT gathering methods to befriend VK profiles online. However, university approval is necessary for the performance of human interaction. It is highly unlikely that the university would have approved such a research, as it implements deceptive techniques. Therefore an alternative methodology is used, by gathering publicly available information accessible to any VK user online. No human interactions take place in this study.

Nevertheless, government and security agencies may be able to implement deceptive techniques and it is therefore worth considering them briefly. Security experts can use a variety of false identities to develop sock puppet accounts. For a similar case study, a minimum of three female sock puppet accounts and three male sock puppet accounts is recommended. Each identity should have similar interests and backgrounds relatable to targets, such as the support of fundamentalist Islamic beliefs. Once plausible identities and accounts are created, targets can be sought out for by "befriending" through VKontakte. It is theorized that female sock puppets with similar interests of male targets will gain the highest befriending rates. This assumption is based on social, relational, and sexual attraction, believing that while on social media "male users are more likely to be interested in dating or serious relationships"[25] than females users.

With all online intelligence activity, a safe intelligence gathering methodology should be used, at least including a secure computer and the use of online anonymity techniques. Video recording and screen capture software can also be used for documentation purposes, as well as detailed spreadsheets and template profiles concerning subjects. Research can follow four main steps over the course of a month: sock puppet development, human subject interaction, information gathering, and analysis. However, for this case study only public online information is gathered for qualitative content analysis.

[25] Thelwall, Mike. "Social networks, gender, and friending: An analysis of MySpace member profiles." *Journal of the American Society for Information Science and Technology* 59, no. 8 (2008): 1329.

4.1 *Targeted Subject Population*

The targeted subject population for this study is composed of individuals supporting the Caucasus Emirate. Subjects are adults, male or female, with a wide range of ages. It is expected that nearly all subjects will display a Russian citizenship with a Caucasian ethnic background. Display of an Islamic fundamentalist identity is also expected for all subjects. These subjects will all have an online presence on the VKontakte platform, thus allowing for SOCMINT gathering. Subjects presenting clear evidence of U.S. citizenship are excluded from the study.

The study assumes that users are aware that all information they display is public knowledge. Collection will begin at the start of the research and ending after two to three weeks of information gathering. No consent forms are necessary since the information is considered open source. Nonetheless, minimization procedures will be used to protect the subjects' identities. No interaction will take place between the researcher and the targets.

Targeted profile names are coded (e.g. subject 1, subject 2), and media found is not saved or displayed in the final product, but used to categorized and develop inferences. Thus the privacy of all participants will be protected. Data is to be stored on a secure computer, located in a locked office on the university campus. This is to ensure that information remains confidential. All raw data that identifies participants is destroyed upon completion of the research.

4.2 *Collection and Analysis*

A list of potential key terms can be developed through the aid of supplementary websites such as "The Cyber & the Jihad Lab" and "kavkazcenter.com". By using a variety of different key terms, search results on VK will provide a wide range of profiles, communities, and media results. By sifting through such search results profiles of interest to the research are likely to be discovered. To be considered for research, a targeted individual or group must display evidence of support or involvement with the Caucasus Emirate. Such evidence can take the form of terror related images and media, or sentiment in support for Caucasus Emirate's activity or propaganda.

This study will focus on collecting intelligence among a target's top five active relationships. SOCMINT techniques such as key word searching, theme analysis, word analysis, image analysis, activity charting, and link charting will be used in an attempt to process the data. Data gathered may include: location and travel information, images and conversations in support of terrorism, and key relationships with users from other organizations.

The purpose of the study is to gather enough data to form a set of hypotheses on the tactics, techniques, and procedures targets implement in their support of terrorist goals. Further analysis of Caucasus Emirate followers will be conducted to determine if additional support is given toward outside terrorist organizations such as ISIS, other groups, or none.

