Sci.Int.(Lahore),26(5),1713-1718,2014 ISSN 10135316; CODEN: SINTE 8

IMPORTANCE AND SIGNIFICANCE OF INFORMATION SHARING IN TERRORISM FIELD

Thamer Abaas [*], Abdul Samad Shibghatullah, Robiah Yusof, Alaa Alaameri
Faculty of Information and Communication Technology, University Technical Malaysia Melaka, Malaysia, Melaka
Alamery.Thamer@gmail.com, Samad@utem.edu.my

ABSTRACT : *Years after the 11th Sept 2001 have led in researchers to re-structure intelligence and counter terrorism in technology information to overcome problems and issues related to terrorism. This work provides an updated research of Information and Communication technology (ICT) related to re-structuring of intelligence and counter-terrorism. For this purpose, the objectives of this work is to conduct a survey on the conceptual view of the researchers who developed tools for electronic information sharing employed in intelligence and counterterrorism and summary of their works in this emerging field. The work discusses the different visions and views of information sharing, critical infrastructure, tools and key resources discussed by the researchers. It also shows some of the experiences in countries considered as international reference on the subject, including some information-sharing issues. In addition, the work carries out a review of current tools, software applications and modelling techniques around anti-terrorism in accordance with their functionality in information sharing tools. The work emphasises on identifying the various counter terrorism related works that have direct relevance to information transportation researches and advocating security informatics studies that are closely integrated with transportation research and information technologies related to the recommendations of the 9/11 commission report in 2004. The importance of this study is that it gives a unified view of the existing approaches of electronic information sharing in order to help developing tools used in intelligence and counter terrorism for future coordination and collaboration in national security applications.*

KEYWORDS: Terrorism, Counter Terrorism, Intelligence, Information Sharing, Decision Making

1.0 INTRODUCTION

Terrorism attack was given importance by the people, especially after the 11th September, 2001 attack in the United States. Many academic works have been proposed and implemented to improve the quality of the International Intelligence to combat terrorism throughout the world. Most of the proposed intellectual works in research focused more on either classification of intelligence or development of various mathematical models that can help to improve the analytical product [1]. Although the existing modern and sophisticated models have been used, there is a vast area, which has yet to be looked into i.e. the government has to upgrade the intelligence levels according to [2]. Looking at the increasing and rampant attacks that happened in certain countries, one can say that one of the reasons that contributed to the failure in curbing this issue was the inability of the government agencies to produce a better and proactive system. Figure 1 shows the increase of terrorist phenomenon around the world. Perhaps a better and elevated intelligence system that has the functionality of sharing information system by all respective intelligence agencies should be developed and used. No doubt that by having a common aim "in fighting crimes and safeguard the national security" and a standard information system in combating terrorism attack would bring to a better environment and efficiency. Somehow this may not be an easy task when it comes into its execution [3]. Terrorism is a multi-dimensional problem, and it does not belong to homeland security or a particular area [4]. The "National Strategy for Homeland Security" report published by the U.S. National Research Council after the Terrorist Attack on U.S., in 11th Sep 2001, describes the science and technology and information sharing and systems as the two of four main foundations that enable and support counter terrorism activities [5]. Governments, such as the US, Canada and European Union are looking for projects to counter terrorism and globalize the information to the people, related projects, systems, and agencies that enable efficient information sharing for national security. Some of the important projects done in this area use tools to improve communication, information sharing and information analysis between intelligence community to support decision making in critical issues: These projects are, such as the Information Sharing Environment (ISE), Fusion Centre, Adaptive Safety Analysis and Monitoring (ASAM) system, NEtwork Modeling Environment for Structural Intervention Strategies (NEMESIS) and Statewide Terrorism Intelligence Center (STIC). These projects are looking for people working in different disciplines and have varying roles and responsibilities; they all rely on timely and accurate information to achieve their national security mission responsibilities [6]. Figure 2 shows the cooperation between entities to get the benefits of information sharing. Sharing of information among dissimilar organizations with distinct security designations compels the stakeholders to coordinate efforts across programs, agencies and other organizations. This helps to preserve the confidentiality, integrity, availability, and accountability of data and the success key for counter terrorism is "speed in which information is shared from time to time manner that depend on availability of information and communication technologies" [8]. This paper is to highlight some ICT tools to support Counter Terrorism Methods and Homeland Security Research from Information Technology fields. This is to understand how the technology can be complemented and supplemented to humans. The scientific and engineering research communities are no exception as they have been called upon to play an important role in this national effort.

