

## Chapter 10

# **EMERGENCY PREPAREDNESS AND RESPONSE**

### **Chapter Overview**

In case of a national emergency, prompt and effective responses are critical to reduce the damage resulting from an attack. In addition to the systems that are designed to defend against catastrophes, information technologies that help develop response plans, identify experts, train response professionals, and manage consequences are beneficial to society. Moreover, information systems that provide social and psychological support to the victims of terrorist attacks can also help society recover from disasters. In this chapter we present two case studies. The first case study uses bibliometric analysis to help identify modern terrorism research experts in the U.S. and internationally. The second case study uses the chatterbot dialog system to help locate terrorism-related information.



## **10.1 Case Study 16: Mapping Terrorism Research**

The recent escalation of global terrorism has attracted a growing number of new, non-traditional research communities owing to the multi-disciplinary dimensions required to gain a better understanding of the terrorism phenomenon. As a result, new researchers face information overload, access, and knowledge discovery challenges. This study provides a longitudinal analysis of terrorism publications from 1965 to 2003, to identify the intellectual structure, changes, and characteristics of the terrorism field. It uses bibliometric and citation analysis to identify core terrorism researchers, their productivity, and knowledge dissemination patterns.

For bibliometric analysis, our initial unit of analysis is the author, whose individual publications, subject areas, journal titles, and institutions provide subsequent analyses. Our first step is to identify a core set of authors and their related publications. We compiled a list of authors from several sources: terrorism publications (Schmid and Jongman, 1988; Reid, 1997), active terrorism experts identified by the KnowNet virtual community (organized by the Sandia National Laboratory), and terrorism research center portals identified on the Internet. Authors identified on the web may represent individuals whose prominence has recently been established or those who have reputable international or non-traditional perspectives on terrorism.

Kennedy and Lum's (2003) list of terrorism research organizations was used to identify a good number of terrorism web-based research portals. We also focused on the Terrorism Research Center (TRC) portal because it is highly recommended by terrorism experts. Using backlink searches in Google, we found thousands of web pages hyperlinked to TRC. We followed TRC's external links to 28 terrorism research organizations and gathered names of terrorism researchers mentioned on the web sites. A total of 131 unique names were identified from using the combined pool of 28 terrorism research center portals, the KnowNet virtual community's recommendations, and those reported by Schmid and Jongman (1988) and Reid (1997).

A bibliography of English-language terrorism publications was compiled for each researcher using commercial databases. The publications include journal articles, books, book chapters, reviews, notes, newspaper articles, conferences papers, and reports. For each core researcher, bibliographic data describing their terrorism-related publications was retrieved. After the citation analysis was conducted, 42 authors were identified as core terrorism researchers based on citation count. A total of 284 researchers/coauthors and their 882 publications made up the sample for this study.

The 42 core researchers are mainly affiliated with academic institutions (23), think tanks (15), media organizations (3), and the government (1). Their bases of operation are located in ten countries including the U.S. (29), the U.K. (4), Ireland (1), Germany (1), Australia (1), Israel (1), Canada (1), France (1), Netherlands (1), and Singapore (1). Specifically, six researchers are from the Rand Corporation including Jenkins, the founder of the Rand terrorism program; three are from the Centre for the Study of Terrorism and Political Violence (CSTPV) at St. Andrews, Scotland; and another three are from the Center for Strategic and International Studies (CSIS), Georgetown University.

To further explore the core terrorism researchers' knowledge creation patterns, authorship data which identify their collaboration patterns and research groups were exploited. There was a high level of coauthorship among the 42 core terrorism researchers where the majority of the researchers (90%) had coauthors. For example, Alexander has 82 coauthors, followed by researchers from the Rand Corporation, such as Jenkins, with 68, Hoffman with 50, and Ronfeldt with 41 coauthors. Wilkinson and Laqueur had less than nine coauthors. They are among the group of core researchers with high author productivity levels. Eight core researchers did not have any coauthors. We also found that Alexander's extensive list of publications is due to his collaborative efforts with 82 coauthors which enabled him to publish books that include 57 anthologies and 10 bibliographies.