4.4 *Expected Results and hurdles*

University approval has not been given for the use of sock puppets and deception. Therefore, without access to a target's full profile, it is unlikely that a total picture can be created based on an individual's VK account. In addition, due to the shutting down of official terrorist profiles on social media, the likelihood of finding blatant supporters of the Caucasus Emirate is expected to be low. Extremist supporters are likely to display strong Islamic fundamental beliefs. Befriending such individuals could lead to other profiles that display more extreme views and connections to the Caucasus Emirate or other terrorist organizations.

Content analysis on such individuals is time consuming and difficult without software programs or a team of analysts. For this study, a minimum target sample of six individuals that support the Caucuses Emirate is estimated to be adequate for the development of a hypothesis concerting the organization's tactics, techniques, and procedures. Future research implementing quantitative statistical analysis and a broader set of targets may produce stronger population representation and confidence levels.

The Caucasus Emirate displays official websites and twitter pages with statements and descriptions of activities and persons. The researcher hopes to discover if personal profiles of supporters of the Caucasus Emirate on VK coincide with official statements of

the organization, such as the support of ISIS as a caliphate. In addition individual profiles on VK may lead to a deeper understanding of the organization's motives and goals. Despite limitations of manpower and resources, the methods used in this study can act as a test for additional research.

5. RESULTS

Access to Vkontakte required a phone number for profile confirmation, sent via text message. Once VK was accessible an anonymous profile was created for the research, containing no self-identifying information of any kind, no profile picture was used, and an anonymous first and last name was used. Research began on VK with key word searches for profiles and groups of interest.

Key words and search terms were developed by using a variety of research tools. The official website of the Caucasus Emirate (vdagestan.com) aided in the development of multitude key words, by identifying popular topics and repeated terms. General key terms concerning Islamic themes, such as Jihad, Tawhid, and Mujahidin, were combined in various orders with regional specific terms such as Caucasus, Emirates, Dagestan, and Chechnya. In addition, with the aid of google translation software, key terms were also used in Russian and the Chechen language.

Searching with the same term in different languages provided different results, as show in table 1. The most direct key term, Caucasus Emirate, was used to search for individuals and groups that have a public interest in the organization. When searching for the organization on VK, results showed an overall larger amount of content when searching in Chechen than for searching in either Russian or English.

Table 1. Key word search results

	"Caucasus Emirate" (English)	**"Кавказский Эмират"** (Russian)	**"Имарат Кавказ"** (Chechen)
People	3	0	11
Communities	2	6	14
Videos	14	7	380
Posts	216	2,967	23,170

The various Caucasus Emirate communities found on VK provided a large pool of profiles of interest. Some of these communities were closed groups, revealing discussion topics to members only. Communities open to the public showed most activity to be outdated, over six months old. Even so, member lists of community members were displayed for the public to see. By reviewing community member lists the research was able to single out individuals based on profile photos displaying mujahidin like images and themes, such as the Jihadist black flag and military like weapons and attire.

Videos on community sites and on profiles showing support of the Caucasus Emirate were used to find additional profiles of interest, by viewing those that commented or liked such videos. By observing who is "likeing" and commenting on certain posts, the research was able to use social creep to further search out new profiles. In addition to videos, specific profiles such as Ali Abu Mukhammad (Али Абу-Мухаммад in Russian), the past leader of the Caucasus Emirate who died recently in 2015, were also used as key search terms for the research. Followers of Ali Abu Mukhammad were mostly from Russia, but also included profiles indicating locations from the Middle East.

Ali Abu Mukhammad is seen as a public figure, and has multiple profiles and communities dedicated to his memory and teachings. An interesting feature on VK is the search tool for specific members on communities, with the ability to narrow down search results to age, gender, region, school, military service, and many other options. The research was able to identify nine followers of a Mukhammad community that was currently online in real time during the time of the research. Of these nine profiles: one was female and eight were male, three displayed Russian as their location, one indicated he was from Georgia, and one indicated he was from Argentina. The other profiles did not display their location. Only one profile showed a self-identifying profile image, while the rest only displayed images of non-self-identifying images such as posters, cars, and scenery as their profile images.