2.0 SEARCH METHODOLOGY

In this paper, we survey the methodologies, applications and tools to conduct studies in counter terrorism, through a literature review and classification of the international journal articles, reports and standards that appeared during the period from 2004 to 2013. The selection was done on the basis of their applicability and best-practice methodologies. This section contains an overview of the search methodology and software applications which support scientific research (Mendeley, EndNote). Figure 3 shows steps involved in the Search methodology.

-distributed information, often find this information to be more timely and accurate. The terrorist attack, Internal Conflicts and Sectarian violence drawn from the source of information from multiple eyes-on-the ground can be more helpful than the official news sources because the information can provide a more local context and rapid updates for those who have to take decisions on how to act [9]. In the same context, we will be reviewing the works related to information sharing tool used in counter terrorism and the ways in which supports from intelligence

Figure 3: The systematic review steps

communities for using ICT as a key factor from 2004-2013. The federal government's war on terrorism has heightened the understanding and appreciation of the many facets of electronic government. Electronic government has been used as a resource in the war on terrorism. It has been proven as a useful tool that can help prevent from attacks, prepare for attacks and recover from attacks. The federal government already has exploited some of e-government's capabilities for sharing information [10]. According to Hsinchun Chenet al. 2004, intelligence and security informatics (ISI) is an emerging field of study aimed at developing advanced information technologies, systems, algorithms, and databases for national and homeland security-related applications, through an integrated technological, organizational, and policy-based approach. They presented three detailed case studies to illustrate how the key intelligence and security informatics ISI in research areas, which include cross-jurisdiction information sharing; terrorism information collection, analysis, and visualization[5].

In [11] Singh et al. introduced Adaptive Safety Analysis and Monitoring (ASAM) system to counter terrorism analysis. This system used Hidden Markov Models (HMMs) and Bayesian Networks (BNs) to develop a model. Patterns of anomalous behaviour were also calculated and identified using features aided in multiple target trackings. The ASAM system can suggest feasible actions to inhibit potential terrorist threats. The ASAM system is an Advanced Counter Analysis Tool that has the following capabilities: Predicting intent and future states through the terrorist activities, Identifying Threats, Option Analysis, Inverting the bath tub and Automation and Model and scenario generation [11].

In [12], Ying Chen et al. suggested that the evolution of Web Services and Service Oriented Architectures (SOA) has the ability to overcome many technological barriers to the Intelligence Community (IC). By combining data mining technology and service rating techniques into a SOA-enabled problem solving space within the intelligence community, analysts are able to utilize the expertise and knowledge from other analysts to quickly discover services in a meaningful way and compose services into workflows. Data mining is the process of extracting patterns and knowledge hidden from large volumes of raw data, and it includes techniques, such as classification, clustering, association rules, and sequential patterns. They help us with service categorization, service discovery, automated service composition and construction of dynamic Communities of Interest (COIs), which empower analysts to collaboratively solve complex problems. These techniques will enable analysts to be successful, even when confronted with the challenge of service overload as more services begin to populate the network [12].

