Fighting Agro-Terrorism in Cyberspace: A Framework for Intention Detection Using Overt Electronic Data Sources

Eli Rohn
Software and Information Systems Engineering Department,
Ben Gurion University, Israel
EliRohn@bgu.ac.il

Gil Erez
Chairman
The Counter Agro Terrorism Research Center, Israel
gil@catrc.org.il

ABSTRACT

Agro Terrorism is "a hostile attack, towards an agricultural environment, including infrastructures and processes, in order to significantly damage national and international political interests"**.** This special session within the early warning track is aimed at reducing agro-terrorism related risks by either means of prevention (intelligence gathering using data mining and chatter mining, for example) or means to response to such an attack by early detection of exotic/foreign pathogenic agents, early prediction of disease dispersion patterns, implementation of biosecurity measures, and the development of future methodologies and techniques related to food defense and post-event response. This paper focuses on intention detection using overt data sources on the World Wide Web as they relate to agro-terrorism threats. The paper focuses on early detection that can lead to prevention of such acts, yet a variety of the techniques presented here are also useful for helping in post-event perpetrators detection.

Keywords

Cyber-terrorism, Intelligence, Authorship, Digital shadow, Information retrieval, Text mining.

INTRODUCTION

The Counter Agro Terrorism Research Center defines Agro Terrorism as "a hostile attack, towards an agricultural environment, including infrastructures and processes, in order to significantly damage national and international political interests" (CATRC 2010). It can be achieved by introducing small quantities of lethal components to every day agricultural inputs, such as water, fertilizers, seeds, sprouts, chicken or livestock feed. It is also possible to easily transmit disease agents from one sick animal to an entire flock or herd, using simple means such as rags. However, while the technicalities are quite simple, they require **intention**, **knowledge** and **guidance**. The last two can be easily provided anonymously, while the first one requires motivation, which can be initiated and enhanced by ideology and indoctrination, both deliverable electronically.

Agro-terrorism related risks can be reduced by either means of prevention (intelligence gathering using data mining and chatter mining, for example) or means to respond to such an attack by early detection of exotic/foreign pathogenic agents, early prediction of disease dispersion patterns, implementation of biosecurity measures, and the development of future methodologies and techniques related to food defense and post-event response.

Using open sources as for collecting intentions related data has a number of benefits. Obtaining the information is relatively inexpensive to obtain; it makes up the greatest volume of information accessible to collectors of such data. The activity of collecting materials from open sources is legal thus freeing collectors from risks of prosecution for espionage. Frequently, it is possible to derive sensitive information by aggregating and comparing data concerning a particular activity, individual, one or more groups or facilities.

This paper concerns itself with the first means of prevention mentioned here – intentions evaluation by intelligence gathering from overt WWW sources using various techniques, such as data mining or chatter mining, analysis of the data, production of filtered memes and their dissemination to various clientele. Information seeking behavior has eight features in common, brought here with adaptation to agro-

terrorism: *Starting* activities such as the initial search for an overview of the overt resources landscape or locating key suspects in electronic communities; *Chaining* – following clues and links in known overt resources; *Scanning* primary and secondary resources; *Differentiating* among resources using filtering strategy; *Extracting* selectively from the resources filtered; *Verifying* the information; *Monitoring* the resources for relevant changes; *Ending* the information retrieval process (Ellis and Haugan 1997). Similarly, the United States intelligence community uses a five-step process to obtain, produce, and make deliverables available to users. The steps are: Planning and Direction, Data Acquisition, Processing and, Production, and Dissemination (Federation of American Scientists 1996). The paper's sections follow the cycle described hitherto and provide an overview of the literature pertinent to each phase.

