Security Informatics
a SpringerOpen Journal

RESEARCH Open Access

# Harvesting and analysis of weak signals for detecting lone wolf terrorists

Joel Brynielsson, Andreas Horndahl, Fredrik Johansson, Lisa Kaati*, Christian Mårtenson and Pontus Svenson

**Abstract**

Lone wolf terrorists pose a large threat to modern society. The current ability to identify and stop these kinds of terrorists before they commit a terror act is limited since they are hard to detect using traditional methods. However, these individuals often make use of Internet to spread their beliefs and opinions, and to obtain information and knowledge to plan an attack. Therefore there is a good possibility that they leave digital traces in the form of weak signals that can be gathered, fused, and analyzed.

In this article we present an analysis method that can be used to analyze extremist forums to detect digital traces of possible lone wolf terrorists. This method is conceptually demonstrated using the FOI Impactorium fusion platform. We also present a number of different technologies which can be used to harvest and analyze pieces of information from Internet that may serve as weak digital traces that can be fused using the suggested analysis method in order to discover possible lone wolf terrorists.

## Introduction

Today, one of the most challenging and unpredictable forms of terrorism is violent terror acts committed by single individuals, often referred to as lone wolf terrorists or lone actor terrorists. These kinds of terror attacks are hard to detect and defend against by traditional police means such as infiltration or wiretapping, since the lone wolves are planning and carrying out the attacks on their own. The problem of lone wolf terrorism is according to many officials presently on the rise and viewed as a greater threat towards society than organized groups. Even though available statistics suggest that lone wolf terrorists account for a rather small proportion of all terror incidents [1], they can often have a large impact on society [2]. Moreover, many of the major terrorist attacks in the United States (with exception for the 2001 attacks against World Trade Center, the Pentagon, and the White House) were executed by single individuals who were sympathetic to a larger cause—from the Oklahoma City bomber Timothy McVeigh to the Washington area sniper John Allen Muhammad. A similar development can be seen in Europe, where several terrorist attacks have been executed by lone wolf terrorists during the last years. One of the most terrifying acts was the two 2011 terror attacks in Norway committed by Anders Behring Breivik, killing 77 persons in total.

Even though lone wolf terrorists cannot in general be captured by traditional intelligence techniques, this does not imply that there is nothing counterterrorist organizations can do to prevent them. In fact, despite the popular use of the term "lone wolf terrorist," many of the perpetrators are only loners in their offline life, but are often very active in communicating their views and radical opinions in various discussion groups or other kinds of social media. According to Sageman [3], most lone wolves are part of online forums, especially those who go on to actually carry out terrorist attacks. This makes the Internet an incredibly important source for finding potential lone wolf terrorists.

There are several communities that encourage and influence individuals to act alone (one example being the English language online magazine Inspire, published by the militant Islamist organization al-Qaeda in the Arabian Peninsula). Moreover, individuals that act alone are also often active on and influencing these kinds of communities. Online extremist forums and web sites allow for aberrant beliefs or attitudes to be exchanged and reinforced, and create environments in which otherwise unacceptable views become normalized [4]. In addition to give a possibility of becoming part of a community, the Internet is

*Correspondence: lisa.kaati@foi.se
FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden

also a platform where lone wolves can express their views. The 2010 suicide bomber in Stockholm, Taimour Abdulwahab al-Abdaly, was for example active on Internet and had a YouTube account, a Facebook account, and searched for a second wife on Islamic web pages. Anders Behring Breivik used several different social networking sites such as Facebook and Twitter, and posted his manifesto "2083—A European Declaration of Independence" on the Internet before committing the two terror attacks in Norway. The possession of several social media accounts is obviously perfectly normal, but the actual social media content can indicate that someone is planning a terror attack.

One of the major problems with analyzing information from the Internet is that it is huge, making it impossible for analysts to manually search for information and analyze all data concerning radicalization processes and terror plans of possible lone wolf terrorists. In addition to all material that the 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 part of Internet that is not indexed by the search engines' web spiders (e.g., due to password protection or dynamically generated content). To produce fully automatic computer tools for finding terror plans is not possible, both due to the large amounts of data and 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, computer-based support tools that aid the analysts in their investigation could enable them to process more data and give better possibilities to analyze and detect the digital traces [5]. In this article, we suggest the use of techniques such as hyperlink analysis and natural language processing to map the existing dark web forums and to find out which forums and users that can be of interest for human analysts to take a closer look at. In order to combine the outputs from the various suggested methods, we propose using information fusion techniques implemented in FOI's Impactorium fusion platform [6-8].

It is important to understand what can and cannot be done by the type of tools that we present in this article. Our aim is not to produce tools for completely automatic analysis of web information. Rather, the goal is to do research on support tools and methods that help law enforcement officers in ongoing investigations of web extremism. The research presented in this article is part of the fusion framework that we are building, and should be seen as suggestions for how components of a full system could be implemented. Some of the components have already been implemented and evaluated (e.g., the suggested alias matching algorithms, see [9]), while other components are not yet implemented and evaluated (e.g., algorithms for discovering warning behaviors such as fixation in postings). A full system for investigation of web extremism must be scalable and also account for privacy and integrity issues as well as what is legally possible and not. An important output of this kind of research is to make legislators aware of the possibilities and limitations of web analysis, in particular concerning opportunities for abuse that might arise if they are implemented operationally.

What is an extreme opinion will of course depend on the viewpoint of the user. This is yet another reason for being careful before implementing systems such as the one described in this article. There must be clear legal guidelines that respect the privacy and integrity of citizens before law enforcement officers can be allowed to do semi-automatic analysis of web content. Controls must be built into the systems, to limit as much as possible the possibilities of abuse.

The rest of this article is outlined as follows. In the section "Lone wolf terrorists," we give a short background to lone wolf terrorism, and the challenge of finding and identifying such individuals before it is too late. In the section "Analysis model" we propose an analysis method for breaking down the problem of analyzing whether a person is a lone wolf terrorist or not into smaller subproblems, such as identifying motives (intent), capabilities, and opportunities. These are broken down further, until more concrete indicators are identified that can be fused in order to make an estimate of how probable it is that an individual is a lone wolf terrorist. This is followed by a short section entitled "Users" containing a description of the potential users of the system and the requirements on their training. The section "Seed identification and topic-filtered web harvesting" describes how topic-filtered web harvesting can be used to collect relevant information, and the section "Techniques for analyzing data" presents techniques that can be used to detect indicators supporting that someone has intent to commit a terror attack. The section "Ranking and assessment of aliases" describes how the gathered indicators can be assessed, and the section "Alias matching" describes how Internet users with multiple aliases can be detected. The section entitled "The FOI Impactorium fusion platform" describes how the Impactorium tool can be used to fuse weak signals for detecting lone wolf terrorists. A discussion about the future potential of this kind of techniques and privacy aspects related to automatic monitoring and analysis tools is provided in the section "Discussion." Finally, some concluding remarks are presented in the section "Conclusions."

## Lone wolf terrorists

The definition of a lone wolf terrorist to be used throughout this article is the one used in [10]:

*A lone wolf terrorist is a person who acts on his or her own without orders from or connections to an organization.*

Lone wolves come from a variety of backgrounds and can have a wide range of motives for their actions. It is observed by [1] that lone wolf terrorists are often creating their own ideologies, combining aversion with religion, society, or politics with a personal frustration. Hence, a lone wolf terrorist can in theory come in any size, any shape, and any ethnicity, as well as representing any ideology [11].