Robert Popp et al. [13] introduced a model named as NEMESIS (Network Modeling Environment for Structural Intervention Strategies). This model utilises communities environment to integrate and share counter terrorism analysis information among different tools. Information technologies are essential for the global war on terrorism. Termed as NEMESIS, this model functions as "a collaborative analysis environment, a networked of various information technologies to collaborate, evaluate, share, and act on the information gathered in the shortest time possible to detect and prevent terrorist attacks". The components of two tools namely, ASAM (Adaptive Safety Analysis and Monitoring System) and ORA (Organizational Risk Analysis) are described in paper. The functionality of these two tools, along with the NEMESIS collaboration is illustrated via a real world example gleaned from open sources. [13]. Yang and Wing [14] suggested the use of the associate constraint network to generate a cross-lingual concept space from a parallel corpus, and benchmarked it with a previously developed technique, the Hop field network. This associate constraint network is a constraint programming based algorithm, and the problem of generating the cross-lingual concept space is formulated as a constraint satisfaction problem. This method can assist crime analysts to determine the relevance of criminals, crimes, locations and activities in multiple languages. It helps them by providing information that is not available in traditional thesauri and dictionaries [14].

According to Willem et al. [15], they developed a conceptual framework to understand the limits of security intelligence within an emerging security network paradigm. The focus is on the normative dimensions governing security networking, and the mechanisms and technologies limiting information deployment among public security agencies. Technologies of control promoting this exclusivity also function to prevent intelligence from becoming common knowledge. Because of its limited value, intelligence is ill-suited for export into security governance writ large [15].

In [16], Bhavani Thuraisingham described the issues, technologies, challenges, and directions for Assured Information Sharing (AIS). AIS is about organizations' sharing information, while at the same time it enforces security policies. They assume that the partners of a

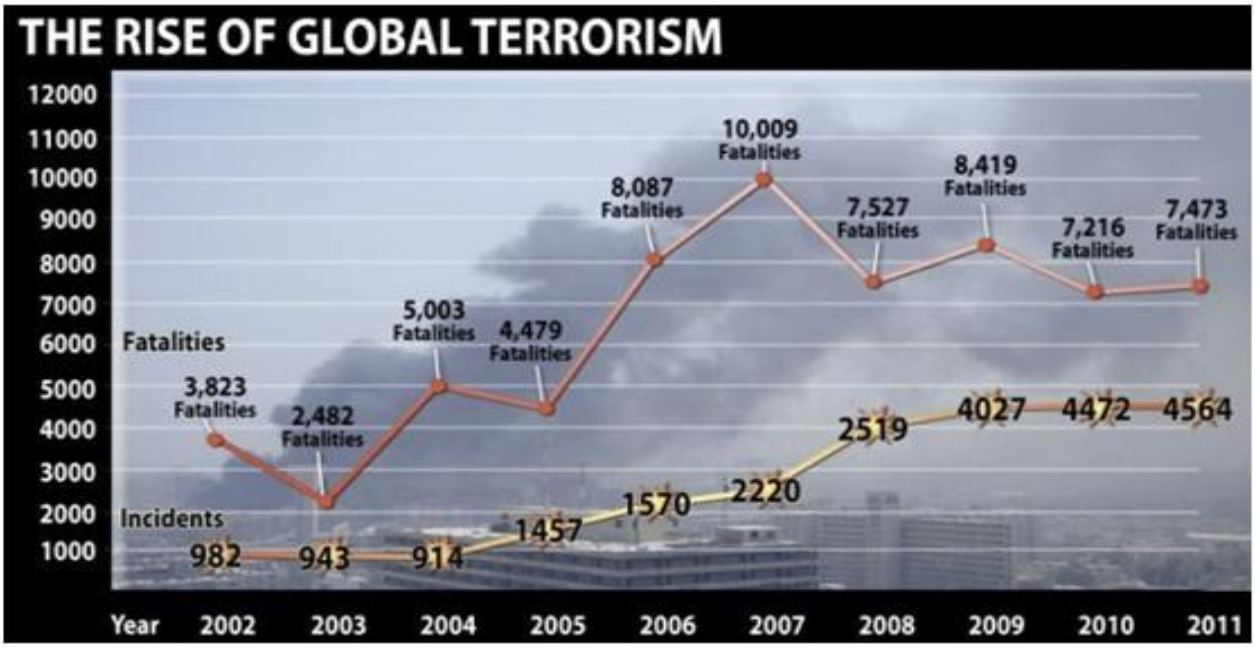

Figure 2: The increase of terrorist activities with time [7]