PLANNING AND DIRECTION

Planning and direction are done at the strategic level and the tactical level. Strategically, intention detection efforts need to sustain or extend the organization's strategy and governance requirements whilst being transparent about benefits, costs and risks. This requires input from and coordination with key stake holders. Identification of stakeholders is by itself not a trivial task; several proven methods exist (Elias, Cavana et al. 2002; Freeman, Harrison et al. 2010). This phase also requires incorporating technologists and business management in the translation of intelligence requirements into service offerings, and the development of strategies at the tactical level to deliver these services in an effective manner. In this step specific collection capabilities are tasked, based on the type of information required, the susceptibility of the targeted activity to various types of collection activity, and the availability of collection assets.

The tactical level of the planning and direction phase requires harnessing proven project management methodologies. A leading professional resource is the Project Management Book of Knowledge, also known as PMBOK (Indelicato 2009; Sanchez-Arias and Solarte-Pazos 2010).

Further, intention detection efforts at the planning stage should be targeted at specific areas of agro-terror. Inflicting damage through the contamination of fertilizers, for example, requires different skills and opportunities compared to inflicting damages through sewage redirection, which is entirely different from spreading viruses that can infect large herds of livestock. Deciding on which area to focus the intention detection efforts should be based on sophisticated risk analysis techniques, offered by several researchers (Parnell, Smith et al. 2010; Fellman, Parnel et al. 2011; Merrick and Parnell 2011). The risk analysis should be reviewed periodically and revised according to changing threat. To this mix, one should add "fashion traits" among terrorists. Blowing up buildings was fashionable in the 1980's and 1990's (US Embassy bombing in Tblisi, Georgia; Khobar Towers military complex bombing; simultaneous bombing of US embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, etc.) Beheading became trendy in the beginning of the 21st century. Suffice to mention Daniel Pearl, Paul Johnson and Nick Burg as examples. The antibiotics-resistant salmonella found in Europe during the summer of 2011(The Independent 2011) along with analysis of current affairs by CATRC suggests that the next trend in Agro-Terrorism might as well be the disruption of a central hub in the food chain by agro-terror means rather than brute force.

COLLECTION

The second step, collection, includes both the acquisition of information and its provisioning to organizational units that perform the processing and production. The collection process encompasses the management of various activities, including developing collection strategies that aim at optimized utilization of accessible intelligence resources. Requirements for collection of intelligence are developed to meet the needs of potential consumers.

Collection activities are given specific tasks to collect information based on identified intelligence requirements. Collection operations depend on secure, rapid and reliable communications to allow for data exchange and to provide opportunities for cross-cueing of assets and tip-off exchanges between assets. Once collected, information is correlated and forwarded for processing and production.

An example of a specific collection task is the ongoing monitoring of professional and scientific biomedical literature, with the aim of finding candidate viruses as potential agro-terrorism weapons. Such a surveillance mechanism serves for early warning which one can consider a preventive means. Geissler enumerated 13 traits a virus should have in order to be used as a potential weapon (Geissler 1986; Geissler and van Courtland Moon 1999). He then identified 21 viruses that meet these criteria. Hu et. al. proposed an "automated, semantic-based data mining system to identify viruses that can be used as weapons in bio-terrorism" by mining biomedical literature (Hu, Yoo et al. 2005). A second example of a specific collection task is finding, in social networks, overlapping communities with interest in such viruses. Using an "algorithm for finding overlapping

communities in social networks… can be helpful in discovering groups of actors that hide their communications, possibly for malicious reasons" (Baumes, Goldberg et al. 2005). A fast algorithm for the same purpose was proposed three years later (Gregory 2008).

PROCESSING

The third step, processing, is the conversion of collected information into a form suitable for the production of intelligence. In this process, incoming information is converted into formats that can be readily used by intelligence analysts in producing intelligence. Processing may include such activities as translation and reduction of intercepted messages into written format to permit detailed analysis and comparison with other information. Other types of processing that can serve counter agro-terrorism activities include detection of correlations in the collected data, and anomalies created by words substitution in non-encrypted messages.