To conduct a successful terror attack, it is necessary to have a number of skills and/or capabilities. For a lone wolf, obtaining the necessary capabilities for an attack might be a problem since they can not in general receive the same kind of systematic training such as, e.g., al-Qaeda terrorists. This may be one of the reasons why lone wolves are rarely suicide bombers, i.e., since such an attack may be too complicated and involves too much preparation [11]. However, the Internet contains much material that potential lone wolf terrorists can use to acquire the knowledge they need to succeed with more simple kinds of attacks. For example, resources such as "the Anarchist Cookbook," "Training with a handgun," "Remote Control Detonation," and "How to make a bomb in the kitchen of your mom" are known to be widespread on the Internet and have been used by lone wolf terrorists for acquiring knowledge on how to build simple pipe bombs, etc.

It is not unusual that lone wolf terrorists are sympathizing with extremist movements, but by definition they are not part of or actively supported by these movements. This makes it very hard to discover and capture lone wolf terrorists before they strike, as traditional methods such as wiretapping and infiltration of the organization are not applicable (since there are no networks or organizations to infiltrate). Moreover, it can be very hard to differentiate between those individuals who are really intending to commit an actual terrorism act, and those who have radical beliefs but stay within the law. In fact, there are very many people that have extremism opinions, but only a minority of those cross the line into taking violent action based on such beliefs.

### Digital traces on the Internet

Even though lone wolf terrorists are in general extremely hard to detect by traditional means, there are often many weak signals available that, if detected and fused, can be used as markers of potentially interesting behavior that have to be analyzed deeper and investigated further. As has been mentioned by Fredholm [12], nearly all radicalization of lone wolf terrorists take place on the Internet. One example of a well-known online resource inspiring homegrown terrorism is the online magazine Inspire, published by the Yemen-based organization al-Qaeda in the Arabian Peninsula (AQAP). Internet based recruitment to terrorist groups is also likely to grow in significance, although recruitment to terror organizations are more often dependent also on offline networks [3,4,13]. These kinds of Internet based radicalization processes often result in various digital traces, created when visiting extremist forums, making postings with offensive content, etc. There are also many other examples where Internet has been used by lone wolves to spread their views and opinions before committing an actual attack. One such example is the anti-abortion activist Scott Roeder who killed the physician George Tiller in Kansas in 2009 [14]. Tiller was one of the few doctors in the United States that performed late abortions, and before the attack Scott Roeder wrote a column on an abortion critical web page where he expressed his views against abortion and Tiller's work. Another example of a lone wolf that was using Internet to express his views is James von Brunn, also known as the Holocaust Museum shooter [15]. Von Brunn was an anti-Semitic white supremacist who was in charge of an anti-Semitic website where he was able to express his views long before the attack.

Once a terror activity has taken place, it is not unusual that, e.g., media collect various digital traces in retrospect, and make complaints about the police's or intelligence service's ineffectiveness or lack of competence. However, although it can be quite easy to find the related evidence once the terror activity already has taken place, it is much more difficult to find out what the relevant clues (weak signals) are before an actual attack has been carried out. There are some signs that can be identified, though. One such sign is activity on radical forums or other forms of social media. Another sign is radical or hateful expressions in written text.

In [16], a number of suggestions of behavioral markers for radical violence that can be identified in written text are presented. These behavioral markers are derived from a list of warning behaviors described in [17]. The behavioral markers considered in [16] are:

**Leakage**, i.e., the communication to a third party of an intent to do harm to a target, such as the postings made by many school shooters before their attacks.

**Fixation**, i.e., an increasingly pathological preoccupation with a person or a cause, such as Clayton Waagner's gathering of target information on abortion doctors.

**Identification**, i.e., the desire to be like an influential role-model, "warrior identification," or identification with a group or larger cause. One example of warrior identification would be the images of Anders Behring Breivik pointing an automatic weapon against the camera.

These behavioral markers can be used as indicators supporting that someone intends to commit a terror attack.

To find relevant digital traces for the behavioral markers, semi-automated analysis is needed since it is impossible for human analysts to manually monitor all the activities of interest on Internet. Such analysis is described in more detail in the section "Techniques for analyzing data." In the next section, an analysis model that can be used to analyze digital traces that a possible lone wolf terrorist might leave on the Internet is presented.

While there is much research on markers for extremist behavior, it is important to realize that the possibility for human biases when defining them always exists. The users who operate the analysis tools must be aware of this and measures must be taken to ensure that, as much as possible, the chosen markers are objective. One way of ensuring this is through extensive training for the analysts. In addition, it must be possible to continuously update and adapt the chosen markers if, for instance, a person has been wrongly identified as an extremist and the reason for the mistake can be identified as a single marker. This highlights the need for always explicitly storing the chain of evidence or markers that have been used for reaching a certain conclusion.

## Analysis model

A classical approach to address complex problems is to break them down into more manageable sub-problems, solve these separately and then aggregate the results into a solution for the overarching problem. This approach is well suited for the analysis of weak signals. For each potential threat actor, which in most cases will be represented by one or many aliases (user names), a model is created through the successive decomposition of the threat hypothesis into a number of indicators, corresponding to the weak signals that we want to capture. Figure 1 shows a (simplified) model of how the decomposition of the hypothesis "Actor X is a potential lone wolf terrorist" could look like. At the first level, the hypothesis is separated in three general threat assessment criteria: *Intent* (or *motive*), *Capability*, and *Opportunity*. If all these are met there is a potential risk for an attack. The next level of decomposition shows a number of indicators that can possibly be detected through reconnaissance on the Internet, and the indicator "Materiel procurement" which could also be detected through other information channels.

Once an initial decomposition is done, parallel sub-processes can be started for the various sub-hypotheses. As an example, assuming that an analyst believes that someone needs to have both intent and capability in order to commit a terror attack, one sub-process can focus on looking for possible intent (e.g., based on radical postings made by the individual) while the other one is focusing on capability (e.g., web sites discussing how to make bombs). The results from the various sub-processes are then fused and can be used to assess whether someone has an increased likelihood of committing an act of terror, resulting in a list of potentially dangerous actors that might be subject to further analysis. It is important to note that since we consider digital traces that are left on the Internet, it is only possible to detect aliases that might have an increased risk of committing an act of terror, but how the physical person behind the alias can be detected is another problem that is outside the scope of this article.

In this work we focus our attention on the problem of finding out whether someone has the intent to commit an act of terror. In the section "Techniques for analyzing data" we describe techniques that can be utilized in order to detect digital traces that can be used as evidence for some of the identified indicators supporting that someone has the intent of committing a terror attack.

## Users

As mentioned previously, this article describes concepts and prototypes that could be implemented in an operational system for web analysis of extremist behavior. The potential user of this system is a law enforcement officer

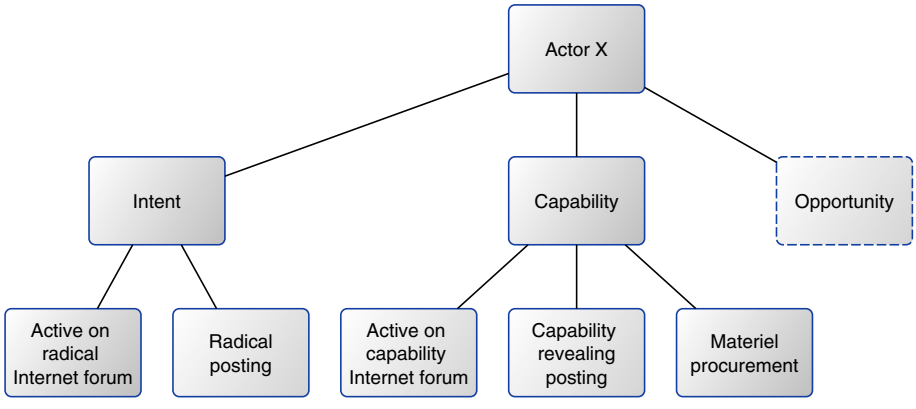


**Figure 1 Breakdown of a hypothesis regarding a possible lone wolf terrorist.**

who today investigates web extremism by browsing well-known extremist web sites and manually searches for signs of planned terror attacks or individuals that have to be investigated more closely. By developing a better support system for this, it will be possible to analyze more data and reduce the risk for false negatives. It is important that the potential introduction of such systems is accompanied by clear regulations regarding what data the user is, and is not, allowed to investigate. Prototype systems such as the one developed by the project described herein could be an important help for legislators and human rights organizations to evaluate the consequences of allowing or banning different kinds of automatic analyses.