Figure 1: The connection between entities [8]

coalition may be trustworthy, semi-trustworthy or untrustworthy and investigate solutions for AIS to handle the different scenarios. [16]. Alessandro Zanasi in [17] suggested the use of text mining technology; Text mining is the most advanced knowledge management technology that allows intelligence analysts to automatically analyze the content of information rich online data banks, suspected web sites, blogs, emails, chat lines, instant messages and all other digital media by detecting links between people and organizations. Specifically, it uses a physical place to concentrate advanced information technologies (including Web 2.0, machine translation, crawlers, text mining and human expertise, not only in information technologies but also in online investigations). Hence, to counter network terrorists, intelligence must learn how to monitor their virtual network activity in the same way it keeps tabs on terrorists in the real world [17].

Farroha et al. [8] explained that the challenges of building a Secure Information Sharing Environment are based on increased need to share data across the agencies and security domains. The task of architecting systems that enables Cross Domain (CD) capabilities is a significant undertaking that

Table 1: Weaknesses of the Reviewed Work

Authors, Years	Work Weaknesses
Hsinchun Chenet al. in 2004	Protection of ICT systems is far from a solved problem. Integration problem manner in various ISI settings.
Singh et al. in 2004	The ASAM system can theoretical to suggest feasible actions to inhibit potential terrorist threats. This is a major extension that is being addressed in their current research.
Ying et al. in 2005	They conclude by revisiting the benefits brought by applying Data Mining technology and Service Rating techniques in SOA enabled collaboration system.
Robert Popp et al in 2005	Organizational Descriptive Language ODL Organizational Risk Analysis ORA
Yang, Wing Li in 2007	therefore the lack of explicit semantic clustering of relevant information and the limits of conventional keyword-driven search techniques (either full or index-based)
Willem et al. in 2007	Limits of networking in a context where security is increasingly seen as a problem of intelligence.
Thuraisingham in 2008	need to develop policies for accountability, risk analysis studies, develop web services, infrastructures such as data grids investigate several additional technologies such as collaborative services, social network analysis, surveillance data sharing, digital identity management, metadata extraction and management as well as policies for identification and authentication for AIS.
Alessandro Zanasi in 2009	Intelligence must learn how to monitor their network activity, also online, in the same way it keeps tabs on terrorists in the real world.
Farroha et al. in 2009	Need to align the Cross Domain technology development with the near, mid and long term information sharing needs of the IC and DoD. Need to ensure Cross Domain policy and governance supports information sharing goals of the Community and keeps pace with emerging technology and architectures.
Harris Wu et al. in 2010	The algorithm is suited for people or groups with similar backgrounds and interests who will likely have overlapping, non-orthogonal local hierarchies.
Jiang and Samanthula in 2011	How about other measures, such as, KL-divergence or using the language model? Which one of the two document representations is more effective, and which one is more efficient to implement securely?. The proposed disclosure control technique only focuses on a single execution of the SSDDh protocol. If the server's document collection does not change very often, multiple execution of the protocol may leak more information. It is essential to analyze this issue.
Jin Lee et al. in 2011	Insufficient interviews with stakeholders. Some individual technology specific effects. Critical cases prerequisite to evaluate and improve IS in this area.
Jingwei Huang, David Nicol in 2013	Need to develop ontology to precisely specify the attribute-based policy model in both logic and language levels, to facilitate metadata annotation, policy specification, and policy decision on M3GS. Need to develop M3GS cloud workflow access control model, and trust-based cloud work- flow optimization to maximize the trustworthiness of M3GS.
Xiaojun Shan, Jun Zhuang in 2013	Practice game-theoretic models may be difficult to implement. A more efficient and general algorithm should be developed for similar models of realistic size and complexity. A more sophisticated objective function could be used to incorporate the terrorist's target valuation and risk preferences.

requires an understanding of data systems, technologies, governance, and cultures. The long term goal is to build a Service Oriented Architecture (SOA) approaches-based Enterprise that enables the community to use the diverse resources across various domains to deliver the information to the intended destination. [8].