Multiple terrorist websites are often hosted on the same servers, usually provided by an uninvolved Western service provider (Carmon 2008). Thus, the discovery of one such source may necessitate additional data collection by scanning the server for additional suspicious content and process the findings thereafter

PRODUCTION

The fourth step, production, is the process of analyzing, evaluating, interpreting, and integrating raw data into finished intelligence products for satisfying current and known future needs. To be effective, the analysis methods used must focus on the consumer's needs. It should be objective, timely, and most importantly provide accurate results. As part of the production process, the analyst must eliminate information that is redundant, erroneous, or inapplicable to the intelligence requirement.

Satisfying most or all of the above constraints and needs, one is better off using automatic or semi-supervised analysis methods. Such analysis may include locating overlapping communities, finding specific messages in a huge haystack of messages, and more.

Correlations detection in the collected data can lead to the identification of overlapping communities, for example. A different method of finding overlapping social networks only uses data of who communicates with whom (the communication graph), and ignores messages content (Baumes, Goldberg et al. 2005).

Since the use of encryption in various communications channels (e.g., encrypted emails or chats) is a flag of interest, overt messages that replace sensitive keywords (e.g., "fertilizer") are a natural choice, providing security through obscurity. Finding such messages of interest among hundreds of millions of messages or other text containers is not trivial, especially if the messages are not associated with a specific and rather static anchor point, such as a telephone number or a physical address. The substitution itself becomes a signature, because when a replacement word is chosen randomly, its frequency of appearance in the text would differ from its natural frequency in a given language. Choosing a word with a similar frequency creates a pattern that is also detectible (Skillicorn 2005; SzeWang, Roussinov et al. 2008).

DISSEMINATION

The final step of the intelligence cycle is dissemination. Dissemination is the conveyance of intelligence to a specific consumer in a usable form. Intelligence can be provided to the consumer in a wide range of formats including verbal reports, written reports, imagery products, and intelligence databases. Traditionally, dissemination has been accomplished through physical exchanges of data and through interconnected data and communications networks. However, as we enter the 21st century, with the exponential increase of intelligence information, it is required to utilize state-of-the-art technologies to assist the proper and timely dissemination of intelligence. Tactical units must not face "traditional" access barriers to pertinent intelligence. Tactical commanders require decentralized access to intelligence that respond immediately to their needs, and existing information technology can assist in attaining this goal. Timely delivery of pertinent information to higher – level decision makers is also a must. In both cases, information technology can be of great help(Resnyansky 2010). Intelligent software agents, technology-mediated global collaboration (Svendsen 2008) can all help improve the intelligence dissemination process, thus reducing the risk of agro-terrorism being actually inflicted on its potential targets. This may require additional research, such as agreed-upon ontologies, or augmenting technologies that nowadays enable sophisticated Web monitoring and clipping, or harnessing state of the art algorithms used for automatic summarization of text.

SUMMARY

The food and agricultural sectors of all nations are vulnerable to terrorism incidents or threats. With worldwide cooperation, collaboration, and information-sharing among representatives from governments, the private sector, and academia, the potential for agro-terrorism can be reduced (FBI 2011).

Supporting the counter agro-terrorism intelligence cycle aimed at intentions detection using state of the art technologies has been outlined for each of the cycle's phases. Intelligence gathering from overt networked resources using technologies for data mining and chatter mining on the one hand, semi-supervised summarization, and harnessing intelligent agents for dissemination are excellent risk-reducing tools that can help fight knowledge-based terror attacks on the food chain.

The purpose of this article was not to elaborate on technology available for each phase of the intelligence cycle, but rather draw the attention of the lesser known threat of agro-terrorism and provide a high-level review, perhaps a teaser, for in depth research and implementation of organizational work methods and tools.