It is important that the users of web analysis systems are properly trained. In addition to the training in legal, privacy and integrity issues that was touched upon above, they must also have proper training in decision theory to be able to avoid as many as possible of the human biases that might otherwise induce them to construct non-objective analysis models and markers. Total impartiality when constructing these if of course a chimera. Hence it is necessary to include checks and balances in the system, both in the technology and in the form of peer reviews of both analysis models (including markers) and the results of analyses.

We believe that serious gaming [18,19] training could be an important component to help ensure that the users of the system meet these requirements. By making the training as realistic as possible, it will be easier to train the analyst to detect their own biases. This is, however, just an idea that has not yet been tested and will not be elaborated upon further in the article.

## Seed identification and topic-filtered web harvesting

The amount of content on the Internet is enormous and it does not make sense to try to search for digital traces from potential lone wolf terrorists without any guidance. Therefore, it is necessary to limit the search and instead focus on a smaller subset of the Internet. Although there are large portions of the web that are not reachable using search engines such as Google, many extremist web sites are well-known, since part of the idea is to communicate ideologies and other messages to the larger masses. Moreover, a majority of extremist web sites contain links to other extremist sites, according to a study presented in [20]. Hence, it makes sense to use well-known extremist sites as seeds[1], and then try to identify other interesting forums and sites that in some way are connected to the web sites, by using the seeds as a starting point (it is not necessarily so that only extremist web sites are of interest, also "normal" web sites containing information regarding an indicator may be interesting to watch).

The process of systematically collecting web pages is often referred to as crawling. Usually, the crawling process starts from one or more given source web page(s) (the seeds described above) and follows the source page hyperlinks to find more web pages [21]. The crawling process is repeated on each new page and continues until no more new pages are discovered or until a certain number of pages (that have been determined beforehand) have been collected. By treating the collected web sites as nodes in a graph, and by creating an edge between two web sites each time a hyperlink is found between them, it becomes possible to create a (large) network that can be analyzed further to find out which the most interesting web sites are. By using hyperlink analysis a large number of potential extremist forums can be found. However, many of the web sites will be perfectly normal, making them rather uninteresting for intelligence analysts. Hence, it is of uttermost interest to be able to automatically separate web sites with interesting content from the ones with normal, uninteresting content (that is, from a counterterrorist perspective). In order to make this kind of analysis, natural language processing (NLP) and text mining can be of great use. As a first step, we suggest having a predefined list of keywords to search for on the crawled web pages. If enough of the terms are encountered on a web page, it is marked as interesting and the web site is added to the queue. However, if they are marked as irrelevant, the web page becomes discarded, and no links are followed from it. The same holds true for URLs that are part of a *white list*, to which the analyst can choose to add web sites matching the keywords but are judged not to be relevant for further analysis (e.g., web sites with the purpose of countering extremist propaganda). While crawling the web it is also possible to discard links that are broken. If a web site is inaccessible due to password protection, the analyst can be asked to either choose to discard the link, or to manually create a user login and enter the user credentials to access material on the site. Our suggested approach is in many ways similar to the approach used for identifying online child pornography networks in [22].

To evaluate our web mining approach, we have implemented a proof-of-concept web spider. The goal is to create a network consisting of web sites, forums (discussion boards), forum posts and aliases. An example of such a network can be found in Figure 2. As can be noted, the network becomes very large and therefore it is important to prune the network using natural language processing techniques. The spider is based on the crawler Crawler4J[2] and extended with methods for Internet forum information extraction.

Given a set of seeds (web page URLs), the web spider expands the network by following all links that can be found on the page that meet a set of conditions. First of

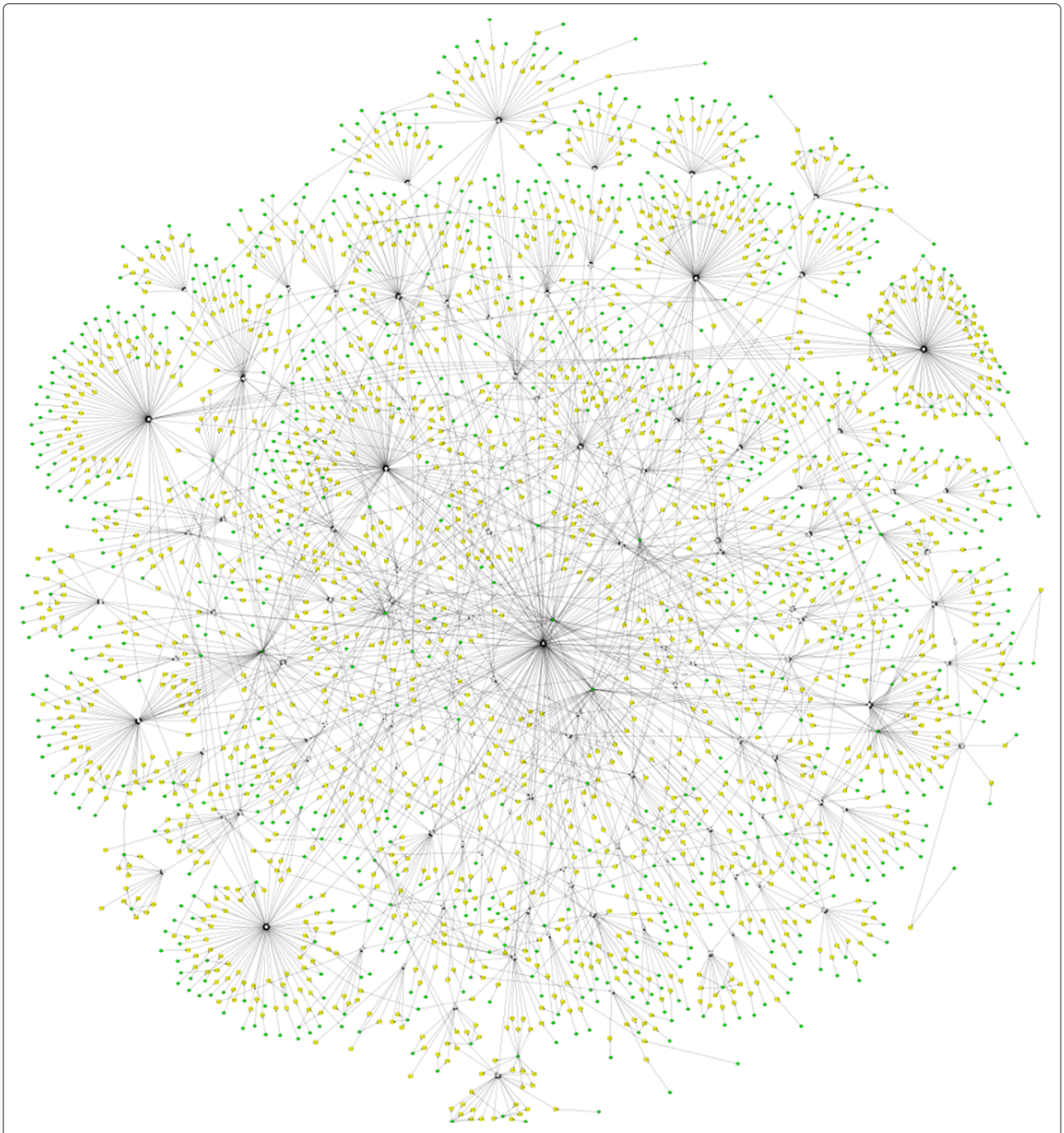

**Figure 2 A network graph created by our web spider based on a single seed.** Nodes in the network represent a discussion board, posts, and aliases.

all the link should point to a web page, and secondly the content of the web page should be classified as interesting (matching a list of one or several predefined keywords). If the page represents a discussion forum, tailored content extraction algorithms are applied. The algorithms extract the user aliases and their posts, and add this information to the network (to be further used in the web site and alias assessment phases). In our initial proof-of-concept implementation, we have developed information extraction algorithms for a specific representative Internet forum.