Harris Wu et al. [18] proposed a collective taxonomy approach to organize a shared, growing document repository. This approach allows for combining both the individually managed local document hierarchies and algorithmically building a global hierarchy. Drawing on the success of Web 2.0 and theories from knowledge management, they argue that a shared document repository with no central organizer may benefit from collective taxonomizing, thus, allowing community members to categorize documents with local document hierarchies and systematically coalesce those local hierarchies into a global taxonomy. Using a design science approach, they develop and evaluate a hierarchy coalescing algorithm. They believed that managing structural knowledge is a key challenge for knowledge sharing and decision making. [18].

Jiang and Samanthula in [19] proposed a distributed framework to identify and share needed and protected information. The framework has many useful applications across multiple domains, such as intelligence sharing, medical and collaborative research and information integration. Presented an initial solution based on existing secure similar document detection techniques, the proposed framework provides an objective and secure way to justify the need-to-know basis and to identify and share the needed intelligence without disclosing any irrelevant but protected information. It can also minimize information disclosure in

coordinated and collaborative intelligence gathering involving multiple entities. They presented a novel solution based on the solvability of systems of linear equations to prevent the inference attack under the semi-honest adversary model. In addition, they also proposed necessary steps to prevent the inference attacks under the accountable computing framework [19].

3.0 Jin Lee et al. in [20] extended the theory of information systems (IS) in the context of large-scale disaster management (DM) for public safety. A model that explains IS usage intention as a reflective measure of IS success in the public sector DM domain was empirically tested. The effects of the expected value of IS for the entire group of collaborating DM agencies, task support, user satisfaction, and three specific information and service quality dimensions on usage intention were examined. The study exemplifies the distinctive climate in the public sector DM domain and bears important implications for IS success research. These findings imply that the previously suggested information systems IS success models for business environments are likely to fall short in their explanatory power and applicability for highly volatile complex disaster environments that require immediate coordinated responses from a large number of organizations. Real DM personnel on duty limited the time they had to survey and interview them after the exercise. Indeed, the restrictions on the data collection were imposed not only for privacy and sensitivity, but also to prevent any vacuum in the emergency response capacity in the surrounding regions. They observed that none of the available ICTs was universally used by all participants in the exercises. Moreover, no agency had access to every ICT, which means that no agency had access to all of the information available. The aggregation of multiple systems was necessary and appropriate in this study. However, such aggregation may cancel out some individual technology specific effects. For future research, it is suggested to find additional, possibly more specific effects, by examining an individual or fully integrated IS. In doing so, different or even incompatible functionalities and information requirements for various stakeholders may be identified. Furthermore, the study may be extended in several directions. First, defining IS success in multi-agency DM is a challenging, yet critical, prerequisite to evaluate and improve IS in this area [20].

4.0 Carter and Rip in [21] explained the role of public health in homeland security that has recently evolved. In the wake of a series of tragic events impacting public health in the United States, the Department of Health and Human Services Centres for Disease Control and Prevention and the Department of Homeland Security have attempted to facilitate information sharing across public health and homeland security organizations. They saw that there remains an information sharing disconnect between public health and the entities tasked with homeland security preparedness. The data presented shed light on the commonly held assumption that public health and homeland security are working together. Recent initiatives to remedy this shortcoming are presented, and recommended for further success is discussed. Public health entities can increase both the amount and quality of information they disseminate and receive that are useful for counter terrorism [21].