REFERENCES

1. Baumes, J., M. Goldberg, et al. (2005). Efficient Identification of Overlapping Communities. IEEE International Conference on Intelligence and Security Informatics ISI 2005, Atlanta, GA, Springer.
2. Carmon, Y. (2008). The Enemy Within: Where Are the Islamist/Jihadist Websites Hosted, and What Can Be Done about It? Security Informatics and Terrorism: Patrolling the Web. C. Gal, P. Kantor and B. Shapira, IOS Press.
3. CATRC. (2010). "Agro Terrorism Defined." Retrieved 12-Jan, 2012, from http://www.catrc.org.il/.
4. Elias, A. A., R. Y. Cavana, et al. (2002). "Stakeholder analysis for R&D project management." R&D Management **32**(4): 301-320.
5. Ellis, D. and M. Haugan (1997). "Modelling the information seeking patterns of engineers and research scientists in an industrial environment." Journal of Documentation **53**(4).
6. FBI. (2011). "International Symposium on Agroterrorism, April 26-28, Kansas City, Missouri." Retrieved 12-Jan, 2012, from http://www.fbi-isa.org.
7. Federation of American Scientists. (1996, May 1996). "Section 2 - Intelligence Collection Activities And Disciplines." Intelligence Threat Handbook Retrieved 06 December, 2011, from http://www.fas.org/irp/nsa/ioss/threat96/part02.htm.
8. Fellman, P. V., G. S. Parnel, et al. (2011). Biowar and Bioterrorism Risk Assessment, Center for non-proliferation studies, Monterey Institute of International Studies.
9. Freeman, R. E., J. S. Harrison, et al. (2010). Stakeholder Theory: The State of the Art, Cambridge University Press.
10. Geissler, E. (1986). Biological and Toxin Weapons Today. Oxford, Oxford University Press.
11. Geissler, E. and J. E. van Courtland Moon (1999). Biological and Toxin Weapons Today: Research, Development and Use from the Middle Ages to 1945. Oxford, Oxford University Press.
12. Gregory, S. (2008). A fast algorithm to find overlapping communities in networks. The 12th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD 2008).
13. Hu, X., I. Yoo, et al. (2005). Mining Candidate Viruses as Potential Bio-terrorism Weapons from Biomedical Literature. IEEE International Conference on Intelligence and Security Informatics ISI 2005, Atlanta, GA, Springer.
14. Indelicato, G. (2009). "A Guide to the Project Management Body of Knowledge (PMBOK (R) Guide), 4th edition." Project Management Journal **40**(2): 104-104.
15. Merrick, J. and G. S. Parnell (2011). "A Comparative Analysis of PRA and Intelligent Adversary Methods for Counterterrorism Risk Management." Risk Analysis **31**(9): 1488-1510.
16. Parnell, G. S., C. M. Smith, et al. (2010). "Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model." Risk Analysis **30**(1): 32-48.
17. Resnyansky, L. (2010). "The role of technology in intelligence practice: linking the developer and the user perspectives." Prometheus **28**(4): 361-374.
18. Sanchez-Arias, L. F. and L. Solarte-Pazos (2010). "The Body of Knowledge of the Project Management Institute-Pmbok (R) Guide, and the Specificities of Project Management - a Critical Review." Innovar-Revista De Ciencias Administrativas Y Sociales **20**(37): 89-100.
19. Skillicorn, D. B. (2005). Beyond Keyword Filtering for Message and Conversation Detection. IEEE International Conference on Intelligence and Security Informatics ISI 2005, Atlanta, GA, Springer.
20. Svendsen, A. (2008). "The globalization of intelligence since 9/11: frameworks and operational parameters." Cambridge Review of International Affairs **21**(1): 129-144.
21. SzeWang, F., D. Roussinov, et al. (2008). "Detecting Word Substitutions in Text." Knowledge and Data Engineering, IEEE Transactions on **20**(8): 1067-1076.

22. The Independent. (2011). "Drug-resistant salmonella found in Europe, Africa: study." Retrieved 19 December, from http://www.independent.co.uk/life-style/health-and-families/drugresistant-salmonella-found-in-europe-africa-study-2333124.html.