In a real-world setting, one needs to address the fact that Internet forums or web sites may have significantly different structures. Hence, a flexible strategy for learning the

structure of a new site is desirable. One way to overcome this obstacle is to let an algorithm guess the structure, try to extract relevant information and let a human (the analyst) verify the results. Another way is to let humans analyze the hypertext representation and locate specific tags that can be used as markers for where to find relevant information and how to separate posts.

## Techniques for analyzing data

Once the collection of relevant data from the Internet is done the content of the web site and forums needs to be analyzed. In this section we present techniques that can be used by intelligence analysts to analyze data with the aim of discovering indicators supporting that someone has intent to commit an act of terror. The goal of the process described in this section is to obtain a list of potential lone wolf terrorists that need further investigation. Comparing our suggested approach to related work already described in existing research literature (see, e.g., [23-25]), two main differences can be identified: 1) our focus on lone wolf terrorists rather than terror organizations, and 2) our focus on semi-automated tools for supporting the analyst, rather than fully automated tools. While it obviously is interesting to construct fully automatic tools for web analysis, it is more realistic to consider a web analysis system that consists of a human user that is supported by tools such as those described in this article. In addition to the problems of making reliable automated tools, there are also cultural and ethical requirements that make it interesting to consider semi-automated tools [5].

From the topic-filtered web harvesting, a set of interesting web sites or forums are collected. The idea is to make a deeper analysis of these sites by making use of natural language processing and text mining techniques. One type of text mining known as affect analysis has earlier been identified as being useful for measuring the presence of hate and violence in extremist forums [26]. To be able to use natural language processing techniques, it is necessary to first preprocess the retrieved content from the web sites. This preprocessing step for example includes removing HTML tags and tokenizing the text into sentences. From the collected data, all aliases are extracted and a model is created for each alias. The fact that all identified aliases are active on web sites that are considered radical qualifies them as candidates for further investigation.

### Intent

We have in [16] identified a set of indicators for someone having the intent to commit an act of terror and becoming a lone wolf terrorist. The list of indicators is not comprehensive and we use it to illustrate how it is possible to automatically detect evidence for indicators using text analysis techniques. The indicators that we use are:

- the fact that someone is active on a radical web page,
- radical expression in postings,
- leakage,
- identification,
- fixation.

In the following sections we describe techniques that can be used to automatically detect these indicators from text.

#### *Active on radical web pages*

The fact that someone is active on a radical web page can be revealed by identifying any kind of activity on the set of web pages that are collected using the topic-filtered web harvesting. The web pages that are collected are all considered to be radical in some sense and therefore we can assume that all users that are active on any of the web pages may be considered radical. This assumption does not necessarily hold true in practice since people may post things on extremist web pages without being extremists themselves. In such cases it is however unlikely that other indicators will be activated for the person anyway.

#### *Radical expression in postings*

Classifiers for estimating the level of radical content or other types of interestingness in a text (e.g., a blog post or a tweet) can be built in various ways. One alternative is to manually create a discriminant-word lexicon that can be used for classifying the text; the higher fraction of terms in the text present in the lexicon, the higher the level of interestingness. To manually create such a list may be a tricky task, and it may also be necessary to update the list with regular intervals, as the popular words to express radical opinions or other kinds of topics may change over time. Within the research field of text mining, it has been shown that handcrafted lexicons are often not the best alternative for text classification tasks. Instead, various unsupervised and supervised learning algorithms are more frequently used. Irrespectively of which type of technique that is used, some input will be needed from an expert. In case a handcrafted list of words is used, the actual terms to use have to be specified by experts. In the case of an unsupervised approach, a list of seed terms has to be suggested by the experts which then can be used to automatically find and classify other terms that, e.g., are synonyms or antonyms to the manually labeled terms, or in other ways are co-occurring with terms with a known label. Finally, in the supervised case, the expert has to manually classify a number of text samples into the classes *radical* and *non-radical* (or *interesting* and *non-interesting* in the more general case). It can be expected that the supervised approach will yield the best performance, but this comes with a cost of finding useful data for training purposes, and the manual annotation of the training data. This kind of methods have previously been proposed in [26].

One type of classifier that is often used for various supervised natural language classification tasks is the naïve Bayes classifier. This is the classifier we currently intend to use in our system. The classifier, however, still needs to be learned using representative training samples, which remains as future work. An advantage of such an approach is that it is easy to interpret for humans, making it possible to verify that a learned model looks reasonable. Furthermore, it is more computationally effective than many alternative algorithms, making the learning phase faster. In order to use such a classifier for discriminating between texts with *radical* and *non-radical* content, a natural first step would be to tokenize the text. By extracting features such as unigrams (single words), bigrams (pairs of words) or trigrams (triples of words) from the tokenized text, this can be used for training the classifier and to classify new texts once the classifier has been trained. Since there would be very many features if allowing for all possible unigrams and bigrams, a necessary step would be feature reduction, in which the most informative features $f_1, \ldots, f_n$ are selected from the training data and used as leaf nodes in the resulting classifier. By extracting features from new texts to be classified, we can according to Bayes' theorem calculate the posterior probability of the text having a certain label (e.g., *radical* or *non-radical*) as:

$$P(label|f_1, \ldots, f_n) = \frac{P(label)P(f_1, \ldots, f_n|label)}{P(f_1, \ldots, f_n)}. \quad (1)$$

Now, by using the conditional independence assumption of the naïve Bayes model, this is reduced to:

$$P(label|f_1, \ldots, f_n) \propto P(label) \prod_{i=1}^{n} P(f_i|label). \quad (2)$$

This conditional independence assumption is rather strong and does not necessarily hold in practice. Given the class label, the occurrence of a word is not independent of all other words, even though this is assumed in Equation 2. This may result in that conditionally dependent words can have too much influence on the classification. Despite this, naïve Bayes methods have been shown to work well for many real-world problems. The needed probabilities on the right side of Equation 2 can easily be estimated from the training data (using Laplace smoothing to account for zero counts).

Other popular choices for text classification tasks is the use of maximum entropy classifiers (relying on the principle of choosing the most uniform distribution satisfying the constraints given by the training data) or support vector machines. Regardless of the choice of classifier, the most important part is to get hold of enough training data of good quality. Once this is solved, the next big question is which features to use. To use unigrams as features is the most straightforward way and will most likely be enough to separate terrorism-related discussions from many other kinds of discussions of no relevance to the subject matter. However, it is not obvious that unigrams are enough for more fine-grained classification, e.g., separating between postings where terrorist acts are discussed or reported on, and where intentions to actually commit terrorism acts are expressed. It may therefore be beneficial to use bigrams or trigrams to allow for a less shallow analysis. The feature set to be used in our implementation will be decided in future experiments.

