ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/260775393

Detecting Linguistic Markers for Radical Violence in Social Media

Article *in* Terrorism and Political Violence · December 2013

DOI: 10.1080/09546553.2014.849948

CITATIONS
56

READS
1,099

4 authors:

Katie Cohen
Swedish Defence Research Agency
6 PUBLICATIONS **67** CITATIONS
SEE PROFILE

Fredrik Johansson
Swedish Defence Research Agency
41 PUBLICATIONS **538** CITATIONS
SEE PROFILE

Lisa Kaati
Swedish Defence Research Agency
52 PUBLICATIONS **493** CITATIONS
SEE PROFILE

Jonas Clausen Mork
Swedish Defence Research Agency
7 PUBLICATIONS **89** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Conceptual modeling of illicit economic flows View project

Project Assessment and Communication of Uncertainty in Intelligence to Support Decision-making (SAS-114) View project

All content following this page was uploaded by Fredrik Johansson on 28 April 2014.

The user has requested enhancement of the downloaded file.

Detecting Linguistic Markers for Radical Violence in Social Media

Katie Cohen, Fredrik Johansson, Lisa Kaati, Jonas Clausen Mork

Swedish Defence Research Agency (FOI)

SE 164 90 Stockholm

Sweden

Contacting author: lisa.kaati@foi.se

Abstract

Lone-wolf terrorism is a threat to the security of modern society, as was tragically shown in Norway July 22, 2011, when Anders Behring Breivik carried out two terrorist attacks resulting in a total of 77 deaths. Since lone wolves are acting on their own, information about them cannot be collected using traditional police methods such as infiltration or wiretapping. One way to attempt to discover them before it is too late is to search for various "weak signals" on the Internet, such as digital traces left in extremist web forums. With the right tools and techniques, such traces can be collected and analyzed. In this work we focus on tools and techniques that can be used to detect weak signals in the form of linguistic markers for potential lone wolf terrorism.

1. Introduction

While terrorism carried out by lone actors remains a marginal, albeit deadly, phenomenon, the acts of Norwegian terrorist Anders Behring Breivik on July 22, 2011, have placed it high up on the agenda of many security services and police forces. Ramón Spaaij[1], however, notes that so-called "Lone Wolf Terrorism" is both uncommon – making up less than two percent of the terrorist incidents in his sample - and less lethal on average than acts carried out by groups and organizations. Nonetheless, there seem to be reasons to be worried. One such reason is that there is a strong argument to be made that the capability threshold for individuals to carry out advanced attacks is becoming lower with time due to the power of the

Internet to bring critical information, e.g. tutorials on bomb-making or geographical information, “to your fingertips”. There is also a concern that the Internet is making it easier than ever to engage in the study and dissemination of extremist views. Finally, a third reason is that many methods employed by security services and police to uncover and prevent group plots are of little use when the perpetrator is acting alone.

One initial conclusion that can be drawn from this is that there is, or will be, a need for new methods within the domain of counter terrorism. A seemingly promising arena for such method development is the Internet, and this will also be our focus in the current paper.

There are several examples of where Internet has been used by lone wolves to spread their views and opinions before an actual attack. One such example is the anti-abortion activist Scott Roeder who in 2009 killed the physician George Tiller in Kansas[2]. Tiller was one of the few doctors in the United States that performed late term abortions, and before the attack, Scott Roeder wrote a column on a critical of web abortion page where he expressed his views against abortion and Tiller’s work. Another example of a lone wolf using the Internet to express his views is James von Brunn, also known as the Holocaust Museum shooter[3]. Von Brunn was a white supremacist who was in charge of an anti-semitic website where he expressed his views long before the attack. Other examples of how the Internet is used to express views and intents can be found in the literature on school-shootings, which is a related phenomenon to lone wolf terrorism. In Semenov et al.[4] it is e.g. stated that a majority of school-shooters in the samples they have analyzed announced their intentions on forums before their actual attacks (including cases such as Pekka-Eric Auvinen and Matti Juhan Saari in Finland and Matthew J. Murray in the United States).

Searching for potential lone wolf terrorists on the Internet is often compared to searching for a needle in a haystack. The Internet contains an overwhelming amount of information, and to manually find and read the content of all sites that might indicate intent or preparation for an act of terrorism is practically impossible. An interesting question is therefore whether automated techniques can be used to find web forums or other kinds of web sites where extreme opinions are exchanged, and to automatically or semi-automatically detect if some individual is planning to commit an act of violence based on analysis of the content of such sites.