Further investigation of the coauthorship relationships provides an understanding of the researchers' collaboration patterns. Figure 10-1 shows the coauthorship network of core terrorism researchers. The nodes represent researchers who coauthored papers.

Some of the most active clusters in the bottom-right corner of Figure 10-1 are the Rand research teams led by Jenkins and Hoffman. Gunaratna, although not employed by Rand, is listed in this cluster because he coauthored publications with Chalk and Hoffman. Hoffman, Gunaratna's Ph.D. advisor at St. Andrews University, Scotland, founded St. Andrews' Centre for the Study of Terrorism and Political Violence (CSTPV) and created the Rand-St. Andrews Terrorism Incident Database, which provides data for their studies (Hughes, 2003).

For the cluster involving Ranstorp (the bottom-left corner of Figure 10-1) from CSTPV, the network is sparse and shares few coauthorships. As chairman of the Advisory Board for CSTPV, Wilkinson has a few collaborations with Alexander but none with researchers at CSTPV who are in this sample. Another cluster includes researchers such as Alexander and Cline (middle of Figure 10-1) at the Center for Strategic and International Studies (CSIS). This cluster displays a pattern of one to many coauthors

because Alexander has 82 coauthors. In this particular case, we found that coauthorships do not seem to be sustainable because many authors produced only a single publication with Alexander and did not publish with other terrorism researchers in this sample.

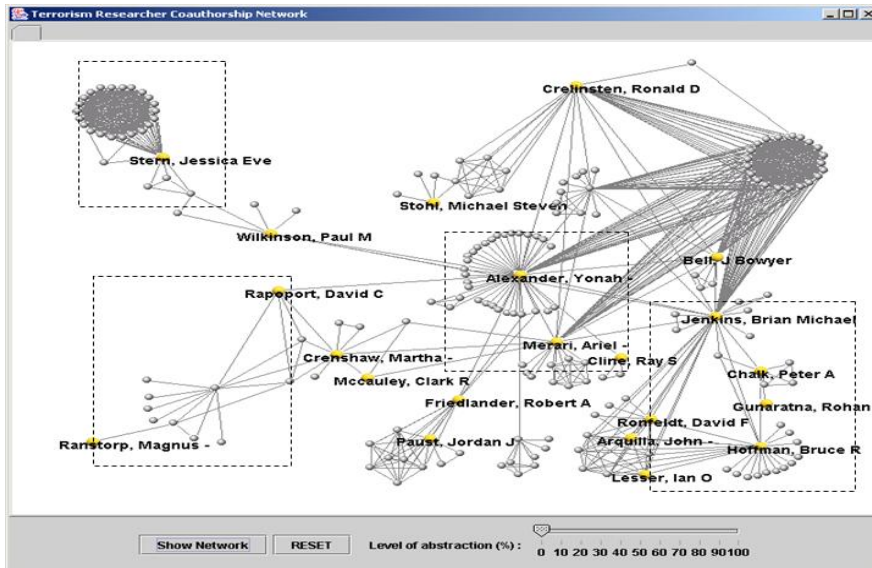


Figure 10-1. Terrorism researchers' coauthorship network.

Since this study is limited to English language publications, 43 of the 131 recommended terrorism researchers have been excluded from our data because their publications were not retrieved. Another inherent limitation of this study brought about by the use of the ISI Web of Science is the exclusion of terrorism studies found in e-journals, congressional testimonials, and recent conference papers as well as non-refereed web materials. This last limitation may have precluded the publications from international, emerging thought leaders.

Despite the foregoing limitations, this study can be seen as significant in that it has assembled useful information that can help lead novice researchers to core terrorism researchers and their key contributions in a challenging field that is growing rapidly. Specifically, it helps identify the most frequently cited terrorism researchers and their publications, dissemination, and collaboration patterns. From this, one may better understand the structure of terrorism research and locate literature produced in particular areas of terrorism. It is a field whose profound implications to our future societies are beyond comprehension.