It should be noted that what ought to be taken to constitute radical behavior is often in the eyes of the beholder. However, since such judgements are made by analysts already today (although manually), creation of algorithms that classify posts according to the same criteria would be no different from todays' situation (except for that the classification of texts then can be made on a much larger scale).

#### *Leakage*

A notable characteristic of lone wolf terrorists is that they often announce their views and intentions in advance. In the samples of school shooters (a phenomenon closely related to lone wolf terrorism) analyzed in [27], it can be seen that a majority of the perpetrators revealed their intentions in social media before carrying out their attacks. Leakage is the communication to a third party of an intent to do harm to a target. Leakage can be either intentional or unintentional and more or less specific regarding the actual attack [17].

Leaked information of intent is likely to contain auxiliary verbs signaling intent (i.e., "…will …," "…am going to …," "…should…") together with words expressing violent action, either overtly or, perhaps more likely, through euphemisms. Based on these observations, leakage can potentially be detected by using a simple approach where the analyzed text after stemming or lemmatization (reducing the end of a word in order to return the word's common base form) is matched against a predefined word list of violent actions. Since there is a large number of synonyms that can be used for the verbs signaling a violent intent, the use of an ontology such as the lexical database WordNet[3] in which semantic relations between synonym sets are expressed can be used. 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 semantic relations, the number of words that must be explicitly defined in the word list of terms to search for can be 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, part-of-speech tagging should also be taken 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 the attention to sites or forums that through automated content analysis or prior knowledge are known to contain content related to violent extremism, false positives can most likely be kept at an acceptable level.

**Example** To illustrate leakage we use a sentence from Anders Behring Breivik's manifesto "2083—A European Declaration of Independence":

> *We will ensure that all category A and B traitors, the enablers of Islamization and the destroyers of our cultures, nations and societies, will be executed.*

In the sentence, a verb signalling intent such as "... will ..." is followed by an expression of violent action ("executed"). In WordNet, "executed" belongs to the same synonym set as "put to death."

#### *Identification*

The warning behavior called identification is defined as a behavior 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 [16]. This rather broad definition shows the complexity of the phenomenon. To make it more manageable, we follow [17] and divide identification into two subcategories: identification with radical action and identification with a role model. Group identification is considered an essential part of the radicalization of lone wolves as well as organized terrorists.

Identification with a group or cause can be expressed for instance by a usage of positive adjectives in connection with mentioning of the group. Similarly, a usage of negative adjectives in connection with mentioning of a group or person may indicate negative identification. To find out which positive or negative sentiments that are present in a text, or which kinds of emotions that are expressed, sentiment and affect analysis techniques can be used. References to the 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 [28] can be used as an indicator of extremism. In [28] the software LIWC is used to analyze the content of al-Qaeda transcripts.

Identification with a warrior, the so-called warrior mentality, can be spotted through the use of a certain terminology, while a sense of moral obligation can be expressed through the usage of words related to duty, honor, justice, etc.

Identification with another radical thinker can, aside from frequent quoting and mentioning, be expressed by a similarity in language. It is common that the same terminology as the role model is used and there is a possibility that even a similar sentence structure is used. In these cases it is possible to use author recognition techniques to identify similarities.

**Example** 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. Other examples of identification can be found among school shooters. One such example is Matthew Murray who killed four people at a church and a missionary training school in Colorado. Murray compared himself to the Columbine shooter Harris and Hui (who was responsible for the shooting at Virginia Tech University) in an Internet posting.

#### *Fixation*

The warning behavior fixation indicates a 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 [17].

Fixation can be observed as a tendency to repeatedly comment 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 a person chooses to share some of the information.

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

**Example** An example text where fixation can be detected can again be found in Anders Behring Breivik's manifesto "2083—A European Declaration of Independence":

> *It is not only our right but also our duty to contribute to preserve our identity, our culture and our national sovereignty by preventing the ongoing* `Islamisation`*. There is no Resistance Movement if individuals like us refuse to contribute... Time is of the essence. We have only a few decades to consolidate a sufficient level of*

*resistance before our major cities are completely demographically overwhelmed by* `Muslims`*. Ensuring the successful distribution of this compendium to as many Europeans as humanly possible will significantly contribute to our success. It may be the only way to avoid our present and future dhimmitude (enslavement) under* `Islamic` *majority rule in our own countries.*

In the text, it can be noted that words related to Islam ("Islamisation," "Muslims," and "Islamic") are mentioned with a high frequency.

## Ranking and assessment of aliases

After collecting relevant data using the topic-filtered web harvesting, the data is analyzed. The first part of the analysis is to identify all aliases that are present in the collected data. Thereafter the data is analyzed using techniques described in the previous section while searching for indicators for intent of committing an act of terror.

### Online instantiation of model templates

Once an alias is identified in the collected data, the alias is added to a list of aliases that need to be analyzed further. Naturally, one indicator for intent is not enough to classify the alias as a potential lone wolf terrorist with good reliability. However, having observed one indicator is a good reason to start looking for other indicators. In order to make a more detailed assessment of the alias, a threat model template (Figure 1) is instantiated for the alias. When a threat model for an alias has been instantiated, all relevant information related to the alias is connected to the indicators in the model. The threat model defines how to combine indicators of intent as well as other relevant indicators and can be used to do a summarized assessment. Moreover, the threat model can be used to determine which indicators we should collect more information about in order to improve the assessment.

### Combined indicator assessment

Since one indicator alone is insufficient for classifying an alias as a potential lone wolf terrorist with certainty, we need to combine the information of several indicators in order to make an adequate assessment. There are several potential ways to combine the indicators of intent that we have described in this article. One way is to require that we need positive evidence for all indicators in order to be able to say that the alias has an evil intent with sufficient credibility. Another way is to use a weighted average model where some of the indicators are more important than others. A third way is to demand that a certain number of indicators, e.g., three out of five, are sufficient in order to say that an alias has intent. A fourth way is to use a more advanced tailored statistical model such as Bayesian belief networks which makes it possible to define complex relationships between indicators. Since the statistical relationship between the indicators presented in this article are unexplored, the use of such a model is not feasible at the moment.

In addition to the current degree of belief that an alias has an intent to commit a terror attack, the change over time in the degree of belief may provide valuable information. For example, an alias for which we have identified two indicators and the degree of belief is increasing slowly but surely, might be as interesting as an alias for which we have identified three indicators and the degree of belief is unchanged or decreasing.

### Representing indicator states/values

The current state of an indicator can be represented in numerous ways. One way is to represent the current state by a binary value that expresses if we have evidence for the indicator or not. Another way is to use discrete values such as "unknown," "weak," "moderate," and "strong." A third way is to let a continuous value represent the probability (or belief mass, if we are using Dempster-Shafer theory) that the indicator is true. Non-binary approaches allow a more detailed way of describing the current state of an indicator but requires a method (manual or automatic) that specifies how to set the indicator state based on available evidence. For example, three radical message board entries are required to set the indicator value to moderate.

## Alias matching

One problem that arises when analyzing data from the Internet is the fact that people may use several different aliases. There are many potential reasons for an individual to use multiple aliases. It could be the case that the first alias has been banned on the forum, or that the author simply forgot the password to the original account. It could also be the case that an alias has lost the others' trust in the discussions, or that the author has developed bad personal relationships with other individuals at the forum. Another potential reason is that the author creates multiple aliases in order to be able to write messages that support his or her own arguments. No matter what the reason is for having multiple aliases, the fact that many people use several aliases makes an analysis more difficult since it is harder to fuse weak signals generated by a single user (individual) that is using multiple aliases.