In addition to all the material that analysts can find through the use of various search engines, there are also enormous amounts of information in the so-called hidden or Deep Web, i.e. the parts of Internet that are not indexed by the search engines' web spiders (e.g. due to password protection or content that is generated dynamically when accessing a webpage). To produce fully automatic computer tools for detecting lone wolf terrorists on the Internet is in our view not possible, both due to the enormous amounts of data (which is only partly indexed by search engines) and due to the deep knowledge that is needed to really understand what is discussed or expressed in written text or other kinds of data available on the Internet, such as videos or images. However, in this work we argue that semi-automatic tools potentially could be of great use for intelligence analysts in their search for traces of lone wolf terrorists and other kinds of extremists on the Internet. Data available on the Internet is obviously only one type of information that can be of interest when trying to detect possible lone wolf terrorist. Other information that may come from sources which are not publicly available, such as medical records, memberships in gun clubs, procurement of guns, records of obtaining bomb-making material, etc. is of course also of utmost importance. However, in this work we only focus on open source information that can be readily accessed through the Internet.

Attacks on public figures, mass murders and acts of lone wolf terrorism, are often signalled by a set of more or less detectable behavioural markers, some of which are preparatory actions, others linguistic expressions of attitudes, motivations, and intentions. Based on a typology of so called *warning behaviours* presented by Meloy et al.[5], we discuss the possibility of tracing three different forms of behavioural markers for radical violence in written text in social media (or other kinds of web content).

2. A typology of warning behaviours for radical violence

The study of behavioural markers for radical violence, also labelled *warning behaviours*, is an essential part of assessing the threat of lone wolf terrorism. Meloy et al. broadly define warning behaviours as any behaviour that "precedes an act of targeted violence, is related to it, and may, in certain cases, predict it". As such, warning behaviours can be viewed as indicators of increasing or accelerating risk. Meloy et al. define eight different warning behaviours, namely (i) pathway warning behaviour, (ii) fixation warning behaviour, (iii) identification warning behaviour, (iv) novel aggression warning behaviour, (v) energy burst warning behaviour, (vi) leakage warning behaviour, (vii) last resort warning behaviour and (viii) directly communicated threat warning behaviour. Here, we will discuss the possibility of detecting *leakage*, *fixation* and *identification* warning behaviours in social media, since these three in our view have the greatest potential to be discovered with text analysis methods applied on public information accessible from the Internet. The actual techniques that can be used to identify such warning behaviours are presented more thoroughly in Section 4.

2.1 Leakage

Leakage, the communication to a third party of an intent to do harm to a target, usually infers a preoccupation with the target and may signal the research, planning and/or implementation of an attack. Data suggest that leakage commonly occurs in cases of targeted violence, ranging from school shootings to attacks on public figures. Leakage can be intentional or unintentional, and more or less specific with regards to the act[6]. Studies on public figure attacks and assassinations have according to Meloy and O'Toole found a suggestive pattern of leakage, where an attack often has been preceded by indirect, conditional or direct threats aimed at people associated to the target, or bizarre or threatening communication to politicians, public figures or police forces. However, according to the same study, threats are typically not posed directly at the target. In different studies, the occurrence of pre-attack leakage ranges from 46% to 67% (and even higher for school shootings[7]). Leakages and threats before school shootings often seem to be more explicit than for many other kinds of terrorist acts. Newman et al.[8] report how Andrew Golden stood on a table in the cafeteria in Jonesboro, Arkansas and announced: "You're all going to die" the same year as the shooting took place. Just the day before the shootings, some other students heard the other shooter Mitchell Johnson say that he "had a lot of killing to do". These kind of direct threats seem to be more common among young mass murderers than in other cases related to lone-wolf terrorism.

Case studies also show that leakage is often accompanied by other warning behaviours[9].

2.1 Fixation

Meloy et al.[10] define fixation warning behaviour as any behaviour indicating an increasingly pathological preoccupation with a person or a cause, for instance increasing perseveration on the object of fixation, increasingly strident opinion, or increasingly negative characterization of the object of fixation. The fixated person expresses a preoccupation with the group or person considered responsible for the subject's grievance by allocating large amounts of time to discussing, theorising about, or studying the perceived enemy. The subject may have gathered an extensive amount of facts about the target. For instance, anti-abortionist Clayton Waagner spent several months gathering target information on 42 different abortion doctors, planning to kill them with stolen firearms, before settling for another approach, i.e. sending more than 500 letters with faux-anthrax to abortion clinics across the USA[11].