## 10.2 Case Study 17: A Dialog System for Terrorism Resources

Terrorism education has become a topic of interest lately. With many agencies and private organizations scrambling to provide terrorism information, the actual process of finding relevant material can sometimes become lost in the chaos. To the credit of the Department of Homeland Security and several private organizations, there is some valuable information available; however, it is mainly geared towards first responders and not the general public.

In both the “9-11 Commission Report” and “Making the Nation Safer,” the authors propose to bridge this gap through the use of C3; systems embodying Command, Control, and Communications elements. These systems would allow for the deployment of communications channels during an emergency to support decision management as well as communicate instructions to the public (Moore and Gibbs, 2003).

One potential approach to C3 is through the use of ALICEbots. ALICEbots (Artificial Linguistic Internet Chat Entity robots) are a type of Question-Answer (QA) chatterbot developed in 1995 by Richard Wallace (Wallace, 2004). The advantage of these chatterbots is in their ability to be quickly programmed with terrorism-specific knowledge, as well as their robust and human-like nature. ALICEbots are built first and foremost for conversation and are a promising vehicle in disseminating terrorism-related information to the public.

ALICEbots work by matching user input against pre-existing XML-based input patterns and returning the template response. This simple method of conversational mimicking eliminates the computational overhead that would normally be associated with deeper reasoning systems. The technique can also permit expansion into new knowledge domains, allowing the ALICEbot to convey an ‘expert appearance’ (Wallace, 2004).

In our research, we aimed to examine the efficacy of shallow Question-Answer (QA) systems for disseminating terrorism-related information to the general public. We created three modified ALICEbots, which differed from each other on the dimension of terrorism knowledge bases used. One chatterbot used only general conversational knowledge, the second used only terrorism domain knowledge, and the third was a combination of both conversation and terrorism knowledge. Referred to as TARA (Terrorism Activity Resource Application) in our research, our system design was based on a modified version of the ALICE Program D chatterbot engine which is freely available at [www.ALICEbot.org](http://www.ALICEbot.org). There are some notable differences between TARA and ALICE, as illustrated in Table 10-1. The only component that remained unaltered was the actual Chat Engine.

Table 10-1. Differences between Original ALICE Program D and the TARA chatterbot.

	Chat UI	Chat Engine	AIML	Logging	Evaluation
<b>Original ALICE</b>	Uses XML to chat with users	Uses off the shelf ALICE Program D	Uses the freely available Standard and Wallace set (Dialog)	Logs everything to a monolithic XML Log file	None
<b>TARA</b>	Uses a customized perl skin to chat and for evaluation purposes	Same as Original ALICE	Depends on the bot as to whether it is Dialog or customized Terrorism knowledge	Keeps XML logs on a per user basis	Customized perl script that allows users to evaluate and suggest new patterns

We used three chatterbots with differing knowledge bases. The control chatterbot “Dialog,” the general conversationalist, was loaded with the standard knowledge set that allowed ALICE to win the early Loebner contests (of machine conversation). This set consists of 41,873 knowledge-based entries. The second chatterbot “Domain,” was loaded with 10,491 terrorism-related entries. The third chatterbot “Both,” was a summation of “Dialog” and “Domain,” which can carry on a general conversation and easily handle terrorism inquiries as well. It contains 52,354 entries, 10 less than a true summation because of an overlap between the dialog and domain knowledge bases.

Terrorism entries were collected through a mixture of automatic and manual means. The majority were gathered automatically from several reputable web sites including <http://www.terrorismanswers.com> and <http://www.11-sept.org>. Manual entry was used sparingly to augment the terrorism knowledge set.

For our system comparison research we used ninety participants, thirty for each chatterbot, who were a mixture of undergraduate and graduate students taking various Management of Information Systems classes. Participants were randomly assigned to one of the chatterbots, asked to interact with the system for approximately one-half hour, and permitted to talk about any terrorism-related topic.

The evaluation method of chatterbot responses was an integrated process where users would chat a line and then immediately evaluate the chatterbot’s response. Users were asked to evaluate each line with the following two measures; appropriateness of response (Yes/No), and satisfaction level of the response using a Likert scale of values (1-7). Users were also given the opportunity to provide open-ended comments on a line by line basis.