Alias matching refers to techniques that can be used to identify a user that has several different aliases. If a user is active on a number of web sites, forums, or other kinds of social media and uses several different aliases, alias matching can be very difficult. In [29] and [9], techniques for detecting multiple aliases in discussion boards are described. Some of the components that can be used to detect multiple aliases are:

- similarities in alias name,
- stylometry,
- temporal information,
- similarities in networks (social networks or network of threads).

If a user is using the same alias everywhere it is simple, and if there are only small variations in user names, entity matching approaches such as the Jaro-Winkler distance metric [30] can be useful. However, if a user uses aliases which are more or less arbitrarily selected, the actual alias name as such cannot be used for the matching process.

Stylometry or analysis of writing style makes use of the assumption that every person has a more or less individual "writeprint" (cf. fingerprint) that is based on the way we write. A writeprint is created using different characteristics that can be discovered in text. Such characteristics could for example be choice of words, language, syntactic features, syntactical patterns, choice of subject, or different combinations of these characteristics [31]. Internet-scale authorship identification based on stylometry is described in [32]. Temporal information can also be used to identify users with multiple aliases. Temporal information could be information about what time of the day messages are posted or frequency of messages during longer time periods. Social network analysis (SNA) [33,34] could also be used to help in the identification of authors by computing structural similarities between different aliases. If two aliases post to the same forums, on the same topics, and regularly comment on the same type of posts, it is more likely that they are in fact the same. It is also possible to use abstraction techniques such as simulation [35] to determine the likelihood with which two aliases are the same. By combining various information about the aliases and the messages written by aliases the possibility to identify users with multiple aliases increases. In [9] we have shown that the combination of temporal information and stylometric information can yield good accuracy when detecting the use of multiple aliases in web forums. The problem of alias matching is important for the system proposed herein since we have to combine all aliases that are used by the user of interest in order to estimate the likelihood that an Internet user has intent to become a lone wolf terrorist.

Identifying the physical person behind an alias is another, although related, problem. If messages have been posted on non-radical forums it might be possible for police or intelligence services to get information about the IP address that has been used when making the posting, but this cannot be expected to be retrieved from extremist forums. Moreover, the IP address may not necessarily be of interest, since people can use dynamic IP numbers, use computers at Internet cafes, connect through VPNs, etc.

## The FOI Impactorium fusion platform

The FOI Impactorium fusion platform [6-8] is a prototype implementation that can be used to fuse information from heterogenous sources. Impactorium can be used to create top-down threat models as the one presented earlier in the section entitled "Analysis model." The threat models can be constructed using a graphical user interface or by using Impactorium's RESTful webservice API. The API makes it possible to create threat models or instantiate model templates as part of an automated process. The API can be used to instantiate a threat model such as the one depicted in Figure 1, when an alias that is active on a radical forum is detected. The API can also be used to update the threat model or add evidence to indicators. For example, an algorithm that performs alias matching can use the API to merge two threat models. Impactorium also provides a subscription mechanism which can be used to instantaneously receive a notification when a model component, such as an indicator or evidence, has been updated or added. This functionality can be used to notify an analyst when the degree of belief that an alias is a potential terrorist exceeds a threshold or to notify other analysis tools that new models have been created.

In Impactorium the values of the different indicators are fused in order to come up with an answer to the original problem, i.e., to which degree the collected evidence or weak signals support the hypothesis that an individual is (or will become) a lone wolf terrorist. A screen shot exemplifying how the values of a threat model are inferred in the Impactorium tool is shown in Figure 3. In the figure, the problem of deciding whether someone has the intent to commit a terror act is broken down into five indicators: active (on a radical web site), radical expression (in a posting), leakage, identification, and fixation. In the figure, evidence for the indicators "active on a radical web site" and "radical expression" has been identified.

Various combination functions such as min, max, average, or weighted sum can be used to make inferences. Except for combining the various digital traces that have been collected, Impactorium also allows for fusion of information coming from other sources, such as intelligence reports or data from sensors. As an example, if customs provide information that an individual has bought large quantities of fertilizers, this information can be inserted into the threat model calculations. In Figure 3, the likelihood that an actor has intent to become a lone wolf terrorist has increased since evidence for two (of the five) indicators are found.

When monitoring extremist web sites, a threat model is created for each alias and information about each alias is gathered. Based on the results of the fusion, a list of aliases worth monitoring more closely is created. An example of such a list is shown in Figure 4. The list can be used by

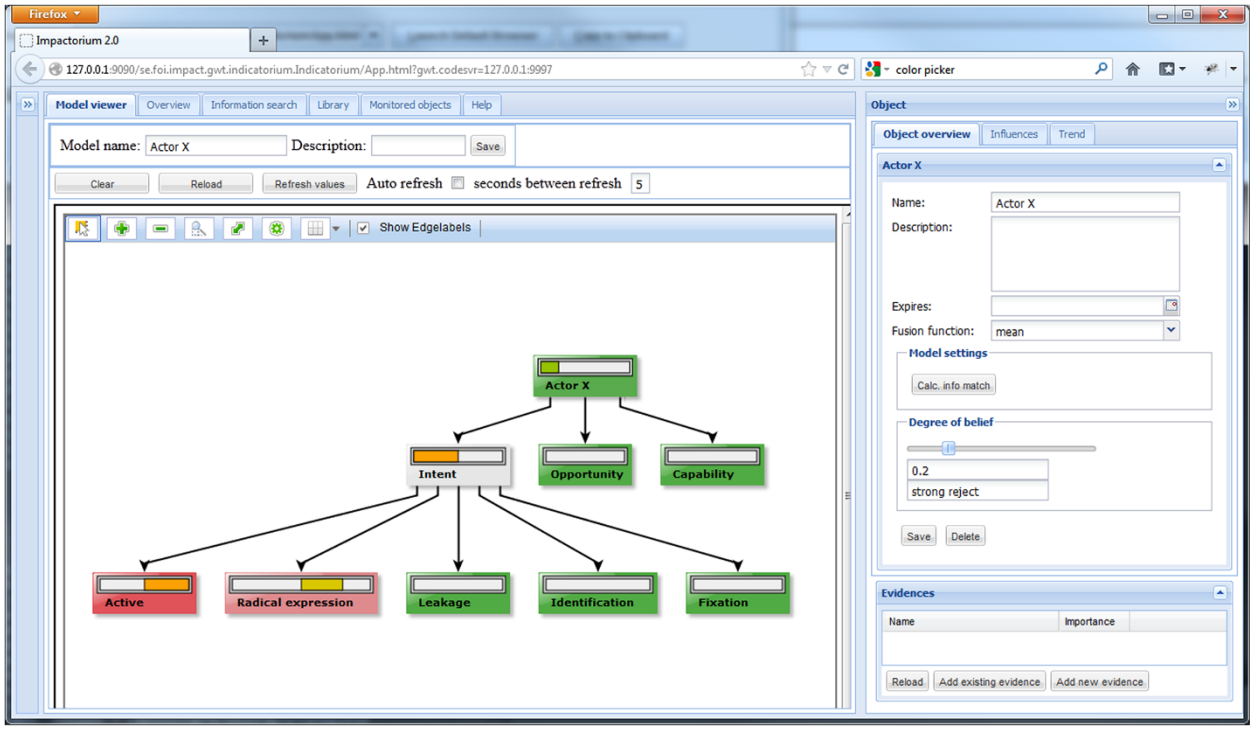


**Figure 3** A threat model in the Impactorium tool, where a number of evidences have been fused.

an analyst to direct further investigations and resources to the aliases on the list that have the highest likelihood of becoming lone wolf terrorists.