Sometimes the subject gathers information with the explicit purpose of using it for preparing an attack. At other times, fact-gathering may start as an expression of fixation, with the idea and planning of an attack taking place after, and sometimes as a result of, the subject having gathered enough information to make it possible.

2.3 Identification

Identification warning behaviour is defined as a behaviour indicating a desire to be a "pseudo-commando", have a warrior mentality, closely associate with weapons or other military or law enforcement paraphernalia, identify with previous attackers or assassins, or identify oneself as an agent to advance a particular cause. Narcissistic ideas and fantasies about oneself are also counted to this group of warning behaviours. This rather broad definition shows the complexity of the phenomenon. Here, in order to make it more manageable, the concept of identification, as defined by Meloy et al., is divided into two subcategories: *identification with radical action* and *identification with a role model*. Since *group identification* is considered an essential part of the radicalisation of lone wolves as well as organised terrorists, (cf. Ginges et al.[12] and Moskalenko and McCauley[13]), it is added as a third subcategory of identification.

2.3.1 Identification with radical action ("warrior mentality")

Lone wolf terrorists and attackers of public figures often tend to identify themselves as a kind of warrior, a person who is prone to use structured violence for a "higher cause". In these cases, use of military terminology and a strong interest in weapons, military strategies and paraphernalia can be seen, usually combined with a narcissistic fantasy of oneself as a rescuer, the one who sees what is wrong and does something about it[14]. Timothy McVeigh's collecting of weapons and other military paraphernalia, together with his expressed desire to be “the ultimate warrior”, and “the first hero” is a telling example of this kind of identification warning behaviour. There are many examples of images and videos posted on the Internet where lone wolf terrorists pose with weapons long before the attack, such as the pictures of Anders Behring Breivik wearing a compression sweater and pointing an automatic weapon against the camera.

2.3.2 Identification with role-model

The subject may be much influenced by, and, to an extent, identify oneself with, some other radical thinker or leader, seeking to emulate their style, ideals or actions. Anders Behring Breivik, for instance, was highly influenced by the Norwegian anti-Islamic blogger Fjordman, whom he quoted extensively in his manifesto[15]. Similarly, many school shooters have been inspired by previous attacks (most notoriously the Columbine massacre by Eric Harris and Dylan Klebold, which according to Larkin[16] has become a cultural script for many subsequent school shooters).

It is also common that radical thinkers acts as influencers and encourage people with the same radical views to take actions. An example of this is when an al Qaeda spokesman Adam Gadahan appeared in video titled “Do Not Rely on Others, Take the Task upon Yourself”. In the video, Gadahan urged Muslims in the United States to take advantage of the relaxed firearm laws to buy guns and carry out attacks on their own[17]. It is important to note that these individuals, when they are serious about going operational, often seek foreign contacts. This pattern is widespread, with the US as epicentre for non-Islamist movements and the Middle East (especially Pakistan, Afghanistan, and the ungoverned territories between) for Islamists.

2.3.3 Group identification

Though acting alone, a lone wolf terrorist does consider him-/herself part of a larger group, namely the group for the benefit of which the terrorist action is committed. Even in cases when the subject is not part of the "beneficial" group (as for instance anti-abortionists), there is usually a very strong sense of moral obligation toward the group, which can be construed as identification with a cause[18]. In any case, identification needs to be strong to motivate radical violence. Strong identification with the in-group often equates collectivistic values, where the needs of the group override the needs of the individual, which, for some, may justify violence against innocents. Moral commitment to the in-group and values associated with group identity appears to be strong indicators of potential radical violence. For instance, a positive correlation between collective commitment values and willingness to take part in political violence has been noted among Israeli settlers on the West Bank[19]. Group identification can be so strong that it borders on the ego-dissolving. The subject's collectivistic values make him/her prone to self-sacrifice, which is usually necessary for someone to actually follow through with an act of political violence[20]. The somewhat paradoxical combination of selfless, collectivistic thinking and a grandiose, narcissistic self-image seems to be present in the attitudes of most known attackers. Negative identification with the enemy group is another important part of radicalization, since it facilitates demonizing or dehumanizing the perceived enemy, which in the next step justifies violence.