6. ANALYSIS

The research could not find official postings of the Caucasus Emirate approving any tactic, technique, or procedure. This may be due to the limitations of the research in man power and lack of access to closed profiles and communities. Online censorship could also be the cause of the lack of activity of the Caucasus Emirate on VK. However, profiles that supported the leadership of the Caucasus Emirate consistently posted videos and links to YouTube and other sites, which could lead to additional evidence on terrorist behavior. In the end there was not enough evidence to develop a proper hypothesis regarding the tactics, techniques, or procedures implemented by the Caucasus Emirate.

Individuals of interest on VK displaying pro-jihadist like comments, images, and behavior had a mix of backgrounds, but a majority came from Russia or displayed Russian as a major language on their profiles. The research discovered hundreds of profiles of interest, but concentrated on an active community of members that may be linked to the Caucasus Emirate based on membership within terror related community groups. Most profiles did not display their current specific location, hid most of their identifying information, and often kept self-identifying images such as face shots obscure or cropped.

Most subjects were male with a mix of social interactions with family, friends, and fellow believers in Islam and other similar interests. Some female subjects wore traditional Islamic clothing, covering their face and head. Many women supported other women to marry mujahedeen fighters. A majority of the media, videos, and posts observed in the research mostly concerned spiritual encouragement and religious teachings. Political and military topics were rare and often concerned a vocal resistance against Russian forces.

A consistent theme among many of the profiles was Islamic music. Sharing music is a technique used to further enhance propaganda and attract younger supports. Art and self-expression is a constant theme among youth on VK, and this is no exception for Islamic youth. Cultural experts can gain further insight into the lives of terrorist groups by understanding such music, its lyrics, and origins. Music found in the research was often titled under “Caucasus Emirate” but had no identifying artist. Songs were often a

mix of acoustic instruments with chanting and inspirational lyrics in various languages, possibly Arabic or Chechen. Some music was more modern with electronic mixes and Russian lyrics. A group of possible interest to cultural analysts is "Патсаны Имарат Кавказ" which seemed to sing in support of the Caucasus Emirate's cause.

7. CONCLUSION

Social media intelligence is a powerful tool for the enhancement of counter terror investigations. SOCMINT can be used to identify profiles, communities, and media of interest on various platforms. Furthermore, SOCMINT presents a multitude of challenges, most notably the separation of useful information from non-useful information. For successful SOCMINT, geographic, language, and cultural analysts would be highly valued as to fully grasp the information displayed in communities and profiles. In addition, it is suspected that the use of sock puppets and online human interaction would lead to more substantial information regarding a terrorist organization's tactics, techniques, and procedures.

Intelligence collection on VK can provide a wide range of information regarding the Caucasus Emirate, such as terrorist profiles and their interests such as music, promotional videos, and public communities. By using VK's unique search tools, analysts and investigators can identify individuals that have similar interests or characteristics with that of terrorists. Monitoring active terrorist websites can further develop key search terms used for SOCMINT. Information gathered on VK can be compared with terror-websites for consistency, as well as used to make inferences. Finally, without a tailored SOCMINT team, processing and analysis on social media becomes problematic. Discerning the meaning of various images, interpreting foreign languages, and the deciphering the context of commentaries is a tedious and challenging endeavor. Indeed future SOCMINT collection and analysis will only be successful with a team of dedicated professionals.

Bibliography

Ajbaili, M. (2014, June 24). *How ISIS conquered social media*. Retrieved February 02, 2015, from Al Arabiya News: http://english.alarabiya.net/en/media/digita/2014/06/24/How-has-ISIS-conquered-social-media-.html

Blank, S. J. (2012). *Russia's Homegrown Insurgency: Jihad in the North Caucasus.* Strategic Studies Institute. U.S. Army War College Strategic Studies Institute.

Boris Gladarev, M. L. (2012). The Role of Social Networking Sites in Civic Activism in Russia and Finland. *Europe-Asia Studies , 64* (8), 1375-1394.

Center for Security Policy. (2015, Jan 15). *Whither Caucus Emirate*. Retrieved March 11, 2015, from http://www.centerforsecuritypolicy.org

Clark, R. M. (2014). *Intelligence Collection.* Thousand Oaks, CA: CQ Press.