The analysis models in Impactorium are meant to be continuously updated and adapted to the current situation. It is thus easy for the user to change them if, e.g., too many false positives are detected. Both the structure of the models and the model parameters (e.g., how much evidence that is needed before an individual is indicated as a potential lone wolf) can be changed. An indicator or

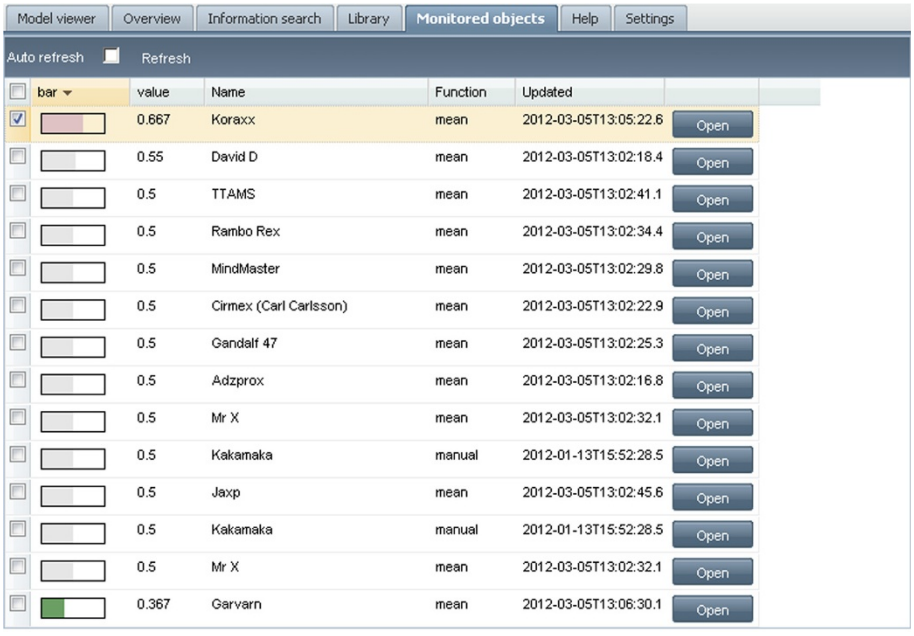


**Figure 4** List of monitored aliases within the Impactorium tool.

marker that has been determined to no longer be useful can also be forgotten.

Since the content of web sites such as extremist forums is not static, the overall process has to be repeated over and over again. The first stages can however be done more seldom than the later phases, since forums and web sites of interest will pop up or become obsolete on a much slower rate than the change in content within the web sites. It is also important to note that duration of time is a significant factor in this process. It is very likely that becoming a lone wolf terrorist is not something that happens over night, but is rather a process that can take several years.

## Discussion

The search for digital traces on Internet that can be fused in order to try to find potential lone wolf terrorists must be considered a fine balance between people's security at the one hand, and people's privacy on the other hand. To automatically search through large masses of text and use text mining techniques to try to identify whether a piece of text should be treated as radical or not can by some people be seen as a violation of privacy. The needs of the law enforcement and intelligence communities and the privacy concerns must be balanced. It should, however, be noted that analysts are already checking extremist forums as of today. It is always a human analyst that should check the reasons for why a user has been classified as having a motive or intent of being a potential lone wolf terrorist, and whether actions should be taken to bind an alias to a physical person, and to collect more information using other means. The analyst can also always decide whether an alias should be removed from the list of "suspect" individuals. This highlights the need for a mixed-initiative [36,37] system with a human-in-the-loop as a central component.

Having such a human-in-the-loop makes it possible to tolerate a higher number of false positives than would be acceptable in a fully automated system. Since there is a trade-off between false positives and false negatives, the increase of false positives should decrease the number of false negatives (i.e., classifying weak signals from potential terrorists as non-interesting). Hence, the suggested method should be thought of as a help for the analyst to filter out a smaller set of data to look at, rather than a method to be fully automated.

In the description of the suggested methodology, we have discussed how many indicators that are needed in order to say something about the intent of an individual, but there is also a question of how much material that is needed in order to trigger a single indicator. This is not a question with an easy answer since it most probably will vary for different indicators. Several radical posts are clearly more interesting than a single radical post, but several leakages are not necessarily worse than a single one. It also depends on whether binary, discrete, or continuous states are used, as mentioned earlier. The thresholds to use for deciding when, or how strongly, an indicator should be triggered remains as future work.

The analysis models and markers and indicators used will need to be continuously updated and adapted, both to keep track of changing behavior on the Internet and in order to, for instance, remove markers and models that have wrongly identified someone as a lone wolf terrorist. It is important that the tools used include ways of doing this, similar to the model adaptation tools that are implemented in the Impactorium tool.

While we have focused on analyzing text in this article, it is worth noticing that a lot of material posted to web sites and social media is not text. On extremist forums, it is not unusual with video clips showing executions, bomb making instructions, etc. There is much ongoing research on image and video content analysis, as well as content-based image retrieval (CBIR, see [38] for an overview) that can be useful in the future, but as far as we know, no mature techniques for identifying radical content in video with good precision exists as of today. Another possibility is to automatically extract speech from audio and video content and transcribe it into text. Such technology is, e.g., available in a beta version for certain English-language videos on YouTube. The technology is still far from perfect, but it can be expected that it will work well in the foreseeable future, and then also for other languages than English.

The techniques we have proposed in this article are not constrained to work for a single language. The classifiers we are suggesting to use for classifying content as being radical or not can work for any language. However, they need to be learned with representative samples for each language of interest. Moreover, many resources for text mining (such as WordNet) are language dependent and only works for English. One way to deal with content in several languages is to develop separate lexicons for the various languages of interest. Another way that demands less resources is to preprocess the text using automatic machine translation into a common language, and then use the preprocessed text as input to the classifier. Such an approach will probably give worse precision, but demand less resources.

Lastly, it is important to point out that the concept tools presented here are research suggestions and not an operative system. The described concept tools are part of an ongoing fusion framework development effort and are partially implemented within that platform, where they will be used for research experiments in the future. A full implementation of support tools for web analysis will need to include support for privacy and integrity control as well as training support to avoid human biases

when constructing the analysis models and identifying the indicators.

## Conclusions

One of the major problems when it comes to detecting possible lone wolf terrorists is that there is no consistent or typical profile of a lone wolf. Moreover, the lone wolves are hard to capture using traditional intelligence methods since there are no physical groups to infiltrate or wiretap. However, there are many concrete actions and activities (that are not necessarily illegal) taken by an individual that can be treated as weak signals and that combined may indicate an interest in terrorism acts. Recognizing and analyzing digital traces from online activities of possible lone wolf terrorists is one key to the difficult problem of detecting lone wolf terrorists before they strike. We have presented a framework for working with such digital traces through the use of techniques such as topic-filtered web harvesting and content analysis using natural language processing. Parts of the proposed system have been implemented, while work remains to be done for other parts.

It is important to highlight that the proposed system is not intended to be fully automatic. The central component of the system will be the human analyst, but this analyst will be supported in the work of finding, analyzing, and fusing digital traces of interest for finding potential lone wolf terrorists. In the future, we would like to perform more detailed experiments with the prototype system, to more properly evaluate the extent to which it is useful for law enforcement officers.

## Endnotes

[1] The actual seeds to use are up to the analyst to define and are outside the scope of this article.

[2] http://code.google.com/p/crawler4j/

[3] http://wordnet.princeton.edu/

**Competing interests**
The authors declare that they have no competing interests.

**Authors' contributions**
All authors drafted, read and approved the final manuscript.

**Acknowledgements**
This research was financially supported by the Swedish Governmental Agency for Innovation Systems (VINNOVA) through the VINNMER program, and by the R&D program of the Swedish Armed Forces.