5.0 Huang and Nicol [22] presented the concepts and architecture of a Mission-oriented Multi-domain Multi-level security Graphics Server (M3GS) in the environment of GIG 2.0 and cloud computing. They identified the needs for, develop the concepts, and sketch architecture for a M3GS as a type of tool that supports cross-domain information sharing. In particular, it provides secure information support for a dynamical team of members from different security domains collaborating on a mission; the server produces the contents of screens fusing information from a variety of sources in different security domains with a variety of security labels. [22].

6.0 Finally, Shan and Zhuang [23] developed a novel hybrid model, where a centralized government allocates defensive resources among multiple potential targets to minimize expected loss caused by an unknown adversary that could be either strategic and nonstrategic depending on the many models that have been developed to study homeland security games between governments (defender) and terrorists (attacker, adversary, enemy), with the limiting assumption of the terrorists being rational or strategic [23]. Table 1 explains the weakness of each of the works presented in this paper.

7.0 FINDING AND DISCUSSIONS

Terror phenomenon appeared to the world with new concepts after the 11 Sep 2001. The counterterrorism delivered by governments gives the highest attention to the protection of their large-scale infrastructure and facilities. Intelligence is one of the main resources for anti-terrorism; however, the processes and practices used for monitoring and reporting incidents differ considerably from country to country. Many governments lack the entity (e.g. electronic intelligence) which could serve as a monitoring centre. This paper presents a review of some of the capabilities of researches for the identification information sharing tools in counter terrorism and homeland security, with the emphasis of electronic systems. The development of security, economic prosperity and communities' infrastructure somehow witnesses the exponential increase of the complexity of larger infrastructures. Significant researches focus on identification, assessment and development of critical electronic information sharing, where the universality of the methodologies, involved hazard maps and risk matrices, sets them apart. Paradigms of system simulation are widely used as a support for decision making on the stages of prioritisation, implementation and monitoring of actions, in order to estimate risk mitigation strategies and policies in critical electronic infrastructure. Electronic information sharing modelling is a relatively new area of research and analysis, but terrorist attacks and natural disasters have shown that the impacts of threats on homeland security need to be thoroughly evaluated. Since a few of the referenced tools are available for commercial use, and that most of the research is currently carried out by a few governments, a limited exchange of information has taken

place in this area. The e-information sharing is one of good tools that give good cooperation and coordination between intelligence communities and counterterrorism. The effective implementation of the decision making plans depends upon the degree to which government and private sector partners engage in systematic, effective, multidirectional information sharing and analysis. We, therefore, strongly encourage them to cooperate with each other, possibly with the help of governmental or supranational organisations or agencies with appropriate levels of authority and responsibility. The actors taking part in a coordination agency in anti-terror could be: electronic infrastructure owners and operators, government agencies and officials with responsibilities on decision making, military and civil intelligence bodies, expert advisory groups and local and regional authorities. Conducting inventory and classifying assets would be the first step toward the promotion of a culture of information sharing into a risk-management framework. Real-time collaboration on risks alerts: information gathering, infrastructure status, emergency responses, membership conditions and expertise should also be established. In the proposed networked scheme, access to information both vertically and horizontally achieved and this implies that partners can share information directly among themselves.

REFERENCES

[1] N. Bharosa, J. Lee, and M. Janssen, "Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises," *Inf. Syst. Front.*, vol. 12, no. 1, pp. 49–65, May 2010.

[2] Y. Dang, Y. Zhang, H. Chen, P. J.-H. Hu, S. a. Brown, and C. Larson, "Arizona Literature Mapper: An integrated approach to monitor and analyze global bioterrorism research literature," *J. Am. Soc. Inf. Sci. Technol.*, vol. 60, no. 7, pp. 1466–1485, Jul. 2009.

[3] B. L. Lugna, "Institutional Framework of the European Union Counter-Terrorism Policy Setting," vol. 8, pp. 101–127, 2006.

[4] T. J. Abaas, A. S. Shibghatullah, and M. M. Jaber, "Use Information Sharing Environment Concept to Design Electronic Intelligence Framework for Support E-Government : Iraq as Case Study," vol. 4, no. 1, pp. 22–24, 2014.