Measurements were conducted on the appropriateness and satisfaction rating of the chatterbot responses. Because the “Both” chatterbot is composed of dialog and domain parts, we took the “Both” chatterbot and broke its responses into its constituent parts of dialog and domain. We then compared those results against the actual Dialog and Domain chatterbots. This comparison is shown in Table 10-2.

Table 10-2. Comparing the components of “Both” against the Dialog and Domain chatterbots.

Comparison	Both’s components		Actual chatterbots	
	Dialog	Domain	Dialog	Domain
Breakdown of numbers				
Number of lines entered into the chatterbot	888	250	1,524	849
Average response appropriateness	68.4%	39.6%	66.3%	21.6%
Average response satisfaction rating	4.51	3.14	4.04	2.43
Standard deviation of response satisfaction	2.12	2.17	2.00	1.90

When comparing the dialog component of “Both” against the actual Dialog chatterbot, the “Both” component rated higher in response appropriateness, 68.4% to 66.3%, as per our expectation. When looking at the domain component of “Both” against the Domain chatterbot, again the “Both” component rated higher, 39.6% compared to 21.6%. Likewise, Response Satisfaction scores from the “Both” chatterbot rate higher than the corresponding “Actual” chatterbots. This analysis shows that the “Both” chatterbot performed better in its constituent areas compared against the stand-alone chatterbots. We believe that this is the result of the dialog portion responding to unrecognized queries and steering communication back to terrorism topics.

We investigated the input/response pairs of the “Both” chatterbot. In particular we were interested in only those user inputs which were in the form of a question (68.4% of the terrorism domain inputs were interrogatives). Table 10-3 summarizes the most frequently observed interrogatives.

Table 10-3. Most frequently observed interrogatives.

Interrogative	Percentage Use
What	27.5%
Do	15.8%
Who	11.1%
How	8.2%
Where	5.8%
Is	5.3%

Investigating the interrogatives further, it was found that the interrogative “what” started the most user queries at 27.5% of all queries. We had expected that interrogatives beginning with “wh\*” would be the most prevalent and indeed they were, making up 51.5% of all interrogatives. It is interesting to note how often “Do” and “Is” were used, as these were unexpected surprises. In the vein of work done by Moore and Gibbs (2003) where students used the chatterbot as a search engine, focusing future efforts of knowledge collection at these selected interrogatives should best improve chatterbot accuracy.

In the future, it would be a good idea to investigate adding more knowledge to the system. Although our domain-specific knowledge base appeared to be sufficient for the task, it would be interesting to test even larger corpuses of knowledge and see what impact they may have over dialog knowledge. Another possible aspect worth considering is the addition of a C3 variant, the “I’m Alive” boards. Following the September 11<sup>th</sup> attacks, multiple boards sprang up around New York City announcing the names and present shelter location of survivors to concerned friends and family members outside of the disaster area. Adding such functionality would be a simple programming exercise and would provide a quicker and more concerted way for bidirectional communications.

### **10.3 Future Directions**

There is little academic research in addressing the needs of the first responders and general public during and after a tragic terrorist event. The devastating effects of such an event often cause significant communication, psychological, and societal chaos well beyond the physical and monetary damages the attack has created. Under the support of the NSF Digital Government Program, several workshops have been conducted to address the needs of the emergency response community. Both technical (e.g., communication interoperability, rescue robots, and disaster relief logistics) and policy (e.g., emergency response authority and plan) challenges and research opportunities were identified. The workshops suggested new funding in emergency preparedness and response research and proposed an academic-agency partnership in addressing short-term and long-term research issues.

## 10.4 Questions for Discussion

1. Who are the first responders and what are some ways to initiate a research partnership with them?
2. What are the immediate needs of the emergency response and disaster relief community? How can information technologies help with their activities?
3. What are some ways to prepare and educate the general public about terrorism and terrorist events? How can information technologies help with such activities?
4. What are some ways to solicit the help of terrorism researchers to address the various social dimensions and consequences of terrorist events?
5. How can the media help in uncovering the myths of terrorism and educating the public? How can the Internet help in such activities?