3. Text analysis techniques for analysing social media

In order to build systems that can help intelligence analysts with monitoring and analysing social media or other parts of the Internet in the search for digital traces of violent extremism, there are a number of tools and techniques that are needed, including web crawlers for collecting the relevant data and various natural language processing techniques for analysing the content. Here we give an overview of a number of text analysis techniques, which can be of great use for intelligence analysts when analyzing the content of web sites or social media.

3.1 Translation services

Rapid progress has recently been made in the research field of text analysis and natural language processing. Few have probably missed the progress that has been made in the area of machine translation, where free services such as Google Translate offer quick and automatic translation between a large number of languages. A strongly contributing factor to these developments is the change from using only traditional linguistic-based methods requiring much work and expert grammatical knowledge, to combining them with methods based on statistics that make use of the enormous amounts of text available from Internet and other places (e.g., translations of various EU documents to all official EU languages). This type of machine translation can be very useful for translating texts from extremist web sites, reducing the need for the analyst to be fluent in the original language of the text. The results obtained from this kind of automatic translation services are seldom as good as if a human expert would translate the content of a web site, but the great advantage with automatic translation is obviously the speed with which large amounts of data can be processed, making it possible to analyze much more websites than would have been possible if the process would have been done fully manually. Automatic translation gives an analyst the possibility to process text written in nearly any language.

3.2 Sentiment analysis

Text analysis techniques referred to as sentiment analysis or opinion mining methods have become an increasingly popular way for companies to determine what opinions regarding their products or brands have been expressed in social media. An important part of sentiment analysis is to retrieve relevant posts and make a classification of whether it contains positive, negative, or neutral opinions regarding the brand of interest. In a similar way one can make use of machine learning to “teach” computer algorithms to learn the difference between radical or non-radical texts, and to identify threats targeted to specific individuals or (ethnic or religious) groups. This kind of techniques has e.g. been used for comparing the levels of violence, anger, hate, and racism expressed in various web forums[21]. However, to use sentiment analysis for identifying radical text still needs a lot of research in order to obtain reliable results.

3.3 Mapping websites

Text analysis can also be used for automatic discovery of potentially "problematic" web sites (e.g. containing material related to violent extremism), and for creating networks of such web sites and their relationships to each other. Computer algorithms can be used to identify radical content on both websites and on individual postings in web forums, in order to identify users (web aliases) that express themselves in such a way that human analysts may want to do further investigations. This issue is further described by Brynielsson et al[22]. It is however important to note that in order to determine relevant keywords that actually indicates radicalism an in-depth knowledge of the milieu in question is required.

3.4 Author recognition

Since people who are commenting on discussion forums and other kinds of social media most often are using aliases, the discovery of someone who expresses violent radical behavior does not necessarily mean that the police can identify whom to investigate further. In fact, in general it ranges from hard to impossible to identify a unique individual just based on the discovery of an interesting alias. There are usually good opportunities for users to create aliases without any traceable connection to themselves. Even when the users are required to verify their identity with a valid email address, nothing prevents them from creating an email address only for this purpose. Even though the actual IP address used for the creation of the email account or the forum posting may be stored, and possibly also handed over to the police when a serious crime is suspected, the individual can make use of various types of anonymous surfing services or internet cafes in order to avoid being traced.

A text analysis technique which today is not mature enough to utilize at present but may become relevant in the future for connecting an alias to a physical individual is author recognition or author identification. In this research area, the algorithms used extract various features from texts, such as the frequency of specific words or word stems (lexical features), and parts-of-speech tags (word classes) or other kinds of sentence constructions (syntactic features), and use them to identify the author of the text. The idea with this is that the writing style of each individual is unique, vaguely similar to the use of fingerprints. This type of technique is at present useful for determining who out of a small set of potential authors that have written a certain text, or from which kind of community (e.g., youths or highly educated) the author comes. However, the techniques are today not good enough to be used for determining who out of a large number of potential authors that has written a piece of text, and the majority of available research focuses on large texts rather than short pieces of text. Nevertheless, the research is progressing fast in this area, and one can expect these methods to become much more useful also on a larger scale in the next few years. A very interesting progress in that direction is the recent paper by Narayanan et al.[23] where promising results are shown for Internet-scale author identification.