Received: 16 January 2013 Accepted: 25 June 2013
Published: 10 July 2013

**References**

1. R Spaaij, The enigma of lone wolf terrorism: an assessment. Stud. Confl. Terrorism. **33**(9), 854–870 (2010)
2. COT, Lone-Wolf Terrorism. Tech. Rep., Instituut voor Veiligheids- en Crisismanagement (2007)
3. M Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century*. (University of Pennsylvania Press, 2008)
4. T Stevens, PR Neumann, Countering Online Radicalisation: A Strategy for Action. Tech. Rep., International Centre for the Study of Radicalisation and Political Violence (2009)
5. J Brynielsson, A Horndahl, L Kaati, C Mårtenson, P Svenson, in *Proceedings of the 14th International Command and Control Research and Technology Symposium (14th ICCRTS)*. Development of Computerized Support Tools for Intelligence Work, (Washington, District of Columbia, 2009)
6. P Svenson, T Berg, P Hörling, M Malm, C Mårtenson, in *Proceedings of the Tenth International Conference on Information Fusion (FUSION 2007)*. Using the impact matrix for predictive situational awareness, (2007)
7. R Forsgren, L Kaati, C Mårtenson, P Svenson, E Tjörnhammar, in *Skövde Workshop on Information Fusion Topics (SWIFT 2008)*. An overview of the Impactorium tools 2008, (2008)
8. P Svenson, R Forsgren, B Kylesten, P Berggren, WR Fah, MS Choo, JKY Hann, in *Proceedings of the 13th International Conference on Information Fusion (FUSION 2010)*. Swedish-Singapore studies of Bayesian Modelling techniques for tactical Intelligence analysis, (2010)
9. F Johansson, L Kaati, A Shrestha, in *Proceedings of the 2013 International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI 2013)*. Detecting Multiple Aliases in Social Media, (2013)
10. F Burton, S Stewart, The 'Lone Wolf' Disconnect. Terrorism Intell. Rep., Stratfor (2008)
11. L Kaati, P Svenson, in *Proceedings of the 2011 European Intelligence and Security Informatics Conference (EISIC 2011)*. Analysis of Competing Hypothesis for Investigating Lone Wolf Terrorists, (2011), pp. 295–299
12. M Fredholm, in *Stockholm Seminar on Lone Wolf Terrorism*. Hunting Lone Wolves – Finding Islamist Lone Actors Before They Strike, (2011)
13. A Bergin, SB Osman, C Ungerer, NAM Yasin, Countering internet radicalisation in Southeast Asia. Tech. Rep. 22, (ASPI, 2009)
14. R Abcarian, in *Los Angeles Times* January 29. Scott Roeder convicted of murdering abortion doctor George Tiller, (2010)
15. Anti-Defamation League, James Von Brunn: An ADL Backgrounder (2009). http://www.adl.org/main_Extremism/von_brunn_background.htm
16. K Cohen, F Johansson, L Kaati, J Clausen Mork, Detecting Linguistic Markers for Radical Violence in Social Media. Accepted Publ Terrorism Pol. Violence (2013)
17. J Reid Meloy, J Hoffmann, A Guldimann, D James, The role of warning behaviors in threat assessment: an exploration and suggested typology. Behav. Sci. Law. **30**(3), 256–279 (2012)
18. C Aldrich, *The Complete Guide to Simulations and Serious Games*. (Pfeiffer, 2009)
19. H Mouaheb, A Fahli, M Moussetad, S Eljamali, The serious game: what educational benefits? Procedia – Soc. Behav. Sci. **46**, 5502–5508 (2012)
20. PB Gerstenfeld, DR Grant, CP Chiang, Hate online: a content analysis of extremist internet sites. Analyses Soc. Issues Public Policy. **3**(1), 29–44 (2003)
21. MR Henzinger, Hyperlink analysis for the Web. IEEE Internet Comput. **5**(1), 45–50 (2001)
22. K Joffres, M Bouchard, R Frank, B Westlake, in *Proceedings of the 2011 European Intelligence and Security Informatics Conference (EISIC 2011)*. Strategies to Disrupt Online Child Pornography Networks, (2011), pp. 163–170
23. L Yang, F Liu, JM Kizza, RK Ege, in *Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2009)*. Discovering topics from dark websites, (2009)
24. E Reid, J Qin, W Chung, J Xu, Y Zhou, R Schumaker, M Sageman, H Chen, in *Proceedings of the Second Symposium on Intelligence and Security Informatics (ISI 2004)*. Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach to Addressing the Threats of Terrorism, (2004), pp. 125–145
25. (H Chen, E Reid, J Sinai, A Silke, B Ganor, eds.), *Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security, Volume 18 of Integrated Series in Information Systems*. (Springer, 2008)
26. A Abbasi, H Chen, in *Proceedings of the Fifth IEEE International Conference on Intelligence and Security Informatics (ISI 2007)*. Affect Intensity Analysis of Dark Web Forums, (2007), pp. 282–288
27. A Semenov, J Veijalainen, J Kyppö, Analysing the presence of school-shooting related communities at social media sites. Int. J. Multimedia Intell. Secur. **1**(3), 232–268 (2010)

28. JW Pennebaker, CK Chung, in *The Content Analysis Reader*. Computerized Text Analysis of Al-Qaeda Transcripts (Sage, 2008)
29. J Dahlin, F Johansson, L Kaati, C Mårtenson, P Svenson, in *Proceedings of the 2012 International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI 2012)*. Combining Entity Matching Techniques for Detecting Extremist Behavior on Discussion Boards, (2012), pp. 850–857
30. WE Winkler, in *Proceedings of the Section on Survey Research Methods*. String Comparator Metrics and Enhanced Decision Rules in the Fellegi-Sunter Model of Record Linkage, (1990), pp. 354–359
31. S Kim, H Kim, T Weninger, J Han, in *Proceedings of the ACM SIGKDD Workshop on Useful Patterns*. Authorship Classification: A Syntactic Tree Mining Approach, (2010), pp. 65–73
32. A Narayanan, H Paskov, NZ Gong, J Bethencourt, E Stefanov, ECR Shin, D Song, in *IEEE Symposium on Security and Privacy*. On the Feasibility of Internet-Scale Author Identification, (2012), pp. 300–314
33. J Scott, *Social Network Analysis: A Handbook*. (London, Sage Publications, 2 edition, 2000)
34. S Wasserman, K Faust, *Social Network Analysis: Methods and Applications*. (Cambridge University Press, 1994)
35. J Brynielsson, L Kaati, P Svenson, Social positions and simulation relations. Soc. Netw. Anal. Mining. **2**(1), 39–52 (2012)
36. MA Hearst, JF Allen, CI Guinn, E Horvitz, Trends & controversies: mixed-initiative interaction. IEEE Intell. Syst. **14**(5), 14–23 (1999)
37. G Tecuci, M Boicu, C Ayers, D Cammons, in *Proceedings of the First International Conference on Intelligence Analysis*. Personal Cognitive Assistants for Military Intelligence Analysis: Mixed-Initiative Learning, Tutoring, and Problem Solving, (McLean, Virginia, 2005)
38. J Ahlberg, F Johansson, R Johansson, M Jändel, A Linderhed, P Svenson, G Tolt, Content-based image retrieval – An introduction to literature and applications. Tech. rep., Swedish Defence Research Agency (2011)

doi:10.1186/2190-8532-2-11
**Cite this article as:** Brynielsson *et al.*: **Harvesting and analysis of weak signals for detecting lone wolf terrorists.** *Security Informatics* 2013 **2**:11.