Cross, D. S. (2013). Russia and Countering Violent Extremism in the INternet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the "Reset". *Journal of Strategic Security , 6* (4), 1-24.

Digital Strategy Consulting. (2013, 11 09). *Top 5 Social Networks in Russia: Traffic and Time Spent*. Retrieved 02 02, 2015, from http://www.digitalstrategyconsulting.com/intelligence/2013/09/top_5_social_networks_in_russia_traffic_and_time_spent.php1/2

Dimitris Gritzalis, M. K. (2015). *The NEREUS Platform: An Open Source Intelligence software tool for exploiting natinal defense capabilities.* Information Security & Critical
Infrastructure Protection (INFOSEC) Lab, Dept. of Informatics. Athens University of Economics & Business.

Drew, Dennis, and Donald Snow. (2006). *Making Twenty-First-Century Strategy: an introduction to modern national security processes and problems,* Maxwell Air Force Base, AL: Air University Press.

Federal Service of Safety (FSB) of the Russian Federation. (1999-2015). *Unified federal list of organizations, including foreign and international organizations recognized by the courts of the Russian Federation as terrorist*. Retrieved 02 02, 2015

Global Terrorism Database. (2013). Retrieved 04 2015, 02, from http://www.start.umd.edu/gtd/

Hahn, G. (2008). Anti-Americanism, Anti-Westernism, and Anti-Semitism among Russia's Muslims. *Demokratizatsiya: The Journal of Post-Soviet Domocratization , 16* (1), 49-60.

Jane's Intelligence Review. (2015). *Stifled voices - Restricting the press and freedom of informaiton.* Intelligence Report, IHS Janes.

Knysh, A. (2012). Islam and Arabic as the Rhetoric of Insurgency: The Case of the Caucasus Emirate. *Studies in Conflict & Terrorism , 35* (4), 315-337.

LexisNexis Risk Solutions. (2012). *Survey of Law Enforcement Personnel and Their Use of Social Media in Investigations*. Retrieved March 1, 2014, from http://www.lexisnexis.com/risk/insights/law-enforcement-social-media-infographic.aspx

McAfee Institute Inc. (2014). Social Media Intelligence Analyst Manual Version V.1. Saint Louis, MO, USA.

Melonie K. Richey & Mathias Binz (2015) "Open Source Collection Methods for Identifying Radical Extremists Using Social Media, International Journal of Intelligence and Counter Intelligence", 28:2, 347-364.

Nicky Antonius, L. R. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The International Technology Management Review , 3* (1), 42-53.

Sir David Omand, J. B. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security , 27* (6), 801-823.

Stratfor Global Intelligence. (2014). *The Kremlin Passes New Internet Restrictions.* Analysis.

Suleymanova, D. (2009). Tatar Groups in VKontakte: The Interplay between Ethnic and Virtual Identities on Social Networking Sites. *Digital Icons: Studies in Russian, Eurasian and Central European New Media, 1* (2), 37-55.

The Cyber & Jihad Lab. (2015). *Tracking Jihadis/Terrorists On Social Media And Online*. Retrieved 02 04, 2015, from http://cjlab.memri.org/category/lab-projects/tracking-jihadi-terrorist-use-of-social-media/

The Soufan Group. (2014, November 21). *TSG IntelBrief.* Retrieved March 11, 2015, from The Chechen Foreign Fighter Threat: http://soufangroup.com/tsg-intelbrief-the-chechen-foreign-fighter-threat/

Thelwall, Mike. "Social networks, gender, and friending: An analysis of MySpace member profiles." *Journal of the American Society for Information Science and Technology* 59, no. 8 (2008): 1321-1330.

Trottier, D. (2012). Policing Social Media. *Canadian Sociological Association* , 412.

Weimann, G. (2010). Terror on Facebook, Twitter, and Youtube. *Brown Journal of World Affairs , 16* (2), 45-54.

Wimann, G. (2014). New Terrorism and New Media. *Commons Lab of the Woodrow Wilson International Center for Scholars*.