If a person is active on a number of web sites, forums, or other kinds of social media, it is common that several different aliases are used. It is therefore of importance to have techniques that can help an analyst to detect individual authors that use several different aliases. Dahlin et al.[24] suggests a number of techniques that can be combined for matching multiple aliases to the same individual. In the paper it is suggested that an author using different aliases can be identified using several features:

1) the used alias names

2) the users an alias is connected to (social network analysis)
3) a profile of the time when the posts were made
4) a stylometric finger print of the messages written by the author using author recognition techniques.

All the techniques that have been briefly discussed above, including the techniques for alias matching, are used in our framework for detection of lone wolf terrorists on the Internet. This framework is described in more technical terms by Brynielsson et al[25].

4. Linguistic markers for identifying warning behaviours in social media

Much of a terrorist's behaviour preceding an attack takes place in real life, where the subject engages in preparations (e.g. buying fertilizer to make a bomb, buying guns, or gathering information about the target), or expresses opinions and values consistent with radical action. However, the subject may also communicate opinions, values, and sometimes also actual intent on the Internet, as argued earlier. Certain mindsets or attitudes, previously observed among known perpetrators of radical violence, might also be detectable in the way the subject expresses him-/herself on, for instance, blogs or discussion boards. We refer to these expressions of attitude or mindset as *linguistic markers for radical violence*. As stated above, the warning behaviours we believe to be most easily detectable in the subject's written communication in social media (e.g. extremist discussion boards) are leakage, fixation and identification. We have identified a set of linguistic markers for each of these warning behaviours. The linguistic markers can be used as input to computer algorithms so that they may be able to recognize signs of radical violence.

4.1 Linguistic markers for leakage

Leaked information of intent is likely to contain auxiliary verbs signalling intent (i.e., "I will…", "…am going to…", "some one should") together with words expressing violent action, either overtly or, perhaps more likely, through euphemisms.

Based on these observations, we think that this kind of leakage potentially can be detected by using a quite simple approach in which the posts are extracted and after stemming or lemmatization (reducing the end of a word in order to return the word's common base form) are matched against a predefined word list of violent actions. Since a large number of synonyms can be used for the verbs signalling a violent intent, we additionally propose the use of an ontology (such as the well-known lexical database WordNet), in which semantic relations between synonym sets are expressed. An example of such a semantic relation would be that the verb "massacre" belongs to the same synonym set as the words "mow down" and "slaughter". By using such knowledge, the number of words that must be explicitly defined in the word list of terms to search for can be heavily decreased. Since the occurrence of a single word expressing a violent action is far from enough for classifying a sentence as being a linguistic marker for leakage, we also propose taking the part-of-speech tagging into account when searching for indications of leakage. This kind of text analysis methods obviously has a hard time coping with ironic statements, leading to a risk of false positives where jokes are classified as a potential marker or leakage. However, by restricting attention to sites or forums that through automated content analysis or prior knowledge is known to contain content related to violent extremism, we think that the false positives can be kept at an acceptable level.

4.2 Linguistic markers for fixation

Fixation can be observed as a tendency to fixate on an issue or a person, which in written communication would result in text wherein one person, group or issue is mentioned by the subject with a significantly higher frequency than it is mentioned by other discussants. Also, frequent combinations of certain key terms, for instance "Jew" and "communism", can reveal a fixation with a certain idea. Fixation taking the form of extensive fact-gathering can only be detected in communication if the subject chooses to share some of the information.

In order to find this kind of fixation in text, we propose counting the relative frequency of key terms relating to named entities such as persons, organizations, etc. To find out which words that relate to named entities, algorithms for so called named entity recognition can be used. Implementations of such algorithms are available in free natural language processing toolkits such as NLTK and GATE.

4.3 Linguistic markers for identification

Identification with a group or cause can be expressed for instance by a usage of positive adjectives in connection with mentioning the in-group. Similarly, a usage of negative adjectives in connection with mentioning of a group or person may indicate negative identification. Activists tend to feel stronger than others about the cause, expressing more anger or grief when something negative happens to the in-group, and greater joy when something positive happens[26], another indicator of identification. The linguistic correlates of strong emotions related to group identification might be an indicator of the strength of the identification. In order to find out which positive or negative sentiments that is present in a text, or which kinds of emotions that are expressed, sentiment and affect analysis techniques can be used, as explained in Section 3.1. References to the in-group can be detected by investigating the use of first person plural pronouns ("we" and "us"), while much use of third person plural pronouns (e.g., "they" and "them") according to Pennebaker and Chung[27] can be used as an indicator of extremism. In that work the software LIWC is used to analyse the content of al-Qaeda transcripts.