[5] H. Chen, F. Wang, and D. Zeng, "Intelligence and Security Informatics for Homeland Security : Information , Communication , and Transportation," vol. 5, no. 4, pp. 329–341, 2004.

[6] ISE, "Information Sharing Environment," 2013. [Online]. Available: http://www.ise.gov/what-ise.

[7] L. Decade, "Global Terrorism Index 2012," 2012.

[8] B. S. Farroha, D. L. Farroha, and M. Whitfield, "Challenges and Alternatives in Building a Secure Information Sharing Environment through a Community-Driven Cross Domain Infrastructure InfOrmati," pp. 1–7, 2009.

[9] L. Palen, S. Vieweg, S. B. Liu, and a. L. Hughes, "Crisis in a Networked World: Features of Computer-Mediated Communication in the April 16, 2007, Virginia Tech Event," *Soc. Sci. Comput. Rev.*, vol. 27, no. 4, pp. 467–480, Apr. 2009.

[10] L. E. Halchin, "Electronic government: Government capability and terrorist resource," *Gov. Inf. Q.*, vol. 21, no. 4, pp. 406–419, Jan. 2004.

[11] S. Singh, J. Allanach, K. Pattipati, and P. Willett, "Stochastic modeling of a terrorist event via the ASAM system," *2004 IEEE Int. Conf. Syst. Man Cybern. (IEEE Cat. No.04CH37583)*, vol. 6, pp. 5673–5678, 2004.

[12] B. C. B. A. H. Ying Chen, "Data Mining and Service Rating in Service-Oriented Architectures to Improve Information Sharing," *2005 IEEE Aerosp. Conf.*, pp. 1–11, 2005.

[13] R. Popp, K. Pattipati, P. Willett, D. Serfaty, W. Stacy, K. Carley, J. Allanach, H. Tu, S. Singh, and N. F. Drive, "Collaborative Tools for Counter-Terrorism Analysis," 2005.

[14] C. C. Yang and K. Wing, "An associate constraint network approach to extract multi-lingual information for crime analysis," vol. 43, pp. 1348–1361, 2007.

[15] W. de Lint, D. O'Connor, and R. Cotter, "Controlling the flow: Security, exclusivity, and criminal intelligence in Ontario," *Int. J. Sociol. Law*, vol. 35, no. 1, pp. 41–58, Mar. 2007.

[16] B. Thuraisingham, "Assured Information Sharing : Technologies , Challenges," pp. 1–15, 2008.

[17] A. Zanasi, "Virtual Weapons for Real Wars : Text Mining for National Security," pp. 53–60, 2009.

[18] H. Wu, M. D. Gordon, and W. Fan, "Collective taxonomizing: A collaborative approach to organizing document repositories," *Decis. Support Syst.*, vol. 50, no. 1, pp. 292–303, Dec. 2010.

[19] W. Jiang and B. K. Samanthula, "A Secure and Distributed Framework to Identify and Share Needed Information," *2011 IEEE Third Int'l Conf. Privacy, Secur. Risk Trust 2011 IEEE Third Int'l Conf. Soc. Comput.*, pp. 1224–1230, Oct. 2011.

[20] J. Lee, N. Bharosa, J. Yang, M. Janssen, and H. R. Rao, "Group value and intention to use — A study of multi-agency disaster management information systems for public safety," *Decis. Support Syst.*, vol. 50, no. 2, pp. 404–414, Jan. 2011.

[21] J. G. Carter and M. Rip, "Homeland Security and Public Health: A Critical Integration," *Crim. Justice Policy Rev.*, vol. 24, no. 5, pp. 573–600, Aug. 2012.

[22] J. Huang and D. Nicol, "Security and Provenance in M3GS for Cross-domain Information Sharing," pp. 0–5, 2013.

[23] X. Shan and J. Zhuang, "Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game," *Eur. J. Oper. Res.*, vol. 228, no. 1, pp. 262–272, Jul. 2013.