The so-called warrior mentality can probably be spotted through a certain terminology, while a sense of moral obligation can be expressed through the usage of words related to duty, honour and justice etc.

Identification with another radical thinker can, aside from frequent quotations and mentions, be expressed by a similarity in language. The subject may use the same terminology as the role model, and can possibly even adapt a similar sentence structure. In these cases it is possible to use author recognition techniques to identify similarities.

5. Discussion

The techniques and tools that have been presented in this work have the potential to support intelligence analysts in their work with finding potential lone wolf terrorists before they strike. However, before such a tool is implemented and put into operational use, there are a number of issues that have to be considered.

Both rights-based and consequentialist ethical traditions acknowledge the moral weight of privacy. In the setting of Internet surveillance and terrorism, however, there is an obvious conflict between this bearer of moral value and the avoidance of harmful consequences of terrorism or, in a rights-based context, the duty of government agencies to protect their citizens. If lone wolf terrorism is truly changing the calculus of privacy vs. harm, then there may be indeed exist strong reasons to reconsider how extensive government surveillance we should allow. At this point, however, it is far from clear that such justification is in place.

Traditionally, at least in a European perspective, invasive methods such as wire-tapping have only been allowed when the police have had independent reasons to believe that a crime has been committed or is being planned. Permission for the interception must be obtained from a court of law. However, such a procedure requires that the police know the identity of the suspect. This is not possible when searching for lone-wolves with unknown identity, where it is instead necessary to watch a larger number of posts, the vast majority of which are in all likelihood completely innocent. The problem can in many aspects be compared to camera-surveillance of public places. The cameras are meant to be used to detect criminal behaviour, but have the drawback of also monitoring innocents. It also challenges the feeling of a place – in our case the Internet – being truly public, in the sense of allowing and accepting the presence of people who fall outside of current norms. A recurring worry is the function creep of surveillance systems: will they really only be used to reduce criminality or will they in fact become powerful tools of oppression? And who will eventually pay the price?

If police or intelligence agencies should be allowed to use social media monitoring and analysis techniques in order to find digital traces of potential lone wolf terrorists, in what way ought we restrict and control such monitoring? To continue the comparison with cameras, the impression is that while automatic surveillance in public places often generates controversy and discussion, patrolling police officers seldom do. We may need to look closer at such phenomena as an important task ahead is to search for ways in which Internet surveillance can be carried out with the same sense of legitimacy as well-accepted forms of law enforcement and crime prevention.

Another issue to consider is which level of accuracy that is required from such a tool before it is put into operational use. If the techniques that have been presented here can be used to detect a lone wolf terrorist before he strikes and avoid innocent people from being killed, is that reason enough to implement such a system? Does it depend on the false positive rate (i.e. the number of innocent people who are labelled as potential lone wolves)? If so, how high can we allow this false positive rate to be? Again, there are many questions without obvious answers. One thing that we would argue strongly for at this point is that we should not aim for a fully automated system; the human intelligence analyst has to be the one who should take the decision of whether or not to investigate someone further, not least due to legal reasons. However, also semi-automated systems would be of little use if the classification performance of the recommendations would be wrong too often. We therefore see a clear need for investigating what performance levels that can be achieved before putting such a system into operational use.

Notes

1. Spaaiij, R. (2012) *Understanding Lone Wolf Terrorism Global Patterns, Motivations and Preventions.* Springerbriefs in Criminology, Springer.
2 Abcarian, R. (2010) *Scott Roeder convicted of murdering abortion doctor George Tiller*. Los Angeles Times, January 29.
3 Von Brunn, J. (2009) *An ADL backgrounder beliefs and activities*. In Anti-Defamation League, June 11.
4 Semenov, A., Veijalainen, J., and Kyppö, J. (2010) *Analysing the presence of school-shooting related communities at social media sites.* Int. J. Multimedia Intelligence and Security, Vol 1, No. 3.
5 Meloy, R., Hoffmann, J., Guldimann, A., James, D. (2012): *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*. Behavioral Sciences and the Law 30: 256-279.
6 Meloy, R and O'Toole, ME. (2011) *The Concept of Leakage in Threat Assessment.* Behavioral Sciences and the Law 29(4):513-27.
7 Semenov, A., Veijalainen, J., and Kyppö, J. (2010) *Analysing the presence of school-shooting related communities at social media sites.* Int. J. Multimedia Intelligence and Security, Vol. 1, No. 3.
8 Newman, K., Fox, C., Roth, W., Mehta, J., and Harding, D. (2004) *Rampage: the social roots of school shootings*. Basic Books, NY, USA.
9 Meloy, R, and O'Toole, ME. (2011) *The Concept of Leakage in Threat Assessment.* Behavioral Sciences and the Law 29(4):513-27.
10 Meloy, R., Hoffmann, J., Guldimann, A., James, D. (2012): *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*. Behavioral Sciences and the Law 30: 256-279.
11 Moskalenko, S. and McCauley, C. (2011) *The Psychology of Lone Wolf Terrorism*. Counselling psychology quarterly, vol. 24, 2, 115-126.
12 Ginges, J., Atran, S., Sachdeva, S., and Medin, D. (2011). *Psychology Out of the Laboratory: The Challenge of Violent Extremism.* American Psychologist, vol. 66, 6.
13 McCauley, C., and Moskalenko, S. (2008) *Mechanisms of Political Radicalization: Pathways Toward Terrorism*. Terrorism and Political Violence, vol. 20, 3.
14 Meloy, R., Hoffmann, J., Guldimann, A., James, D. (2012): *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*. Behavioral Sciences and the Law 30: 256-279
15 Taylor, J. (2011). *Unmasked: the far-right blogger idolised by Breivik.* The Independent. Retrieved 2 July 2012 from http://www.independent.co.uk/news/world/europe/unmasked-the-farright-blogger-idolised-by-breivik-2332696.html
16 Larkin, R. W. (2009) *The Columbine Legacy*. The American Behavioral Scientist, vol. 52, 9, 1309-1326
17 Michael, G. (2012) *Lone Wolf Terror and the Rise of Leaderless Resistance*. Vanderbilt University Press.
18 McCauley, C., and Moskalenko, S. (2008) *Mechanisms of Political Radicalization: Pathways Toward Terrorism*. Terrorism and Political Violence, vol. 20, 3.
19 Ginges, J., Atran, S., Sachdeva, S., and Medin, D. (2011). *Psychology Out of the Laboratory: The Challenge of Violent Extremism.* American Psychologist. Vol 66, 6.

[20] Moskalenko, and S. McCauley, C. (2011) *The Psychology of Lone Wolf Terrorism*. Counselling psychology quarterly, vol. 24, 2, 115-126.

[21] Abbasi, A., Chen, H., Thoms, S., and Fu, T. (2008) *Affect analysis of web forums and blogs using correlation ensembles*. IEEE Transactions on Knowledge and Data Engineering, Vol. 20, No. 9, pp. 1168-1180.

[22] Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C., and Svenson, P. (2012) *Analysis of Weak Signals for Detecting Lone Wolf Terrorists*. Proceedings of EISIC 2012, pp. 197-204.

[23] Narayanan, A., Paskov, H., Zhenqiang Gong, N., Bethencourt, J., Stefanov, E., Chul Richard Shin, E., and Song, D. (2012) *On the Feasibility of Internet-Scale Author Identification*. Proceedings of the 2012 IEEE Symposium on Security and Privacy, pp. 300-314.

[24] Dahlin, J., Johansson, F., Kaati, L., Mårtensson, C. and Svenson, P. (2012) *Combining Entity Matching Techniques for Detecting Extremist Behavior on Discussion Boards.* Proceedings of International Symposium on Foundation of Open Source Intelligence and Security Informatics 2012.

[25] Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C., and Svenson, P. (2012) *Analysis of Weak Signals for Detecting Lone Wolf Terrorists*. Proceedings of EISIC 2012, pp. 197-204.

[26] McCauley, C., and Moskalenko, S. (2008). *Mechanisms of Political Radicalization: Pathways Toward Terrorism*. Terrorism and Political Violence, vol. 20, 3.

[27] Pennebaker, J. W. and Chung, C. K. (2008). *Computerized text analysis of al-Qaeda transcripts.* In Krippendorf, K. and Bock, M. A., editors, The Content Analysis Reader. Sage.

View publication stats